The eG Installation Guide

Restricted Rights Legend

Trademarks

Copyright

Table of Contents

Table of Figures

1

Introduction

This manual delves into the detailed procedure for installing and configuring eG Enterprise. Before getting into the details, it is imperative for a user to understand the architecture of eG Enterprise. A thorough understanding of its architecture can enable the user to deploy and use eG Enterprise effectively. This chapter provides the details of the eG architecture.

1.1 System 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 and the following sections describe these components in detail.

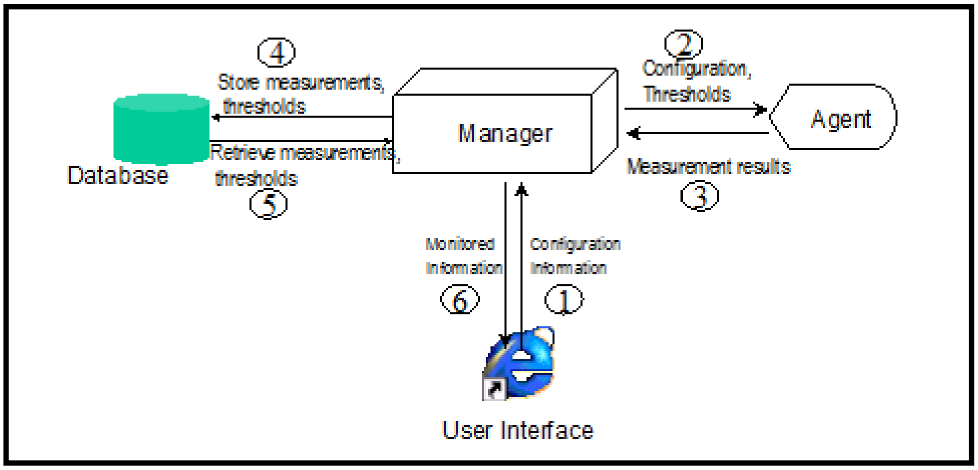

4
Store measurements, thresholds
Database
Retrieve measurements, thresholds
5
Manager
2
Configuration, Thresholds
Agent
Measurement results
3
Monitored Information
6
Configuration Information
1
User Interface

Figure 1.1: The main components of eG Enterprise

1.1.1 Manager

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.

1.1.2 Agents

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 environment. The tests can be executed from locations external to the servers and network components that are responsible for the operation of the IT infrastructure. Agents that make such tests are called **external agents**. These agents take an external view of the IT infrastructure and indicate if the different services supported by the IT infrastructure are functioning properly or not.

Often external agents alone may not be sufficient to completely gauge the health of an IT infrastructure and to diagnose problems when they occur. For example, it may not be possible to measure the CPU utilization levels of a web server from an external location. To accommodate such situations, eG Enterprise uses **internal agents**. An internal agent runs on a server that supports the IT infrastructure and monitors various aspects pertaining to the server (e.g., CPU, memory, and disk utilization, the processes executing on it, and the applications).

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. Details of the statistics collected by the web adapter are provided in the *eG Measurements Manual*.

eG agents have been pre-programmed to execute specific tests for web servers, SSL servers, LDAP servers, DNS server, Database servers, and application servers. Please see the *eG Measurements Manual* for details on the tests included in eG Enterprise. 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.

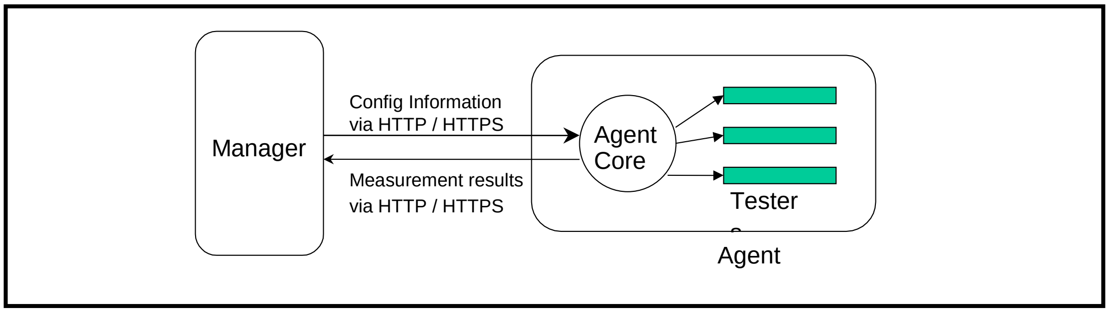


Figure 1.2: The manager-agent communication in the eG architecture

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 1.3 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 1.3, 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).

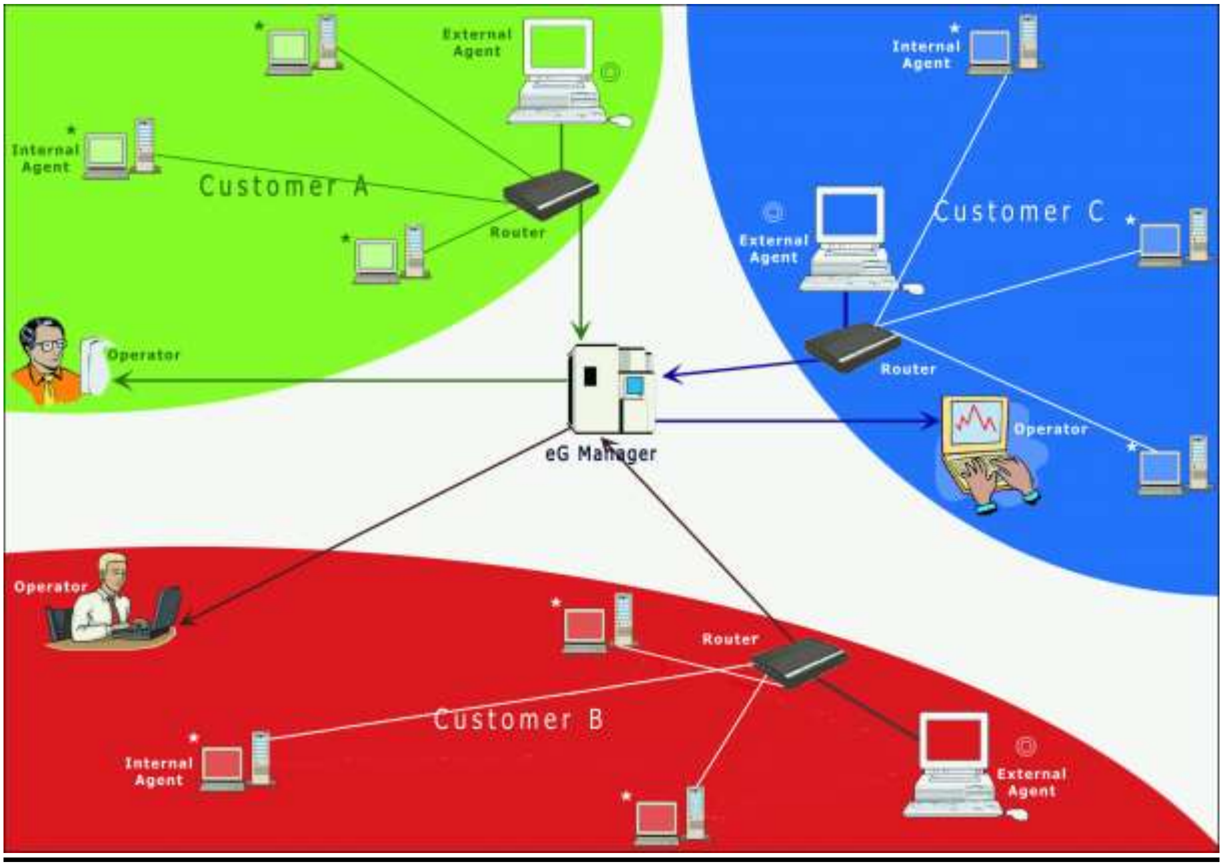


Figure 1.3: A typical deployment architecture of eG Enterprise

1.1.3 Database

The eG database is responsible for persistent storage of the measurement results. Separate tables are maintained for each of the tests being executed by eG agents. 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.

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.

1.1.4 User Interface

A web-based user interface enables a user to interact with eG Enterprise. The recommended browser for the eG user interface is Internet Explorer 10, 11, and Edge, Mozilla Firefox v18 or higher, and Chrome v28 (or above). Broadly, the eG user interface 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 user interface 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.

The previous sections have highlighted the key components of eG Enterprise. In the following chapters, we will describe the first two stages involved in deploying eG Enterprise, namely:

1. **Installation** of the eG manager and the agents. This stage mainly involves deployment of the software on the appropriate servers, creating user accounts, and setting up the directory structures.
2. **Configuration** of the eG manager and the agents. In this stage, the environment is set up for the proper operation of eG Enterprise and the manager and agent processes are started.

1.2 Factors Governing the Location of the Manager

The first step in installing eG Enterprise is the installation of the eG manager. To understand the considerations that govern the exact location where the eG manager should be installed in a target environment, consider Figure 1.4, which depicts the various components of the eG manager. The discovery process is responsible for auto-discovery of the environment and for determining the configurations of the agents. To present a web-based user interface, the eG manager includes a Tomcat server for Unix environments. For Windows environment, the eG manager requires an Internet Information Server (IIS) to be co-located with it, on the same host.

The various factors that should be taken into account while determining the exact location of the eG manager in the target environment are:

a. **Performance impact of the eG manager:** For monitoring smaller environments, in which five agents or less are to be used, the eG manager can be co-located on any of the staging servers of the infrastructure. For larger environments, it is advisable that users dedicate a host for supporting the eG manager.

b. **Network bandwidth usage:** As can be seen from Figure 1.4, several of the eG manager components communicate with the database server to store measurement results and to retrieve the results for display. Co-locating the database server with the eG manager minimizes the network bandwidth usage. Moreover, this configuration can also reduce response times seen by users accessing the eG manager.

   The location of the eG manager relative to the agents also governs the network bandwidth usage. For example, the eG manager may be located at an ISP site, external to the target environment. In this case, the results reported by the agents have to be communicated over an external network all the way back to the manager. To minimize network bandwidth usage, the eG manager should be located as close as possible to the agents deployed in the target environment.

   At the same time, since eG Enterprise’s default external agent is co-located with the manager, the eG manager should be located so that measurements made by the external agent are representative of the quality of service perceived by users of the IT infrastructure. For example, the eG manager can be located on a server that is directly connected to the access router of the IT infrastructure. Doing so ensures that the eG external agent uses the same data path that is used by users of the infrastructure.

c. **Firewall set-up:** In Figure 1.4, while the web server/Tomcat communications are internal to the eG manager, accesses from users and agents to the eG manager involve remote communication to and from the eG manager’s web server port (7077 is the default port). If there are any firewalls used in the target environment, it is essential to ensure that the firewalls are configured to allow all communications to and from the web server component of the eG manager. In the event the eG database is hosted on a server other than the one hosting the eG manager, the firewall rules should also allow the manager-database communications.

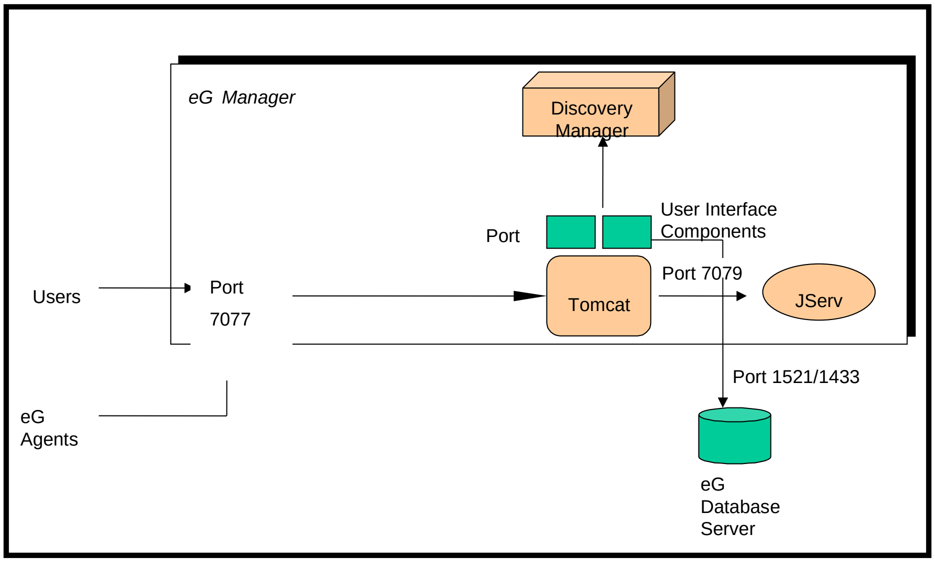


Figure 1.4: The main components of the eG manager

1.2.1 Sizing the Hardware and Database Required by an eG Manager

The hardware sizing for the eG manager and database (i.e., CPU speed, memory required, disk space required, etc.) depends on the number of servers to be monitored, the frequency of the monitoring and on the number of days of raw metrics that are to be stored in the database. eG Innovations engineers will provide a sizing calculator that will allow you to determine the hardware requirements for the eG manager and database depending on your specific requirements.

2

Installing and Configuring 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, Red Hat Linux, and Windows 2000/2003/2008 operating system environments. This chapter describes the steps involved in installing and configuring eG Enterprise on Solaris and Linux operating systems. For detailed instructions of installing and configuring the manager and the agents on Windows operating systems, refer to the next chapter.

2.1 Installing the eG Manager

2.1.1 System Requirements

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

- Solaris 10 (or higher) or 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

- JDK 1.7 (or its variants)

Note

JDK 1.8 is not supported.

- For the eG database, use Oracle database server (version 10G or higher) / Microsoft SQL Server (version 2008 / 2012 / 2014 / 2016) / Microsoft Azure SQL database.

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.

- A minimum of 2 GB RAM would be required for installing the eG manager on a 32-bit host; for a 64-bit host on the other hand, a minimum of 4 GB RAM would be required

- A minimum of 1 GB of disk space free
- 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.

The following sections present the specific instructions for Solaris and Linux operating systems.

2.1.2 Installing the Manager on Solaris

Prior to installing an eG manager on Solaris, ensure that the following recommended settings are in place:

➢ **Solaris file descriptors (ulimit)**

Description:

Specifies the maximum number of open files supported. If the value of this parameter is too low, a **Too many files open** error is displayed.

How to view or set:

Use the following command to display the current settings.

ulimit -a

Use the following command to set the values

ulimit -n 8192

Check the UNIX reference pages on the **ulimit** command for the syntax of different shells.

Recommended value: 8192

On Solaris, setting the maximum number of open files property using `ulimit` has the biggest impact on your efforts to support the maximum number of RMI/IIOP clients.

To increase the hard limit, add the following command to `/etc/system` and reboot it once:

set rlim_fd_max = 8192

➢ Solaris TCP_TIME_WAIT_INTERVAL

Description:

Notifies TCP/IP on how long to keep the connection control blocks closed. After the applications complete the TCP/IP connection, the control blocks are kept for the specified time. When high connection rates occur, a large backlog of the TCP/IP connections accumulate and can slow server performance. The server can stall during certain peak periods. If the server stalls, the **netstat** command shows that many of the sockets that are opened to the HTTP server are in the CLOSE_WAIT or FIN_WAIT_2 state. Visible delays can occur for up to four minutes, during which time the server does not send any responses, but CPU utilization stays high, with all of the activities in system processes.

How to view or set:

Use the **get** command to determine the current interval and the **set** command to specify an interval.

For example:

```
ndd -get /dev/tcp tcp_time_wait_interval
ndd -set /dev/tcp tcp_time_wait_interval 30000
```

Default value: The default time wait interval for a Solaris operating system is `240000` milliseconds, which is equal to 4 minutes.

Recommended value: 60000 milliseconds

➢ Solaris TCP_FIN_WAIT_2_FLUSH_INTERVAL

Description:

Specifies the timer interval prohibiting a connection in the FIN_WAIT_2 state to remain in that state. When high connection rates occur, a large backlog of TCP/IP connections accumulate and can slow server performance. The server can stall during peak periods. If the server stalls, using the **netstat** command shows that many of the sockets opened to the HTTP server are in the CLOSE_WAIT or FIN_WAIT_2 state.

Visible delays can occur for up to four minutes, during which time the server does not send any responses, but CPU utilization stays high, with all of the activity in system processes.

How to view and set:

Use the **get** command to determine the current interval and the **set** command to specify an interval.

For example,

```
ndd -get /dev/tcp tcp_fin_wait_2_flush_interval
ndd -set /dev/tcp tcp_fin_wait_2_flush_interval 67500
```

Default value: 675000 milliseconds

Recommended value: 67500 milliseconds

➢ Solaris TCP_KEEPALIVE_INTERVAL

Description:

The keepAlive packet ensures that a connection stays in an active and established state.

How to view or set:

Use the **ndd** command to determine the current value or to set the value.

For example:

```
ndd -get /dev/tcp tcp_keepalive_interval
ndd -set /dev/tcp tcp_keepalive_interval 300000
```

Default value: 72000 milliseconds

Recommended value: 15000 milliseconds

➢ Solaris TCP_KEEPALIVE_PROBES

Description:

Specifies the kernel how many TCP keepalive probes to send out before it decides if a specific connection is broken.

How to view or set:

Use the **ndd** command to determine the current value or to set the value.

For example:

```
ndd -set /dev/tcp tcp_keepalive_probes 5000
```

Default value: `9000` milliseconds

Recommended value: 5000 milliseconds

➢ Solaris kernel semsys:seminfo_semume

Description:

Limits the maximum semaphore undo entries per process. Because this setting specifies a maximum value, the parameter does not cause the use of additional memory unless it is needed.

How to view or set:

This value is displayed as the semume parameter if the **/usr/sbin/sysdef** command is run. There can be an entry in the **/etc/system** file for this tuning parameter. Set this parameter through the **/etc/system** entry:

```
set semsys:seminfo_semume = 200
```

Default value: `10`

Recommended value: 200

➢ Solaris kernel semsys:seminfo_semopm

Description:

Displays as the semume parameter if the **/usr/sbin/sysdef** command is run. An entry in the **/etc/system** file can exist for this tuning parameter. This number is the maximum value of System V semaphore operations per semop call. The default value for this option is too low for highly concurrent systems.

How to view or set:

Set this parameter through the **/etc/system** entry:

```
semsys:seminfo_semopm = 16384
```

Default value: None

Recommended value: 16384

- **Connection backlog**

Description:

Change the following parameter when a high rate of incoming connection requests result in connection failures:

How to view or set:

```
ndd -get /dev/tcp tcp_conn_req_max_q
ndd -set /dev/tcp tcp_conn_req_max_q 8192
```

Default value: For Solaris 8, the default value is 128.

Recommended value: 8192

Note

Please note that the actual implementation and syntax may vary from one version of the operating system to another and from one version of kernel to another. Please verify compatibility with your system.

The eG manager software is provided as two standard Solaris packages, both named **eGmanager** - one for Solaris hosts supporting the **AMD** processor and another for those hosts usng the **Sparc** processor. Both these packages can be installed using the **pkgadd** utility. Using the **pkgrm** utility, the eG manager can be uninstalled.

The broad steps for installing or uninstalling the eG manager do not vary based on what processor is used by the target Solaris host. However, **make sure that you use the correct package for installation**.

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 a temporary folder (say, **/tmp**) on the target Solaris host, copy the **eGmanager** package that corresponds to that host. For instance, to install the eG manager on a Solaris host that supports the **AMD** processor, copy the **eGmanager** package in the **AMD** folder.

2. To start the installation process, execute the command:

   pkgadd -d <path of the package eGmanager>

3. The list of available packages will be displayed next. Enter **all** to install all the packages related to the eG manager.

```
1  eGmanager     eG Manager
                   (SunOS) version 6.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

4. We recommend that the eG manager 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:

```
Processing package instance <eGmanager> from </tmp/Gmanager>
eG Manager
(Sparc/AMD64) version 6.0
eG Innovations, Inc.

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

   Specify the user account to be used for executing eG Enterprise. The default value is **"egurkha"**.

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

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

---

5. 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 to the **/opt/egurkha** directory.

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

6. `Would you like the eG manager 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 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.

7. 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 <eGmanager> [y,n,?] y
```

8. 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.

Please note that the eG Manager requires JDK 1.6
***********************************************************************
Installation of <eGmanager> was successful.
```

2.1.3 Installing the Manager on Linux/CentOS

For installation on Linux/CentOS systems, the eG manager is provided as a tar file (named **eGmanager_linux.tar**). The same tar file can be used for installing the eG manager on 32-bit Linux/CentOS host and on a 64-bit Linux/CentOS host. During installation, setup automatically detects whether the target host is a 32-bit or a 64-bit host and copies the relevant files to the directory chosen for installation.

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

   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.

   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 installaxtion 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. `Would you like the eG manager 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 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.

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 1.6 or higher.
*****************************************************************
```

2.2 Configuring the eG Manager

After the installation, the eG manager needs to be configured for proper functioning. The steps involved in configuring the eG manager are the same for Solaris and Linux systems, and are listed below:

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

   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.

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

To enable the setup process to configure the eG Enterprise's execution environment to execute Java programs, next specify the Java home directory (say **/opt/java1.6.0_10**). If the configuration process cannot locate the specified Java home directory, it returns the following error message:

```
The setup process failed to locate /opt/java1.6.0_10
```

Then, the configuration process looks for the Java library (lib) subdirectory of the Java home directory. Within this directory, the setup process checks for a specific file called **tools.jar**. For example, if the user specifies **/opt/java1.6.0_10** as the Java home directory, the configuration process will look for the file **/opt/java1.6.0_10/lib/tools.jar**. If the process fails to locate the Java lib directory, it will explicitly ask the user to specify the Java lib directory and also display the following message:

```
The setup process failed to locate /opt/java1.6.0_10/lib/tools.jar...
```

9. Once the Java lib directory has been located, the setup process will look for a Java fonts directory within the Java home directory. For example, if the Java home directory is set to **/opt/java1.6.0_10**, the setup process will check for the fonts directory in the location **/opt/java1.6.0_10/jre/lib/fonts**. If this directory is not found, the following error message appears and the setup process will prompt the user to specify the Java fonts directory.

```
The setup process failed to locate /opt/java1.6.0_10/jre/lib/fonts...
```

10. 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
```

Refer

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

11. 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 Section 2.2.3.

12. If **y** is specified at step 11, 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.

13. 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**.

14. 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:
```

15. 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
```

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

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

17. 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
```

18. 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
```

19. 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 :
```

20. 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
```

21. 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.

22. 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

While configuring multiple managers, ensure that each of the managers uses a separate database.

23. The next step involves setting up of the eG manager for database access. The installation process prompts the user to choose whether to use Oracle or Microsoft's SQL server as the backend database server that hosts the eG manager.

```
Database configuration for the eG Manager
*********************************************************************
The eG Manager requires a database server for storing its measurements.
*********************************************************************
Choose the type of database server which you want to use for the eG Manager:
```

```
[1] Oracle Database Server
[2] Microsoft SQL Server
```

```
Select the database server type by number:
```

To pick the Oracle Database Server, enter **1**. For the MS SQL Server Database, enter **2**.

If you choose the former, refer to Section 2.2.1. If you choose the latter, please refer to Section 2.2.2 for further details.

2.2.1 Using an Oracle Database

This section provides instructions to configure the manager if Oracle is used as the database server for the eG manager. Refer to Section 2.2.2 if MS SQL Server is to be used as the database server.

1. Once Oracle is chosen as the database server, the installation process instructs the user to appropriately size the tablespace that is to be used to host eG's database.

```
*****************************************************************************
To set up the eG database, please ensure that you have an Oracle database instance
running.
******************************************************************************
```

   Once a database instance has been configured to conform to the sizing requirements of eG Enterprise, enter **y** here to proceed with configuring the eG manager.

```
Do you want to continue the setup y/n? [y]
```

2. Configure eG Enterprise for database access by entering the following:

   - The hostname or IP address of the server that hosts the Oracle database (use the hostname if DNS is supported)

   - The port number of the Oracle server [default is **1521**]

   - The name of an Oracle instance (SID) that the eG manager should use.

```
Enter the hostname (or IP address) of the Oracle server:
Enter the port number of the Oracle server [1521]:
Enter the name of an Oracle instance (SID) that the eG Manager should use: egurkha
```

3. The eG manager requires a special database user account to store its measures. The user should next enter:

   - the eG database user name [default is **egurkha**]

   - the password for the database user [default is **egurkha**]

```
***********************************************************************
Database access configuration for the eG Manager
***********************************************************************
The eG Manager requires a special database user account to store its measures.
Enter the eG database user name [egurkha]:
Enter the password for egurkha:
Please re-enter the password for egurkha:
```

Note

Make sure that the eG database user name you provide does not contain any special characters.

4. The configuration process next prompts the user to specify if the database user name specified has already been created. If this is not the case, the configuration process prompts for the user's consent to create the database user account.

```
Does the 'egurkha' account already exist y/n? [n] :
Do you want to create the ‘egurkha’ account now y/n? [y] :
```

5. If the user chooses not to have the user account created by the configuration process, the user account has to be created manually with *connect, resource, and select_catalog* privileges.

Note

When manually creating a new database user account for eG purposes, make sure that the eG database user name you provide does not contain any special characters.

6. In the event that the user agrees to have the account created by the configuration process, the user is prompted to specify the default and temporary database tablespaces with which the user account should be associated.

```
Oracle requires that a user account be associated with a default and a temporary
tablespace.
Please enter the default tablespace for the user egurkha:
Please enter the temporary tablespace for the user egurkha:
```

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. The setup now prompts the user to enter the database administrator's name and password.

```
New user creation requires database administrator privileges.
Enter the DBA user name :
```

```
Enter the DBA password :
```

Make sure that the *DBA user name* you provide does not contain any special characters.

8. Once the user account is created, the configuration process proceeds to create the various database tables required by eG Enterprise. The following error message appears if the configuration process does not succeed.

```
Database user creation started ...
Database user created successfully ...!
Configuration of the eG Manager continues...
****************************************************************
Attempting to load the eG tables into the database ...
If any error appears during the configuration, there may be a problem with the
Oracle database parameters you supplied. Please check and restart the manager
configuration.
Press <Enter> to continue, <CTRL-C> to end
**************************************************************************
```

9. Upon successful installation of the manager, the following message will be displayed to the user:

```
***********************************************************************
If there were no errors, the eG Manager has been configured.
Please 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
mailto:support@eginnovations.com to request for a license.
***********************************************************************
```

2.2.2 Using an MS SQL Server Database

2.2.2.1 Prerequisites for using an MS SQL Server Database

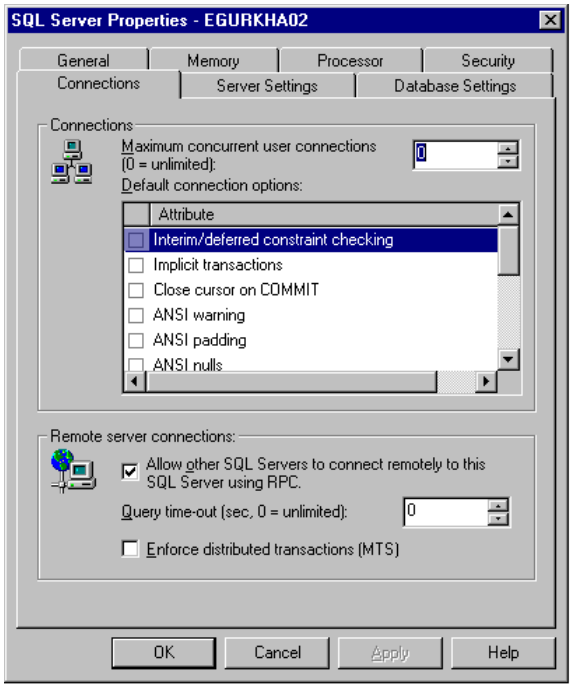
Before even commencing the configuration process of the eG manager using an MS SQL Server database, ensure that the following are in place:

- **The MS SQL Server should allow 'unlimited' concurrent connections**

  Given below are the steps to be followed to fulfill this requirement on an MS SQL Server 2000:

  - Select the **Connections** tab. A dialog box depicted by Figure 2.1 below will appear.

  - Then, click on the **Server Settings** tab page in Figure 2.1. Figure 2.2 will appear.



Connections

Maximum concurrent user connections (0 = unlimited): 0

Default connection options:

- ☐ Interim/deferred constraint checking
- ☐ Implicit transactions
- ☐ Close cursor on COMMIT
- ☐ ANSI warning
- ☐ ANSI padding
- ☐ ANSI nulls

Remote server connections:

☑ Allow other SQL Servers to connect remotely to this SQL Server using RPC.

Query time-out (sec, 0 = unlimited): 0

☐ Enforce distributed transactions (MTS)

Figure 2.1: Setting the maximum concurrent user connections

- 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.

- **Multi-protocol support should be configured on the MS SQL server**

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

  - On the MS SQL server host, follow the menu sequence, Start -> Programs -> Microsoft SQL Server -> Client Network Utility, to open the MS SQL server's **Client Network Utility** (see Figure 2.2).

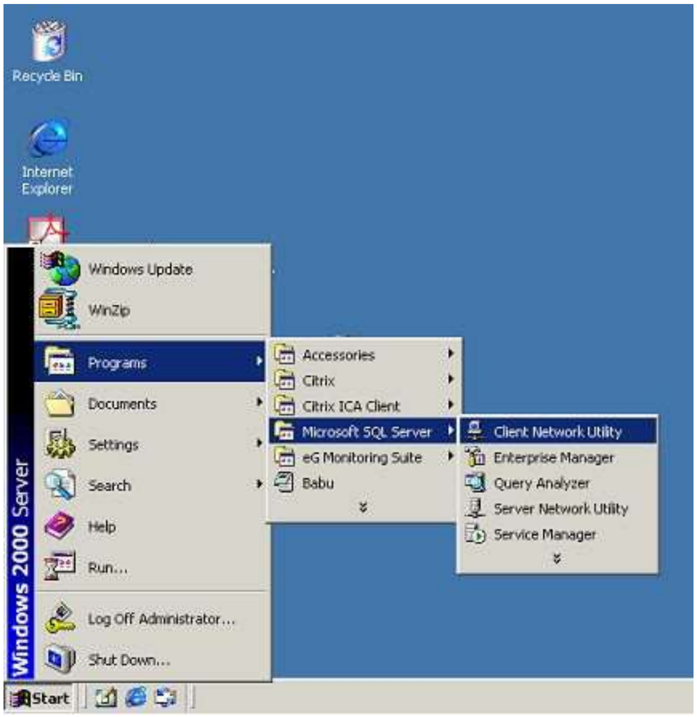
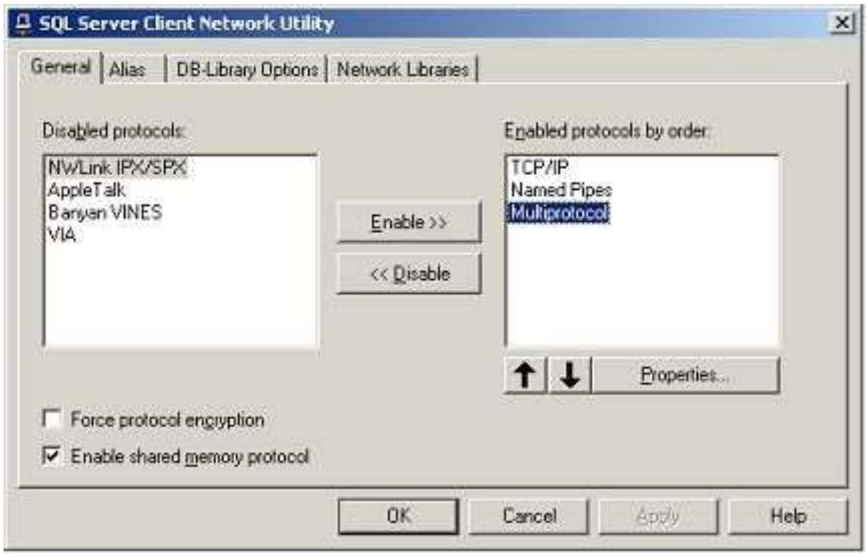


Figure 2.2: Opening the Client Network Utility

- In the **General** tab of Figure 2.3 that appears next, check whether the **Multiprotocol** option is available in the **Enable protocols by order** list. If not, then select it from the **Disabled protocols** list and select the **Enable** button to enable it.



Disabled protocols:
NWLink IPX/SPX
AppleTalk
Banyan VINES
VIA

Enabled protocols by order:
TCP/IP
Named Pipes
Multiprotocol

☐ Force protocol encryption
☑ Enable shared memory protocol

Figure 2.3: Enabling Multiprotocol support using the SQL Client Network Utility

- Finally, click the **Apply** and **OK** buttons in Figure 2.3 to register the changes.

- Next, follow the menu sequence depicted by Figure 2.4 to open the MS SQL server's **Server Network Utility**.

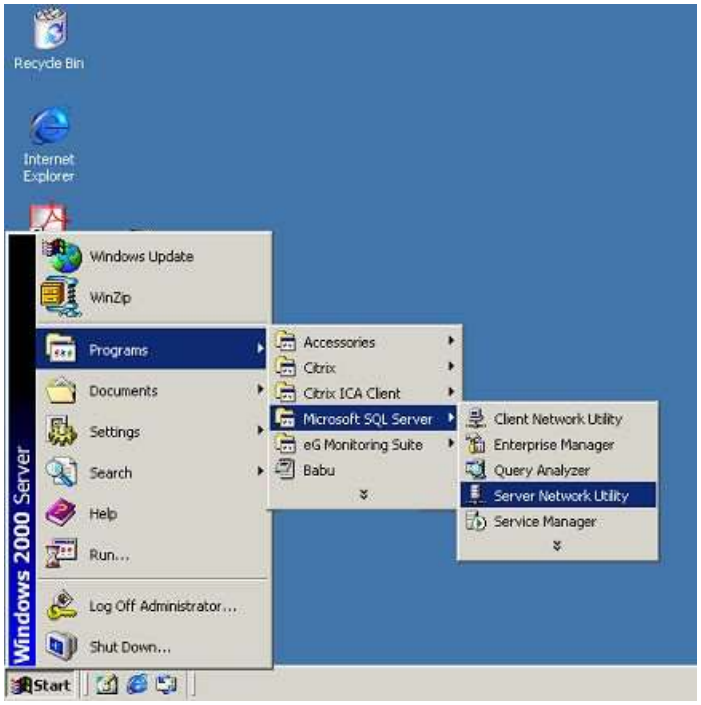
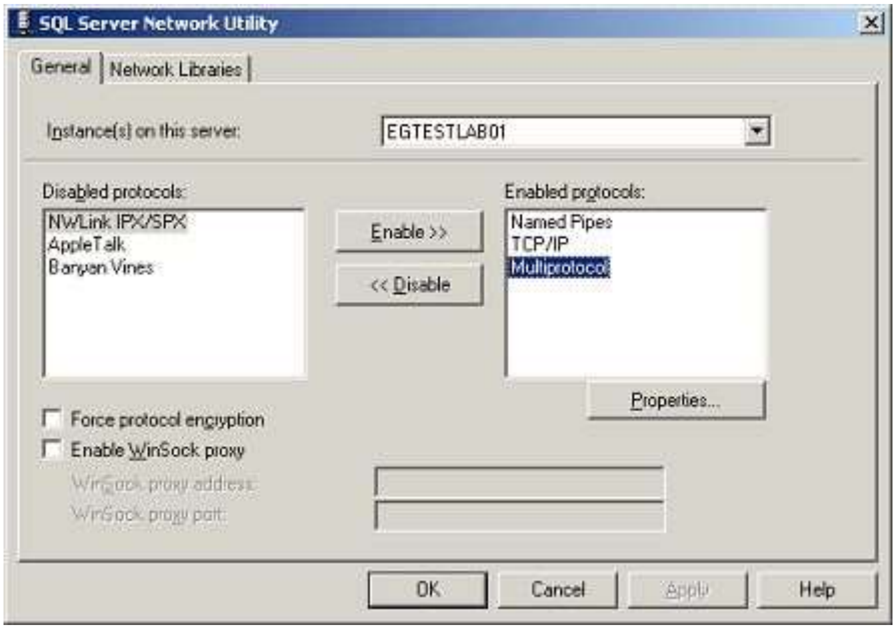


Figure 2.4: Opening the Server Network Utility

- When Figure 2.5 appears, check whether the **Multiprotocol** option is available in the in the **Enable protocols by order** list. If not, then select it from the **Disabled protocols** list and select the **Enable** button to enable it.



Instance(s) on this server: EGTESTLAB01

Disabled protocols:
NWLink IPX/SPX
AppleTalk
Banyan Vines

Enabled protocols:
Named Pipes
TCP/IP
Multiprotocol

□ Force protocol encryption
□ Enable WinSock proxy
WinSock proxy address:
WinSock proxy port:

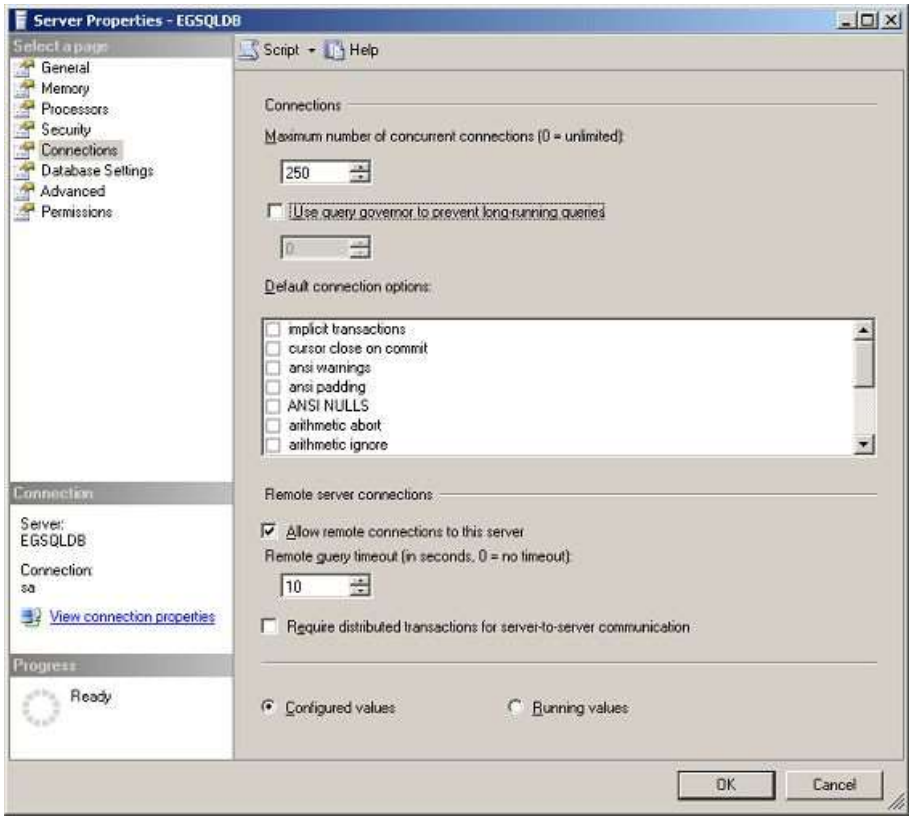
Figure 2.5: Enabling Multiprotocol support using the SQL Server Network Utility

- Finally, click the **Apply** and **OK** buttons in Figure 2.5 to register the changes.

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

  To ensure this, do the following:

  - On the MS SQL Server host, open the **SQL Server Enterprise Manager**.
  - From the tree-structure on the left panel of the enterprise manager, select the name of the SQL server to be used as the eG backend, right-click on it, and choose **Properties**.
  - Figure 2.6 then appears. Next, click on the **Connections** page in the left panel of Figure 2.6. In the **Connections** section that is then displayed in the right panel, make sure that the **Use query governor to prevent long-running queries** option is disabled. If not, then uncheck the check box to disable it.



Connections

Maximum number of concurrent connections (0 = unlimited): 250

□ 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): 10

□ Require distributed transactions for server-to-server communication

● Configured values ○ Running values

Server: EGSQLDB

Connection: sa

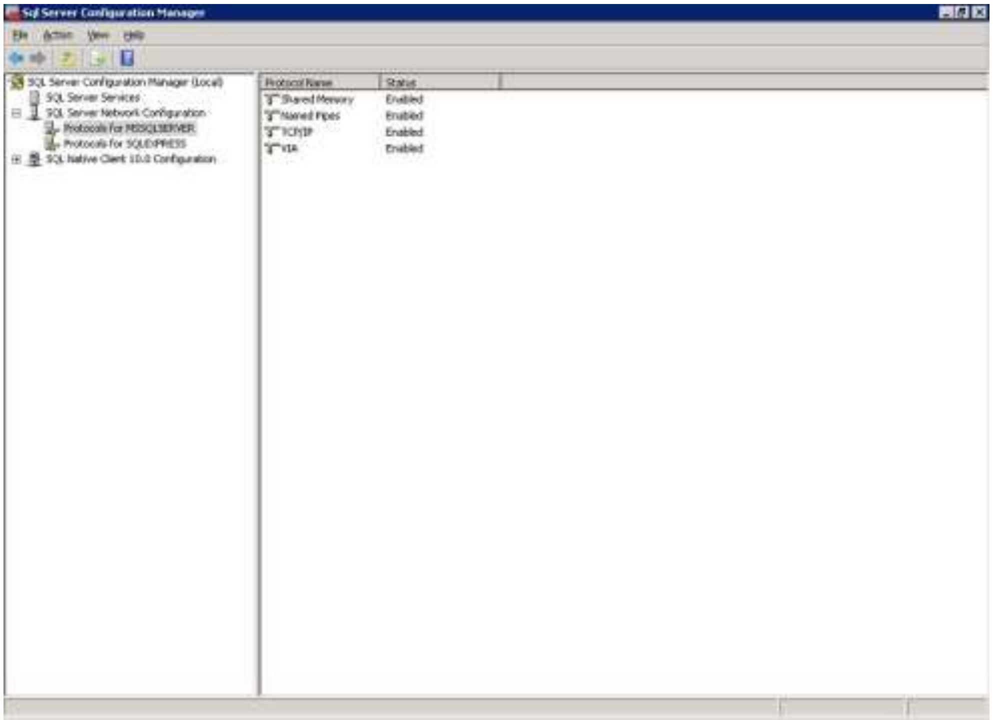
Figure 2.6: Enabling long-running queries to be executed on the MS SQL server

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

- **If the MS 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:

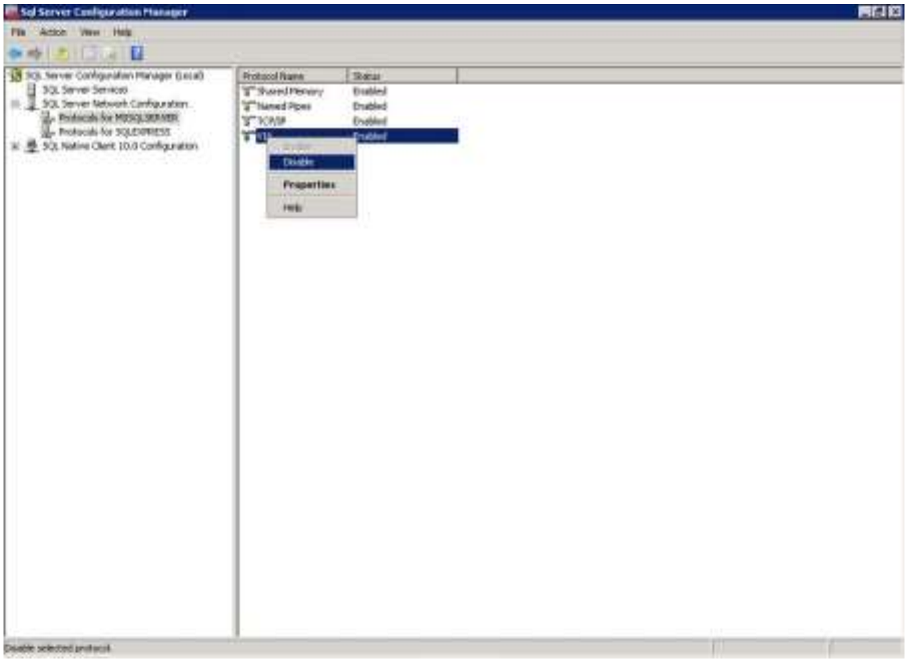
  - On the MS SQL Server 2008 host, open the **SQL Server Configuration Manager**.
  - In the left panel of the configuration manager, click on the **Protocols for <SQLSERVERNAME>** node as depicted by Figure 2.7. The list of protocols that the SQL server supports will then be displayed in the right panel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

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

Figure 2.8: Disabling the VIA protocol

- Next, check whether the other protocols listed in the right panel of Figure 2.8 are **Enabled**. If not, then enable those protocols.

- **If the MS SQL Server 2008 is used as the eG backend, then ensure that the 'SQL Server' service and 'SQL Server Agent' service are running on the SQL Server host.**
- **If the MS 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.**

2.2.2.2 Configuring the eG Manager to use an MS SQL Server Database

This section aids you in proceeding with the installation process, if you choose MS SQL Server as the database server for eG manager.

1. The installation process instructs the user to appropriately size the database.

```
*********************************************************************************
When setting up the eG database, please ensure that you have sufficient space to
host the eG database.
*********************************************************************************
```

2. To configure the eG manager for database access, next enter:

   a. the hostname or IP address of the server that hosts the MS SQL database (use the hostname if DNS is supported)

   b. the port number of the MS SQL server [default is **1433**]

   Prior to this, provide your confirmation for proceeding with the setup by pressing **y**.

```
Do you want to continue the setup y/n? [y]
Enter the hostname (or IP address) of the MS SQL server:
Enter the port number of the MS SQL server [1433]:
```

If the MS SQL server being configured uses named instances, then specify *none* instead of the port number.

3. Next, indicate whether the MS SQL server to be used as the eG backend is SSL-enabled or not.

```
Does the SQL database server support SSL? y/n [n]
```

4. Then, specify whether/not the SQL server is NTLM v2-enabled.

```
Does the SQL database server with NTLMv2? y/n
```

5. The installation process next asks the user as to whether an existing database instance can be used, or whether a new instance should be created.

```
**********************************************************************
Database access configuration for the eG Manager
*********************************************************************
The eG Manager requires a database to store its measures.
Do you want to use an existing database y/n? [y]: n
```

If you choose to use a new database, press **n**, and proceed to specify the name of the new database.

```
Enter the new database name [egurkha]:
```

As new database creation warrants administrator privileges, the credentials of the administrator will then be requested:

```
New database creation requires database administrator privileges.

Enter the DBA user name (eg., sa or in the form domainname/db_admin_username) : sa
Enter the DBA password :
```

Note

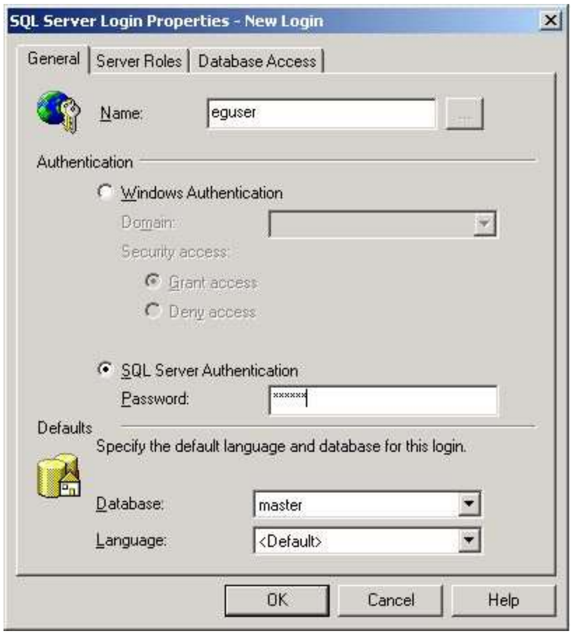
Make sure that the *DBA user name* you provide does not contain any special characters.

If **Windows Authentication** is enabled on the MS SQL server, then ensure that the credentials of a valid Windows domain user with database administrator privileges are provided when setup requests for a DBA user name. Also, make sure that the user name is of the format *domainname|username*. For eg., if the name of the database administrator is *dbadmin* and the domain name is *chi*, the user name you specify should be: *chi|dbadmin*.

On the other hand, if **Mixed Mode Authentication** is enabled on the MS SQL server, then the database administrator name that you specify need not necessarily be preceded by the domain name. In this case therefore, your user name specification can be of either of the following formats: *username* or *domainname\username*.

However, if **SQL Server Authentication** is enabled on the MS SQL server, then the database administrator name should **not be prefixed by a domain name**. Your specification should then be only, *username*.

By default, manager setup displays the **sa** user name at this prompt. If, due to security concerns, you decide not to use the **sa** user name and password, then you can create a user with the following server roles: **Security Administrators** and **Database Creators**, and then provide that user's credentials when setup prompts you for the DBA's user name and password. Figure 2.10 depict how to create a new user with the aforesaid privileges using the **SQL Server Enterprise Manager**.



Name: eguser

Authentication

○ Windows Authentication

Domain:

Security access:

● Grant access

○ Deny access

● SQL Server Authentication

Password: ******

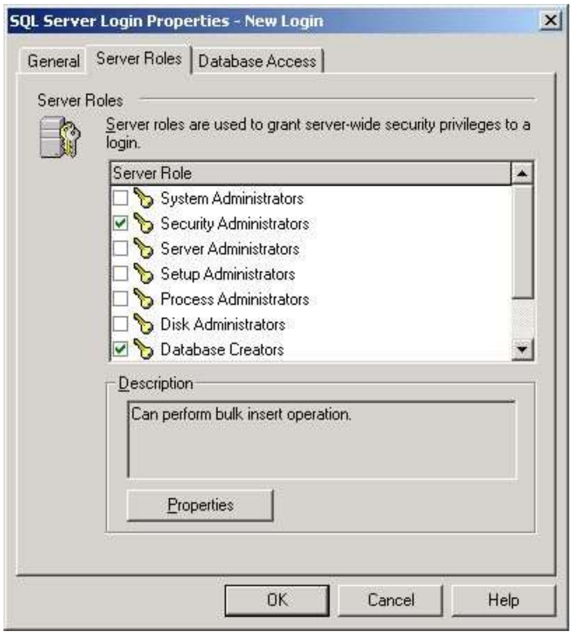
Defaults

Specify the default language and database for this login.

Database: master

Language: <Default>

Figure 2.9:Creating a new user



Server Roles

Server roles are used to grant server-wide security privileges to a login.

Server Role

☐ System Administrators
☑ Security Administrators
☐ Server Administrators
☐ Setup Administrators
☐ Process Administrators
☐ Disk Administrators
☑ Database Creators

Description

Can perform bulk insert operation.

Figure 2.10: Granting the requisite privileges to the new user

Note

- Make sure that user name you provide for the new DBA user does not contain special characters.

- If MS SQL 2008 is used as the eG backend, then ensure that the **dbcreator**, **securityadmin**, and **public** roles are assigned to the user. Also, either provide a **strong password** for the user, or make sure that the **Enforce password policy** option is disabled while creating the user profile in the **SQL Enterprise Manager**.

While Figure 2.9 and Figure 2.10 illustrate the procedure to be followed to create a new user on an MS SQL server with **SQL Server Authentication** enabled, remember the following while creating a user on an MS SQL server with **Windows Authentication** enabled:

- The username you specify should be that of a valid user to the Windows domain of which the MS SQL server is a part;

- The username specification should be of the format: *domainname\username*

6. On the contrary, if you choose to use an existing database, then press **y** (at step 3) and enter the name of an existing database.

```
Please enter the database name :
```

7. Next, specify the details of the user account that will be used to host the eG database:

   - the eG database user name [default is **egurkha**]

   - the password for the database user [default is **egurkha**]

```
The eG Manager requires a special database user account to store its measures.
Enter the eG database user name [egurkha]:
Enter the password for egurkha:
Please re-enter the password for egurkha:
```

Note

Make sure that the eG database user name you provide does not contain any special characters.

Here again, the **Authentication** mode set for the MS SQL server in question will have to be considered. Iif **Windows Authentication** is enabled on the MS SQL server, then the new user should be a valid Windows domain user. Accordingly, the user name should be of the format *domainname|username*. For eg., if the name of the new user is *egdb* and the domain name is *sig*, the user name you specify in Figure 3.41 should be: *sig|egdb*.

On the other hand, if **Mixed Mode Authentication** is enabled on the MS SQL server, then the special user account you create need not necessarily be preceded by the domain name. In this case therefore, your user name specification can be of either of the following formats: *username* or *domainname|username*.

However, if **SQL Server Authentication** is enabled on the MS SQL server, then the user name should **not be prefixed by a domain name**. Your specification should then be only, *username*.

Note

If MS SQL Server 2008 is being used as the eG backend, then ensure that the password provided for the eG 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.

8. The configuration process next prompts the user to specify if the database user name specified has already been created.

```
Does the 'egurkha' account already exist y/n? [n] :
```

If the user response is **y** here, then the following message will appear:

```
User 'egurkha' exists! Continuing ...
```

Note

- Before attempting to set an existing database user name as the eG database user, make sure that *dbowner* privileges are granted to such a user.
- Also, make sure that the existing database user name does not contain any special characters.

If the user response is **n**, then the configuration process prompts for the user's consent to create the database user account.

```
Do you want to create the 'egurkha' account now y/n? [y] :
```

Enter **y** to invoke the following:

```
New user creation requires database administrator privileges.
Enter the DBA user name (eg., sa or in the form domain/dbaccount) :
Enter the DBA password :
```

Note

Make sure that the *DBA user name* you provide does not contain any special characters.

After providing the required information, if errors occur in the user creation process, the following message will come up:

```
Database user may not be created, possible reasons are ...
Database connection failed ...
```

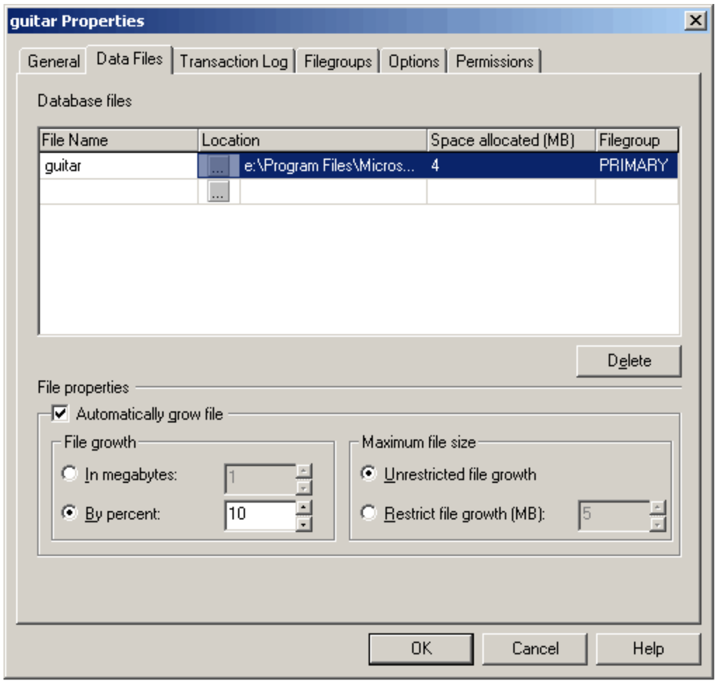
9. Once the user account is created, the configuration process proceeds to create the various database tables required by eG Enterprise. The following error message appears next:

```
****************************************************************************
Attempting to load the eG tables into the database ...
If any error appears during the configuration, there may be a problem with the MS
SQL database parameters you supplied. Please check and restart the manager
configuration.
Press <Enter> to continue, <CTRL-C> to end

Database table creation started ...
Database table creation completed successfully ...!
****************************************************************************
```

10. Upon successful installation of the manager, the following message will be displayed to the user:

```
****************************************************************************
If there were no errors, the eG Manager has been configured. Please use the
command /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
mailto:support@eginnovations.com to request for a license.
*****************************************************************************
```

11. Once you are through with the configuration, go to the **SQL Server Enterprise manager**. Select the appropriate server, followed by the databases. On clicking the database folder, a list of databases currently available on that server will pop up. Now, select an appropriate database, right-click on it and select **Properties**. From the dialog box that comes up, select the **Data Files** tab. A screen as shown in Figure 2.11 below will appear.



Database files

File Name	Location	Space allocated (MB)	Filegroup
guitar	e:\Program Files\Micros...	4	PRIMARY

File properties

☑ Automatically grow file

File growth

○ In megabytes: 1

● By percent: 10

Maximum file size

● Unrestricted file growth

○ Restrict file growth (MB): 5

Figure 2.11: Configuring the database

12. Here, you can configure your database appropriately and save the configuration by clicking the **OK** button.

2.2.3 Using a Microsoft Azure SQL Database

Microsoft Azure SQL Database is a relational database-as-a-service that delivers predictable performance, scalability, business continuity, data protection, and near-zero administration to cloud developers and solution architects.

If you have already created a SQL database on Azure, then, you can configure the eG manager to use this database as its backend. The procedure for this is as follows:

1. When setup prompts you to pick a database server for use as the eG backend, enter **2** to pick the *Microsoft SQL Server* option.

```
Database configuration for the eG Manager
************************************************************************
The eG Manager requires a database server for storing its measurements.
************************************************************************
Choose the type of database server which you want to use for the eG Manager:

[1] Oracle Database Server
[2] Microsoft SQL Server

Select the database server type by number: 2
```

2. The installation process instructs the user to appropriately size the database.

```
**********************************************************************************
When setting up the eG database, please ensure that you have sufficient space to
host the eG database.
**********************************************************************************
```

3. To configure the eG manager for database access, next enter:

   a. the fully-qualified SQL server name that Azure auto-generates when creating a SQL database

   b. the port number of the SQL server instance that Azure auto-generates [default is **1433**]

   Prior to this, provide your confirmation for proceeding with the setup by pressing **y**.

```
Do you want to continue the setup y/n? [y]: y
Enter the hostname (or IP address) of the MS SQL server:
swo2fn9hhb.database.windows.net
Enter the port number of the MS SQL server [1433]: 1433
```

4. By default, the SQL server instance that Azure creates is SSL-enabled. Therefore, when requested to confirm whether the SQL server is SSL-enabled or not, type **y**.

```
Does the SQL database server support SSL? y/n [n]: y
```

5. Since you have already created a SQL database on Azure, enter **y** when setup prompts you to use an existing database for storing measures.

```
***********************************************************************
Database access configuration for the eG Manager
**********************************************************************
The eG Manager requires a database to store its measures.
Do you want to use an existing database y/n? [y]: y
```

6. Enter the name of the Azure SQL database that pre-exists.

```
Please enter the database name : egdb
```

7. Next, specify the details of the user account that will be used to host the eG database:

   - the login name that you provided when creating the SQL database on Azure
   - the password that you provided for the login name at the time of creating the Azure SQL database

```
The eG Manager requires a special database user account to store its measures.
Enter the eG database user name [egurkha]: eguser
Enter the password for egurkha:  ****
Please re-enter the password for egurkha: ****
```

Note

- By default, the SQL database on Azure uses SQL authentication only. Therefore, make sure you specify the user name here without prefixing it with a domain name.
- Make sure that the eG database user name you provide does not contain any special characters.

8. The configuration process next prompts the user to specify if the database user name specified has already been created.

```
Does the 'eguser' account already exist y/n? [n] :
```

Type **y** here to confirm that the user exists.

```
User 'egurkha' exists! Continuing ...
```

9. The configuration process proceeds to create the various database tables required by eG Enterprise. The following error message appears next:

```
***************************************************************************
Attempting to load the eG tables into the database ...
If any error appears during the configuration, there may be a problem with the MS
SQL database parameters you supplied. Please check and restart the manager
configuration.
Press <Enter> to continue, <CTRL-C> to end

Database table creation started ...
Database table creation completed successfully ...!
***************************************************************************
```

10. Upon successful installation of the manager, the following message will be displayed to the user:

```
***************************************************************************
If there were no errors, the eG Manager has been configured. Please use the
command /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
mailto:support@eginnovations.com to request for a license.
****************************************************************************
```

Note

1. Before starting the manager, make sure that you have the proper license file in **/opt/egurkha/bin**.
2. To view the license, execute the command

   /opt/egurkha/bin/viewCert <License File Name>

3. When the eG manager is started properly, the following processes will be started up:

   a. One Tomcat process

   b. The eG manager's recovery process ("**eGmon**")

4. 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 Unix systems, the script **/opt/egurkha/bin/set_manager_default** can be used for this purpose. The output below specifies how the **set_manager_default** script can be used.

```
$/opt/egurkha/bin/set_manager_default
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!
**********************************************************************
```

2.3 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/jdk1.6.1_06
```

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 12 to 22 of Section 2.2 will follow.

2.4 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 Section 2.4.1. If you pick option (b), use the procedure detailed in Section 2.4.2.

2.4.1 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.

2.4.1.1 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* **2048** *-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.

2.4.1.2 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**

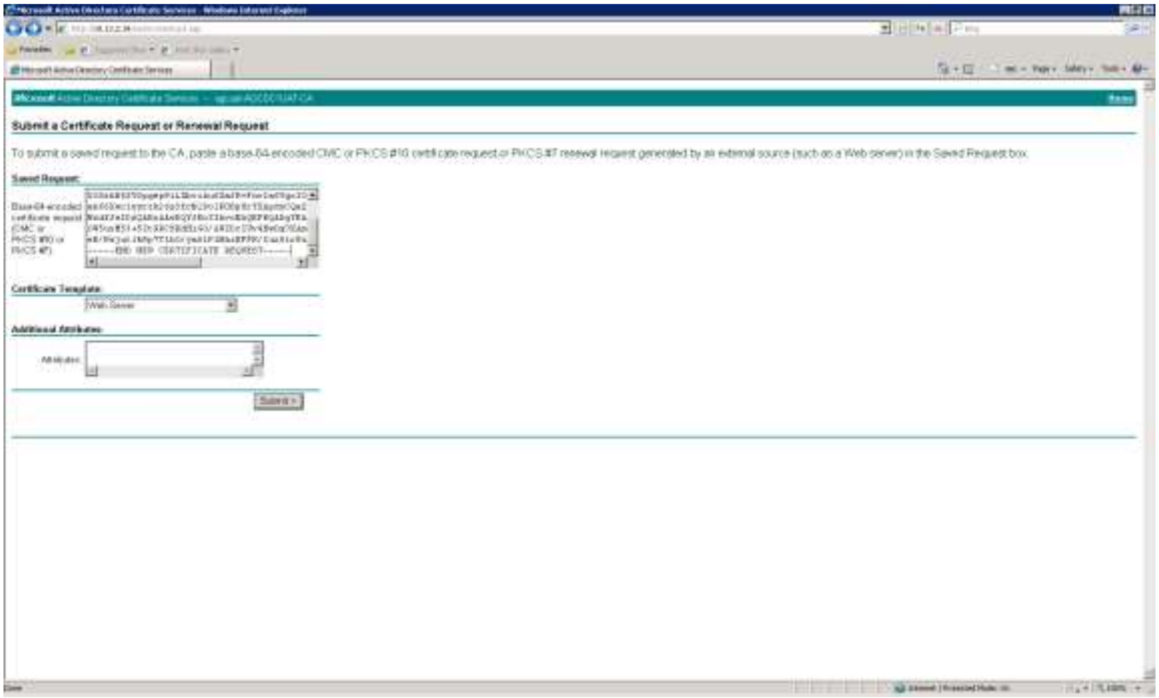
   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-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 2.4.1.1 of this document).**
   - **-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 2.4.1.1**
   - **-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 2.4.1.1 of this document).** 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 2.4.1.1 of this document).**

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.

2.4.1.3 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 2.12 will then appear.



Microsoft Active Directory Certificate Services -- ugcuat-AGCDCUAT-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):

```
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

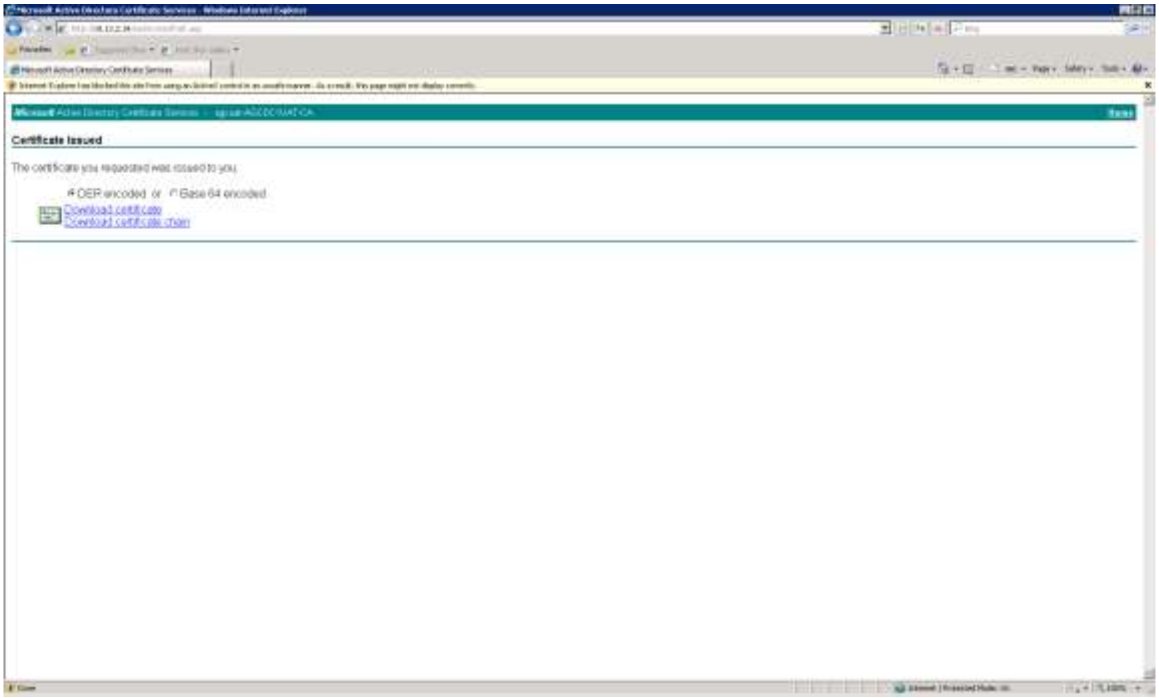
Web Server

Additional Attributes:

Figure 2.12: Requesting for a certificate

2. Open the text file containing the certificate request (which was created using the procedure detailed in Section 3.4.1.2 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 2.12. Then, click the **Submit** button.

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



Microsoft Active Directory Certificate Services -- ugcuat-AGCDCUAT-CA

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Figure 2.13: Downloading the certificate

2.4.1.4 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. 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 2.4.1.1) .**
   - **-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 2.4.1.1 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. 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 2.4.1.1 above.
- **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 2.4.1.1 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 2.4.1.1 above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 2.4.1.1 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 2.4.1.1) **.**
   - **-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 2.4.1.1 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 2.4.1.1 **of this document.**
   - **-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** 2.4.1.1 **of this document**

2.4.1.5 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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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,app
lication/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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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.

2.4.2 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:

1. Generating the keystore file

2. Generating a certificate request
3. Submitting the certificate request to the Certificate Authority (CA) and obtaining a certificate
4. Importing the certificate into a keystore
5. Configuring Tomcat for using the keystore file

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

2.4.2.1 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* **2048** *-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.

2.4.2.2 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 2.4.2.1 of this document).**
   - **-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 2.4.2.1**
   - **-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 2.4.2.1 of this document).** 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 2.4.2.1 of this document).**
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.

2.4.2.3 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.

2.4.2.4 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 2.4.2.1)** **.**
   - **-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 2.4.2.1 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 2.4.2.1 above.
- **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 2.4.2.1 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 2.4.2.1 above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 2.4.2.1 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 2.4.2.1**) **.**
   - **-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 2.4.2.1 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 2.4.2.1 of this document.**
   - **-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 2.4.2.1 of this document**

2.4.2.5 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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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,app
lication/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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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.

2.5 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.

2.6 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.

2.7 Starting the 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".
**********************************************************************
```

2.8 Recommended Browser Settings for the eG Manager

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

- Internet Explorer 10, 11, or Edge
- Mozilla Firefox v18 or above
- Chrome v28 or above

No additional plugins 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 Section 3.9 of Chapter 3 of this document are in place.

2.9 Increasing the Memory of the eG Manager Process

The eG manager runs as a Java process. The maximum heap memory that can be allocated to a 32-bit eG manager process is limited to 1.5 GB. The maximum heap memory allocation to a 64-bit eG manager process on the other hand, is limited to 3 GB.

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 overrding 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.

2.10 Installing the eG Agent

The eG agents are responsible for making periodic measurements of the infrastructure and collecting a variety of statistics. eG agents must be deployed on the eG server as well as on web servers, DNS servers, LDAP servers, application servers, database servers, payment gateways, etc. While the agent that executes on the eG server is an external agent, the agents executing on the other servers are internal agents. The installation and configuration of the external and internal agents is similar. The main difference between these agents is in the nature of tests that these agents execute.

Internal agents are not required for network devices such as routers, load balancers, etc. which are monitored using the Simple Network Management Protocol (SNMP). The eG external agent is capable of monitoring routers, load balancers, and other network devices.

2.10.1.1 System Requirements

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.

2.10.2 Installing an Agent on Solaris

The eG agent software for Solaris is provided as a standard **Solaris** package called **eGagent**. To install the agent, follow the steps below:

1. 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.

2. The list of packages available are displayed next as shown below:

```
The following packages are available:
  1  eGagent     eG Agent
                 (Sparc/AMD64) version 6.0
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.

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

3. 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**".

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.

```
Enter the directory where the eG Agent should be installed [/opt]:
```

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

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.

4.
```
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.

   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.
```

5. 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
```

6. 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.
```

2.10.3 Installing an Agent on Linux

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**. The steps involved in installing an agent on these platforms are:

1. To start the installation process, 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.

2. 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.

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

   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.

4. Enter the directory in which the eG agent should be installed [/opt]:

   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**.

5.
   ```
   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.

6. 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
   ```

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. 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.
************************************************************
```

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.
- A license is not required for installing an eG agent. However, the licensing terms of the eG manager should support the number of agents being deployed.

2.10.4 Installing an Agent on AIX

The standard eG agent software for **AIX** has been provided as a tar file named **eGagent_aix.tar**. An accompanying script called **iAgent_aix** drives the installation process for the agent. The steps involved in installing this agent are as follows:

1. To start the installation process, execute the **iAgent_aix** script, with the **eGagent_aix.tar** file located in the same directory as **iAgent_aix**.

Note

The agent installation must be performed from a super-user account.

2. 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**". 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.

```
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]:
```

3. Enter the directory in which the eG agent should be installed [/opt]:

Next enter the path to the directory in which the eG agent will reside. The default base directory for eG

Enterprise 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**.

4. `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.

5. 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.

```
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
```

6. The following message will be displayed upon successful installation of the agent.

```
**********************************************************************************
The eG agent has been successfully installed!
Please login as ‘egurkha’ and run the script
          /opt/egurkha/bin/setup_agent to configure the agent.
**********************************************************************************
```

2.10.5 Installing an eG Agent on HP-UX

2.10.5.1 System Requirements

For the eG agent to function effectively, the system on which the agent is being installed should have the following:

- HP-UX 11 or higher
- 64 MB RAM and 50 MB of disk space

2.10.5.2 The Installation Process

The standard eG agent software for **Hpux** is provided as a depot file by name **eGAgent_hpux.depot.** An accompanying script called **iAgent_hpux** drives the installation process for the agent.

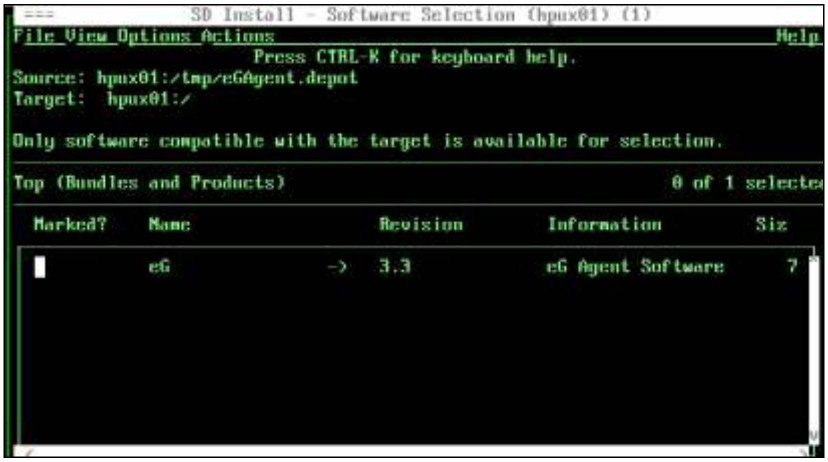
The steps involved in installing an agent on HP-UX are:

1. Execute the **`iAgent_hpux`** script from the super-user account.

```
# ./iAgent

05/22/02 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.
```

```
 05/22/02 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...
```

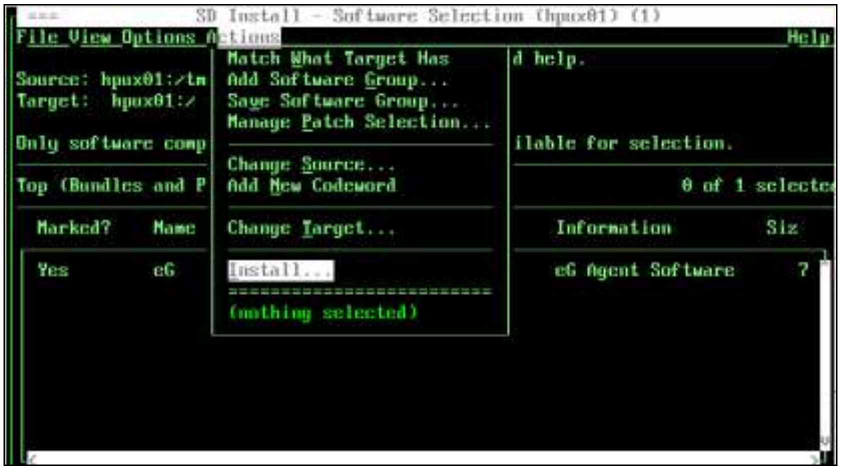
2. On pressing Enter, the screen depicted by Figure 2.6 appears:



```
===              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 2.14: The swinstall terminal interface

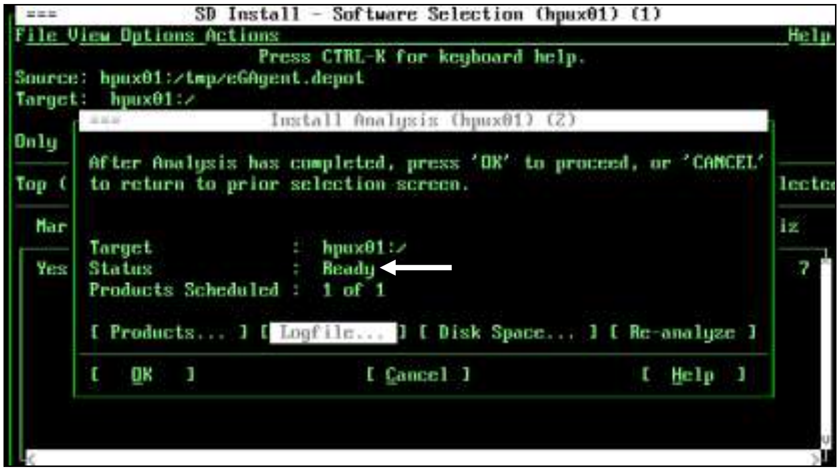
3. Highlight the software using the spacebar and mark the software by pressing **m**. Then, using the tab key, move to the menu bar on top and select **Install** from the **Actions** menu as depicted by Figure 2.15 below. This will begin the install analysis process.



```
===                SD Install - Software Selection (hpux01) (1)
Source: hpux01:/tm                                 d help.
Target:  hpux01:/

Only software comp                                 ilable for selection.

Top (Bundles and P                                          0 of 1 selecte

  Marked?     Name                                    Information        Siz

  Yes         eG                                      eG Agent Software    ?
```

Figure 2.15: Commencing the install analysis process

4. The screen that displays the status of the install analysis will then appear (see Figure 2.16):

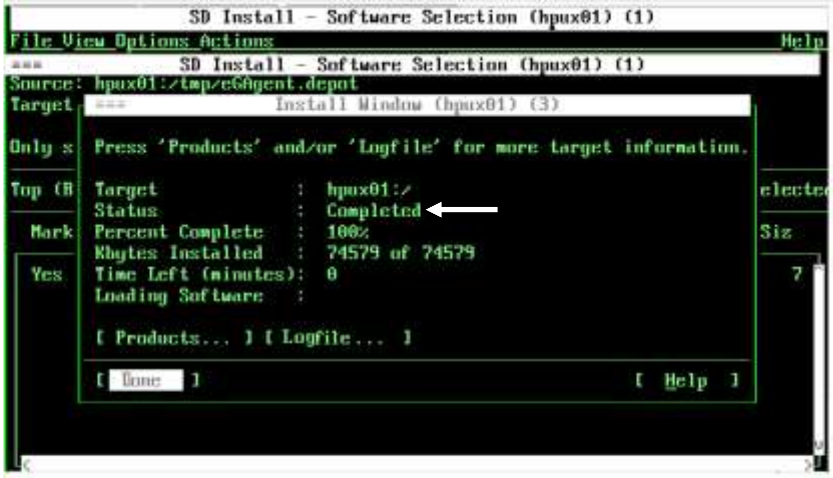


```
===                SD Install - Software Selection (hpux01) (1)
                        Press CTRL-K for keyboard help.
Source: hpux01:/tmp/eGAgent.depot
Target:  hpux01:/
       ===              Install Analysis (hpux01) (2)

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

        Target              :  hpux01:/
        Status              :  Ready
        Products Scheduled  :  1 of 1
```

File View Options Actions
Help
[Products...] [Logfile...] [Disk Space...] [Re-analyze]
[OK]
[Cancel]
[Help]

Figure 2.16: A screen displaying the status of the install analysis process

5. Once the status changes to **Ready**, press Enter to bring up the screen depicted by Figure 2.17:



```
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 2.17: Completing the install analysis process

6. Once the status becomes **Completed**, press **Done.**

7. Now, press **Tab** and choose File -> Exit to exit.

8. The install process will then prompt you to specify the name of the eG user.

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

9. 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]:
```

10. 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]:
```

11.

```
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.

12. 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.
*****************************************************
```

2.10.6 Installing an eG Agent on an HP-UX Server Running an Itanium Processor

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. The steps involved in installing an agent on such a host are discussed hereunder:

1. 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.

2. 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.

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

   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.

4.
   ```
   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.

5. 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
   ```

6. 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.

7. 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.
************************************************************
```

Note

A license is not required for installing an eG agent. However, the licensing terms of the eG manager should support the number of agents being deployed.

2.10.7 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!
```

2.11 Configuring the eG Agent

After the installation, an agent needs to be configured on the server on which it is installed. 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 Solaris and Linux 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. 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 Section 2.12 of this document 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.

6. 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.

7. The next step involves configuration of any Coldfusion application servers for monitoring by the eG agent.

   ```
   Do you want to configure any Coldfusion servers running on <the host> for
   monitoring by the eG Agent? y/n [y]
   ```

   The steps involved in this process are enumerated in Section 2.19.

8. Next, the setup will request your confirmation to configure any Sybase Adaptive servers for monitoring by the

eG agent.

```
Do you want to configure any Sybase Adaptive servers running on <the host> for
monitoring by the eG Agent? y/n [y]
```

The steps involved in this process are enumerated in the *Configuring and Monitoring Database Servers* document.

9. If you are configuring an agent on a Solaris host, then you would be prompted to configure the web server executing on the host. Enter **y** to invoke the **setup_webadapter** script; this script enables you to configure a web adapter on the Solaris host for monitoring the transactions to the web server on it. If you do not want to monitor a web server, then enter **n** here.

```
Do you want to configure any web servers running on sun08 for monitoring by the eG
Agent? y/n [n] :
```

10. In case of Linux agents, the configuration process terminates after the Coldfusion server and Sybase adaptive server configurations have been completed. If at a later stage, the user desires to configure any Coldfusion servers for monitoring by the eG agent, the user need not start the configuration process all over again. Instead, to configure a Coldfusion server, use the command **/opt/egurkha/bin/setup_cf***.* Similarly, for configuring a Sybase Adaptive server, use the command **/opt/egurkha/bin/setup_sybase.sh**. Upon successful termination of the agent setup process, the following message is displayed:

```
***********************************************************************************************
To configure any application at a later time for monitoring by the eG agent,
please follow the steps below:
 - Database Servers: Configure database servers for monitoring by
                     the eG agent through the eG user interface.

 - Coldfusion Servers: To configure a Coldfusion server for monitoring,
                       please have the Coldfusion server's
                       administrator execute the script
                                  /opt/egurkha/bin/setup_cf.

- Sybase Adaptive Servers: To configure a Sybase Adaptive server for
                          monitoring, please have the Sybase server's
                       administrator execute the script
                       /opt/egurkha/bin/setup_sybase.sh

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
***********************************************************************************************
```

In case of Solaris agents, if you have chosen to configure a ColdFusion server, Sybase server, and a web server for monitoring, then agent configuration ends only when all the three components are properly configured. You can however, configure each of these servers at a later point of time also, without reconfiguring the agent. To configure a Coldfusion server, use the command **/opt/egurkha/bin/setup_cf***.* Similarly, for configuring a Sybase Adaptive server, use the command **/opt/egurkha/bin/setup_sybase.sh**. To configure the iPlanet/SunONE web server on the agent host, then configure the web adapter using the command **/opt/egurkha/bin/setup_webadapter**.

```
To configure different applications at a later time
 for monitoring by eG, please follow the steps below:
```

```
 - Database Servers: Configure database servers for monitoring by
                     the eG Agent through the eG user interface.

 - Web Servers:      To configure any web servers running on sun08
                     for monitoring by the eG Agent, please have each of
                     the web server's administrators execute the script
                                /opt/egurkha/bin/setup_webadapter
                     This script will augment the web server's startup
                     files with eG monitoring capability.

 - Coldfusion Servers: To configure a Coldfusion server for monitoring,
                       please have the Coldfusion server's administrator
                       execute the script
                                  /opt/egurkha/bin/setup_cf.

 - Sybase Adaptive Servers: To configure a Sybase Adaptive server
                      for monitoring,please have the Sybase server's
                      administrator execute the script
                            /opt/egurkha/bin/setup_sybase.sh

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
```

2.12 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.

2.12.1 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 3.4.1.1 or 3.4.2.1 of this document).** 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 3.4.1.1 or 3.4.2.1 of this document).** 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 3.4.1.1 or 3.4.2.1 of this document)**.

- **-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.

2.12.2 Importing the SSL Certificate into the JRE of the eG Agent

To achieve this, do the following:

1. Open the Shell prompt and set the path:

   PATH = /opt/egurkha/jre/bin:$PATH

2. 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 3.4.1.1 or 3.4.2.1 of this document, 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:

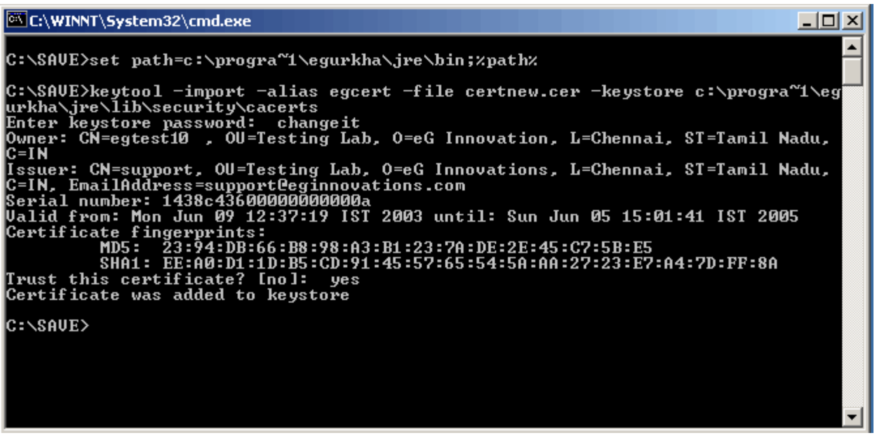
     keytool –list –v –keystore egmanager.bin

     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 **Section 3.13.1**

- **-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 3.4.1.1 or 3.4.2.1 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 3.4.1.1 or 3.4.2.1, as the case may be)**. For the default certificate bundled with the eG manager, the password should be *eginnovations.*

3. Finally, the command will request your confirmation to make the imported certificate a trusted one. Enter **yes** to trust the certificate.
4. If the processing was successful, then a message stating that the *"Certificate was added to keystore"* will appear. Figure 2.18 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 2.18: The process of importing and trusting the manager certificate

5. Now, start the agent. 0.

2.13 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.

This document discusses how to install an agent on Unix hosts in the silent mode.

2.13.1 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 Section 2.7.3 of the *eG Installation Guide*. 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

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 make sure that you create this user account on the target host soon after you save all the changes to the **silent_install** script.

b. **eGgroup**: Specify the group to which the eG user belongs.

c. **eGInstallDir**: Specify the location on the target host in which the agent is to be installed.

d. **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.

e. **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.

f. **eGManager**: Specify the IP address of the eG manager to which the agent should report.

g. **eGManagerPort**: Specify the port at which the eG manager listens.

h. **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**.

i. **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.

j. **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.

k. **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.**

l. **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**.

m. **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**.

n. **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**.

o. **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.

p. **setNickName**: If you want to set a nick name for the agent, set this flag to **y**. If not, set this flag to **n**.

q. **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 *eG Installation Guide*.

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.

2.13.2 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 Section 2.7.2 of the *eG Installation Guide*. 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 Section 1.1 of 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.

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.

2.13.3 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 Section 2.7.4 of the *eG Installation Guide*. 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 1.1 above.

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.

2.13.4 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 2.7.5 of the *eG Installation Guide*. 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 1.1 of 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.

2.13.5 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 2.6.6 of the *eG Installation Guide*. 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 1.1 of 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_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.

2.14 Dealing with Operating System Variations

The eG Enterprise Suite uses the Sun Microsystems Java 2 Enterprise Edition as the core platform on which it operates. Typically, the Java Runtime Environment (JRE) version 1.6 and 1.7 are bundled as part of the eG agent installable for Linux (32-bit and 64-bit). To ensure backward compatibility with older versions of Linux that may not support JRE 1.7, JRE 1.6 is set as the default. This means that if the Linux kernel on which the agent is installed supports JRE 1.7, then the agent will use JRE 1.7 that it is bundled with. On the other hand, if the Linux kernel does not support JRE 1.7, then the eG agent uses JRE 1.6 only.

The eG agent for Solaris (AMD/SPARC) environments is bundled with JRE 1.5 and 1.7, with JRE 1.5 being the default.

On the other hand, the eG agent for AIX and HPUX is bundled with JRE 1.6 only.

The eG agent for Windows 2008/Windows 7/Windows 8/Windows 10/Windows 2012 (32-bit and 64-bit) environments on the other hand is bundled with JRE 1.7.

The table below discusses this clearly.

eG Agent	JRE 1.5	JRE 1.6 (32-bit/64-bit)	JRE 1.7 (32-bit/64-bit)
Linux (32-bit)		**✓(default)**	✓
Linux (64-bit)		**✓(default)**	✓
Solaris (Sparc/AMD)	**✓ (default)**		✓
AIX		✓	
HPUX (PA-RISC/Itanium)		✓	
Windows 2008/7/8/ 10/2012 (32-bit/64-bit)			✓

This section discusses how to handle the operating system and related JRE variations while installing an eG agent.

2.14.1 Deploying the eG Agent on Solaris Environments

- **SPARC/Solaris:** To deploy the eG agent on a Solaris host running a SPARC processor, use the standard **Solaris** agent package. The procedure for deployment has been discussed in Section 2.10.2 of this manual.
- **AMD 64-bit/Solaris:** To monitor a 64-bit host running the AMD processor, use the **Solaris64-AMD** agent package. The steps for deploying this eG agent package are the same as that for the standard package, and have been discussed elaborately in Section 2.10.2 of this manual.

The JRE bundled with the eG agent supports both 32-bit and 64-bit. By default however, the eG agent runs the 32-bit JRE only. For additional memory, you may want to configure the eG agent on a 64-bit Solaris host to use the 64-bit JRE, instead of the 32-bit JRE. For this, follow the steps below:

1. Login to the eG agent host.
2. Edit the **starta** file in the **/opt/egurkha/bin** directory.
3. Look for the line that begins with *nohup java*.
4. In that line, next to *nohup java*, insert *-d64.*
5. The line will now look as follows:

   nohup java -d64 -client -Xrs -Deg.name=EgMainAgent -Deg.logback.configurationFile=/opt/egurkha/lib/eg_logback.xml $XMX -Dsun.net.inetaddr.ttl=900 EgMainAgent $ > /dev/null 2>&1 &*
6. Save the file.
7. Restart the agent.

8. To verify whether the eG agent is using the 32-bit or the 64-bit JRE, do the following:

    - Login to the agent host as the *eG install user*.
    - From the prompt, run the following command:

      ps -aef | grep 'java'

    - If the eG agent is using the 64-bit JRE, then, on a Solaris SPARC host, the aforesaid command will return an output that contains the string **sparcv9** (as highlighted in the sample output below).

      ```
      eguser 11237     1  14 07:00:09 pts/1       1:08
      /opt/egurkha/jre/bin/sparcv9/java -client -Xrs -Deg.name=EgMainAgent -
      Deg.logba
      eguser 11292 10799   0 07:00:57 pts/1       0:00 grep java
      ```

      On a Solaris AMD host on the other hand, if the command output includes the string **amd64**, then it means that the eG agent on that host is using the 64-bit JRE.

    - If the eG agent is using the 32-bit JRE instead, the aforesaid command will return the following output (both on SPARC and AMD):

      ```
      eguser 27234     1   0 17:26:54 pts/2      21:22 java -client -Xrs -
      Deg.name=EgMainAgent -Deg.logback.configurationFile=/opt/egu
        eguser 10834 10799   0 06:57:37 pts/1       0:00 grep java
      ```

2.14.2 Deploying the eG Agent on Linux Environments

- **32-bit Agent:** The standard eG agent software for 32-bit Linux hosts is provided as a tar file named **eGagent_linux.tar**. An accompanying, **iAgent_linux** script, drives the installation process. The procedure for deployment has been discussed in Section 2.10.2 of this manual.
- **64-bit Agent:** To monitor a 64-bit Linux host, use the **eGagent_linux_x64** agent package. An accompanying, **iAgent_linux_x64** script, drives the installation process. The procedure for deployment has been discussed in Section 2.10.2 of this manual.

Note

To install the eG agent on 32-bit/64-bit Tru64/FreeBSD/CentOS/openSUSE operating systems, you will have to use the corresponding **Linux** package, and follow the installation procedure discussed in Section 2.10.3 of this document.

2.14.3 Deploying the eG Agent on HPUX Environments

- **PA-RISC/HPUX:** To deploy the eG agent on an HPUX host running a **PA-RISC** processor, use the standard **Hpux** agent package.
- **Itanium/HPUX:** To monitor an HPUX host running an Itanium processor, use the **Hpux_Itanium** agent package.

The install procedures for both the above-mentioned options are available in Section 2.10.5 and Section 2.10.6 (respectively) of this manual.

2.14.4 Deploying the eG Agent on AIX Environments

To deploy an eG agent on AIX, use the standard **AIX** agent package. The procedure for deployment has been explained clearly in Section 2.10.4 of this document.

2.15 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

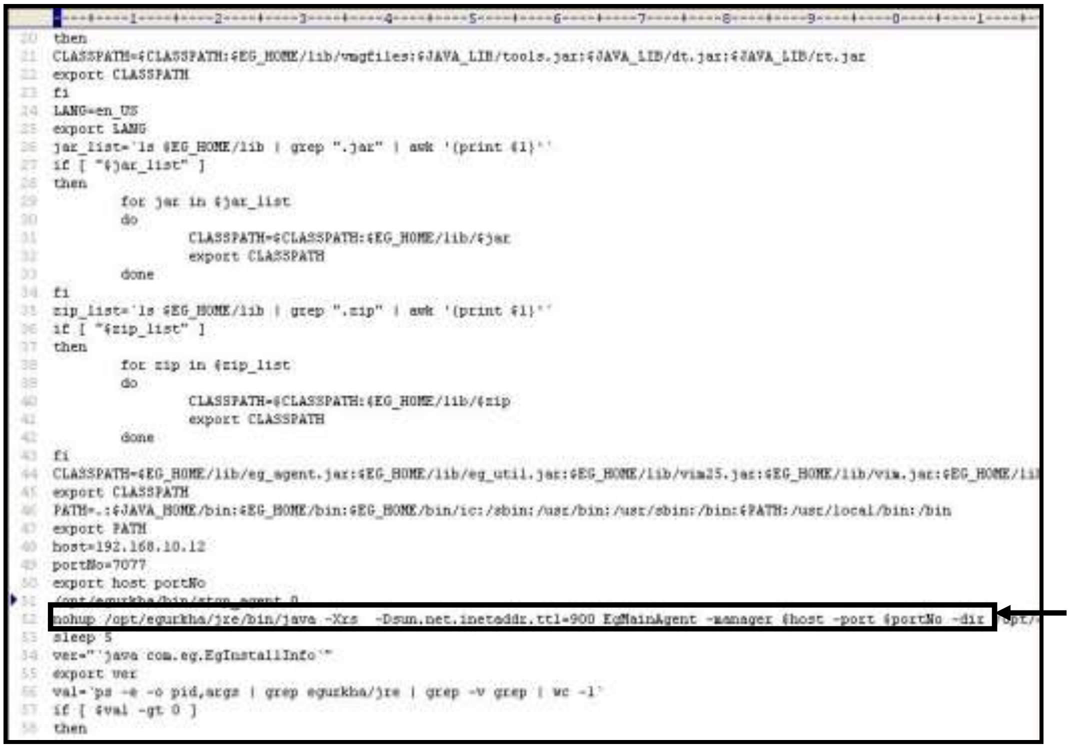
The following processes will run when the agent starts:

- 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 the *eG User Manual*) 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 2.19).



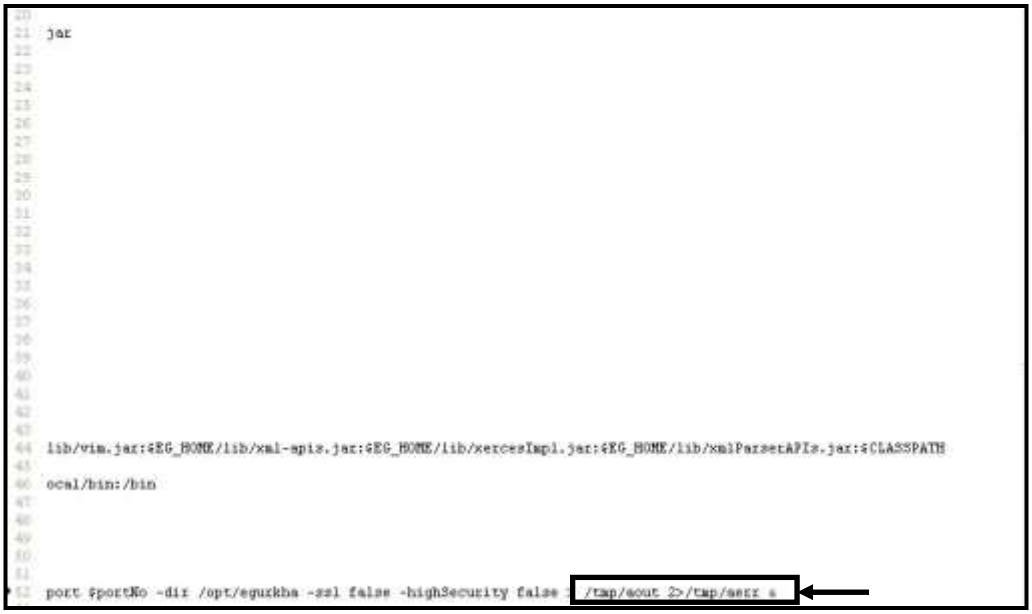
```
then
CLASSPATH=$CLASSPATH:$EG_HOME/lib/vmgfiles:$JAVA_LIB/tools.jar:$JAVA_LIB/dt.jar:$JAVA_LIB/rt.jar
export CLASSPATH
fi
LANG=en_US
export LANG
jar_list=`ls $EG_HOME/lib | grep ".jar" | awk '{print $1}'`
if [ "$jar_list" ]
then
        for jar in $jar_list
        do
                CLASSPATH=$CLASSPATH:$EG_HOME/lib/$jar
                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 2.19: The start_agent script

3. At the end of the line indicated by Figure 2.19, 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 2.20). Similarly, to enable error logging, replace the second occurrence of **/dev/null** with the full path to the error log file (see Figure 2.20).



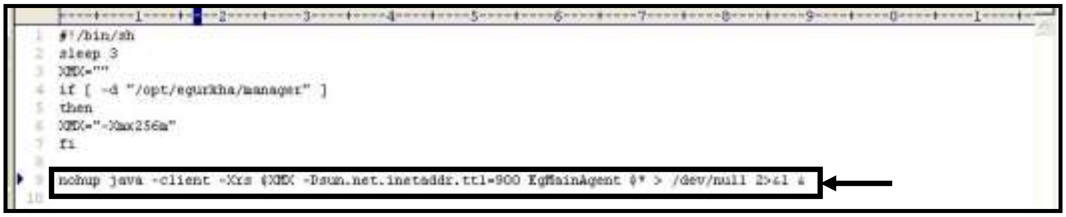
```
jar

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 2.20: The edited start_agent script

6. Finally, save the **start_agent** script.
7. Restart the agent. 0.

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:

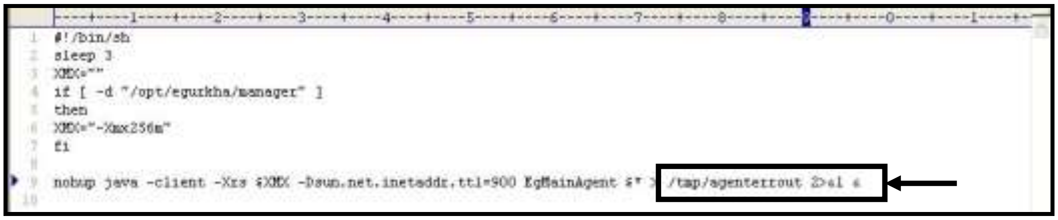
1. Open the **starta** file.
2. Edit the line that begins with **nohup java –client -Xrs . . .** (see Figure 2.21).



```
#!/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 2.21: The starta script

3. At the end of the line indicated by Figure 2.21, 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 2.22).



```
#!/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 2.22: The edited starta script

6. Finally, save the **starta** script.
7. Restart the agent. 0.

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.

2.16 Performance Impact of the eG Agent

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 100 MB. 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.

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.

2.17 Increasing the Memory of the eG Agent

The eG agent runs as a Java process. The maximum heap memory that can be allocated to a 32-bit eG agent process is limited to 1.5 GB. The maximum heap memory allocation to a 64-bit eG agent process on the other hand, is limited to 3 GB. 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 256 MB of memory to the eG agent, your *–Xmx* specification should be as follows:

-Xmx256M

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.

2.18 The eG Web Adapter

eG Enterprise's unique web adapter technology enables individual transactions performed by users of a web site to be tracked in real-time.

In the sections that follow, we will be discussing how to configure the eG web adapter for different web servers.

2.18.1 Configuring the eG Web Adapter for an iPlanet/SunONE Web Server (before Version 6.0)

The web adapter is part of the eG agent package for Solaris. When the agent on Solaris is configured, it is enabled to communicate with the web adapter to report statistics in real-time to the eG manager.

For configuring the eG web adapter for an iPlanet/SunONE web server (before version 6.0), you can use the **setup_webadapter** script in the **/opt/egurkha/bin** directory. The steps involved in configuring the iPlanet/SunONE web server to use the web adapter technology are:

Note

A user can install the eG web adapter capability only for the web servers that he/she has the permission to administer.

1. First, run the command on the iPlanet / SunONE web server host:

   /opt/egurkha/bin/setup_webadapter

   The **setup_agent** script on Solaris executes this command automatically. Hence, if you get here from step 9 of Section 2.11 above, you do not have to explicitly run this command.

2. Upon executing the above command, the following message will appear. Type **n** to continue with the setup.

```
Only a SunONE/iPlanet web server can be configured for monitoring using this
script.

For monitoring an Apache or IBM web server, please refer to the eG Installation
Manual.

Do you want to continue  y/n? [y]: y
```

3. Upon confirming, you will view the following message. Type **y** here to continue.

```
Note: Only a web server administrator has permissions to configure the eG web
adapter capability for a web server.

Do you want to continue  y/n? [y]: y
```

4. Next, setup will want to know whether the current user is the web server's administrator or not.

```
Are you the administrator of this web server? y/n [y]:
```

Entering **y** or **n** here will bring up the following query:

```
Please enter the user name of the web server's administrator:

Next, you will need to enter the web server administrator's password...

Password:
```

5. Next, enter the root directory of the web server to be configured. Also, indicate whether the web server is SSL-enabled.

```
Enter the root directory of the SunONE / iPlanet web server: /usr/local/web
Is this web server enabled for SSL support? y/n [n]:
```

6. Based on the server type and the root directory, the **setup_webadapter** script proceeds to modify the web server startup scripts to use the eG web adapter when the web server starts up.

7. Then the user has to specify whether this web server is enabled for SSL support. If the user chooses **y**, the setup process configures the web adapter for SSL support. The following error message appears if the web server is not configured with Dynamic Shared Object (DSO) support.

```
*****************************************************************
This web server has not been configured with DSO support ...
The eG SSL enabled web adapter cannot be installed.
Please reconfigure this web server with DSO support and
run the command /opt/egurkha/bin/setup_webadapter to
configure the web server with eG agent's web adapter capability
*****************************************************************
```

8. Next, the configuration process prompts the user to determine if the user is the administrator of the web server that is to be configured for monitoring by an eG agent. If the user is not the web server administrator, the configuration process prompts the user for the web server administrator's login name and password.

9. The configuration process attempts to update the web server's startup file(s) to include eG-specific start-up information. The configuration process terminates with the following message:

```
*****************************************************************
If there are any errors in the above process, you may not have
permission to update the web server's configuration.
Please have the web server's administrator run the command
   /opt/egurkha/bin/setup_webadapter
If there were no errors, the web adapter has been successfully configured. For the
web adapter to be effective, please restart the configured web server.
*****************************************************************
```

10. In the case of an iPlanet web server (prior to version 6.0), the **start** and **stop** files are modified after retaining a copy of them called **start.pre_egurkha** and **stop.pre_egurkha**. To uninstall the web adapter capability, replace

the existing **start** and **stop** files with **start.pre_egurkha** and **stop.pre_egurkha** respectively.

2.18.2 Configuring the eG Web Adapter for a SunONE Web Server Version 6.x on Solaris

To configure the eG web adapter for a SunONE web server version 6.x on Solaris, follow the steps given below:

1. Login as a SunONE install user.
2. Open **magnus.conf** file in the **<SUNONE_INSTALL_DIR>/<SERVER_NAME>/config/** directory. For instance, if the SunONE web server is installed in the directory **/opt/SUNWwbsvr**, and the name of the server is **https-test**, then the **magnus.conf** file will be in the directory: **/opt/SUNWwbsvr/https-test/config** directory. Append the following lines in the file:

   Init fn="load-modules" shlib="/opt/egurkha/lib/sun1webadapter_6.so" funcs="onServerInit,onChildInit,onLog"
   Init fn="onServerInit" WEB_SERVER_ROOT=<SunONE_install_dir>/<Server_Name>

   For example, if the SunONE web server is installed in the directory **/opt/SUNWwbsvr**, and the name of the server is **https-test**, then you will have to append the following lines in the **magnus.conf** file:

   Init fn="load-modules" shlib="/opt/egurkha/lib/sun1webadapter_6.so" funcs="onServerInit,onChildInit,onLog"
   Init fn="onServerInit" WEB_SERVER_ROOT=/opt/SUNWwbsvr/https-test
3. Save the file.
4. Next, open the **obj.conf** file from the same location, and insert the following line as the last line of the series that begins with the string, *PathCheck fn*:

   PathCheck fn="onChildInit"

   Similarly, insert the following line as the last line of the series that begins with the string, *AddLog fn*:

   AddLog fn="onLog"
5. Save the file.
6. Finally, restart the web server.

The web adapter for an Apache or an IBM HTTP web server, on the other hand, can be configured only manually, and not through the eG agent setup procedure. The steps involved in the manual web adapter configuration process have been detailed hereunder.

2.18.3 Configuring the eG Web Adapter for an Apache/IBM HTTP Web Server on a 32-bit Unix Operating System

To manually configure the eG web adapter on an Apache web server 1.x on Unix, do the following:

1. First, login to the Unix server as the Apache install user.
2. Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following lines to the end of the file:

   LoadModule eg1_module libexec/mod_eg1.so
3. Copy the file **mod_eg1.so** from the **/opt/egurkha/lib** directory to **<APACHE_HOME>/libexec** in the **<APACHE_INSTALL_USER>** directory.
4. Stop and restart the Apache server.

The same procedure applies while configuring the web adapter on an IBM HTTP Server 1.x on Unix.

To configure the web adapter on Apache 1.x on HPUX/AIX servers, the procedure is almost the same as what has been discussed above; however, the only difference is that you will have to append the following lines to the end of the **<APACHE_HOME>/conf/httpd.conf** file:

LoadModule mod_egurkha libexec/mod_egurkha.so

Then, copy *mod_egurkha.so* to the **<APACHE_HOME>/libexec** directory.

To manually configure the eG web adapter on an Apache web server 2.0 on Unix, do the following:

1. First, login to the Unix server as the Apache install user.
2. Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following line:

   LoadModule eg2_module modules/mod_eg2.so
3. Copy the file **mod_eg2.so** from the **/opt/egurkha/lib** directory to **<APACHE_HOME>/modules** under **<APACHE_INSTALL_USER>.**
4. Stop and restart the Apache server.

The same procedure applies for configuring an IBM HTTP Server 2.0 on Unix

Note that you cannot configure the web adapter on Apache web server 2.0 / IBM HTTP Server 2.0 for HPUX.

To manually configure the eG web adapter on an Apache web server 2.2 on Unix, do the following:

1. First, login to the Unix server as the Apache install user.
2. Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following line:

   LoadModule eg2_module modules/mod_eg22.so
3. Copy the file **mod_eg22.so** from the **/opt/egurkha/lib** directory to **<APACHE_HOME>/modules** under **<APACHE_INSTALL_USER>.**
4. Stop and restart the Apache server.

To configure the eG web adapter on Apache 2.2 on HPUX/AIX, follow the same procedure explained above.

To manually configure the eG web adapter on an Apache web server 2.4 on Linux, do the following:

1. First, login to the Unix server as the Apache install user.
2. Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following line:

   LoadModule eg2_module modules/mod_eg24.so
3. Copy the file **mod_eg24.so** from the **/opt/egurkha/lib** directory to **<APACHE_HOME>/modules** under **<APACHE_INSTALL_USER>.**
4. Stop and restart the Apache server.

   To configure the eG web adapter on Apache 2.4 on HPUX/AIX, follow the same procedure explained above.

To manually configure the eG web adapter on an IBM HTTP Server 2.x on AIX, do the following:

1. First, login to the AIX server as the IBM HTTP install user.

2. Edit the **<IBM_HTTP_HOME>/conf/httpd.conf** file to append the following line:

   LoadModule eg2_module modules/mod_ibm_eg2.so

3. Copy the file **mod_ibm_eg2.so** from the **/opt/egurkha/lib** directory to **<IBM_HTTP_HOME>/modules** under **<IBM_HTTP_INSTALL_USER>.**
4. Stop and restart the IBM HTTP server.

To manually configure the eG web adapter on an IBM HTTP Server 6.x on Unix (Linux/Solaris/AIX), do the following:

1. First, login to the Unix server as the IBM HTTP install user.
2. Edit the **<IBM_HTTP_HOME>/conf/httpd.conf** file to append the following line:

   LoadModule eg2_module modules/mod_ibm_eg6.so

3. Copy the file **mod_ibm_eg6.so** from the **/opt/egurkha/lib** directory to **<IBM_HTTP_HOME>/modules** under **<IBM_HTTP_INSTALL_USER>.**
4. Stop and restart the IBM HTTP server.

   Note that the eG web adapter cannot be configured on an IBM HTTP Server 6.x on HPUX.

2.18.4 Configuring the eG Web Adapter for an Apache Web Server on a 64-bit Linux Operating System

To configure the eG web adapter for an Apache web server on a 64-bit Linux host, do the following:

1. The eG agent for the 64-bit Linux host is bundled with the following shared libraries to be used by the eG web adapter, if configured on the host:

   - mod_eg24.so
   - mod_eg22.so
   - mod_eg2.so
   - libeg_reptr_cat.so
   - libeg_reptr_total.so
   - libeg_reptr_site.so

   These files are available in the **/opt/egurkha/lib/lib64** directory on the host.

2. To enable the eG web adapter for Apache 2.0, following the steps given below:

   - First, login to the Linux host as the Apache install user.
   - Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following line:

     LoadModule eg2_module modules/mod_eg2.so

   - Copy the file **mod_eg2.so** from the **/opt/egurkha/lib/lib64** directory to **<APACHE_HOME>/modules** under **<APACHE_INSTALL_USER>**.
   - Copy the **libeg*.so** files from the **/opt/egurkha/lib/lib64** directory to the **/opt/egurkha/lib** directory.
   - Stop and restart the Apache server.

3. To enable the eG web adapter for Apache 2.2, following the steps given below:

   - First, login to the Linux host as the Apache install user.
   - Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following line:

     LoadModule eg2_module modules/mod_eg22.so

   - Copy the file **mod_eg22.so** from the **/opt/egurkha/lib/lib64** directory to **<APACHE_HOME>/modules** under **<APACHE_INSTALL_USER>**.
   - Copy the **libeg*.so** files from the **/opt/egurkha/lib/lib64** directory to the **/opt/egurkha/lib** directory.
   - Restart the eG agent.
   - Stop and restart the Apache server.

4. To enable the eG web adapter for Apache 2.4, following the steps given below:

   - First, login to the Linux host as the Apache install user.
   - Edit the **<APACHE_HOME>/conf/httpd.conf** file to append the following line:

     LoadModule eg2_module modules/mod_eg24.so

   - Copy the file **mod_eg24.so** from the **/opt/egurkha/lib/lib64** directory to **<APACHE_HOME>/modules** under **<APACHE_INSTALL_USER>**.
   - Copy the **libeg*.so** files from the **/opt/egurkha/lib/lib64** directory to the **/opt/egurkha/lib** directory.
   - Stop and restart the Apache server.
   - Start the eG agent.

2.18.5 Configuring the eG Web Adapter for an IBM HTTP Server on a 64-bit Unix Operating System

To manually configure the eG web adapter on a 64 bit IBM HTTP Server 8.x on Unix (Linux/Solaris/AIX), do the following:

1. First, login to the Unix server as the IBM HTTP install user.
2. Edit the **<IBM_HTTP_HOME>/conf/HTTPd.conf** file to append the following line:

   LoadModule eg2_module modules/mod_ibm_eg8.so

3. Copy the file **mod_ibm_eg8.so** from the **/opt/egurkha/lib/lib64** directory to **<IBM_HTTP_HOME>/modules** under **<IBM_HTTP_INSTALL_USER>.**
4. Stop and restart the IBM HTTP server.

Note that the eG web adapter cannot be configured on an IBM HTTP Server 8.x on HPUX.

2.19 Configuring the Coldfusion Server

The eG agent on Unix is bundled with a setup script that enables monitoring of a Coldfusion server that may be running on that host. This is why, when configuring the eG agent on Unix, you can also configure any Coldfusion server that may be running on the agent host for monitoring.

Alternatively, you can configure the Coldfusion server after agent configuration. The steps involved in the process are as follows:

1. Execute the following command

   /opt/egurkha/bin/setup_cf

   The **setup_agent** script executes this command automatically. Hence, if you get here from step 8 of Section 2.10.4, you do not have to explicitly run this command.

2. Then, decide if you want to configure an agent to monitor a Coldfusion server. The default is **y**.

3. Next, the user needs to enter the document root of the web server with which the Coldfusion server is associated.

4. Next, the configuration process prompts the user to determine if the user is the administrator of the web server that is to be used for monitoring by the eG agent. If the user is not the web server administrator, the configuration process prompts the user for the web server administrator's login name and password.

5. The following message comes up upon the termination of the configuration process.

```
*************************************************************
If there were any errors in the above steps, you may not have
permissions to update the files in the web server's document root.
Please have the web server's administrator execute
this script, namely /opt/egurkha/bin/setup_cf  to configure
a Coldfusion server for monitoring by the eG agent.
*************************************************************
```

2.20 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

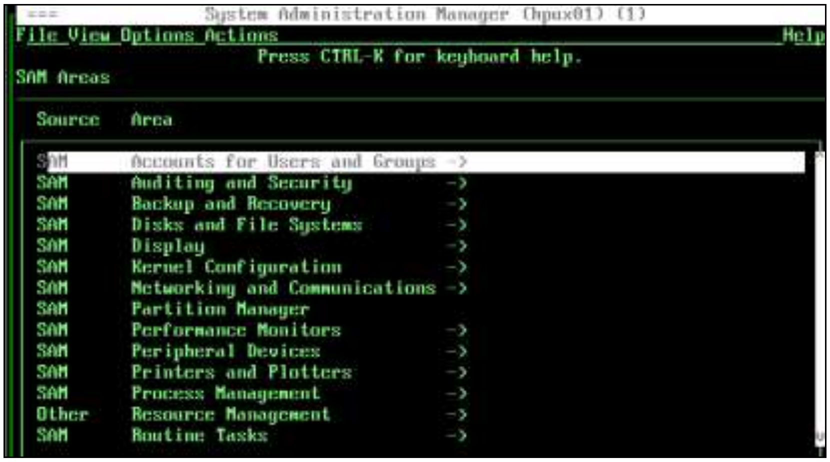
3. Next, on Solaris, use the **pkgrm** command to uninstall the eGmanager and eGagent packages.

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 2.23 below appears next.

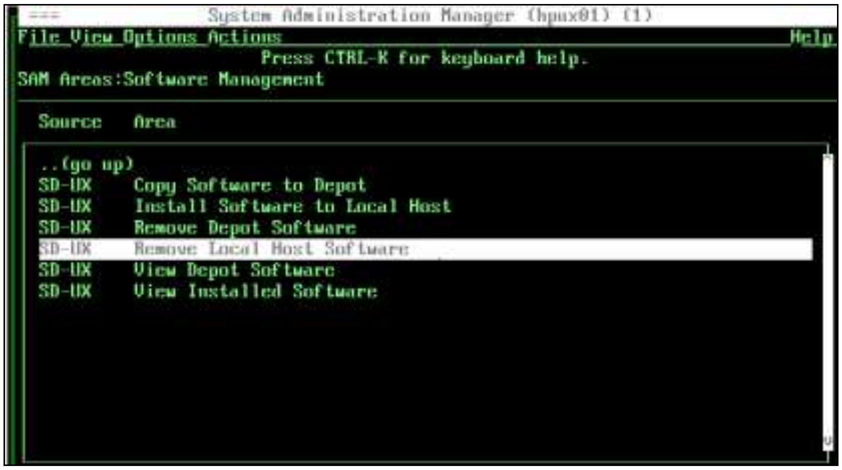


```
 ===              System Administration Manager (hpux01) (1)
File View Options Actions                                        Help
                         Press CTRL-K for keyboard help.
SAM Areas

  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 2.23: Selecting the Software Management option

- Using the down-arrow key on the key board, select the **SD-UX Software Management** option from Figure 2.23, and then press Enter.

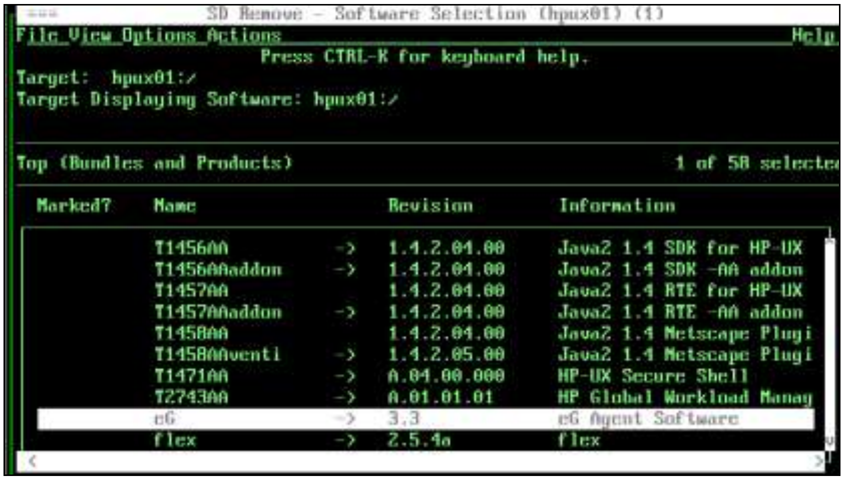
- Using the next screen (see Figure 2.24), choose to remove the eG agent software executing on the local host, by selecting the **Remove Local Host Software** option. To select this option, use the down-arrow key until the option is reached, and then press the Enter key.



```
 ===              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 2.24: Choosing to remove a software on the local host

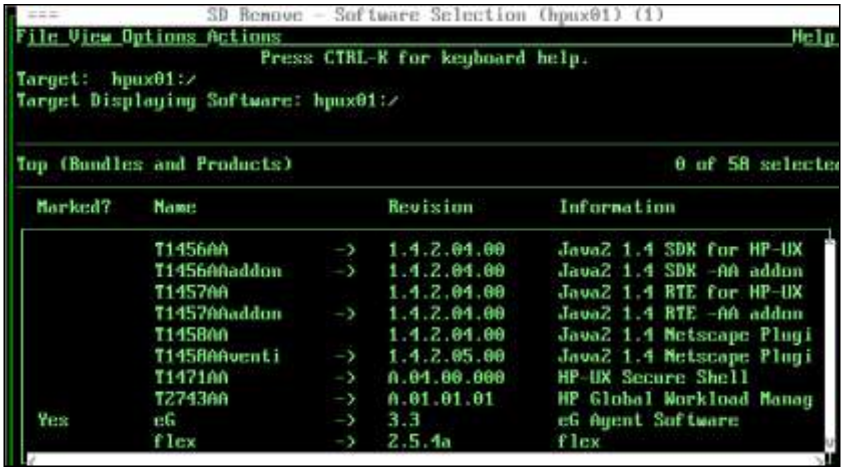
- From the screen that appears next, select the eG Agent software to be removed. To remove the selected eG agent software, first, mark it for removal by pressing the “m” key on the keyboard (see Figure 2.25).



```
===                 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 2.25: Marking the eG agent software for deletion

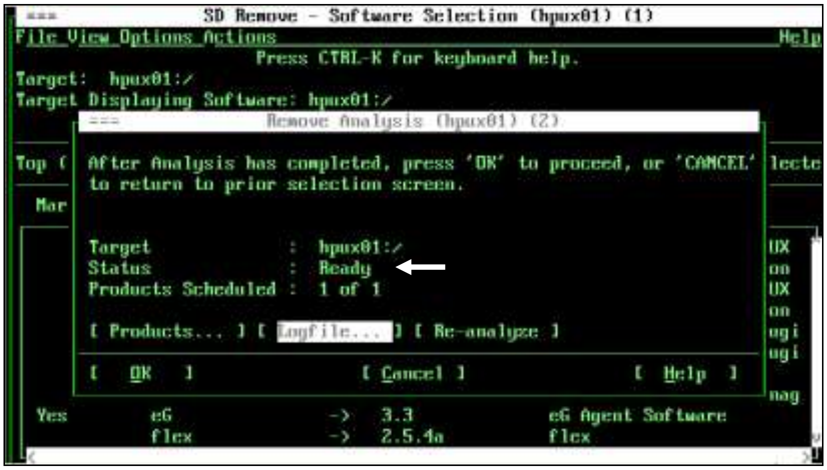
- Then, press the Tab key and choose Actions -> Remove as depicted by Figure 2.26 below.



```
===                 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 2.26: Selecting the Remove option from the Actions menu

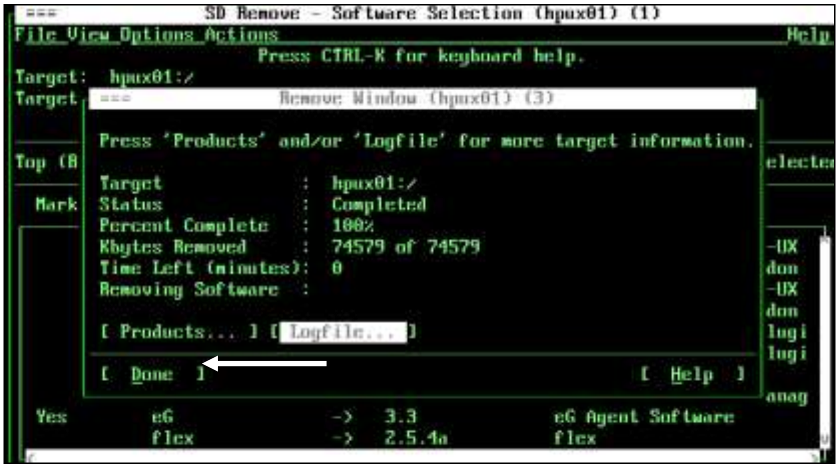
- Then, press the Enter key and wait until the **Status** of the remove analysis changes to **Ready** (see Figure 2.27). Then, using the Tab key, choose the **OK** button to confirm deletion of the selected eG software.



```
===                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 2.27: Confirming removal of the eG software by selecting the OK button

- Once the software is removed, status will become **Completed** (see Figure 2.28). 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 (A                                                                  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... ]                                 logi
                                                                       logi
        [  Done  ]                                       [ Help ]
                                                                       anag
 Yes        eG              ->   3.3            eG Agent Software
            flex            ->   2.5.4a         flex
```

Figure 2.28: 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

Installing and Configuring on Windows Environments

This chapter describes the steps involved in installing and configuring eG Enterprise on Windows 2003/2008/2012 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 the first chapter.

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.

3.1 Installing and Configuring the Manager

3.1.1 Pre-requisites for Installation

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

- JDK 1.7 (or its variants)

Note

JDK 1.8 is not supported.

- Windows 2008 server (OR) Windows 7 (OR) Windows 8 (OR) Windows 2012 (OR) Windows 10 (OR) Windows 2016
- Only systems with a static IP address (i.e. no DHCP address) should be used for installing the eG manager

- A minimum of 1 GB disk space
- Oracle database server (version 10G / 11G / 12c) / Microsoft SQL Server (version 2008 / 2012 / 2014) for the eG database. The database can be installed on the same system as the eG manager, or it can be installed on a separate system. 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.
- Internet Explorer 10, 11, or Edge, Mozilla Firefox v18 or higher, or Chrome v28 or above as the browser
- 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.

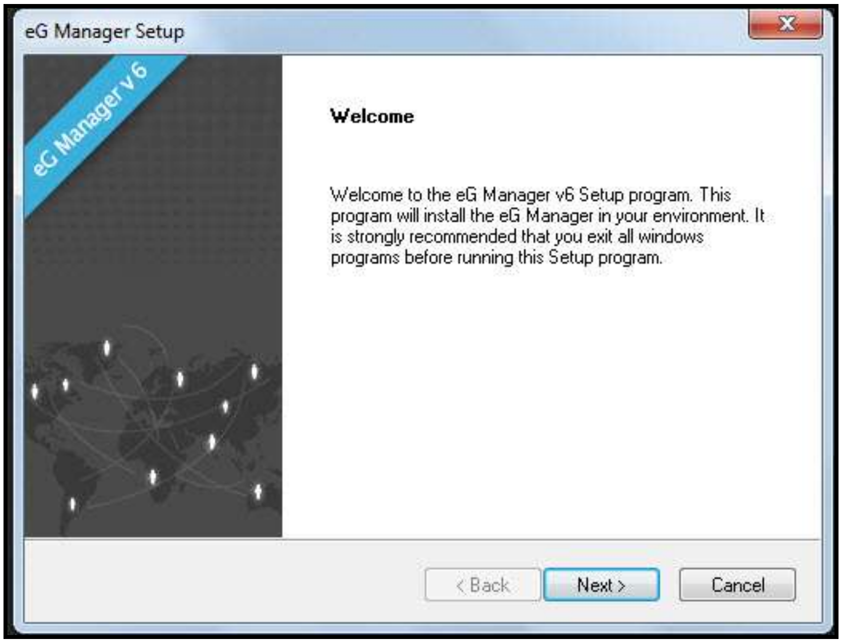
3.1.2 Installing and Configuring the eG Manager on Windows Platforms

To install the eG manager on a Windows platforms, you have to choose from the following self-extracting programs:

- The **eGManager_win2008.exe**, if you are installing the eG manager on a 32-bit Windows 2008/Windows 7 host;
- The **eGManager_win2008_x64.exe**, if you are installing the eG manager on a 64-bit Windows 2008/Windows 7 host;
- The **eGManager_win2012.exe**, if you are installing the eG manager on a 32-bit Windows 8/Windows 2012/ Windows 10 host;
- The **eGManager_win2012_x64.exe**, if you are installing the eG manager on a 64-bit Windows 8/Windows 2012/ Windows 10 host;
- The **eGManager_win2016_x64.exe**, if you are installing the eG manager on a Windows 2016 (64-bit) host;

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.



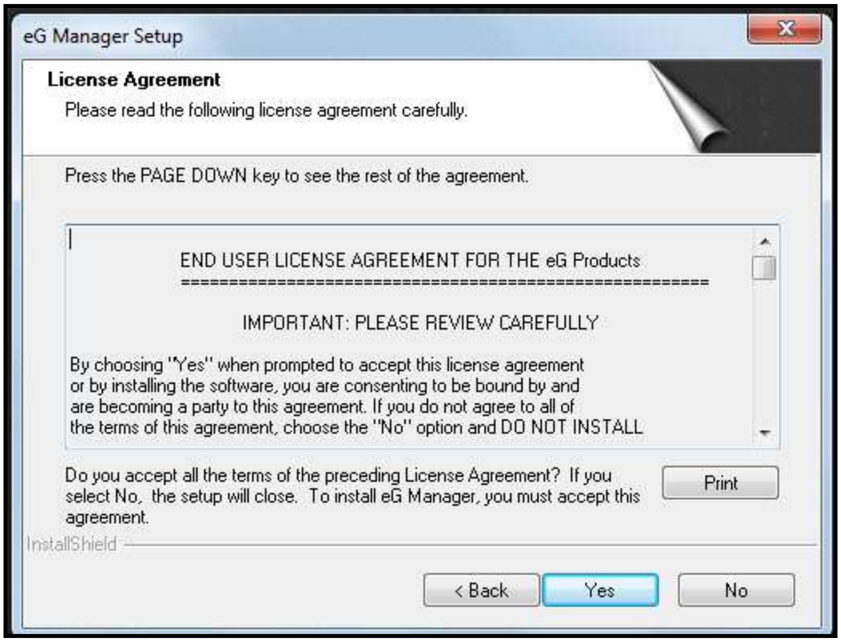
eG Manager Setup

Welcome

Welcome to the eG Manager v6 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 3.1: The Welcome screen of the installation wizard

2. Accept the license agreement that follows by clicking the **Yes** button therein (see Figure 3.2).



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

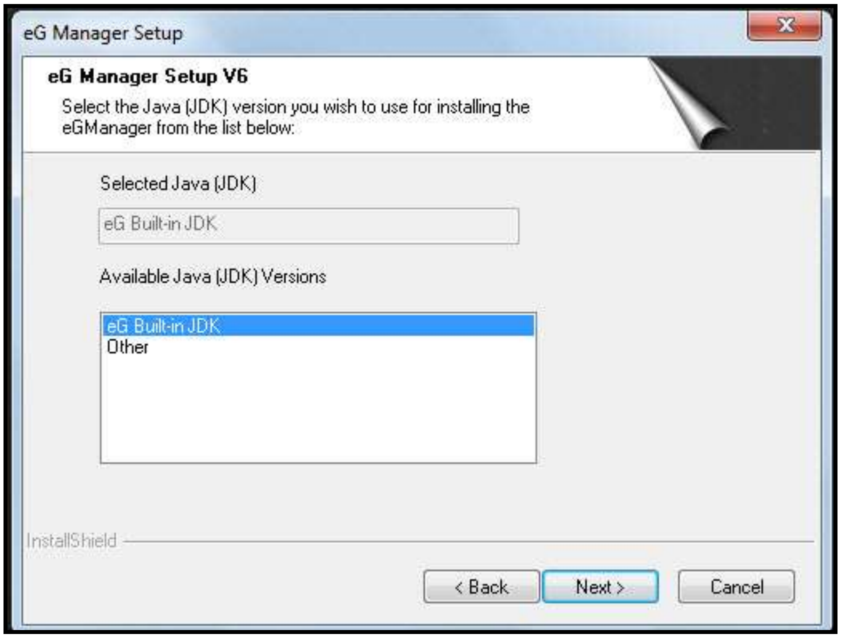
By choosing "Yes" when prompted to accept this license agreement or by installing the software, you are consenting to be bound by and are becoming a party to this agreement. If you do not agree to all of the terms of this agreement, choose the "No" option and DO NOT INSTALL

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 3.2: Accepting the license agreement for installing the eG manager

3. Setup then automatically discovers all the versions of JDK available on the target host, and lists them as depicted by Figure 3.3. The user will have to simply select the JDK version he/she wants to use for their eG manager installation from the displayed list. **It is recommended that you use JDK 1.7.0_79 (or its variants) for**

installing the eG manager.



eG Manager Setup

eG Manager Setup V6

Select the Java (JDK) version you wish to use for installing the eGManager from the list below:

Selected Java (JDK)

eG Built-in JDK

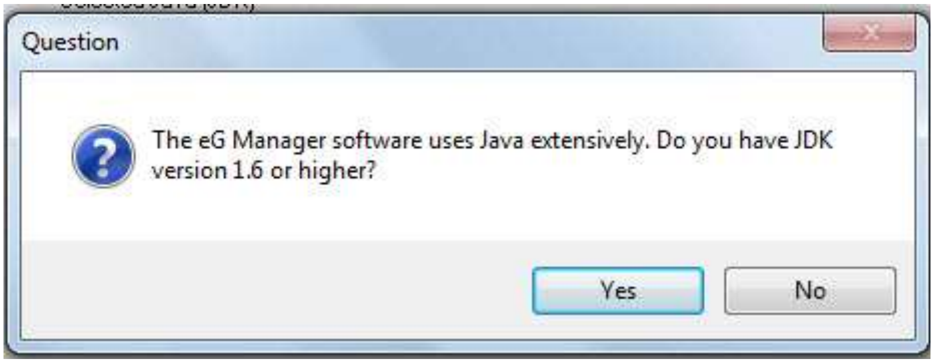
Available Java (JDK) Versions

eG Built-in JDK
Other

Figure 3.3: Selecting a JDK version to use for manager installation

4. Upon selecting a JDK version, eG Enterprise automatically determines the location of the JDK-related files on the target host, and uses them to configure the eG user's Java execution environment to execute Java programs to proceed with the installation. Clicking on the **Next** button in Figure 3.3 will then lead the user straight to step 8 of the setup process.

5. On the other hand, if the JDK version the user wishes to use is not listed in Figure 3.3 for some reason, he/she can pick the **Other** option from Figure 3.3. Figure 3.3 then appears, where the user is prompted to specify if his/her environment contains the required JDK (see Figure 3.3). **It is recommended that you use JDK 1.6 (or its variants) for installing the eG manager.**



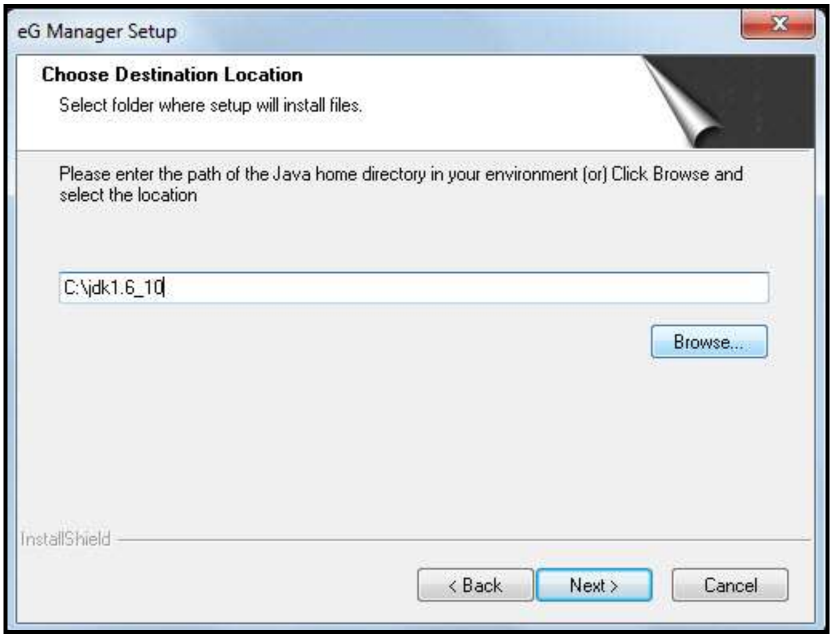
Question

The eG Manager software uses Java extensively. Do you have JDK version 1.6 or higher?

Figure 3.4: Setup enquiring the availability of JDK in the environment

6. If JDK is already available in the environment, specify the Java home directory to enable the setup process to

configure the eG user's execution environment to execute Java programs as in Figure 3.5. The user can also use the **Browse** button to select the location of the Java home directory.



eG Manager Setup

Choose Destination Location

Select folder where setup will install files.

Please enter the path of the Java home directory in your environment (or) Click Browse and select the location

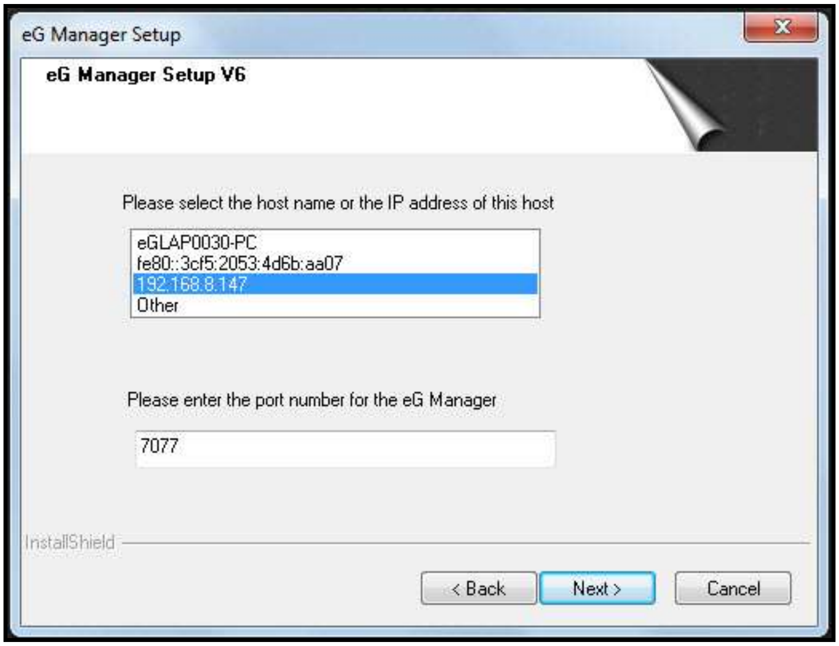
C:\jdk1.6_10

Figure 3.5: Specifying the location of the Java home directory for installing the eG manager

Note

If the message box of Figure 3.4 appears even after you have specified/selected JDK 1.6 or higher, then check whether the **<JDK_INSTALL_DR>\bin** directory on the eG manager host is a *Read-only* directory. If so, grant *Read-Write* permissions to that directory, and then proceed with the eG manager installation.

7. The setup process now requires the hostname and port number of the host on which the eG manager is being configured (see Figure 3.7). 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 Figure 3.7. 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 Figure 3.8. This will invoke Figure 3.8 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.


eG Manager Setup

eG Manager Setup V6

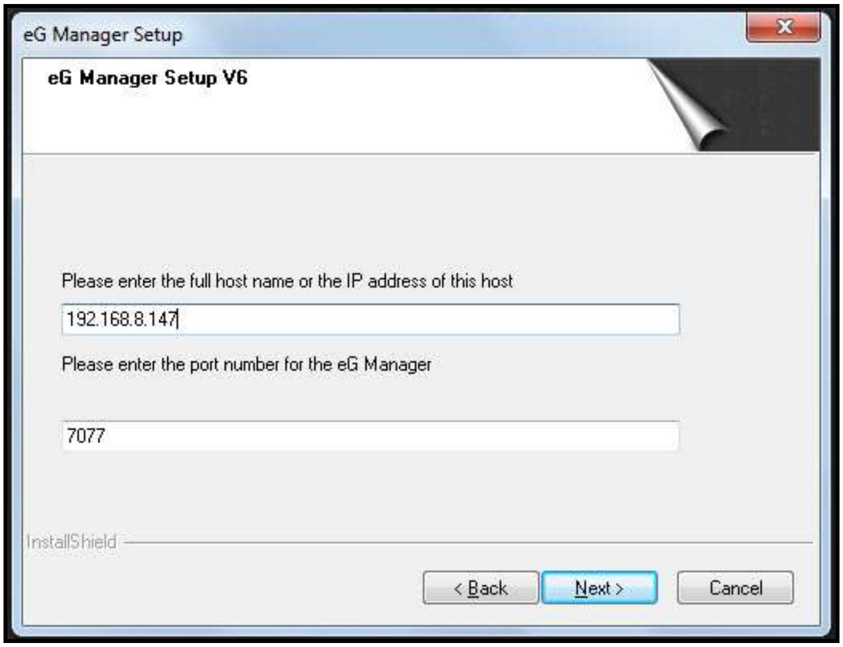
Please select the host name or the IP address of this host

eGLAP0030-PC
fe80::3cf5:2053:4d6b:aa07
192.168.8.147
Other

Please enter the port number for the eG Manager

7077

Figure 3.6: Selecting the IP address/host name to use for the eG manager


eG Manager Setup

eG Manager Setup V6

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

192.168.8.147

Please enter the port number for the eG Manager

7077

Figure 3.7: Hostname and port number of the system on which the eG manager will execute

Note

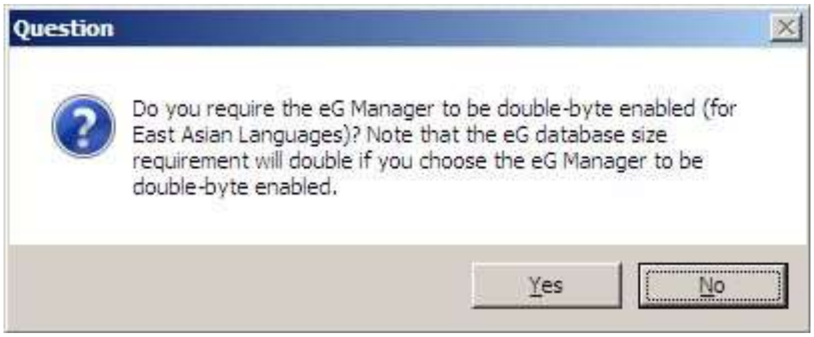
- While specifying the host name/IP address of the manager, please take care of the following aspects:

  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 3.7.

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 clicking the **Yes** button in Figure 3.8. 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

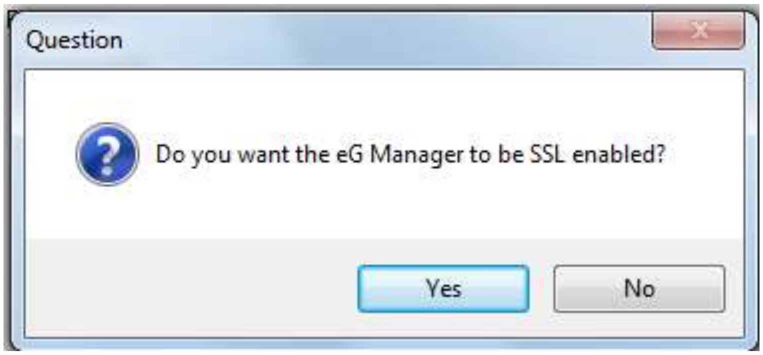
Do you require the eG Manager to be double-byte enabled (for East Asian Languages)? Note that the eG database size requirement will double if you choose the eG Manager to be double-byte enabled.

Figure 3.8: Enabling double-byte support for the eG manager

Refer

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

9. Setup then prompts you to indicate if the eG manager is to be SSL-enabled. If so, click **Yes** in Figure 3.9. If not, click **No**.

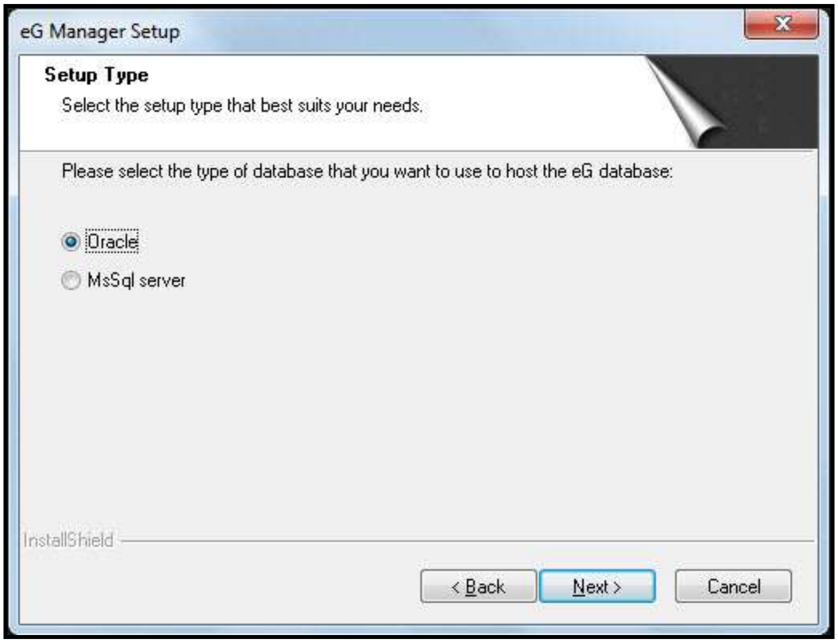


Question

Do you want the eG Manager to be SSL enabled?

Figure 3.9: Indicating whether/not to SSL-enable the eG manager

10. 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 tables/objects in the database. In the next step (shown in Figure 3.10) specify the type of database that should be used to host the eG database.



eG Manager Setup

Setup Type

Select the setup type that best suits your needs.

Please select the type of database that you want to use to host the eG database:

● Oracle

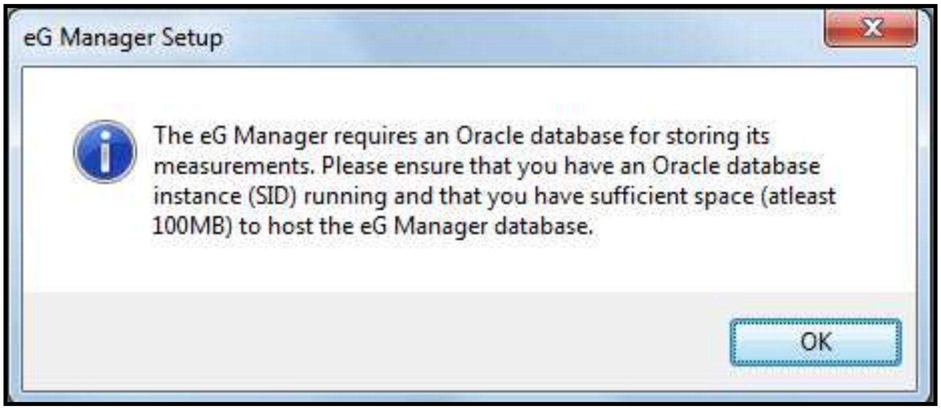
○ MsSql server

Figure 3.10: Specify the type of database server to be used to host the eG database

If you choose **Oracle** here, refer to Section 3.1.2.1 for further details. If you select **Ms SQL Server**, then refer to Section 3.1.2.2 for more information.

3.1.2.1 Using an Oracle Database

1. The user must now ensure that the Oracle database instance is running and that there is sufficient space (atleast 100MB) to host the eG database.

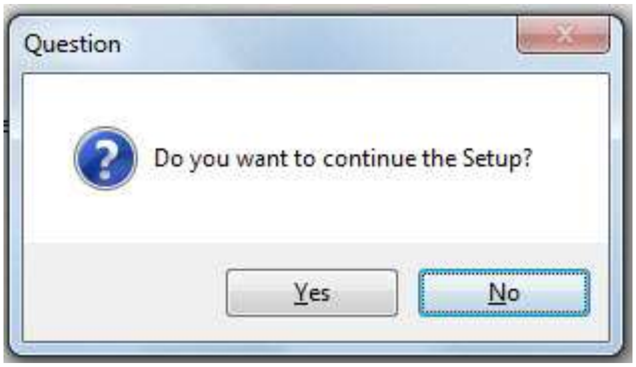


eG Manager Setup

The eG Manager requires an Oracle database for storing its measurements. Please ensure that you have an Oracle database instance (SID) running and that you have sufficient space (atleast 100MB) to host the eG Manager database.

Figure 3.11: Message box specifying the conditions to be checked for hosting the eG database

2. To proceed, click on the **OK** button in Figure 3.11. When this is done, a message box prompting the user for his confirmation to continue with the setup will appear (see Figure 3.12).



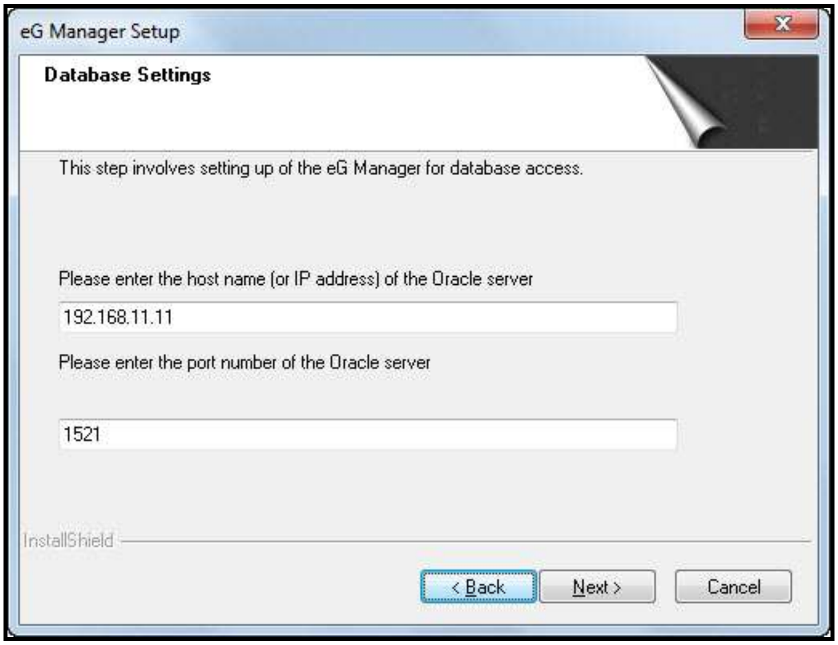
Question

Do you want to continue the Setup?

Figure 3.12: A message box requesting the user's confirmation to proceed with the setup

3. To configure the eG manager system to use an Oracle database server, next enter:

- the hostname or IP address of the server that hosts the Oracle database (use the hostname if DNS is supported) in Figure 3.13
- the port number of the Oracle server [default is **1521**] in Figure 3.14
- the name of an Oracle instance that the eG manager should use in Figure 3.15.



eG Manager Setup

Database Settings

This step involves setting up of the eG Manager for database access.

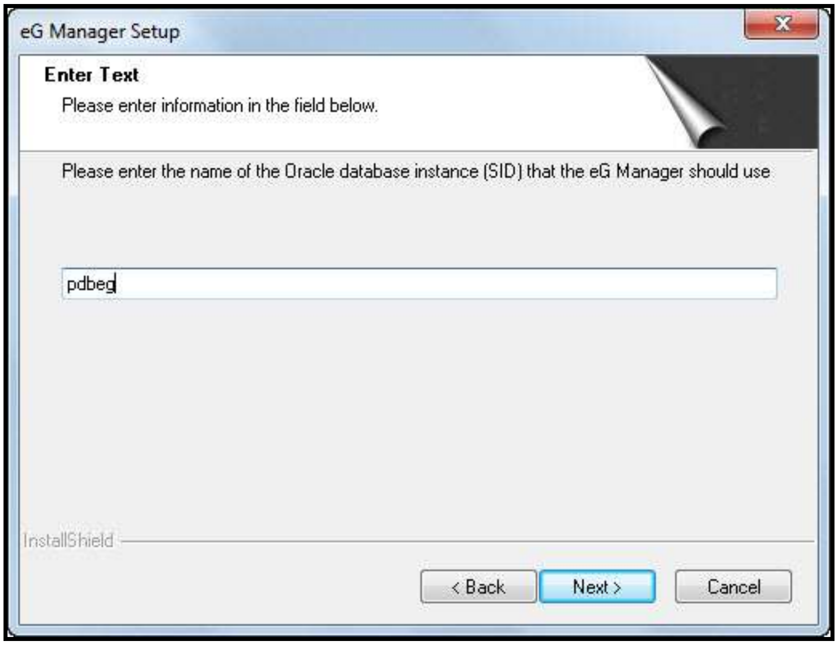
Please enter the host name (or IP address) of the Oracle server

192.168.11.11

Please enter the port number of the Oracle server

1521

Figure 3.13: Hostname and port of the database server hosting the eG database



eG Manager Setup

Enter Text

Please enter information in the field below.

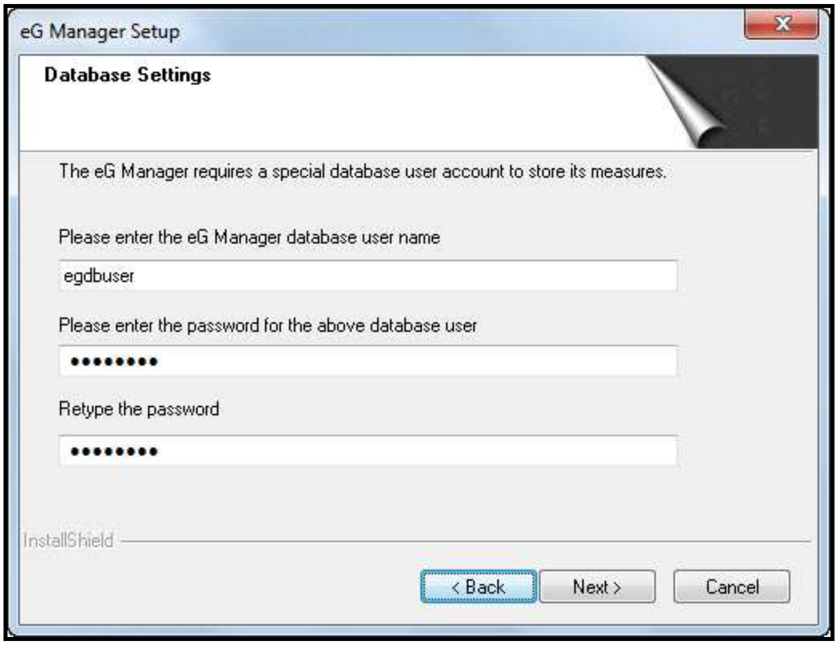
Please enter the name of the Oracle database instance (SID) that the eG Manager should use

pdbeg

Figure 3.14: Specifying the Oracle instance for eG database

4. The eG manager requires a special Oracle database user account to store its measures. The user should next enter the following details as in Figure 3.15.

   - the eG database user name [default is **egurkha**]
   - the password for the database user


eG Manager Setup

Database Settings

The eG Manager requires a special database user account to store its measures.

Please enter the eG Manager database user name

egdbuser

Please enter the password for the above database user

••••••••

Retype the password

••••••••

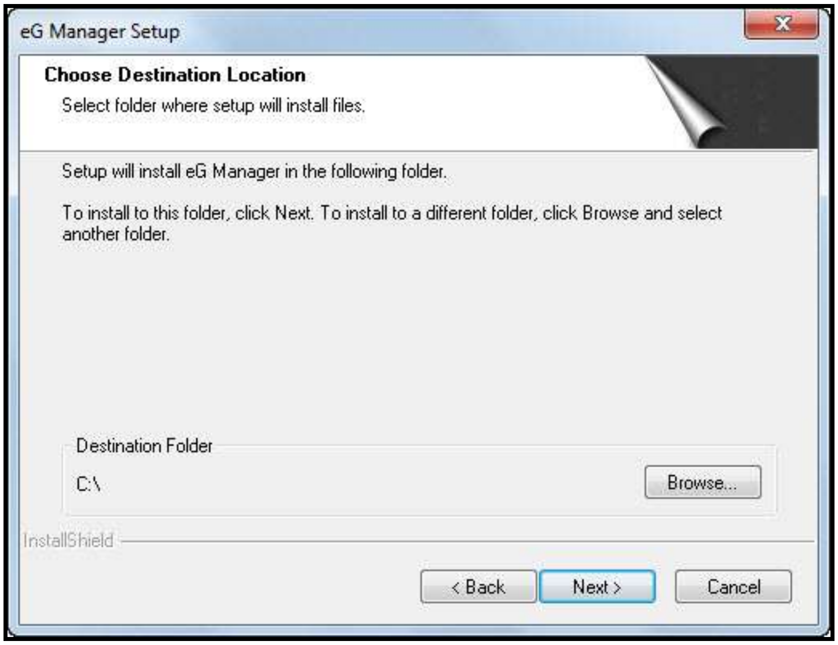
Figure 3.15: Specifying the user information that is to be used to create the eG database

Note

- If you set an existing database user as the eG database user at step 4, 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 use

- Whether you are using an existing database user or creating a new user (be it through the manager setup process or directly on the Oracle database server), make sure that the eG database user name you provide does not contain any special characters.

5. Next, specify the destination directory for installing the eG manager (see Figure 3.16):



eG Manager Setup

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Manager in the following folder.

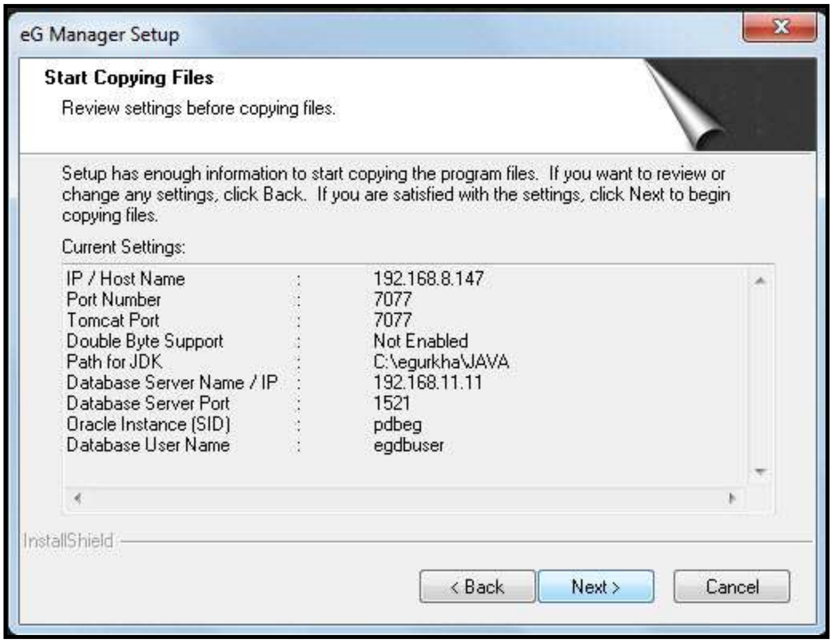
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 3.16: Specifying the destination directory for the eG manager

6. The next step summarizes all the details that have been provided so far by the user as in Figure 3.17.



eG Manager Setup

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.

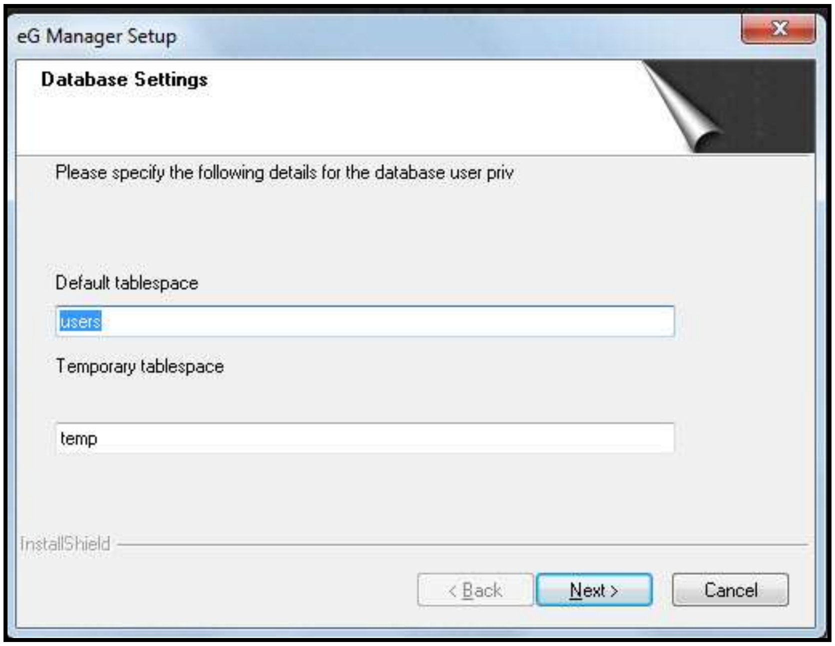
Current Settings:

```
IP / Host Name            :    192.168.8.147
Port Number               :    7077
Tomcat Port               :    7077
Double Byte Support       :    Not Enabled
Path for JDK              :    C:\egurkha\JAVA
Database Server Name / IP :    192.168.11.11
Database Server Port      :    1521
Oracle Instance (SID)     :    pdbeg
Database User Name        :    egdbuser
```

Figure 3.17: Information specified by the user at the various stages of the setup

7. The setup next tries to access the database server and create the user account specified in step 4. If the user name already exists in the database, an alert message appears. The user needs to now specify if he/she wants to use the same account or not. If the user chooses not to use the same account, he/she is made to repeat step 4 to create a new user account. However, if the user chooses to proceed by selecting the **Yes** option in the message box, he/she is directly taken to step 10 of this setup process.

8. 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 3.18). The default values for the data and temporary tablespace values are *users* and *temp,* respectively.



eG Manager Setup

Database Settings

Please specify the following details for the database user priv

Default tablespace: users

Temporary tablespace: temp

Figure 3.18: The setup program requests for the default and temporary tablespaces in order to create a new user account

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;
```

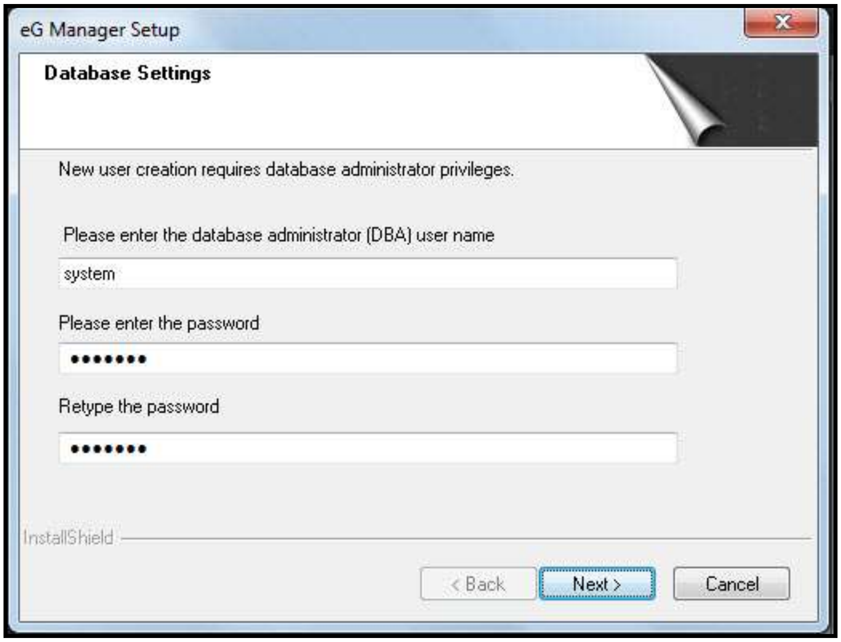
```
create temporary tablespace egurkhatemp01
tempfile 'C:\Oracle\ORADATA\egurkha\eGurkhaTemp01.dbf' size 512M
autoextend off extent management local uniform;
```

- 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.

9. Database administrator privileges are required for creating a new database user. The Setup now prompts the user to enter the database administrator's name and password as in Figure 3.19. The default value for the DBA

user name will be **system**. For more information about your environment, contact your database administrator.



eG Manager Setup

Database Settings

New user creation requires database administrator privileges.

Please enter the database administrator (DBA) user name

system

Please enter the password

•••••••

Retype the password

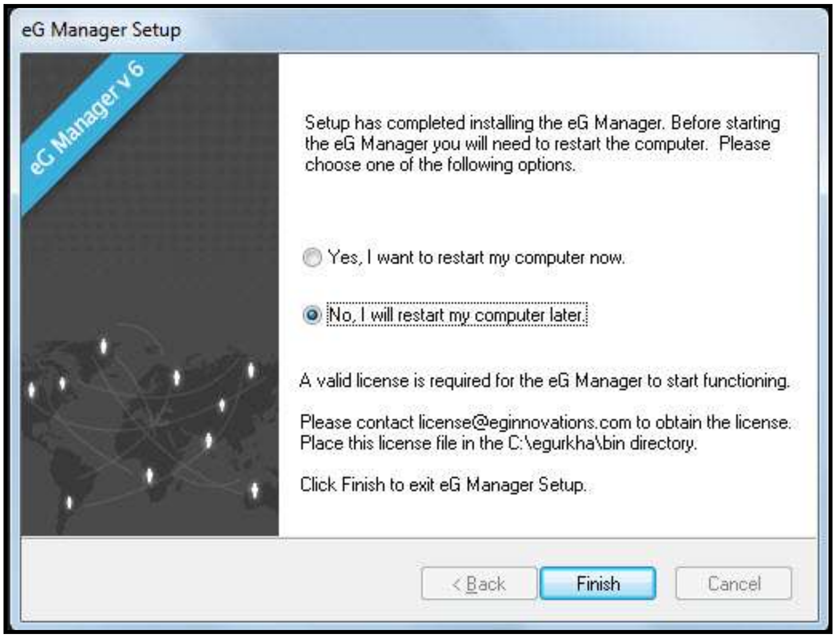
•••••••

Figure 3.19: Setup program seeking the name and password of a database administrator

Note

Make sure that the *DBA user name* does not contain any special characters.

10. If the configuration process succeeds, the following screen will be displayed (see Figure 3.20). The Setup requires the user to restart the system. This can be done immediately or at a later point of time. A valid license must be obtained for the eG manager to function. This license should be placed in the bin directory of the egurkha folder (for e.g., C:\Program Files\egurkha\bin). Clicking on the **Finish** button will exit the Setup.



eG Manager Setup

Setup has completed installing the eG Manager. Before starting the eG Manager you will need to restart the computer. Please choose one of the following options.

○ Yes, I want to restart my computer now.

● No, I will restart my computer later.

A valid license is required for the eG Manager to start functioning.

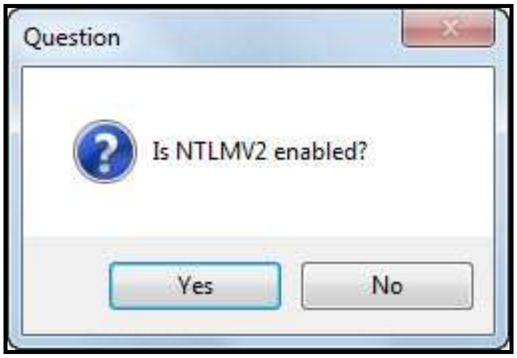
Please contact license@eginnovations.com to obtain the license. Place this license file in the C:\egurkha\bin directory.

Click Finish to exit eG Manager Setup.

Figure 3.20: Setup program indicating the completion of the eG manager installation

3.1.2.2 Using an MS SQL Database

If you choose to configure an MS SQL server database as the eG backend, then setup first requests you to indicate whether/not the Microsft SQL server in your environment is NTLMv2-enabled (see Figure 3.21). If so, click the **Yes** button in the message box of Figure 3.25. If not, click the **No** button.

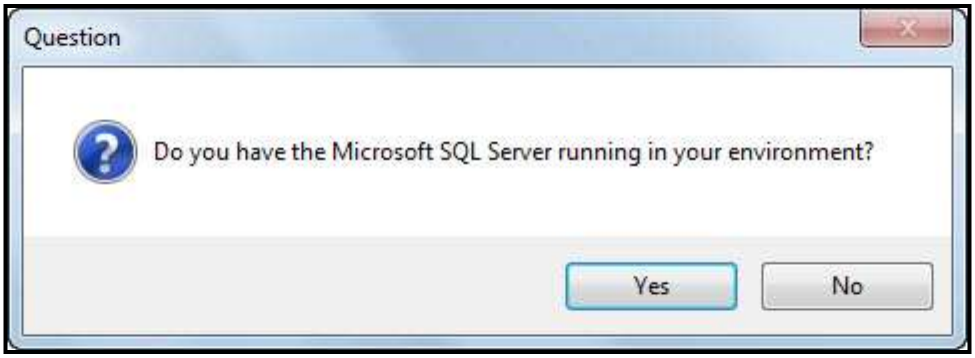


Question

Is NTLMV2 enabled?

Figure 3.21: A message box requesting you to confirm whether or not the Microsoft SQL server is NTLMv2-enabled

Next, setup will request you to confirm whether/not a Microsoft SQL server is running in your environment.



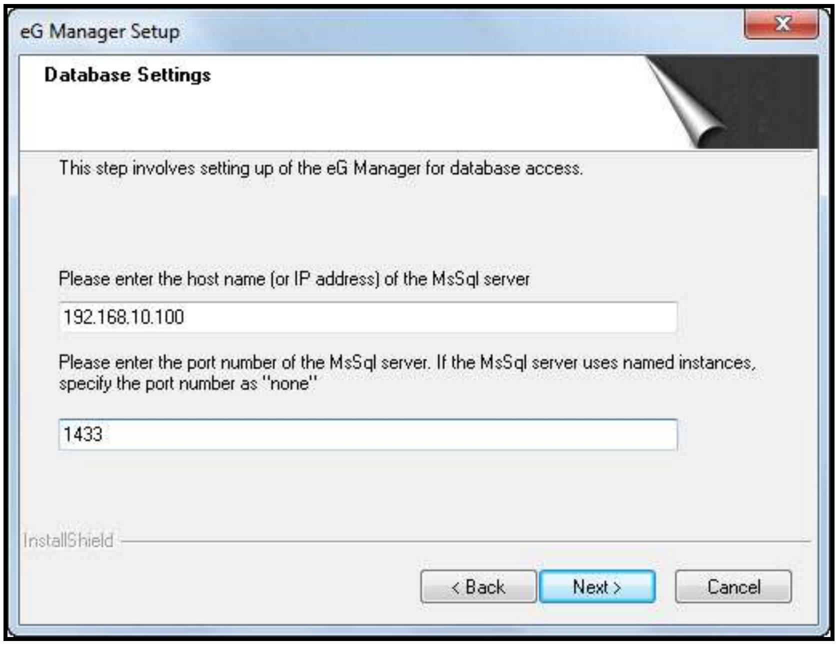
Do you have the Microsoft SQL Server running in your environment?

Figure 3.22: A message box requesting you to confirm whether/not a Microsoft SQL server is running in your environment

If you select **Yes** from Figure 3.22, then before proceeding with the setup, ensure that the **Prerequisites** discussed under Section 2.2.2.1 of **Chapter 2** of this document are fulfilled.

Subsequently, follow the steps given below:

1. If an existing MS SQL server is chosen to host the eG database, then first enter the location of the MS SQL server by specifying the hostname and port on which the MS SQL server is hosted. If the MS SQL server being configured uses named instances, then specify 'none' instead of the port number in Figure 3.23. Then, click the **Next** button to proceed.



Database Settings

This step involves setting up of the eG Manager for database access.

Please enter the host name (or IP address) of the MsSql server

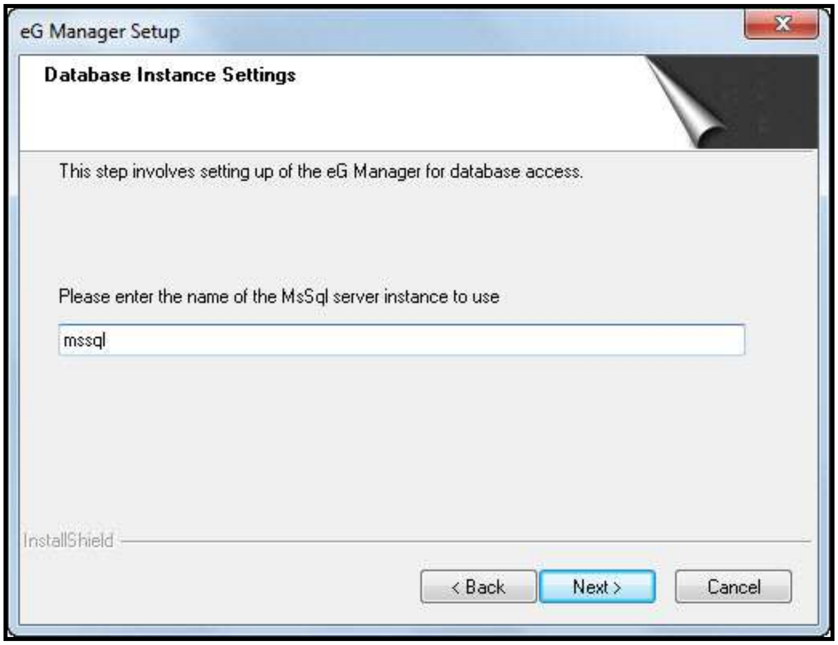
192.168.10.100

Please enter the port number of the MsSql server. If the MsSql server uses named instances, specify the port number as "none"

1433

Figure 3.23: Specifying the location of the MS SQL server to be used for the eG database

2. If 'none' is specified in Figure 3.23, then clicking on the **Next** button will open Figure 3.24 wherein the instance name is to be specified. Then, click the **Next** button in Figure 3.24.


eG Manager Setup

Database Instance Settings

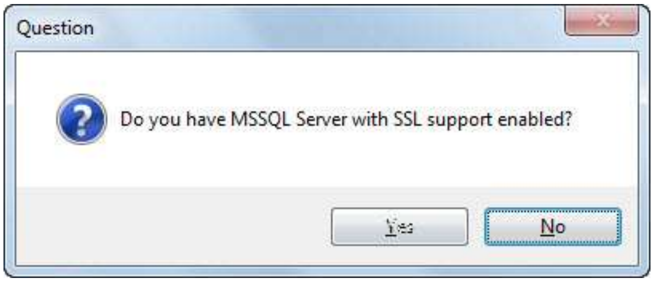
This step involves setting up of the eG Manager for database access.

Please enter the name of the MsSql server instance to use

mssql

Figure 3.24: Specifying the name of the SQL server instance to use

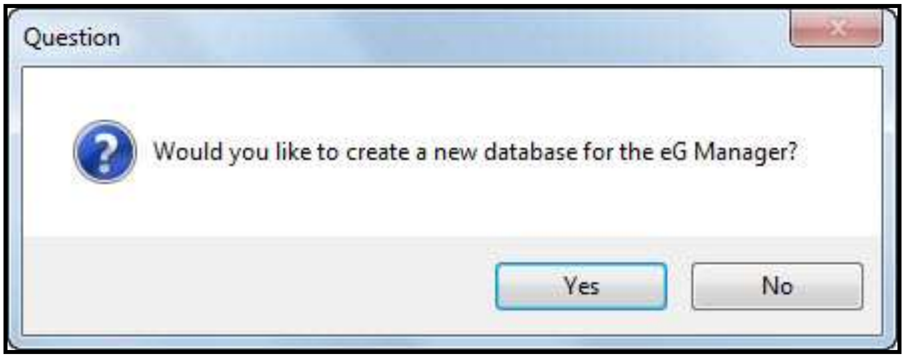
3. Then, you need to indicate whether the MS SQL server to be used as the eG backend is SSL-enabled or not. If not, press the **No** button in Figure 3.25. If it is SSL-enabled, then click on the **Yes** button.


Question

Do you have MSSQL Server with SSL support enabled?

Figure 3.25: A message box confirming the SSL status of the MS SQL server

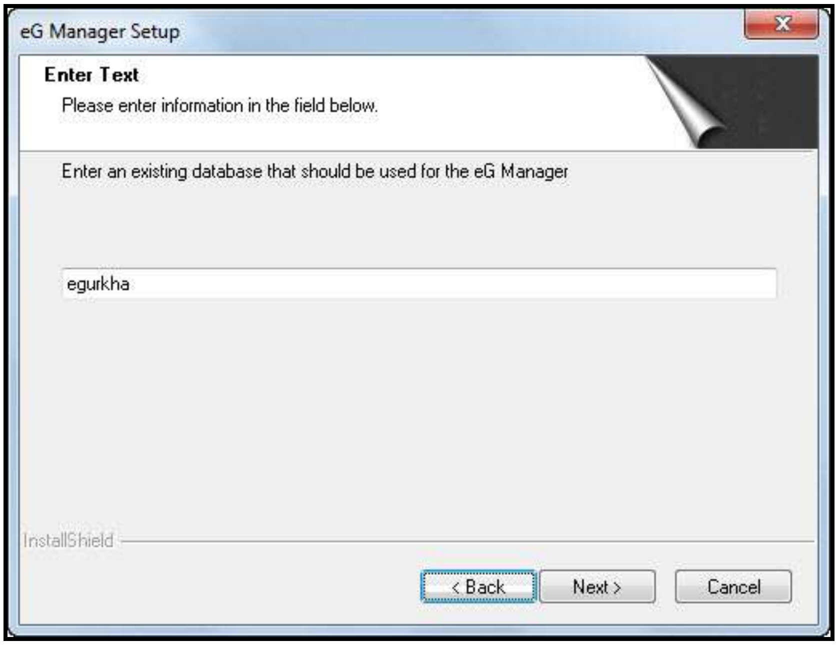
4. Next, specify whether a new database has to be created to host the eG database.


Question

Would you like to create a new database for the eG Manager?

Figure 3.26: Specifying whether a new database has to be created for the eG database

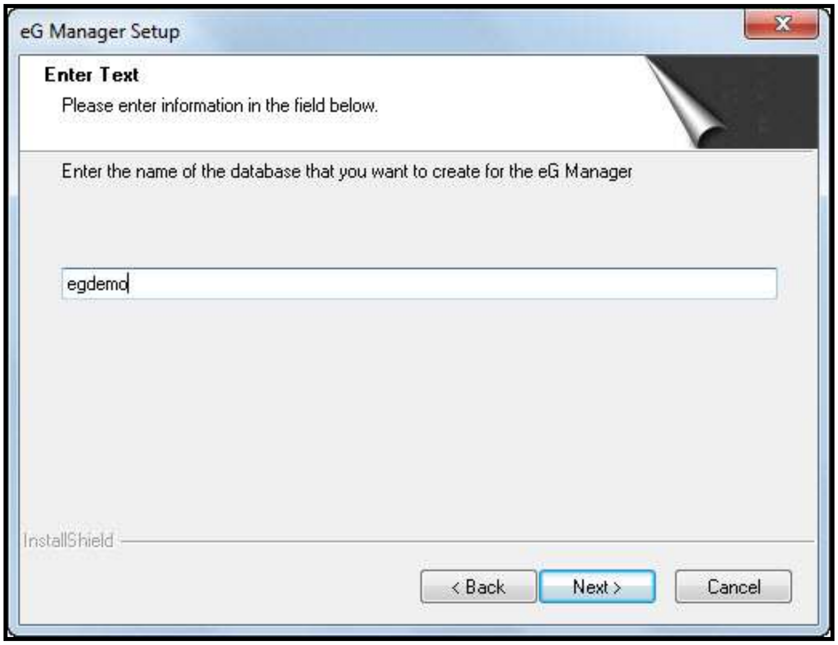
5. If a new database has to be created, indicate the name of the database instance (see Figure 3.28). If an existing database is to be used, the installation process prompts for the name of the existing database instance (see Figure 3.27).



Enter an existing database that should be used for the eG Manager

egurkha

Figure 3.27: Indicating the name of the existing database to be used



Enter the name of the database that you want to create for the eG Manager

egdemo

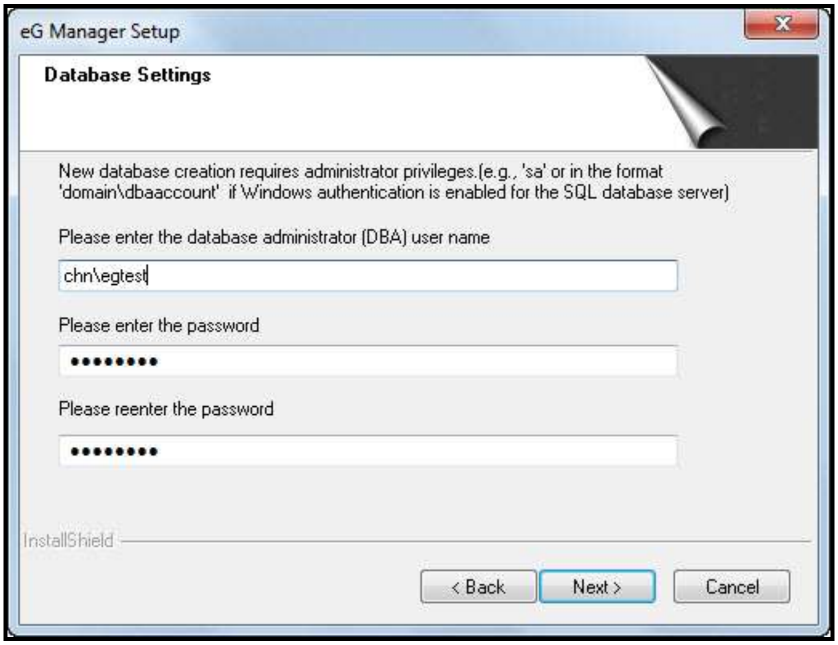
Figure 3.28: Indicating the name of the new database that is to be created

6. Since a new database instance can be created only by an administrator of the database server, next specify the user name and password for the database administrator. If **Windows Authentication** is enabled on the MS SQL

server, then ensure that the credentials of a valid Windows domain user with database administrator privileges are provided in Figure 3.29. Also, make sure that the user name is of the format *domainname\username*. For eg., if the name of the database administrator is *dbadmin* and the domain name is *chi*, the user name you specify in Figure 3.29 should be: *chi\dbadmin*.

On the other hand, if **Mixed Mode Authentication** is enabled on the MS SQL server, then the database administrator name that you specify need not necessarily be preceded by the domain name. In this case therefore, your user name specification can be of either of the following formats: *username* or *domainname\username*.

However, if **SQL Server Authentication** is enabled on the MS SQL server, then the database administrator name should **not be prefixed by a domain name**. Your specification should then be only, *username*.



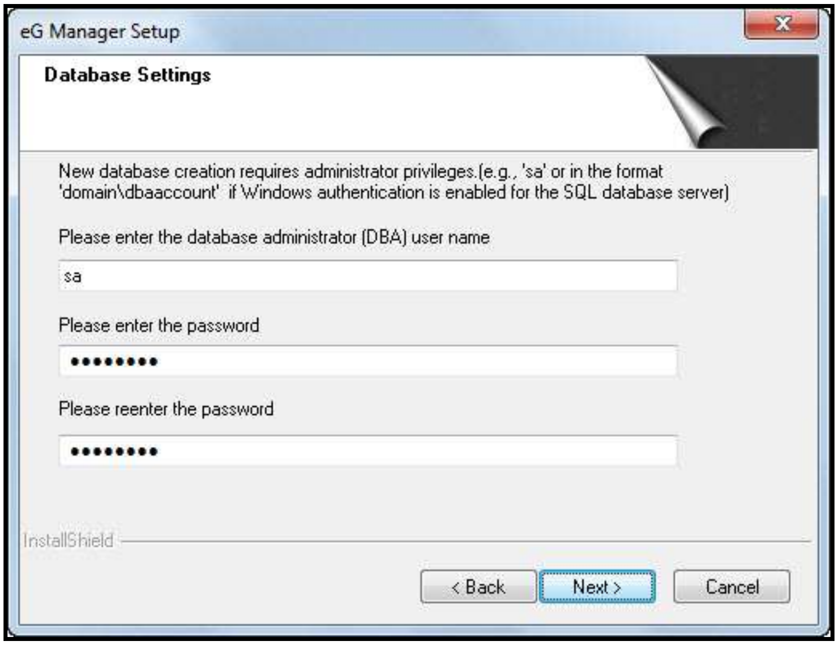
New database creation requires administrator privileges.(e.g., 'sa' or in the format 'domain\dbaaccount' if Windows authentication is enabled for the SQL database server)

Please enter the database administrator (DBA) user name: chn\egtest

Please enter the password: ••••••••

Please reenter the password: ••••••••

Figure 3.29: Specifying the database administrator user name and password for an MS SQL server with Windows Authentication enabled



New database creation requires administrator privileges.(e.g., 'sa' or in the format 'domain\dbaaccount' if Windows authentication is enabled for the SQL database server)

Please enter the database administrator (DBA) user name

sa

Please enter the password

●●●●●●●●●

Please reenter the password

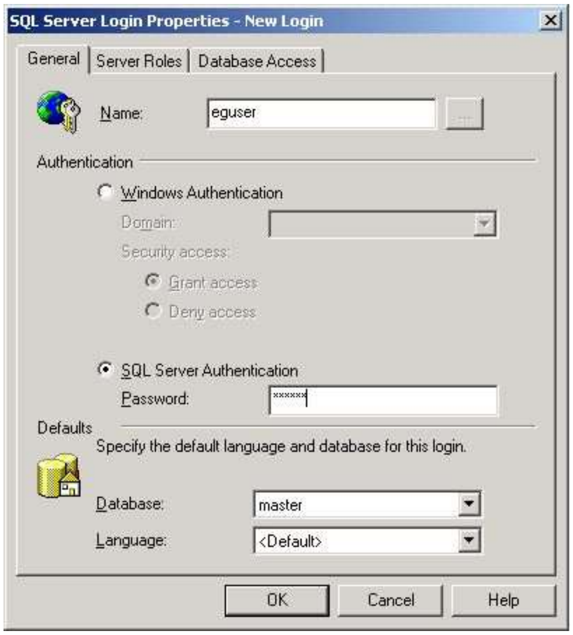
●●●●●●●●●

Figure 3.30: Specifying the user name and password of a database administrator on an MS SQL server with SQL Server authentication

Note

Ensure that the *DBA user name* you provide does not contain any special characters.

By default, manager setup displays the **sa** user name as depicted by Figure 3.30. If, due to security concerns, you decide not to use the **sa** user name and password, then you can create a user with the **Security Administrators** and **Database Creators** roles, and then provide that user's credentials in Figure 3.29. Figure 3.31 and Figure 3.32 depict how to create a new user with the aforesaid privileges using the **SQL Server Enterprise Manager**.



SQL Server Login Properties - New Login

General | Server Roles | Database Access

Name: eguser

Authentication

○ Windows Authentication

Domain:

Security access:

● Grant access

○ Deny access

● SQL Server Authentication

Password: ******

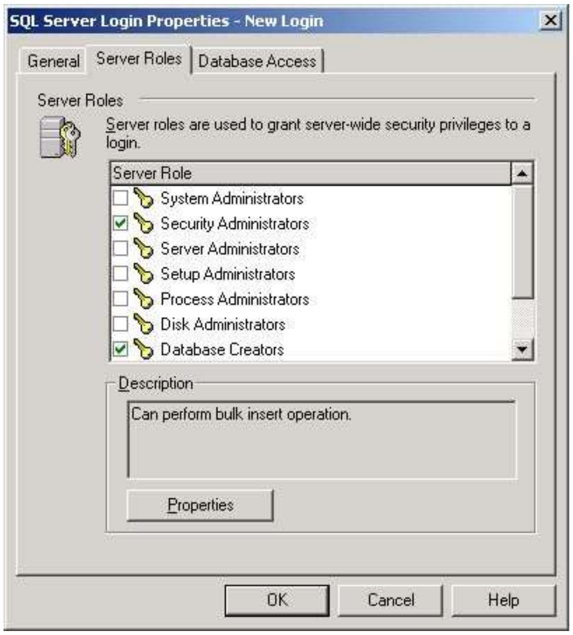
Defaults

Specify the default language and database for this login.

Database: master

Language: <Default>

Figure 3.31: Creating a new user



SQL Server Login Properties - New Login

General | Server Roles | Database Access

Server Roles

Server roles are used to grant server-wide security privileges to a login.

Server Role

- □ System Administrators
- ☑ Security Administrators
- □ Server Administrators
- □ Setup Administrators
- □ Process Administrators
- □ Disk Administrators
- ☑ Database Creators

Description

Can perform bulk insert operation.

Figure 3.32: Granting the requisite privileges to the new user

Note

- Make sure that the user name of the database administrator that you create newly does not contain any special characters.
- If MS SQL 2008 is used as the eG backend, then ensure that the **dbcreator**, **securityadmin**, and **public** roles are assigned to the user. Also, either provide a **strong password** for the user, or make sure that the **Enforce password policy** option is disabled while creating the user profile in the **SQL Enterprise Manager**.

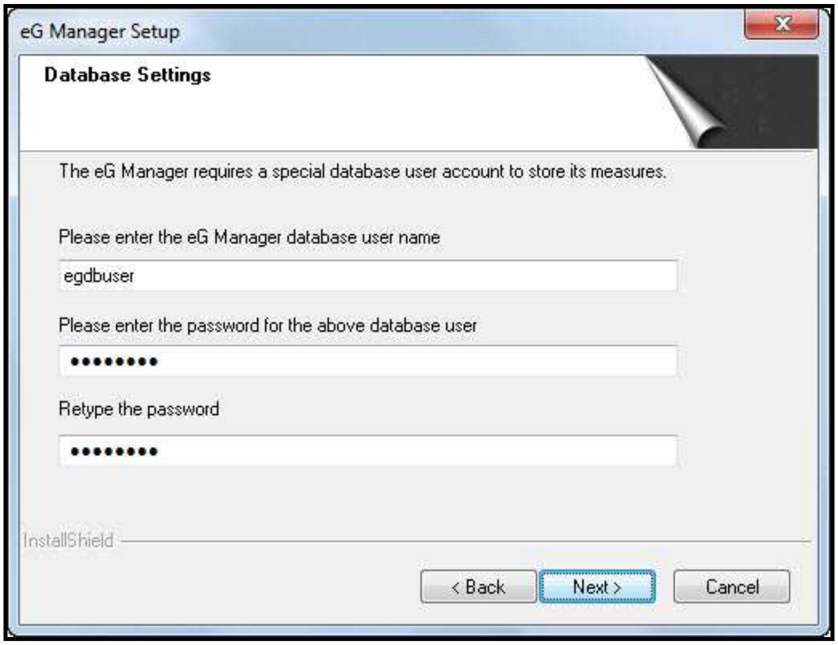
While Figure 3.31 and Figure 3.32 illustrate the procedure to be followed to create a new user on an MS SQL server with **SQL Server Authentication** enabled, remember the following while creating a user on an MS SQL server with **Windows Authentication** enabled:

- The username you specify should be that of a valid user to the Windows domain of which the MS SQL server is a part;
- The username specification should be of the format: *domainname|username*

7. The eG database is created in the MS SQL server's database using a special user account. Next, specify the user name and password to be used for this account. Here again, if **Windows Authentication** is enabled on the MS SQL server, then the new user should be a valid Windows domain user. Accordingly, the user name should be of the format *domainname|username*. For eg., if the name of the new user is *egdb* and the domain name is *sig*, the user name you specify in Figure 3.41 should be: *sig|egdb*.

   On the other hand, if **Mixed Mode Authentication** is enabled on the MS SQL server, then the special user account you create need not necessarily be preceded by the domain name. In this case therefore, your user name specification can be of either of the following formats: *username* or *domainname|username*.

   However, if **SQL Server Authentication** is enabled on the MS SQL server, then the user name should **not be prefixed by a domain name**. Your specification should then be only, *username*.



eG Manager Setup

Database Settings

The eG Manager requires a special database user account to store its measures.

Please enter the eG Manager database user name

egdbuser

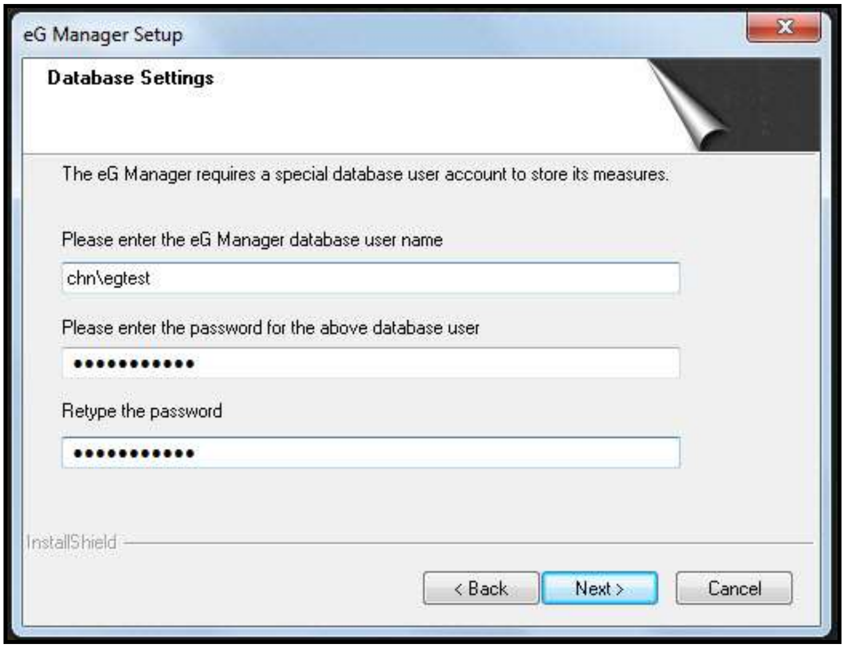
Please enter the password for the above database user

●●●●●●●●

Retype the password

●●●●●●●●

Figure 3.33: Specifying the user name and password to be used to host the eG database on an MS SQL server with SQL server authentication enabled



eG Manager Setup

Database Settings

The eG Manager requires a special database user account to store its measures.

Please enter the eG Manager database user name

chn\egtest

Please enter the password for the above database user

●●●●●●●●●●●●

Retype the password

●●●●●●●●●●●●

Figure 3.34: Specifying the user name and password to host the eG database on an MS SQL server with Windows Only Authentication enabled

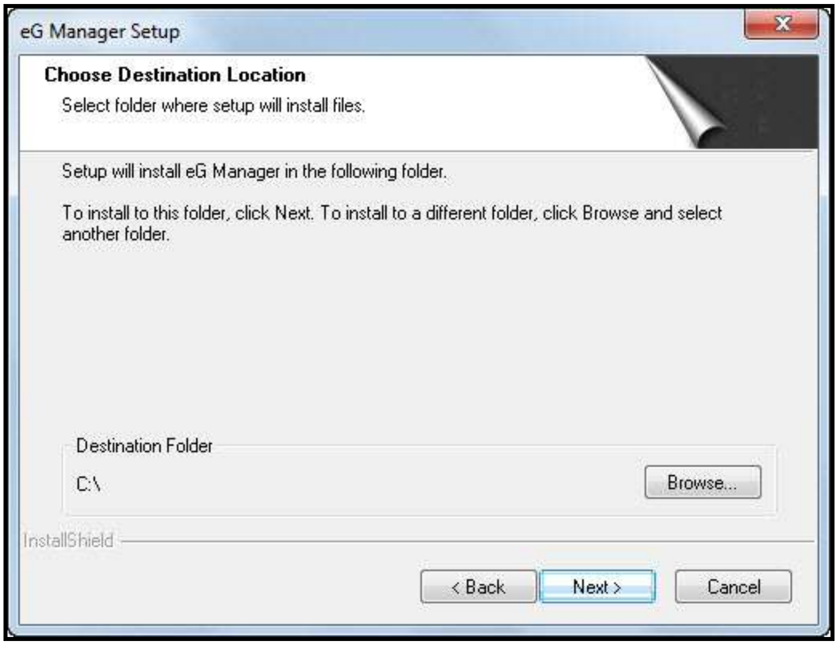
Note

- 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.
- If MS SQL Server 2008 is being used as the eG backend, then ensure that the password provided in Figure 3.33 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.

8. The installation process then prompts the user to select the destination location for the eG manager (see Figure 3.35).



eG Manager Setup

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Manager in the following folder.

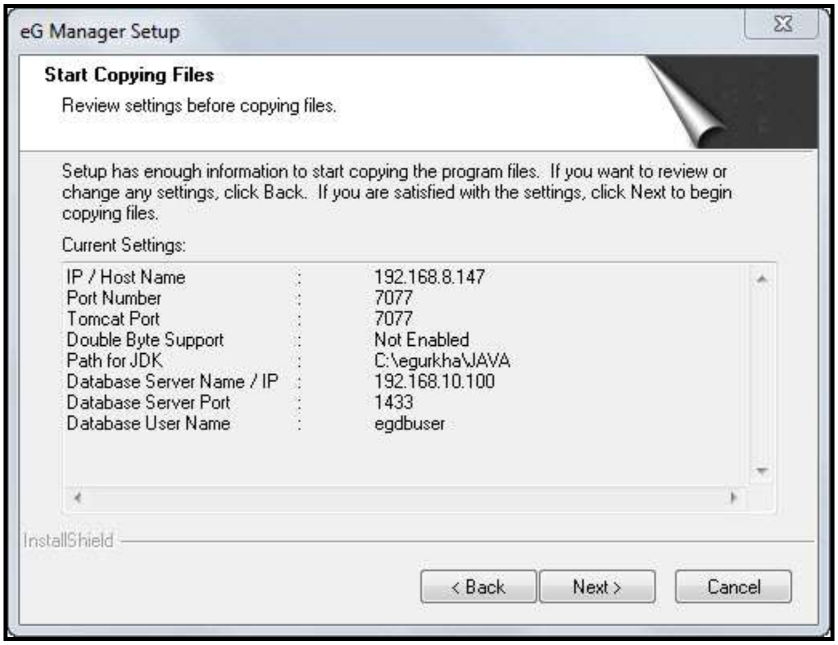
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 3.35: Location of the eG manager

9. The next step summarizes all the details that have been provided so far by the user as in Figure 3.36.



eG Manager Setup

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.

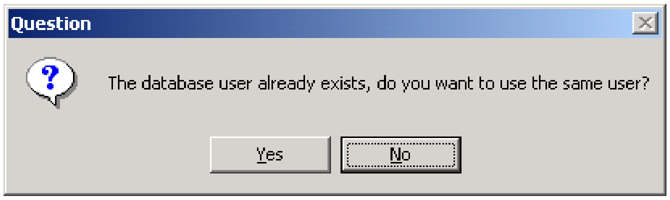
Current Settings:

```
IP / Host Name              :      192.168.8.147
Port Number                 :      7077
Tomcat Port                 :      7077
Double Byte Support         :      Not Enabled
Path for JDK                :      C:\egurkha\JAVA
Database Server Name / IP   :      192.168.10.100
Database Server Port        :      1433
Database User Name          :      egdbuser
```

Figure 3.36: Information specified by the user at the various stages of the setup

10. Setup next tries to access the database server and create the user account specified in Step 5. If the user name already exists in the database, an alert message as shown in Figure 3.37 appears. The user needs to now specify if he/she wants to use the same account or not. If the user chooses not to use the same account, he/she is made to repeat step 5 to create a new user account. However, if the user chooses to proceed by

selecting the **Yes** option in Figure 3.37, he/she is directly taken to step 13 of this setup process.



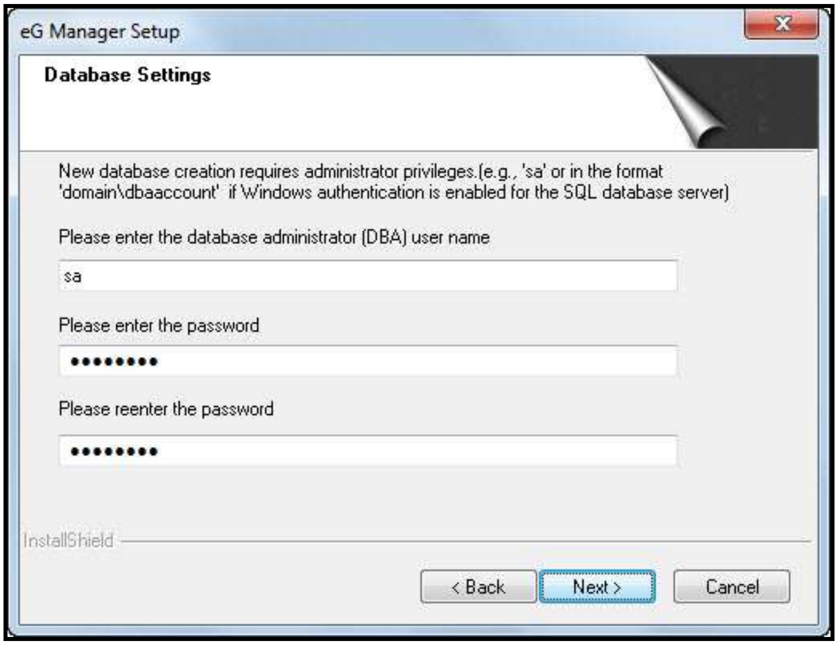
The database user already exists, do you want to use the same user?

Figure 3.37: Message box indicating the existence of a database user

Note

If you want to set an existing database user as the eG database user, then make sure you grant *dbowner* privileges to such a user.

11. Database administrator privileges are required for creating a new database user. The Setup now prompts the user to enter the database administrator's name and password as in Figure 3.38. The default value for the DBA user name will be **sa**. For more information about your environment, contact your database administrator.



New database creation requires administrator privileges.(e.g., 'sa' or in the format 'domain\dbaaccount' if Windows authentication is enabled for the SQL database server)

Please enter the database administrator (DBA) user name

sa

Please enter the password

••••••••

Please reenter the password

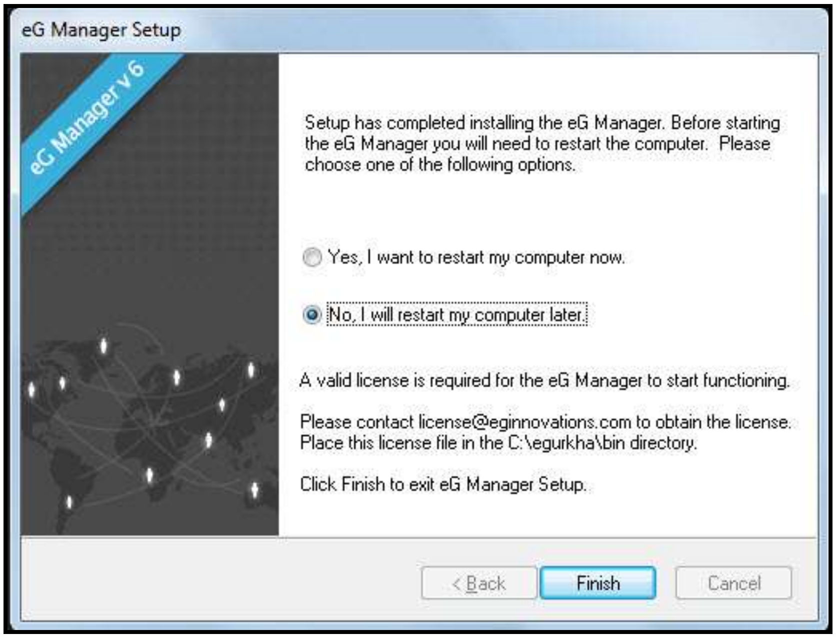
••••••••

Figure 3.38: Setup program seeking the name and password of a database administrator

Note

Ensure that the *DBA user name* you provide does not contain any special characters.

12. If the configuration process succeeds, the following screen will be displayed (see Figure 3.39). The Setup requires the user to restart the system. This can be done immediately or at a later point of time. A valid license must be obtained for the eG manager to function. This license should be placed in the bin directory of the egurkha folder (for e.g., C:\Program Files\egurkha\bin). Clicking on the **Finish** button will exit the Setup.



Setup has completed installing the eG Manager. Before starting the eG Manager you will need to restart the computer. Please choose one of the following options.

○ Yes, I want to restart my computer now.

● No, I will restart my computer later.

A valid license is required for the eG Manager to start functioning.

Please contact license@eginnovations.com to obtain the license. Place this license file in the C:\egurkha\bin directory.

Click Finish to exit eG Manager Setup.

Figure 3.39: Setup program indicating the completion of the eG manager installation

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:

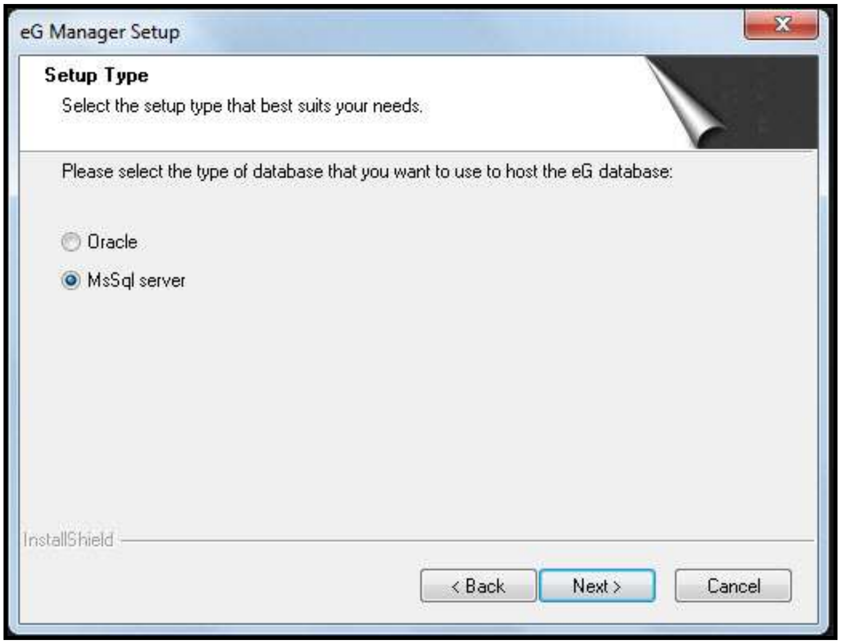
```
Do you want to set the eG manager for agentless monitoring by default? y/n[n]: y
*******************************************************************************
Changes to the eG manager default setting have been successfully made!
*******************************************************************************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

3.1.3 Configuring the eG Manager to Use a Microsoft Azure SQL Database

Microsoft Azure SQL Database is a relational database-as-a-service that delivers predictable performance, scalability, business continuity, data protection, and near-zero administration to cloud developers and solution architects.

If you have already created a SQL database on Azure, then, you can configure the eG manager to use this database as its backend. The procedure for this is as follows:

1. When setup prompts you to pick the database server that should be used to host the eG database, pick the **MsSql server** option (see Figure 3.83).



eG Manager Setup

Setup Type

Select the setup type that best suits your needs.

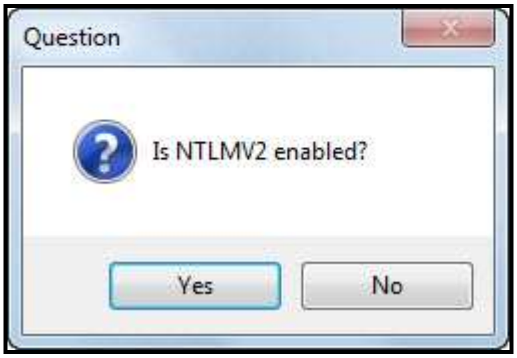
Please select the type of database that you want to use to host the eG database:

○ Oracle

● MsSql server

Figure 3.40: Specify the type of database server to be used to host the eG database

2. Then, setup requests you to indicate whether/not the Microsft SQL server in your environment is NTLMv2-enabled (see Figure 3.41). Select **No** here to proceed.



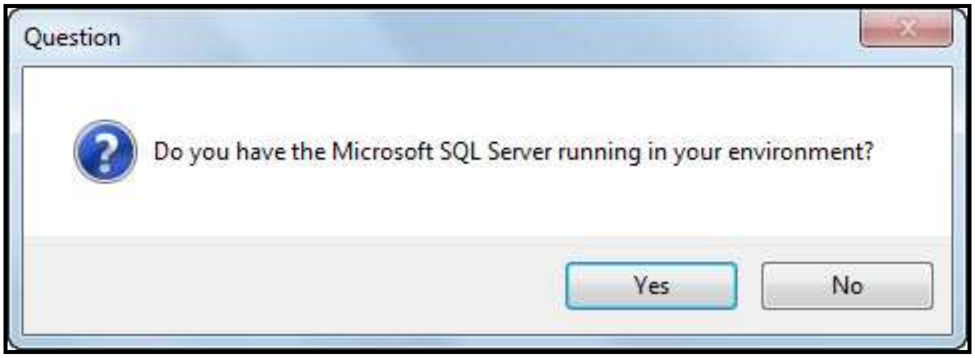
Question

Is NTLMV2 enabled?

Figure 3.41: A message box requesting you to confirm whether or not the Microsoft SQL server is NTLMv2-enabled

3. Next, setup will request you to confirm whether/not a Microsoft SQL server is running in your environment.

Select **Yes** here to use the Microsoft Azure SQL database.

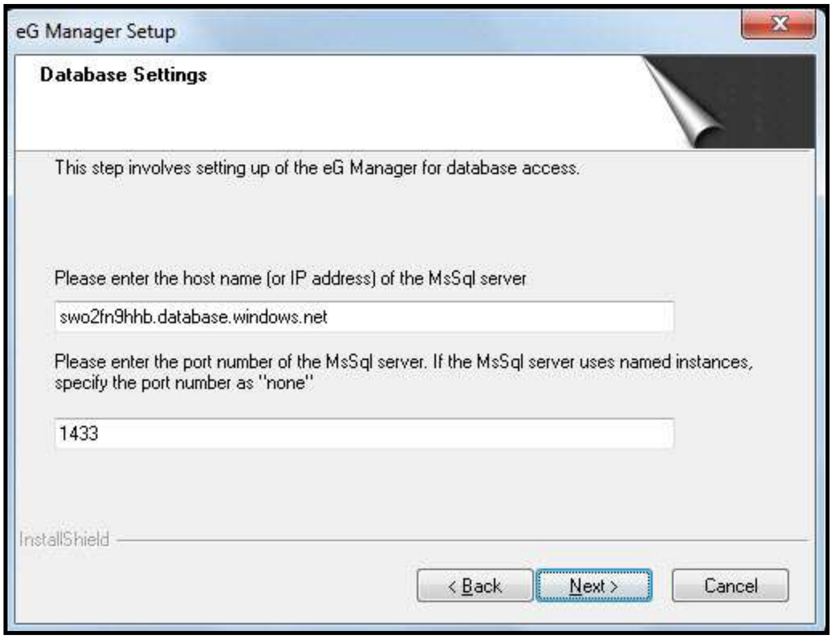


Do you have the Microsoft SQL Server running in your environment?

Figure 3.42: A message box requesting you to confirm whether/not a Microsoft SQL server is running in your environment

4. When Figure 3.87 appears, specify the following and then click the **Next** button:

   - the fully-qualified SQL server name that Azure auto-generates when creating a SQL database
   - the port number of the SQL server instance that Azure auto-generates [default is **1433**]



This step involves setting up of the eG Manager for database access.

Please enter the host name (or IP address) of the MsSql server

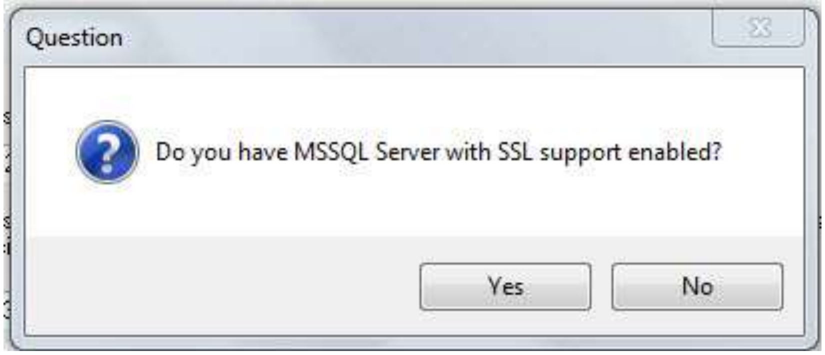
swo2fn9hhb.database.windows.net

Please enter the port number of the MsSql server. If the MsSql server uses named instances, specify the port number as "none"

1433

Figure 3.43: Specifying the location of the MS SQL server to be used for the eG database

5. By default, the SQL server instance that Azure creates is SSL-enabled. Therefore, when requested to confirm whether the SQL server is SSL-enabled or not, click **Yes** (see Figure 3.88).

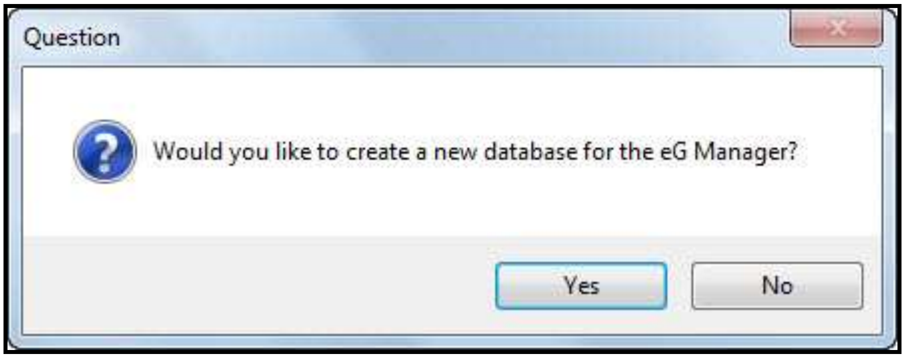


Question

Do you have MSSQL Server with SSL support enabled?

Figure 3.44: Confirm whether/not the SQL database on Azure is SSL-enabled

6. Next, specify whether a new database has to be created to host the eG database. Since you intend to use the SQL database that is already created on Azure to store measures, click **No** in Figure 3.89.

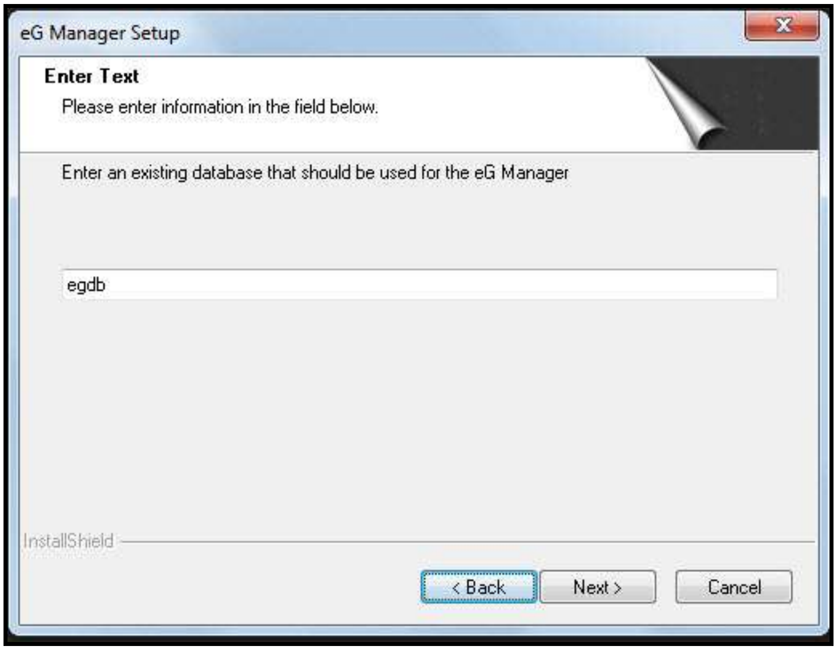


Question

Would you like to create a new database for the eG Manager?

Figure 3.45: Specifying whether a new database has to be created for the eG database

7. Enter the name you assigned to the SQL database when you created it on Azure.



eG Manager Setup

Enter Text

Please enter information in the field below.

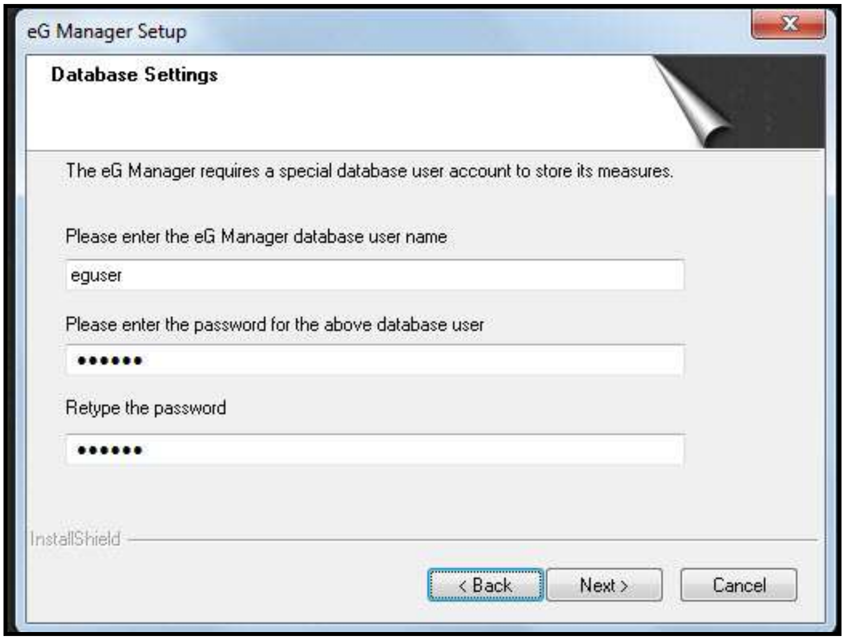
Enter an existing database that should be used for the eG Manager

egdb

Figure 3.46: Indicating the name of the SQL database you created on Azure

8. Next, specify the details of the user account that will be used to host the eG database. For this, configure the following in Figure 3.94:

   - the login name that you provided when creating the SQL database on Azure
   - the password that you provided for the login name at the time of creating the Azure SQL database



eG Manager Setup

Database Settings

The eG Manager requires a special database user account to store its measures.

Please enter the eG Manager database user name

eguser

Please enter the password for the above database user

••••••

Retype the password

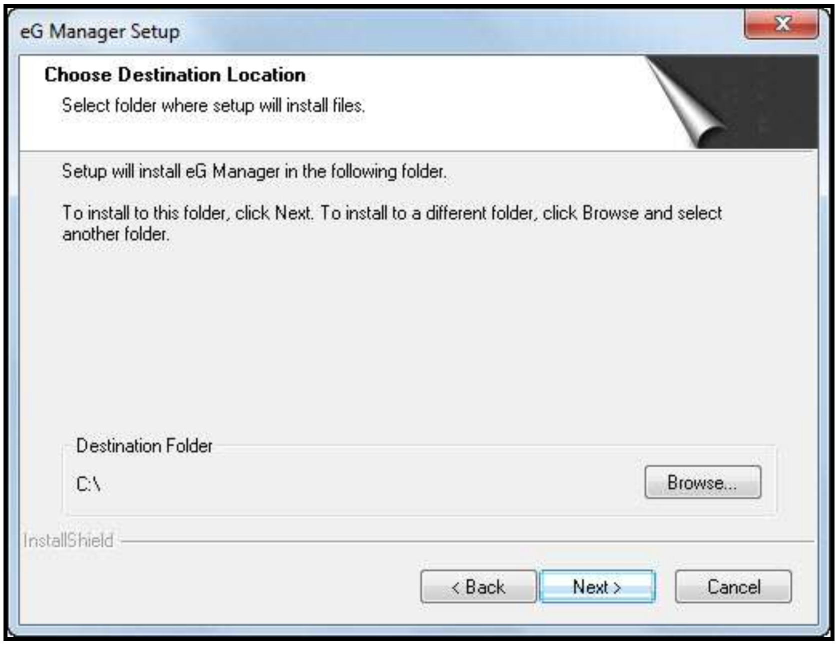
••••••

Figure 3.47: Specifying the user name and password to be used to store measures in a SQL database on Azure

Note

By default, the SQL database on Azure uses **SQL authentication** only. Therefore, make sure you specify the user name in Figure 3.98 without prefixing it with a domain name.

9. The installation process then prompts the user to select the destination location for the eG manager (see Figure 3.35).



eG Manager Setup

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Manager in the following folder.

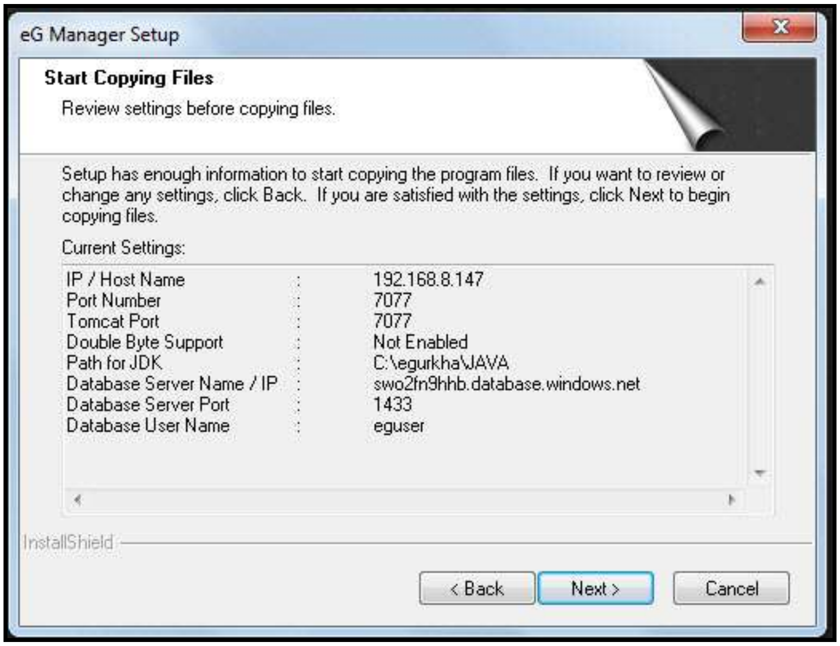
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 3.48: Location of the eG manager

10. The next step summarizes all the details that have been provided so far by the user as in Figure 3.36.



Review settings before copying files.

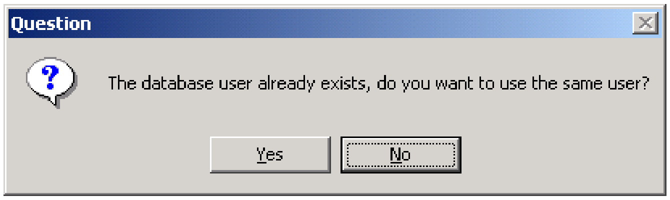
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
IP / Host Name              :    192.168.8.147
Port Number                 :    7077
Tomcat Port                 :    7077
Double Byte Support         :    Not Enabled
Path for JDK                :    C:\egurkha\JAVA
Database Server Name / IP   :    swo2fn9hhb.database.windows.net
Database Server Port        :    1433
Database User Name          :    eguser
```

Figure 3.49: Information specified by the user at the various stages of the setup

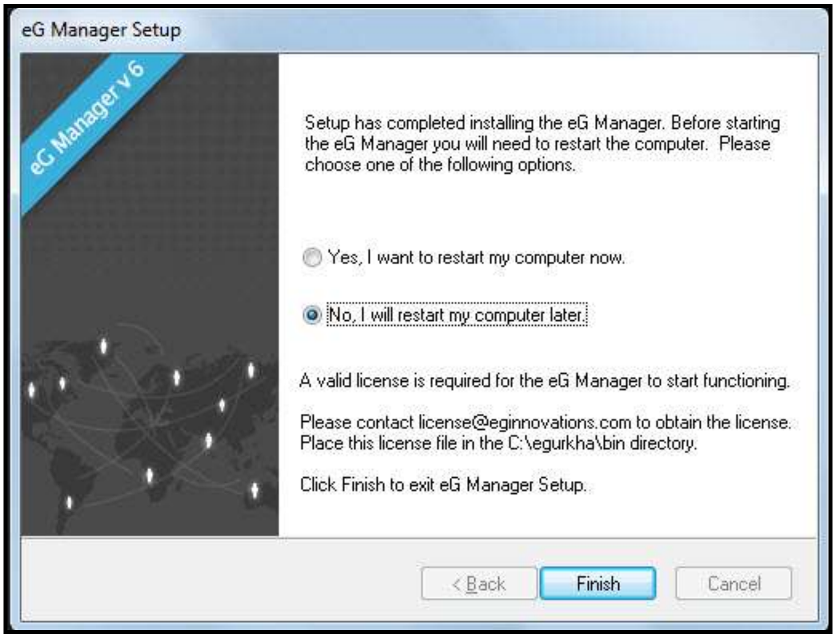
11. Setup next tries to access the database server using the user account specified in step 8 above. When doing so, it figures out that the user name already exists and prompts you to confirm whether/not to continue using the same name. Click **Yes** here to proceed.



The database user already exists, do you want to use the same user?

Figure 3.50: Message box indicating the existence of a database user

12. If the configuration process succeeds, the following screen will be displayed (see Figure 3.39). The Setup requires the user to restart the system. This can be done immediately or at a later point of time. A valid license must be obtained for the eG manager to function. This license should be placed in the bin directory of the egurkha folder (for e.g., C:\Program Files\egurkha\bin). Clicking on the **Finish** button will exit the Setup.



Setup has completed installing the eG Manager. Before starting the eG Manager you will need to restart the computer. Please choose one of the following options.

○ Yes, I want to restart my computer now.

● No, I will restart my computer later.

A valid license is required for the eG Manager to start functioning.

Please contact license@eginnovations.com to obtain the license. Place this license file in the C:\egurkha\bin directory.

Click Finish to exit eG Manager Setup.

Figure 3.51: Setup program indicating the completion of the eG manager installation

3.1.4 Configuring the eG Manager to use an MS SQL Server 2005 on Windows 2003

The eG Enterprise manager can use an Oracle server/MS SQL Server (2005 or 2008 or 2012) as the eG backend, and this MS SQL server can support any of the 3 authentication types - **Windows Only Authentication**, **SQL Server Authentication** , or **Mixed Mode Authentication**. If **SQL Server Authentication** is enabled, the installation of the eG manager is straightforward. On the other hand, if **Mixed Mode Authentication** is enabled for the MS SQL Server 2005 operating on a Windows 2003 system, several precautions must be taken when installing the eG manager to use this database backend.

By default, a Windows 2003 Active Directory server imposes strict local and domain-based group policies. One such policy relates to **password complexity**. Windows 2003, by default, mandates the use of **strong passwords**. 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)

Hence, before setting MS SQL Server 2005 as the eG backend, verify the following:

- Whether the MS SQL Server 2005 is operating on Windows 2003
- Whether **Mixed Mode Authentication** is enabled for the MS SQL Server 2005

If so, then, while configuring the eG manager to use MS SQL Server 2005 as the eG backend, ensure that the password you provide for the eG database user is a **strong password**. If not, the eG manager installation will fail. If the eG manager installation fails, before clicking on the **OK** button of the error message, check the file **<EG_INSTALL_DIR>\manager\logs\error_log** for any errors that may have been reported during the installation process. If the password provided is not a strong password, the corresponding error message is logged in the error_log file.

If you prefer, you can manually create a new eG database and a corresponding user on the MS SQL Server 2005, using the **SQL Server Management Studio**. Once you have succeeded in this process, you can then proceed to install the eG manager using the eG database and user that you created manually.

To create an eG database and an eG user on the MS SQL Server 2005, do the following:

1. Open the **SQL Server Management Studio** follow the menu sequence depicted by Figure 3.52.

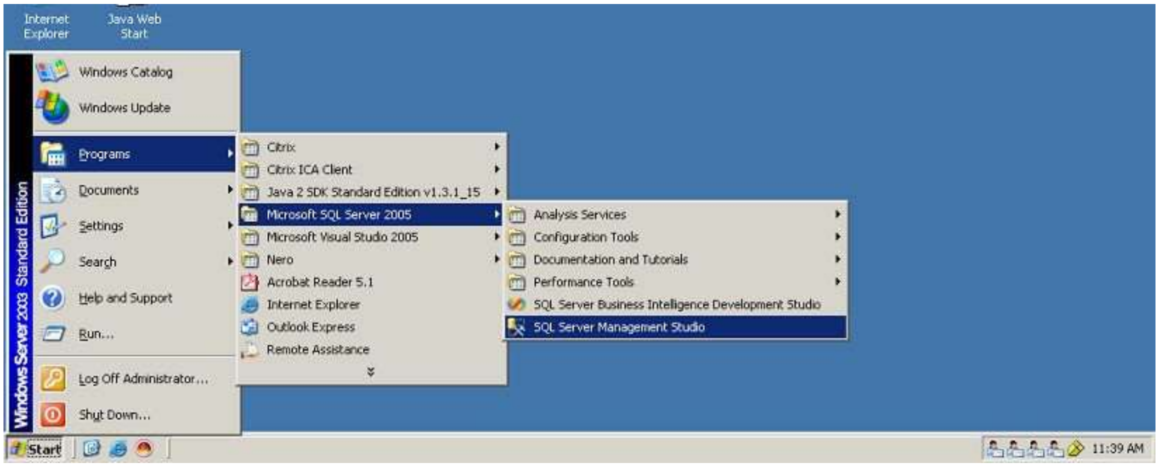


Figure 3.52: Opening the SQL Server Management Studio

2. Login using the *sa* user by providing the appropriate password.
3. Next, from the tree-structure in the left pane of the **Microsoft SQL Server Management Studio**, select the **Databases** node, right-click on it, and select the **New Database** option to create a new database for the eG manager (see Figure 3.53).

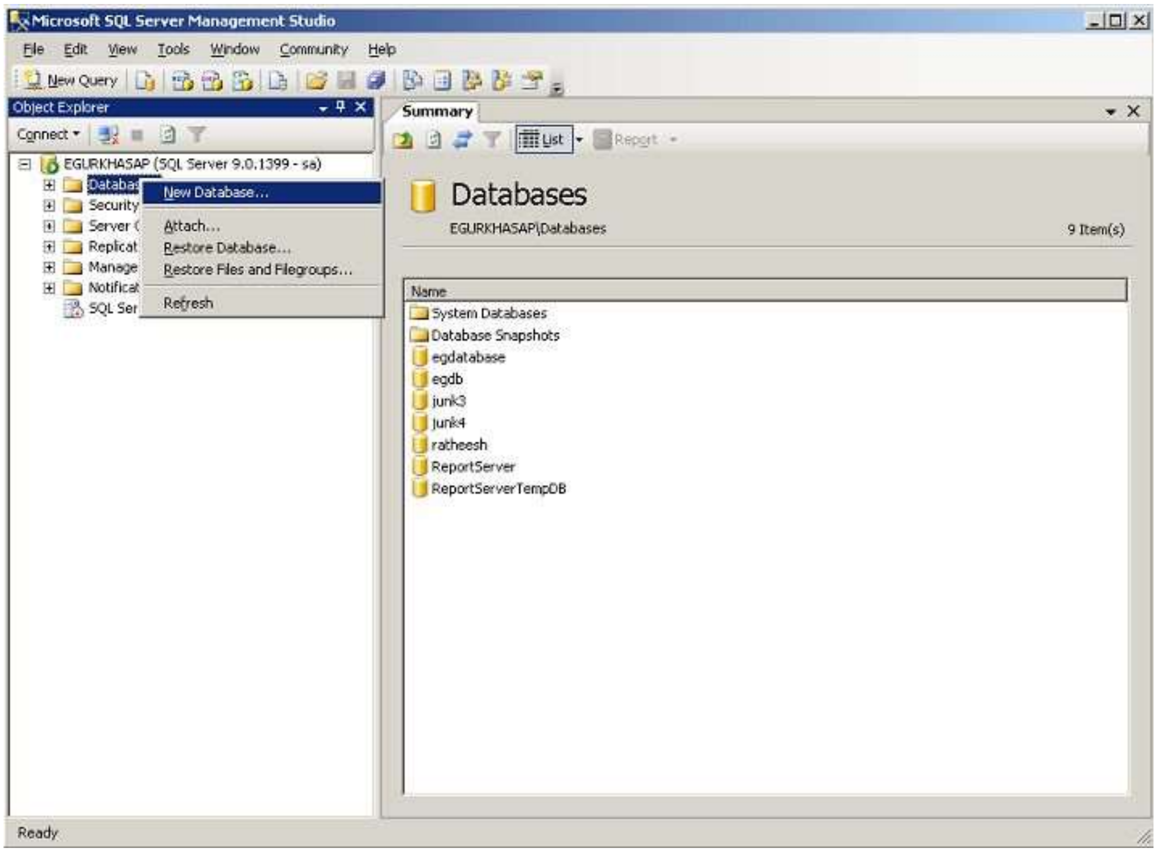
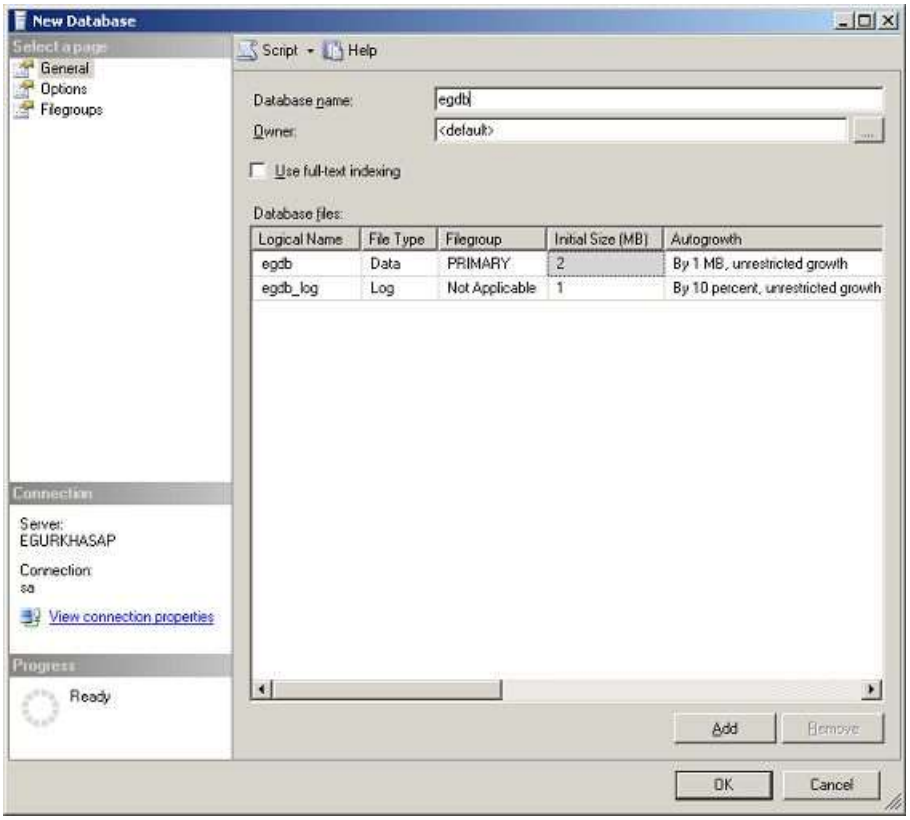


Figure 3.53: Selecting the New Database option

4. In the right pane of Figure 3.54 that appears, enter the name of the eG database and click the **Add** button therein.



Database name: egdb

Owner: <default>

☐ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth
egdb	Data	PRIMARY	2	By 1 MB, unrestricted growth
egdb_log	Log	Not Applicable	1	By 10 percent, unrestricted growth

Server:
EGURKHASAP

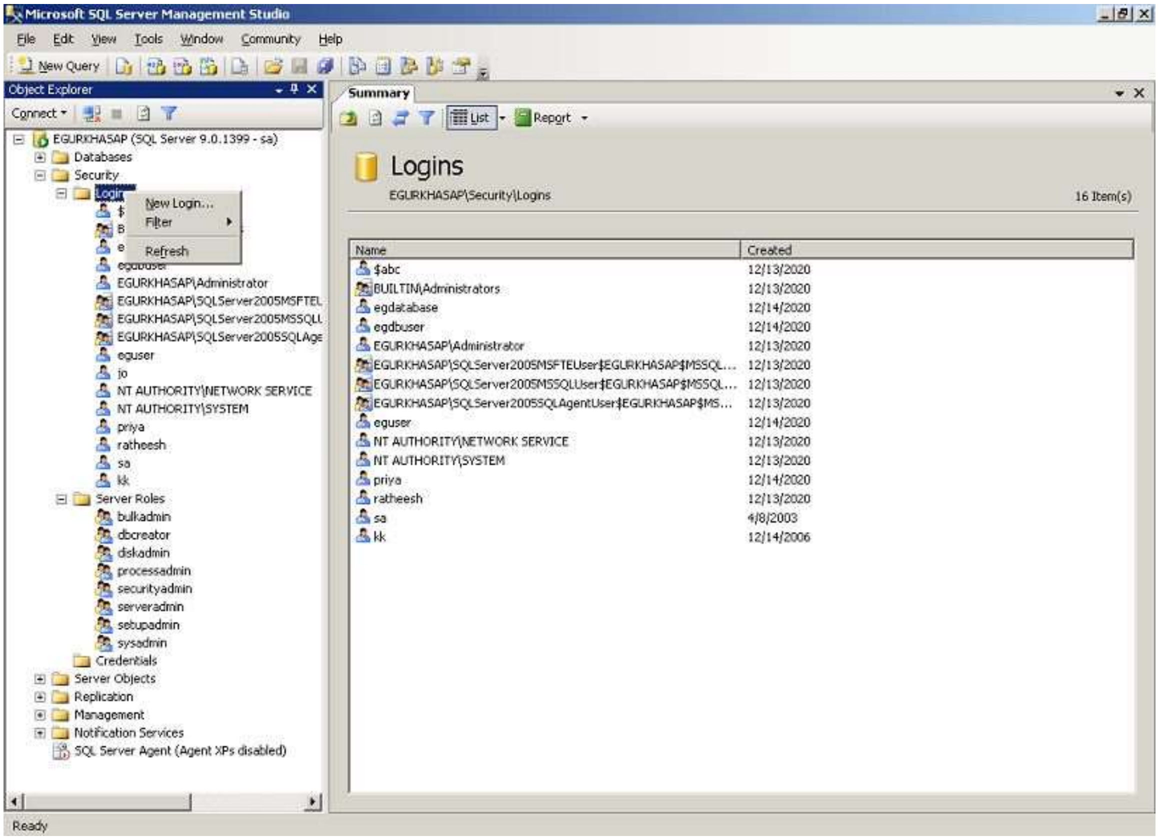
Connection:
sa

Ready

Figure 3.54: Creating the eG database

5. You will then return to the main window of the **Microsoft SQL Server Management Studio**.

6. Then, to create a new eG database user, expand the **Security** node in the tree-structure in the left pane, right-click on the **Logins** sub-node, and select the **New Login** option (see Figure 3.55).



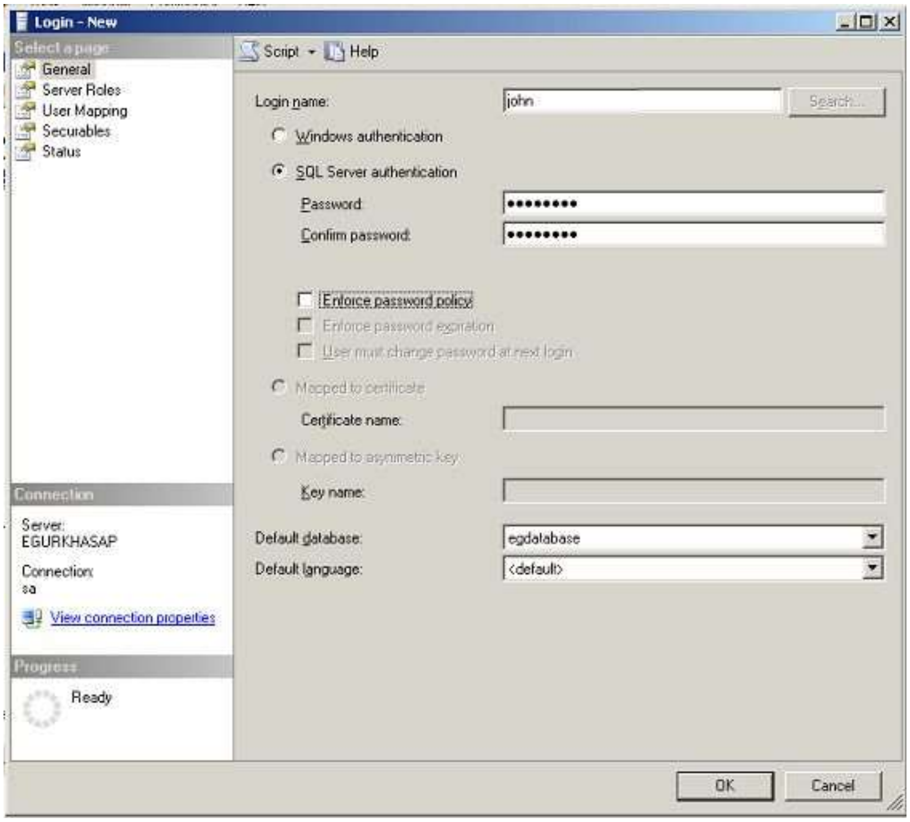
Logins

EGURKHASAP\Security\Logins 16 Item(s)

Name	Created
$abc	12/13/2020
BUILTIN\Administrators	12/13/2020
egdatabase	12/14/2020
egdbuser	12/14/2020
EGURKHASAP\Administrator	12/13/2020
EGURKHASAP\SQLServer2005MSFTEUser$EGURKHASAP$MSSQL...	12/13/2020
EGURKHASAP\SQLServer2005MSSQLUser$EGURKHASAP$MSSQL...	12/13/2020
EGURKHASAP\SQLServer2005SQLAgentUser$EGURKHASAP$MS...	12/13/2020
eguser	12/14/2020
NT AUTHORITY\NETWORK SERVICE	12/13/2020
NT AUTHORITY\SYSTEM	12/13/2020
priya	12/14/2020
ratheesh	12/13/2020
sa	4/8/2003
kk	12/14/2006

Figure 3.55: Selecting the New Login option

7. In Figure 3.56 that appears, specify the user name of the eG user, and then provide password for the user. If you have not provided a strong password, an error message such as the one shown in Figure 3.57 will appear. If you prefer, you override the password-related policies by deselecting the **Enforce password policy** check box in Figure 3.56. Doing so automatically disables the options below this check box.



Login name: john

○ Windows authentication

● SQL Server authentication

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

Certificate name:

○ Mapped to asymmetric key

Key name:

Default database: egdatabase

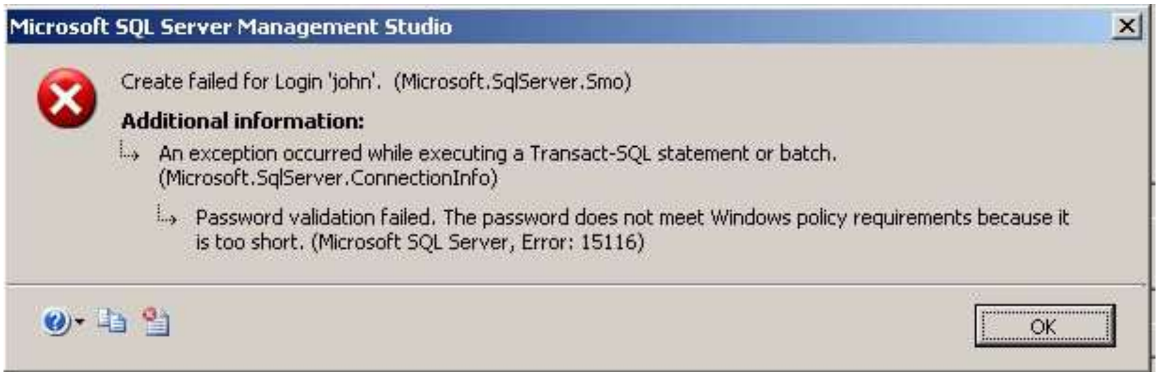
Default language: <default>

Server:
EGURKHASAP

Connection:
sa

Ready

Figure 3.56: Creating the eG database user



Create failed for Login 'john'. (Microsoft.SqlServer.Smo)

Additional information:

An exception occurred while executing a Transact-SQL statement or batch. (Microsoft.SqlServer.ConnectionInfo)

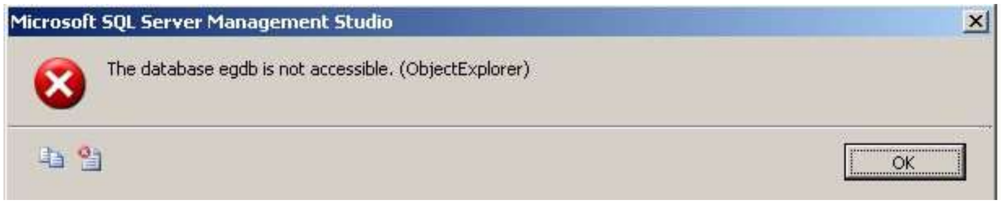
Password validation failed. The password does not meet Windows policy requirements because it is too short. (Microsoft SQL Server, Error: 15116)

Figure 3.57: The error message that appears if a strong password is not provided when the password policies are being enforced

8. Finally, register the changes, by clicking on the **OK** button in Figure 3.56.

9. Now, log out of the **Microsoft SQL Server Management Studio**, and relogin as the newly created eG user, say, *john*.

10. Try accessing the eG database that you had previously created, say *egdb*, by clicking on the corresponding database name under the **Databases** node in the left pane of the studio. Doing so, invokes the error message depicted by Figure 3.58.


Microsoft SQL Server Management Studio

The database egdb is not accessible. (ObjectExplorer)

Figure 3.58: The error message that appears if the eG user does not have access to the database that is to be used

11. This error message appears because the user *john* has not been allowed access to the *egdb yet*. To provide access to the *egdb* database to user *john*, login to the SQL Server Management Studio as the *sa* user. Then, expand the **Logins** sub-node in the **Security** node of the tree-structure in the left pane of the studio, right-click on the **john** node therein, and select **Properties** (see Figure 3.59).

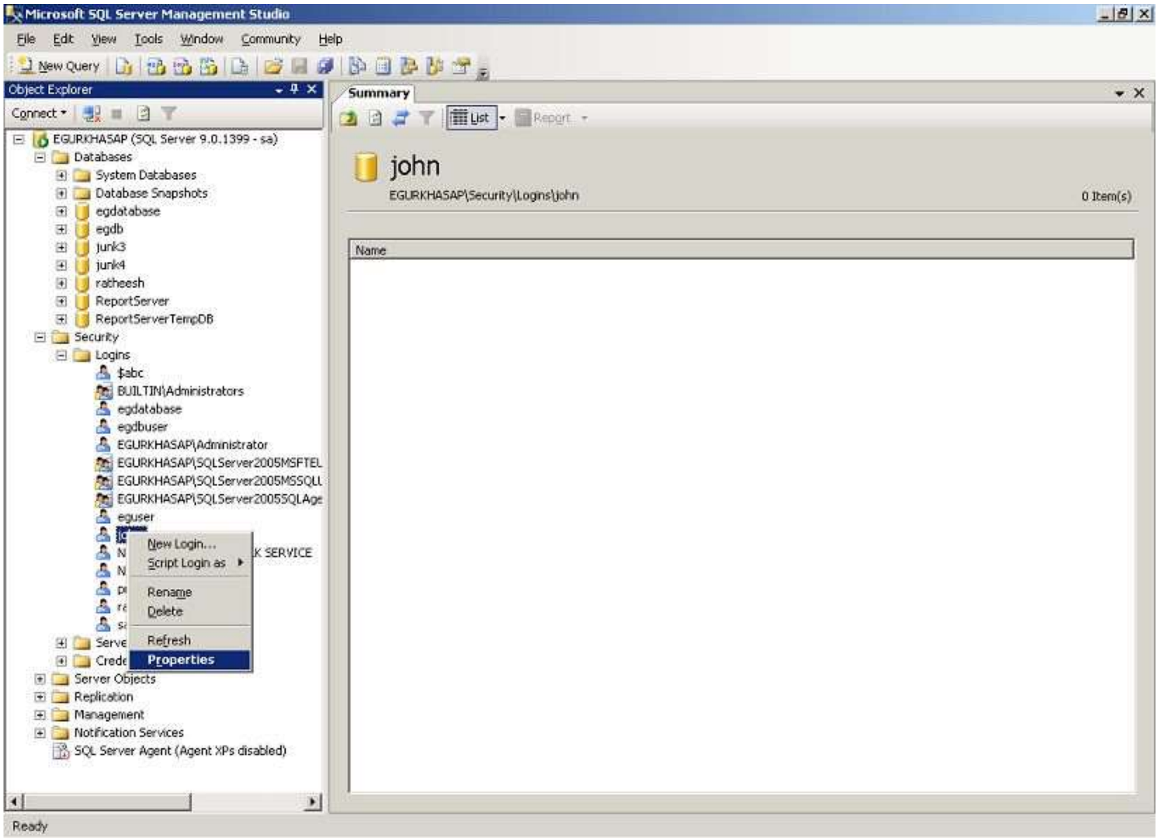
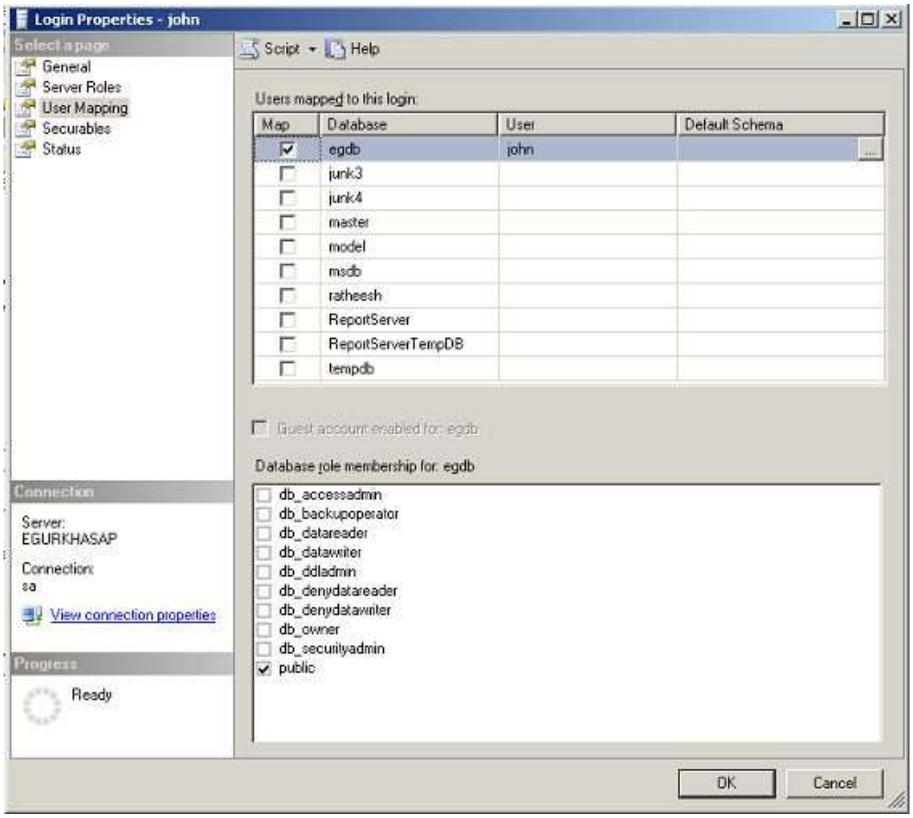


Figure 3.59: Selecting the Properties option of the eG user

12. Next, select the **User Mapping** option from the left pane of Figure 3.60 that appears. All the available databases will then be displayed in the right pane. Click on the **Map** checkbox preceding *egdb* in the database list to map the *egdb* database to user *john*.



Users mapped to this login:

Map	Database	User	Default Schema
☑	egdb	john	
□	junk3		
□	junk4		
□	master		
□	model		
□	msdb		
□	ratheesh		
□	ReportServer		
□	ReportServerTempDB		
□	tempdb		

□ Guest account enabled for: egdb

Database role membership for: egdb

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
□ db_owner
□ db_securityadmin
☑ public

Server:
EGURKHASAP

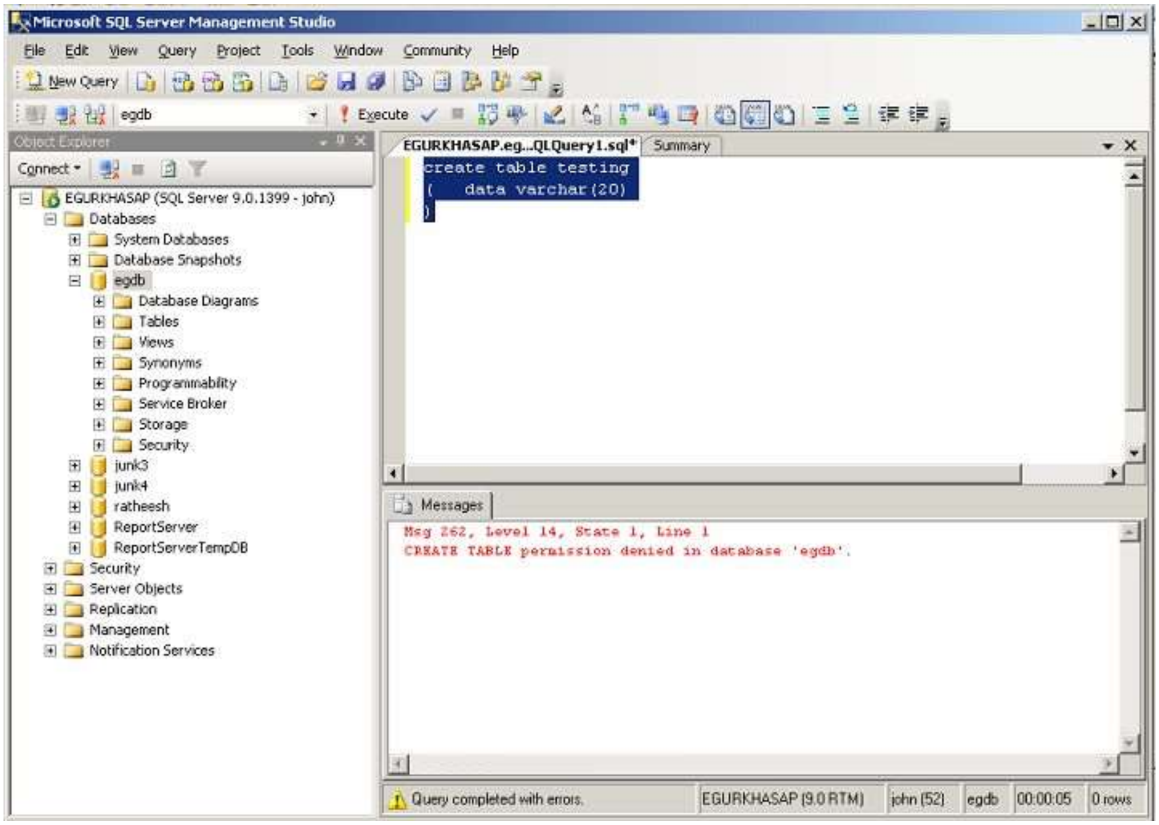
Connection:
sa

View connection properties

Figure 3.60: Mapping the eG database to the eG user

13. Finally, click the **OK** button to save the changes.

14. Next, try logging in as the eG user (*john* in this example) and executing a query on the *egdb* database. To attempt this, once you return to the main window of the studio, select *egdb* from the **Databases** node in the left pane of the studio, right-click on it, and pick the **New Query** option. Then, in the space provided in the right pane, build the query that you wish to execute (see Figure 3.61), and then click the **Execute** button on the toolbar.



```
create table testing
(    data varchar(20)
)
```

```
Msg 262, Level 14, State 1, Line 1
CREATE TABLE permission denied in database 'egdb'.
```

Figure 3.61: The eG user is executing a query on the eG database

15. The error message depicted by the **Messages** section of Figure 3.61 will then appear. This is because, the eG user *john* does not have the right to execute queries on the eG database, *egdb*. To grant table creation and query execution permissions to *john*, login to the SQL server using the *sa* credentials. Then, expand the **Databases** node in the tree-structure in the left pane of the studio, right-click on the **egdb** node within, and select **Properties** (see Figure 3.62).

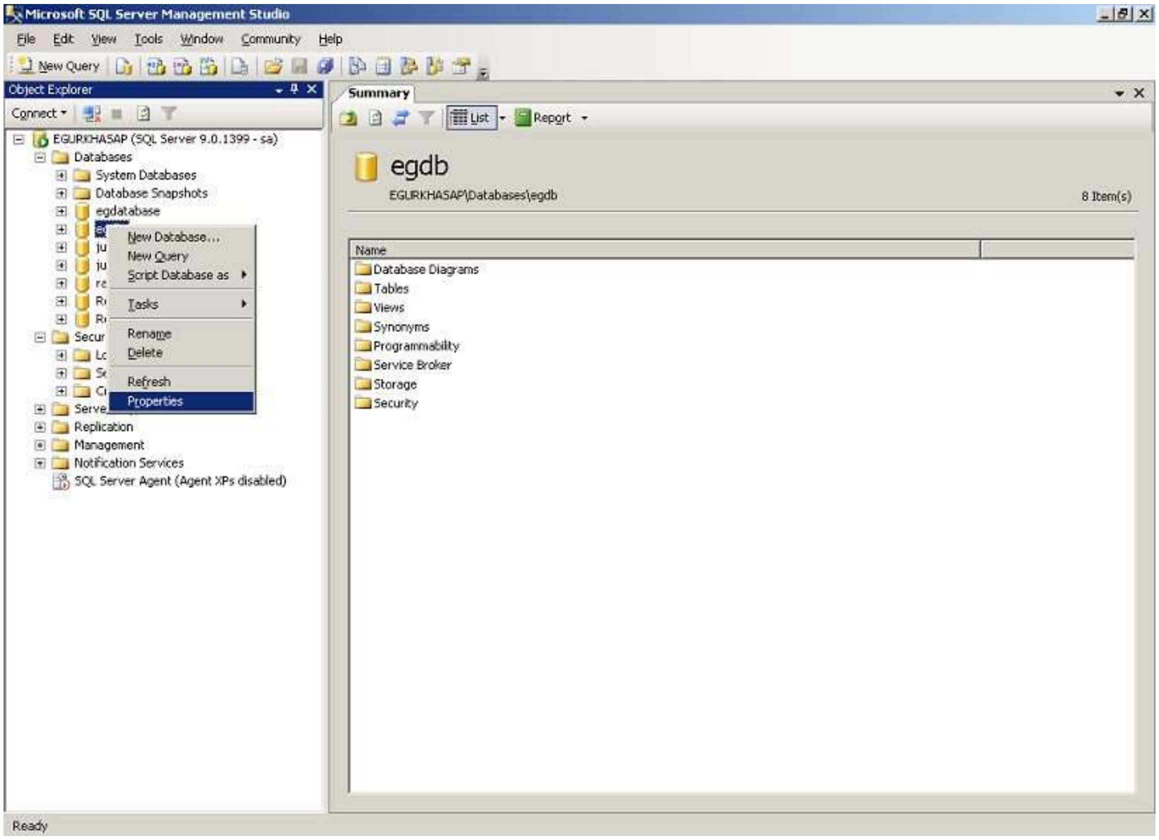
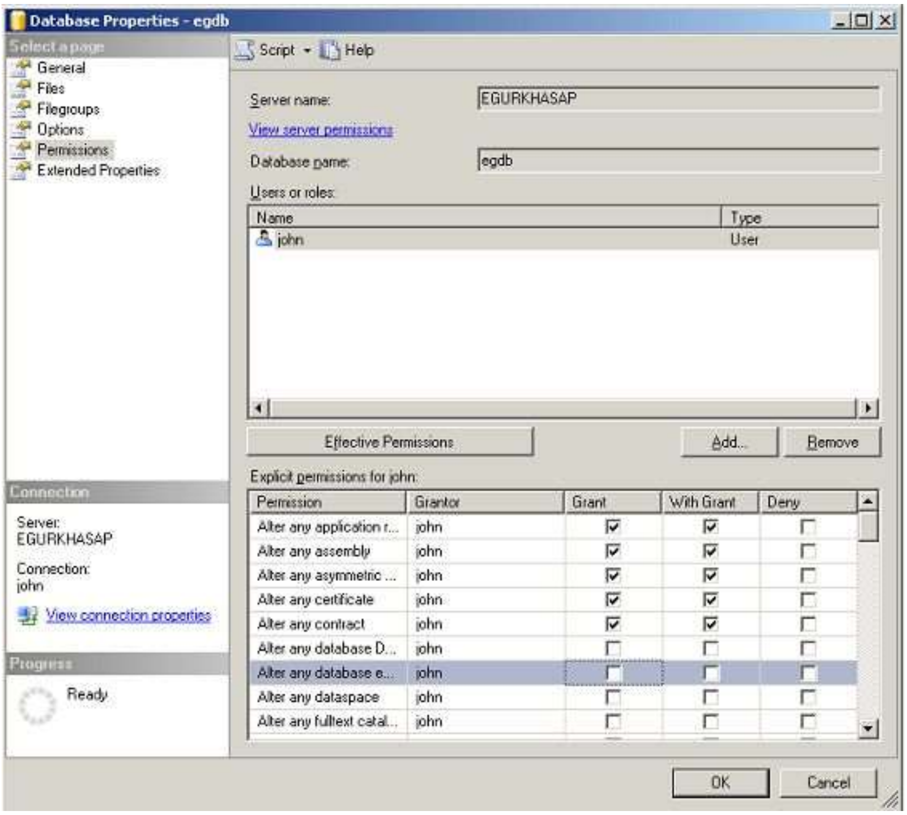


Figure 3.62: Selecting the Properties option of the eG database

16. From the left pane of the **Database Properties** window (see Figure 3.63) that opens, select **Permissions**. From the **Users or roles** list displayed in the right pane of Figure 3.63, select the eG user *john*. To grant all permissions to user *john*, click on the **Grant** check boxes against each of the privileges listed in the **Explicit permissions for john** section. When the **Grant** check box is clicked, the **With Grant** check box also gets selected.



Server name: EGURKHASAP

Database name: egdb

Users or roles:

Name	Type
john	User

Connection:
Server: EGURKHASAP
Connection: john

Explicit permissions for john:

Permission	Grantor	Grant	With Grant	Deny
Alter any application r...	john	☑	☑	□
Alter any assembly	john	☑	☑	□
Alter any asymmetric ...	john	☑	☑	□
Alter any certificate	john	☑	☑	□
Alter any contract	john	☑	☑	□
Alter any database D...	john	□	□	□
Alter any database e...	john	□	□	□
Alter any dataspace	john	□	□	□
Alter any fulltext catal...	john	□	□	□

Figure 3.63: Granting permissions to the eG user

17. Once all permissions are **Granted**, click on the **OK** button to register the changes.

18. Next, proceed to install the eG manager using the MS SQL Server 2005 backend. While doing so, remember to use the eG database and the eG database user which were manually created (i.e., *egdb* and *john* in our example).

As indicated earlier, if the eG manager installation fails, before clicking on the **OK** button to close the installation program, check the contents of the file **<EG_INSTALL_DIR>\manager\logs\error_log**. For example, once a user is created in the SQL database server, one of the password policies in effect may mandate that the user change his/her password before they can login. In such a case, the following error message is reported in the **error_log** file.

```
ERRORjava.sql.SQLException: Login failed for user 'eguser'.  Reason: The password of the account must be changed
```

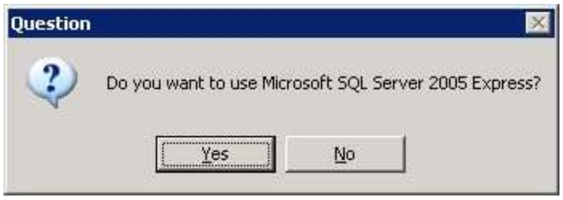
If the user does not have permission to access the database that has been specified during the installation process, the following error is logged:

```
ERRORjava.sql.SQLException: Cannot open database "egdb" requested by the login. The login failed.
```

3.1.5 Installing and Using MS SQL Server 2005/2008/2012 Server Express as the eG Backend

If you click **No** in Figure 3.22, it indicates that an MS SQL server is not already available in the target environment. If you are installing the eG manager on a Windows 2008/2012 server or a Windows Vista/7/8 host, then, upon the non-availability of an MS SQL server, the setup process will present you with the following options (see Figure 3.64):

- To exit the setup
- To install the Microsoft SQL Server 2005/2008/2012 Express, and use it as the eG backend



Question

Do you want to use Microsoft SQL Server 2005 Express?

Figure 3.64: A message box requesting your confirmation for quitting setup or installing MSDE

Clicking **No** in Figure 3.64 will terminate the eG manager configuration process. On the other hand, if **Yes** is clicked, then setup will install the MS SQL Server 2005/2008/2012 Express Edition, and create the eG database on it. Microsoft SQL Server 2005/2008/2012 Express Edition is a free, easy to use, redistributable version of SQL Server designed for building simple data-driven applications.

Note

MS SQL Server 2005/2008/2012 Express Edition can only serve as a temporary substitute for the MS SQL server, as it provides only limited storage and scalability capabilities. Owing to such constraints, it is strongly recommended that you restrict the usage of the Express edition to short-term monitoring of a relatively small number of components - to be precise, a maximum of 25 components. We also recommend that you acquire a licensed version of the MS SQL server as soon as possible, install the server, and migrate the eG database to it.

Before proceeding to install MS SQL Server 2005/2008/2012 Express Edition, ensure that the **hardware and software pre-requisites for installation are in place**.

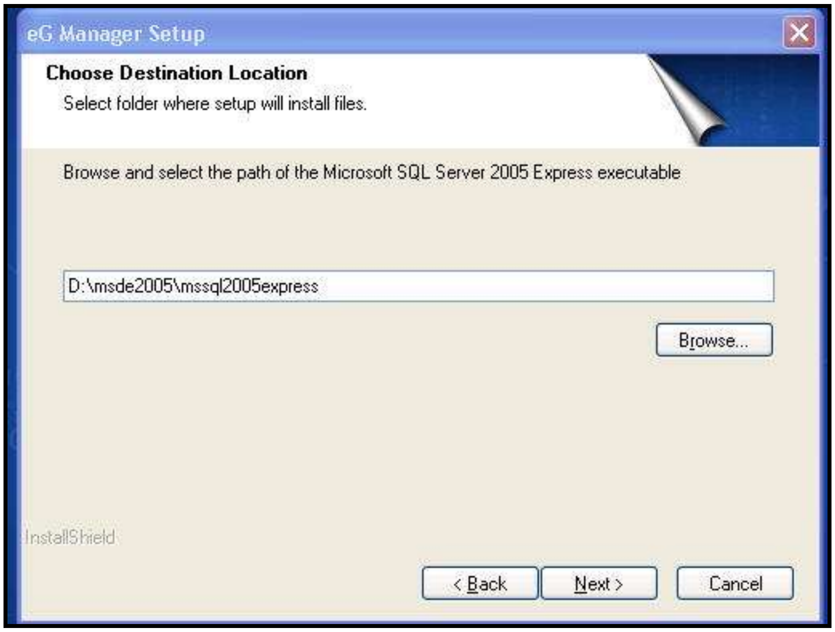
Once the software and hardware pre-requisites are fulfilled, download the free MS SQL Server 2005/2008/2012 Express Edition installable from the Microsoft web site. For instance, to download the MS SQL Server 2012 Express Edition, use the URL: **http://www.microsoft.com/en-in/download/details.aspx?id=29062** . Download the installable to any location on your local disk. Then, open the command prompt, and move to the directory to which you have downloaded the executable. Next, issue the following command at the prompt: **<ExecutableName>/x**

This command attempts to extract the installation-related files from the executable. When prompted for the directory to which the files are to be extracted, specify a directory on your local host and click the **OK** button therein to proceed with the extraction. All the necessary files will then be extracted from the executable into the specified directory.

Then, follow the steps given below:

1. Click on the **Yes** button in Figure 3.64 to confirm MS SQL Server 2005/2008/2012 Express installation.

2. In Figure 3.65 that appears, provide the full path to the MS SQL Server 2005/2008/2012 Express installable that was **extracted** to a directory on your local host. You can use the **Browse** button for this purpose. After specifying the path, click the **Next** button to move on.



eG Manager Setup
Choose Destination Location
Select folder where setup will install files.

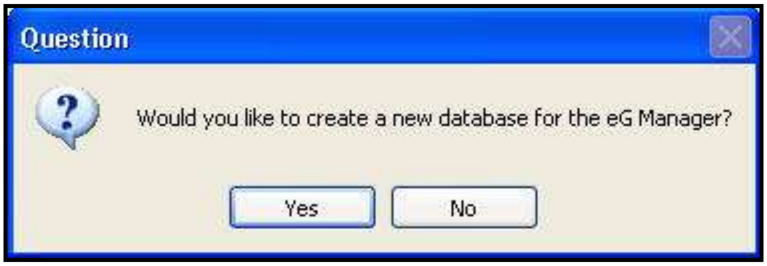
Browse and select the path of the Microsoft SQL Server 2005 Express executable

D:\msde2005\mssql2005express

Browse...
InstallShield
< Back
Next >
Cancel

Figure 3.65: Providing the path to the MS SQL Server 2005 Express executable

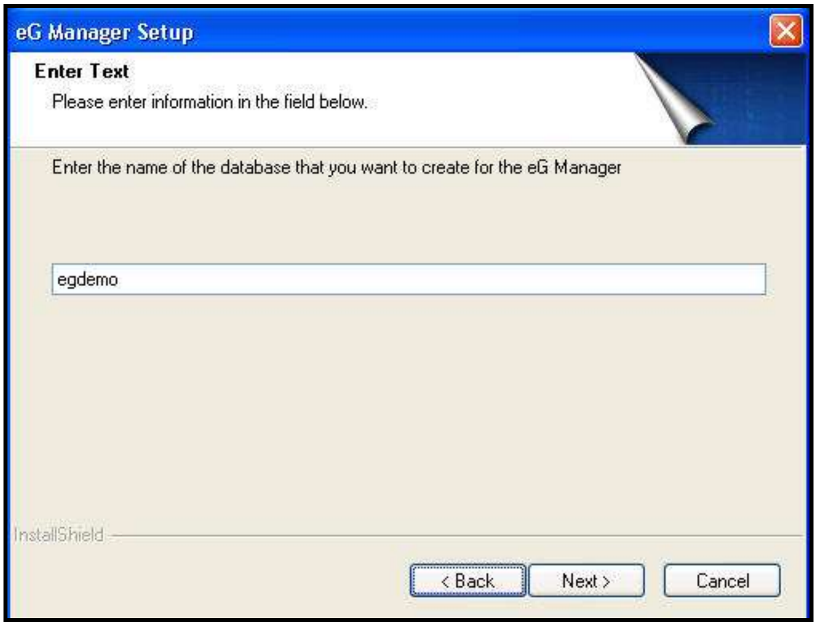
3. Next, click the **Yes** button in Figure 3.66 to create a new database for the eG manager on SQL Server Express Edition.



Would you like to create a new database for the eG Manager?

Figure 3.66: A message box requesting you to confirm whether/not a new database is to be created

4. Figure 3.67 then appears. Here, specify the name of the new database, and click the **Next** button to continue.



eG Manager Setup

Enter Text

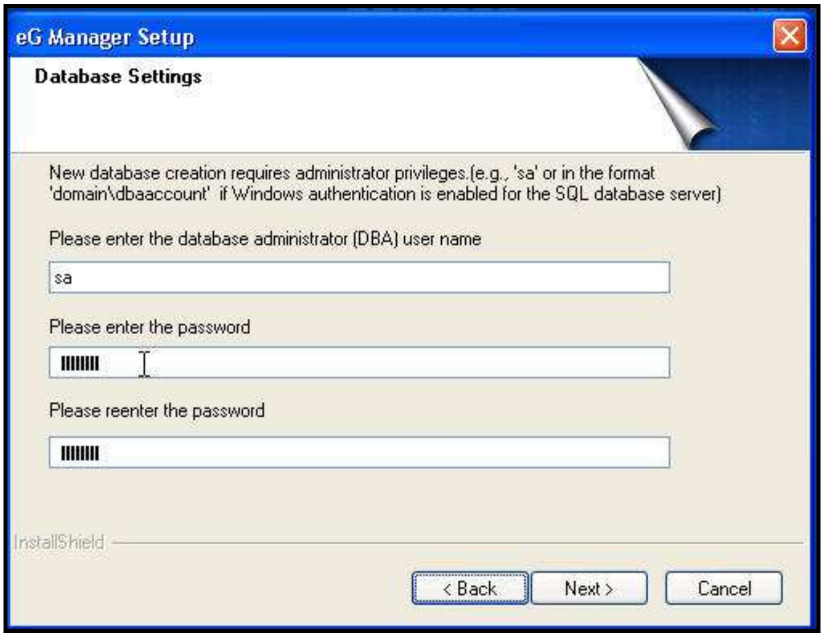
Please enter information in the field below.

Enter the name of the database that you want to create for the eG Manager

egdemo

Figure 3.67: Specifying the name of the new database for the eG manager

5. Since database creation requires administrator privileges, create a database administrator user with user name *sa* by specifying a password in Figure 3.68. Then, click the **Next** button therein.



eG Manager Setup

Database Settings

New database creation requires administrator privileges.(e.g., 'sa' or in the format 'domain\dbaaccount' if Windows authentication is enabled for the SQL database server)

Please enter the database administrator (DBA) user name

sa

Please enter the password

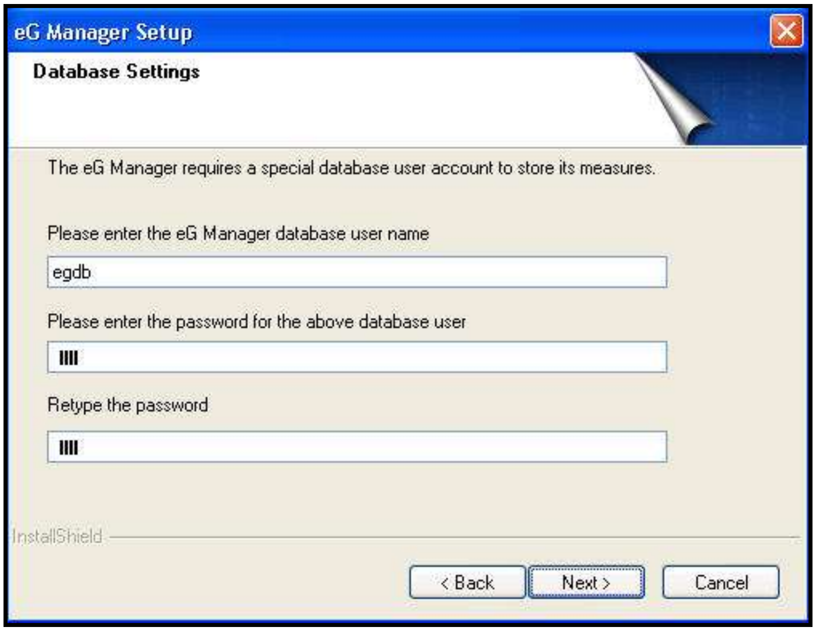
IIIIIII

Please reenter the password

IIIIIII

Figure 3.68: Creating a DBA with user name *sa*

6. Further, the eG manager needs a special database user account to store its measures. Therefore, provide the name and password of this special user in Figure 3.69 that appears next, and then click the **Next** button.



eG Manager Setup

Database Settings

The eG Manager requires a special database user account to store its measures.

Please enter the eG Manager database user name

egdb

Please enter the password for the above database user

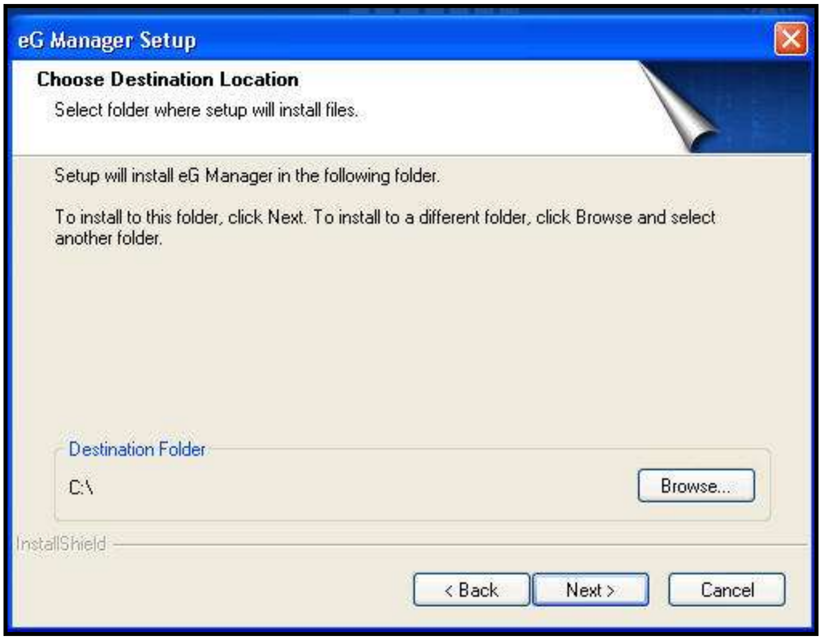
IIII

Retype the password

IIII

Figure 3.69: Creating a special database user account

7. Subsequently, specify the folder in which the eG manager is to be installed (see Figure 3.70), and click the **Next** button.



eG Manager Setup

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Manager in the following folder.

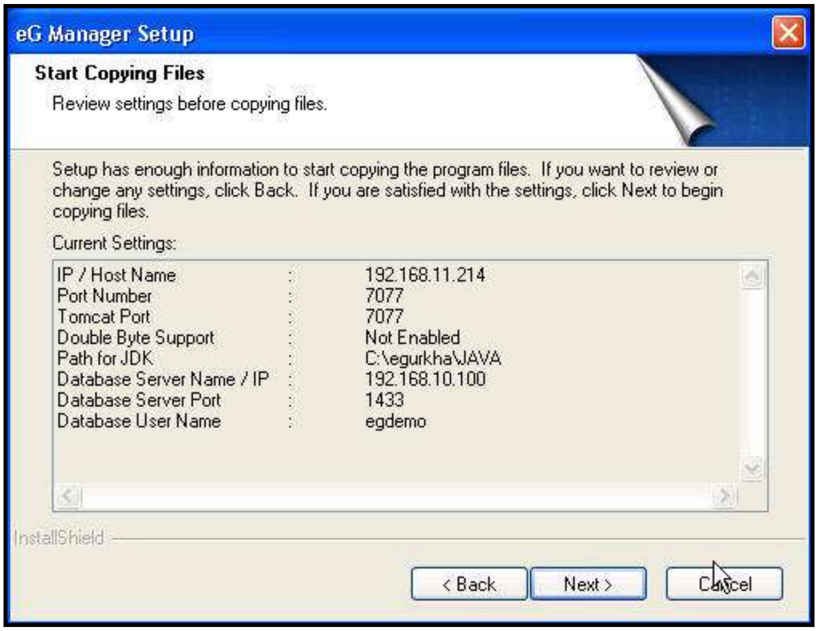
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 3.70: Specifying the eG manager install directory

8. A summary of the installation inputs that you have provided will then appear (see Figure 3.71). Review the inputs and click the **Next** button to resume setup.



eG Manager Setup

Start Copying Files

Review settings before copying files.

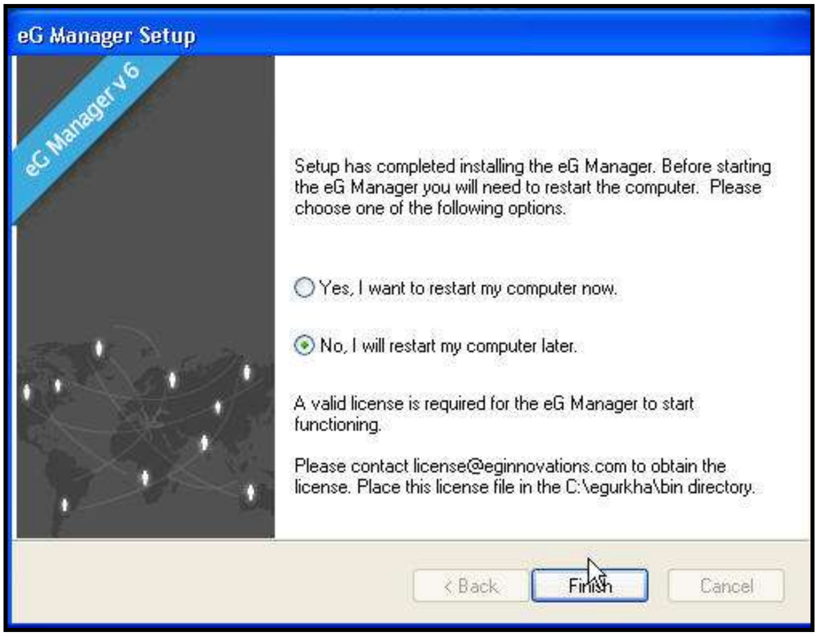
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
IP / Host Name             :    192.168.11.214
Port Number                :    7077
Tomcat Port                :    7077
Double Byte Support        :    Not Enabled
Path for JDK               :    C:\egurkha\JAVA
Database Server Name / IP  :    192.168.10.100
Database Server Port       :    1433
Database User Name         :    egdemo
```

Figure 3.71: Summary of the installation settings

9. If the configuration process succeeds, the following screen will be displayed (see Figure 3.71). The Setup requires the user to restart the system. This can be done immediately or at a later point of time. A valid license must be obtained for the eG manager to function. This license should be placed in the bin directory of the egurkha folder (for e.g., C:\Program Files\egurkha\bin). Clicking on the **Finish** button will exit the Setup.



eG Manager Setup

Setup has completed installing the eG Manager. Before starting the eG Manager you will need to restart the computer. Please choose one of the following options.

○ Yes, I want to restart my computer now.

● No, I will restart my computer later.

A valid license is required for the eG Manager to start functioning.

Please contact license@eginnovations.com to obtain the license. Place this license file in the C:\egurkha\bin directory.

Figure 3.72: Setup program indicating the completion of the eG manager installation

3.2 Silent Mode Installation of the eG Manager and Agents

Silent mode installation is a standard way to ensure repeatability of the installation process. Administrators use this process when installing the same software in multiple locations/servers.

Usually, the process of a silent install involves saving all the configurations/inputs provided and reapplying these during subsequent installation without human intervention. The key advantages of a silent install are repeatability, and the prevention of human errors that may occur during manual installation.

3.2.1 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 *eG Installation Guide* 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.

3.2.2 Silent Mode Installation of the eG Agent

To install an eG agent on Windows in the silent mode, the following broad steps need to be followed:

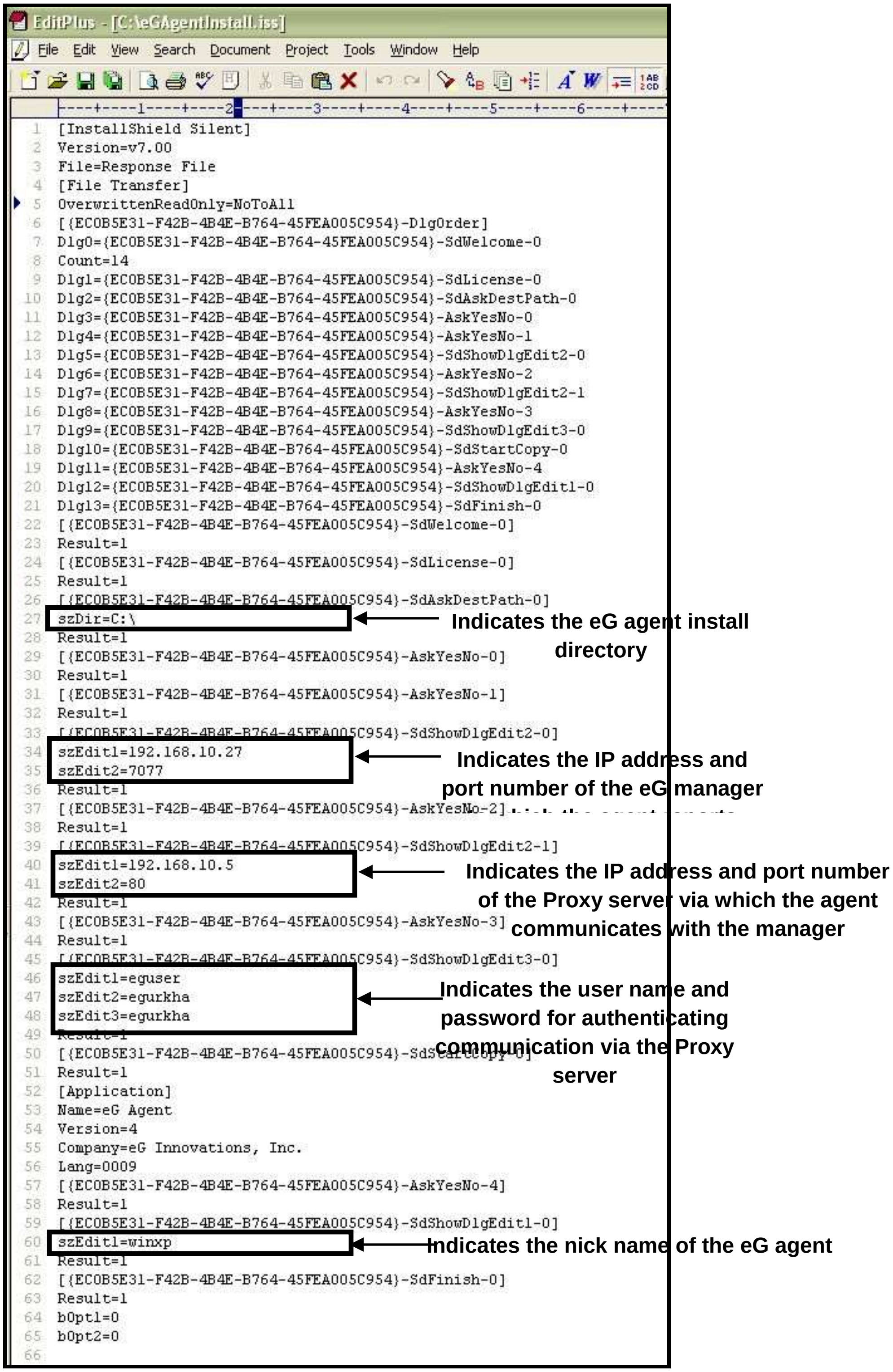
- Create the silent mode script for the agent installation;
- Use the script along with the eG agent executable to install agents on other hosts

Each of these steps has been explained in-depth in the sections below.

3.2.2.1 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 *eG Installation Guide* for the detailed procedure for installing an eG agent on Windows in the normal mode.
4. Figure 3.73 depicts a sample script file and explains its key components.



```
[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 3.73: Contents of the script file

3.2.2.2 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.

3.2.2.2.1 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.

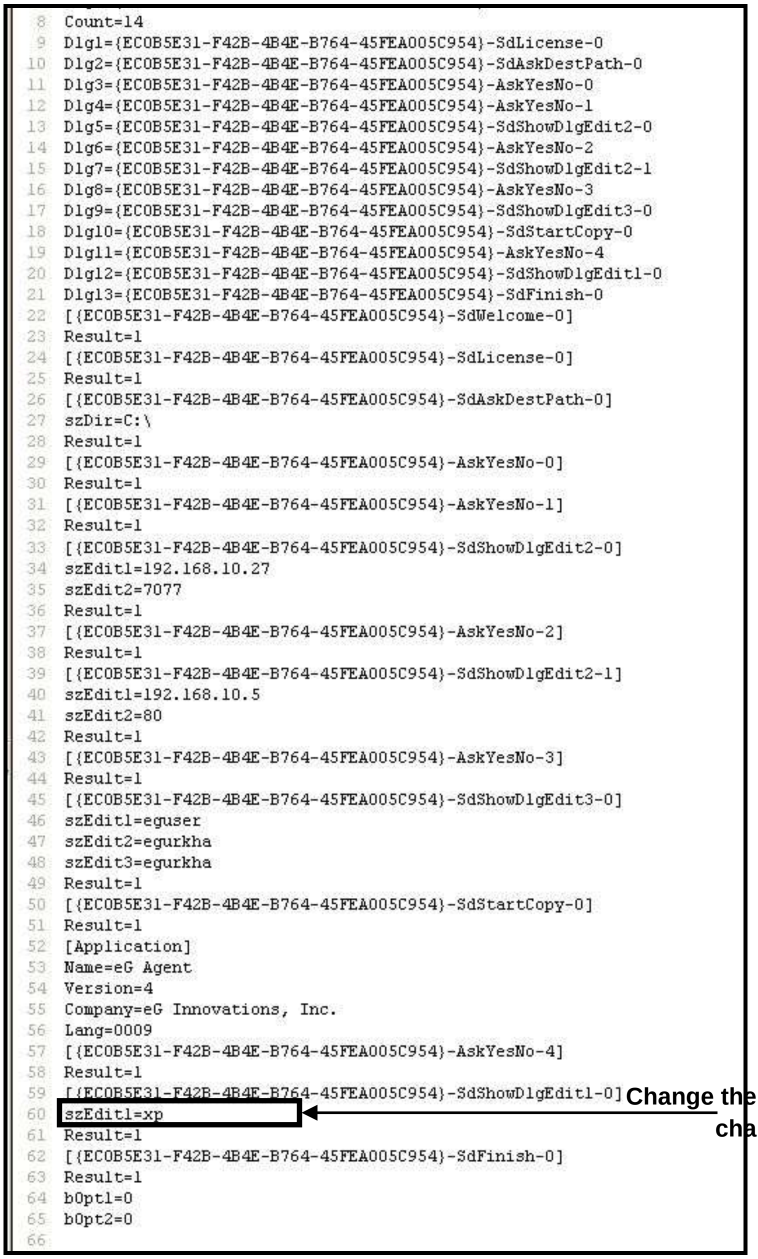
3.2.2.2.2 Silent Mode Installation of an eG Agent after making Minor Changes to the Script File

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.



```
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 3.74: 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 3.2.2.2.1 above.

3.2.2.2.3 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 3.2.2.1, and then use it to install the eG agent. The procedure for installation is the same as discussed in Section 3.2.2.2.1 above.

3.2.2.3 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 *eG Installation Guide* 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 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**, steps 12 to 22 of Section 2.2 will follow.

3.4 SSL-Enabling the eG Manager

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:

- 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)

- 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 Section 3.4.1. If you pick option (b), use the procedure detailed in Section 3.4.2.

3.4.1 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.

3.4.1.1 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* **2048** *-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.

3.4.1.2 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**

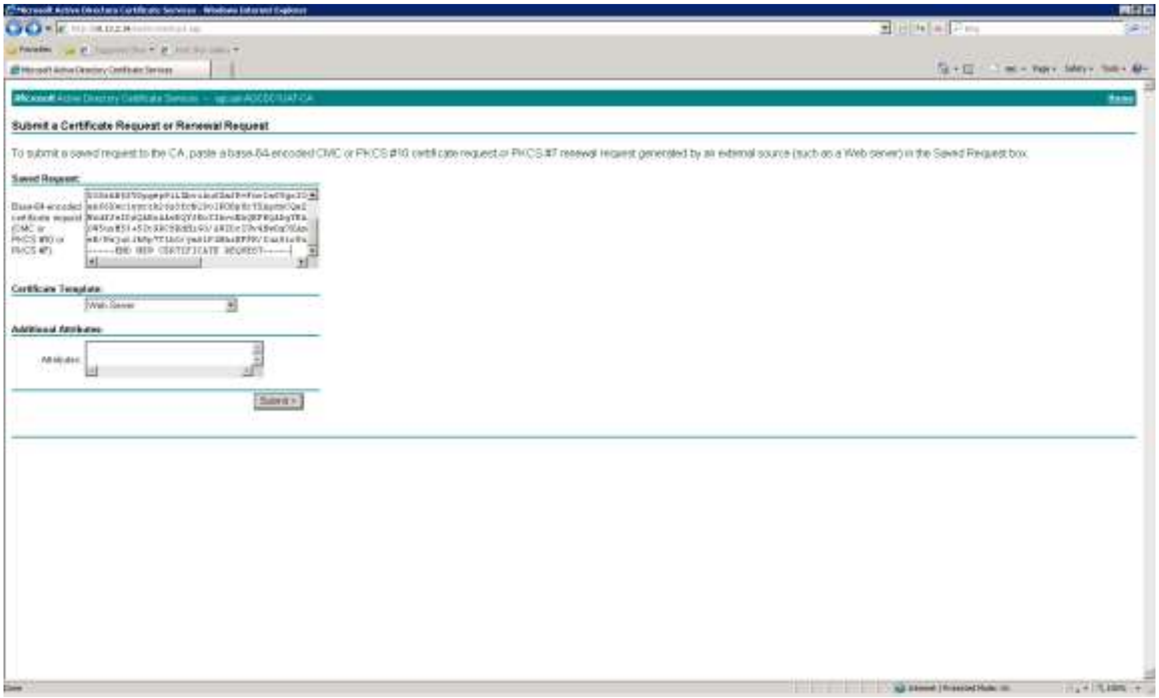
   The text in **Bold** in the above command line indicates those inputs that can change according to the requirements of your environment. These inputs have been described below:

   - **-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 3.4.1.1 of this document).**
   - **-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 3.4.1.1**
   - **-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 3.4.1.1 of this document).** 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 3.4.1.1 of this document)**.

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.

3.4.1.3 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 3.75 will then appear.


Microsoft Active Directory Certificate Services - Windows Internet Explorer
Favorites
Microsoft Active Directory Certificate Services
Microsoft Active Directory Certificate Services -- egcuatAGCDCTUAT-CA
Home
Submit >

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): -----END NEW CERTIFICATE REQUEST-----

Certificate Template: Web Server

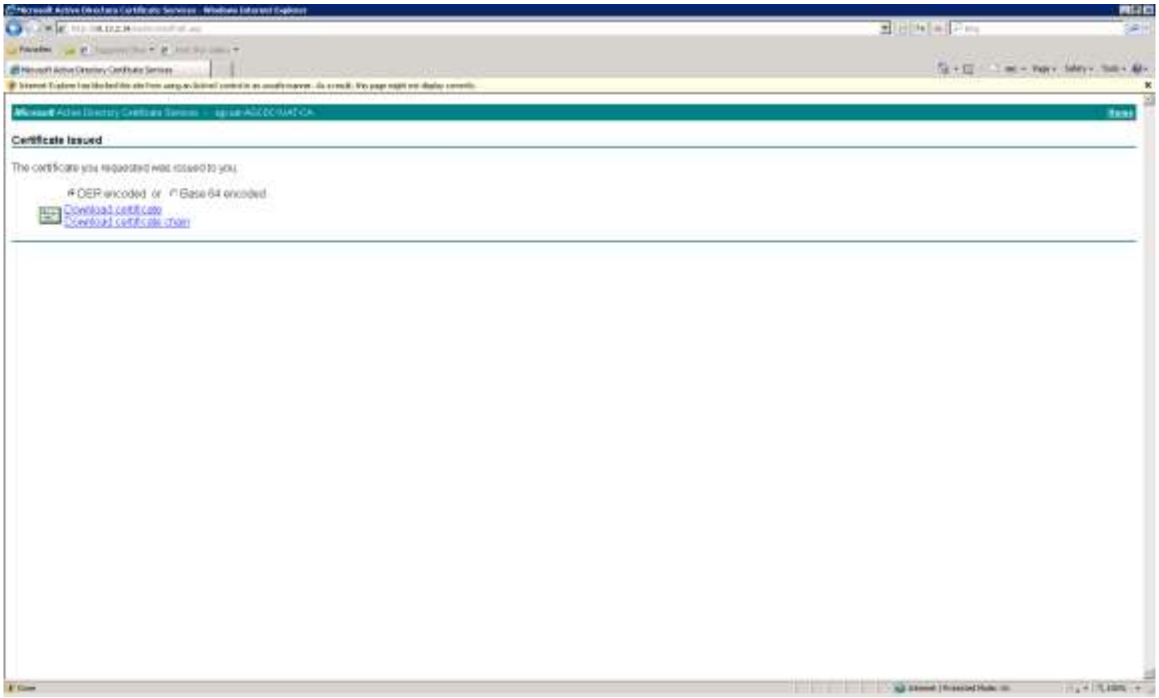
Additional Attributes:

Attributes:

Figure 3.75: Requesting for a certificate

2. Open the text file containing the certificate request (which was created using the procedure detailed in Section 3.4.1.2 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 3.75. Then, click the **Submit** button.

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



Microsoft Active Directory Certificate Services - Windows Internet Explorer

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

Figure 3.76: Downloading the certificate

3.4.1.3.1 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 3.4.1.1)** **.**
- **-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 3.4.1.1 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. 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 3.4.1.1 above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 3.4.1.1 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 3.4.1.1 above.
- **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 3.4.1.1 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 3.4.1.1) **.**
- **-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 3.4.1.1 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 3.4.1.1 **of this document.**
   - **-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 3.4.1.1 of this document**

3.4.1.3.2 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"
                       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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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>"  />
```

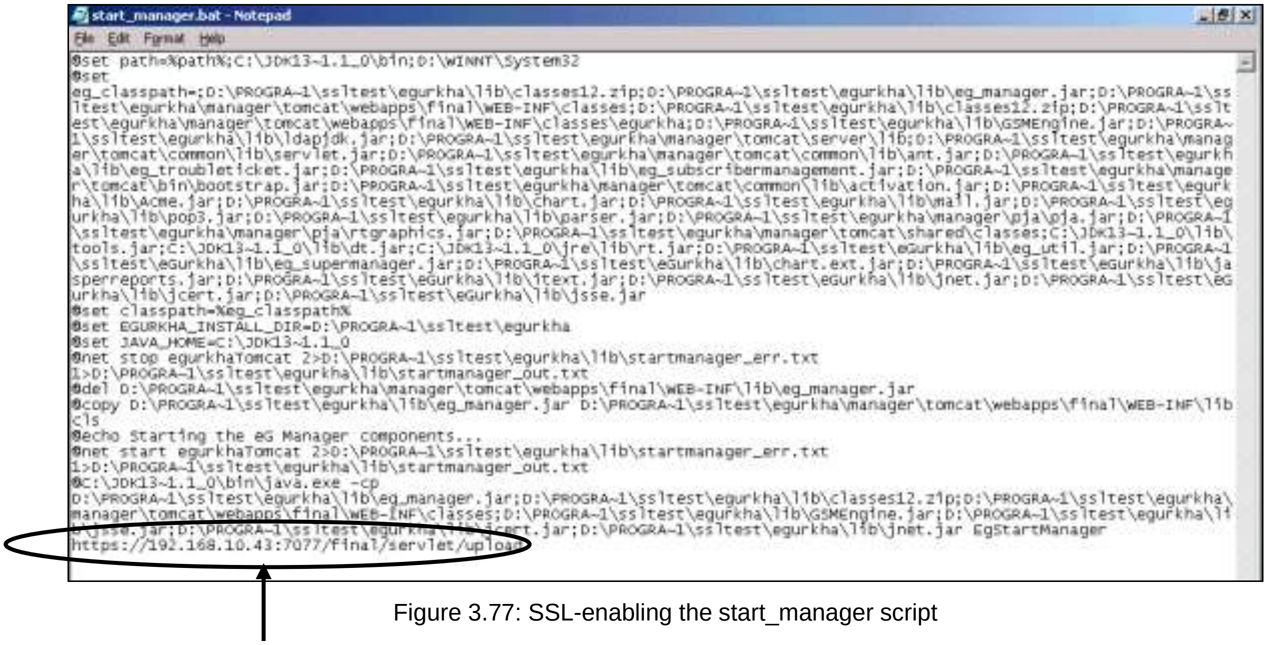
Set the *port* parameter in the XML block to reflect the SSL port number that you have configured for the eG manager. Also, note that three new parameters, namely - **keyAlias**, **keystoreFile** and **keystorePass** - have been inserted into the SSL block. While the **keystoreFile** parameter has to 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 3.4.1.1 above.

4. 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,app
lication/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml" server="eG Tomcat Server"/>
    -->
```

5. Save the file.

6. Then, SSL-enable the **start_manager.bat** script. For this, first open the **start_manager.bat** file (see Figure 3.77) 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 3.76).



```
@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\egurkha\lib\startmanager_err.txt
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.txt
@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 3.77: SSL-enabling the start_manager script

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

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 **<EG_INSTALL_DIR>\manager\config** directory) begins with **https://** instead 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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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.

3.4.2 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:

1. Generating the keystore file
2. Generating a certificate request
3. Submitting the certificate request to the Certificate Authority (CA) and obtaining a certificate
4. Importing the certificate into a keystore
5. Configuring Tomcat for using the keystore file

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

3.4.2.1 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* **2048** *-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.

3.4.2.2 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 3.4.2.1 of this document).**
   - **-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 3.4.2.1**
   - **-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 3.4.2.1 of this document).** 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 3.4.2.1 of this document).**

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.

3.4.2.3 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.

3.4.2.4 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. 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 3.4.2.1) .**
   - ➢ **-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 3.4.2.1 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 3.4.2.1 above.
   - **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 3.4.2.1 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 3.4.2.1 above.
- **-keypass** and **–storepass** : Provide the same **keypass** and **storepass** that you specified when generating the keystore; refer to Section 3.4.2.1 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 3.4.2.1**) **.**
   - **-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 3.4.2.1 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 3.4.2.1 of this document.**
- **-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 3.4.2.1 of this document**

3.4.2.4.1 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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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,app
lication/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_W
ITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA25
6,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>"  />
```

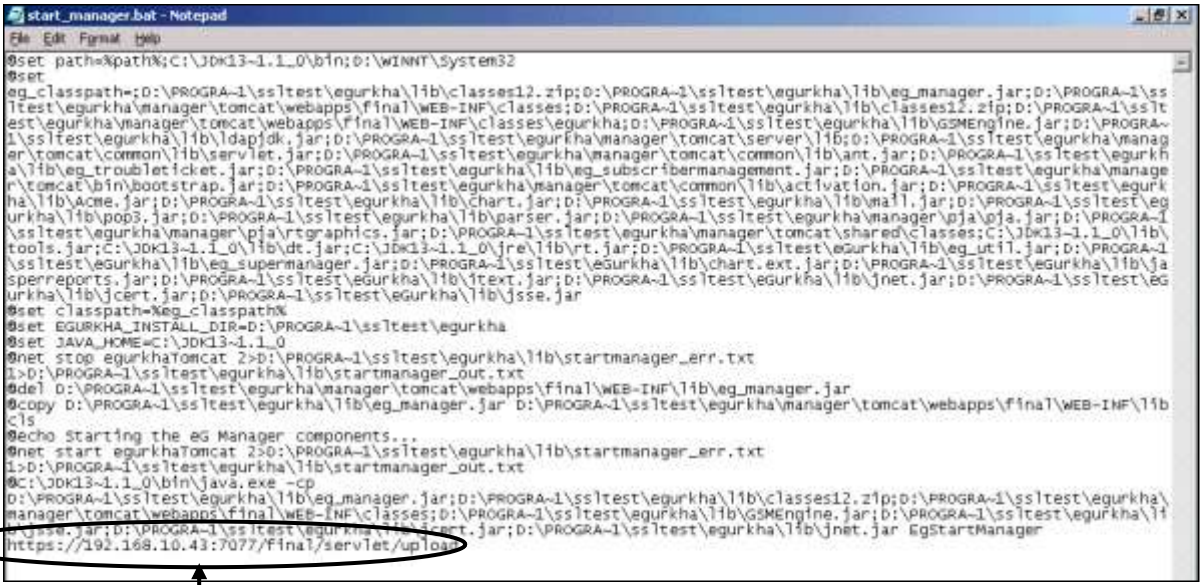
Set the *port* parameter in the XML block to reflect the SSL port number that you have configured for the eG manager. Also, note that three new parameters, namely - **keyAlias**, **keystoreFile** and **keystorePass** - have been inserted into the SSL block. While the **keystoreFile** parameter has to 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 3.4.1.1 above.

4. 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,app
lication/pdf,application/x-
javascript,application/javascript,application/json,application/x-shockwave-
flash,application/xhtml+xml,application/xml+xhtml" server="eG Tomcat Server"/>
    -->
```

5. Save the file.

6. Then, SSL-enable the **start_manager.bat** script. For this, first open the **start_manager.bat** file (see Figure 3.77) 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 3.76).



```
@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\egurkha\lib\startmanager_err.txt
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.txt
@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 3.78: SSL-enabling the start_manager script

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

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 **<EG_INSTALL_DIR>\manager\config** directory) begins with **https://** instead of **http://**. Then, save the file.

8. Finally, start the eG manager.

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.

Note

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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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_WI
TH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TL
S_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.

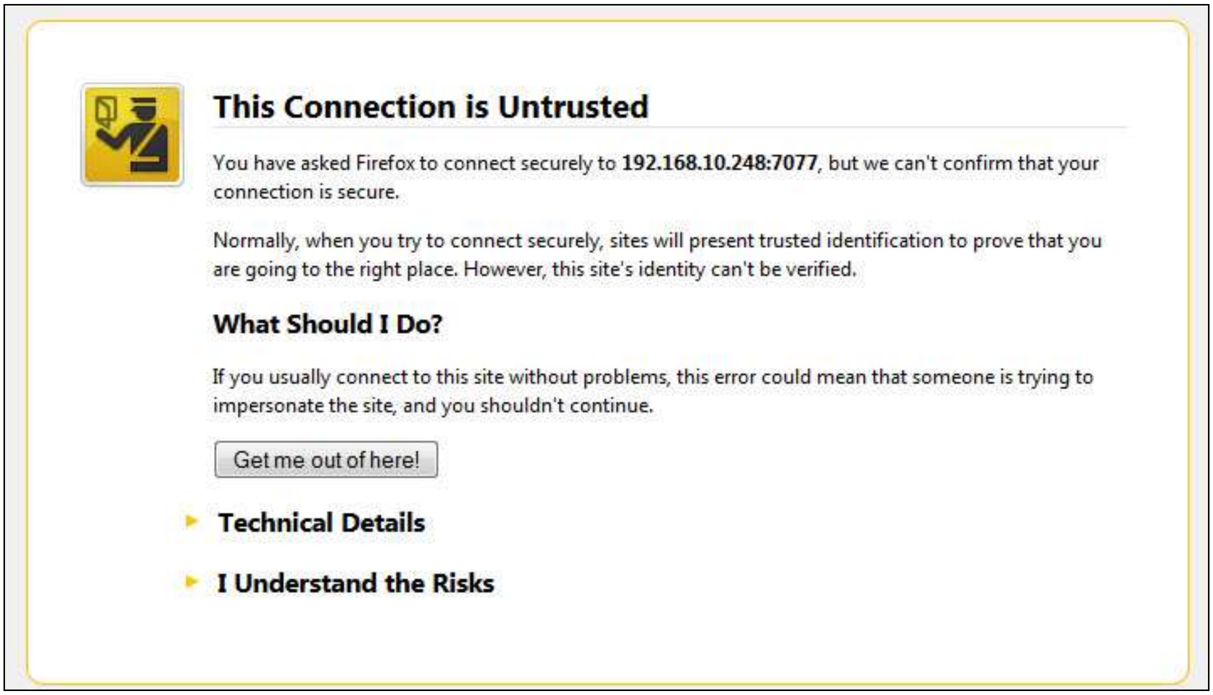
- If you had SSL-enabled the eG manager using the default certificate that eG provides, then, once the above changes are made, copy the default certificate from the **<EG_INSTALL_DIR>\bin\latest_certificate** folder (on Windows; on Unix, this will be the **/opt/egurkha/bin/latest_certificate** folder), 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.

3.4.3 Troubleshooting 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.

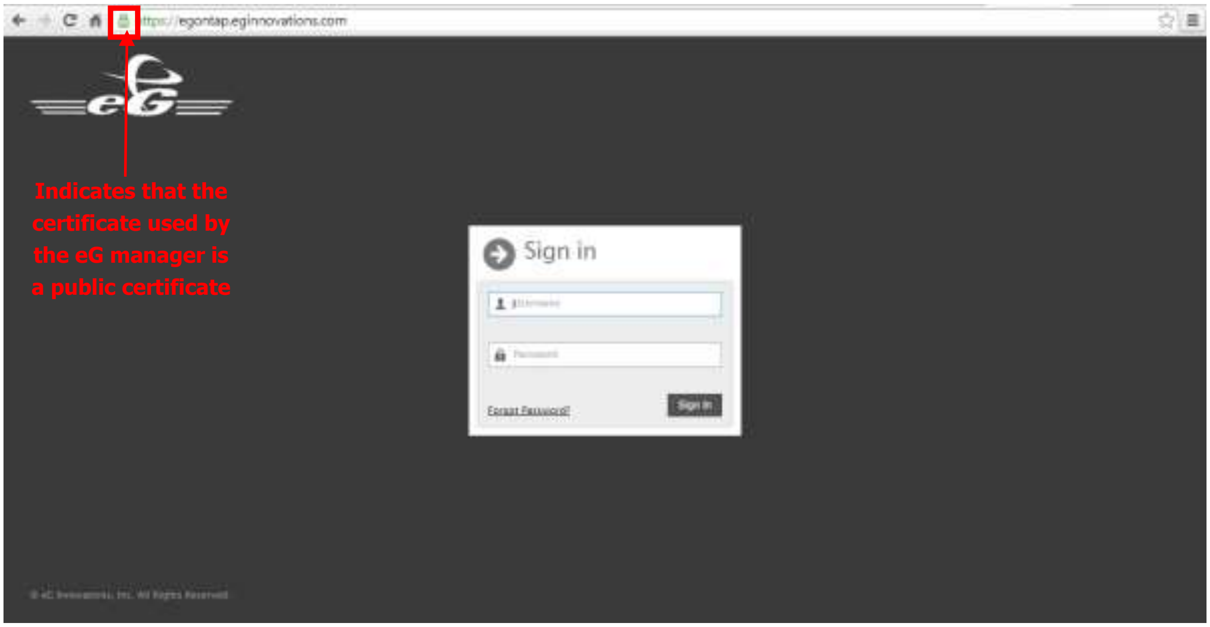
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

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 3.79: The error message that appears when connecting to an eG manager using a self-signed SSL certificate

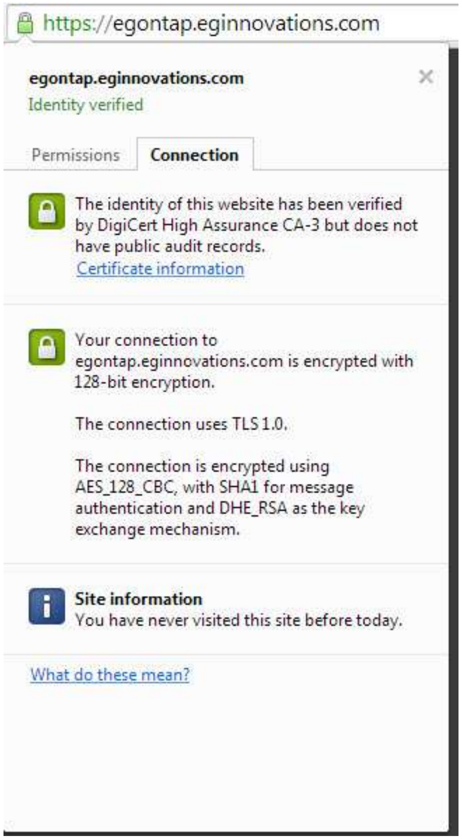
A public certificate on the other hand is a trusted certificate issued by a valid Certificate Authority. If such a certificate is used to SSL-enable an eG manager, then, a 'lock' symbol will appear in the address bar of the browser when attempting to connect to that manager (see Figure 3.80).



Indicates that the certificate used by the eG manager is a public certificate

Figure 3.80: 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 3.81).



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.

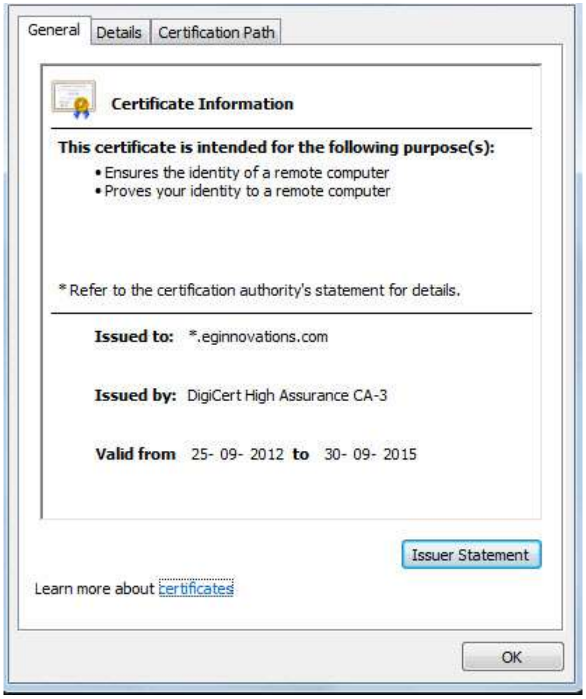
Site information

You have never visited this site before today.

What do these mean?

Figure 3.81: Viewing the connection details

To view the certificate details, click the **Certificate Information** link in Figure 3.81. Figure 3.82 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

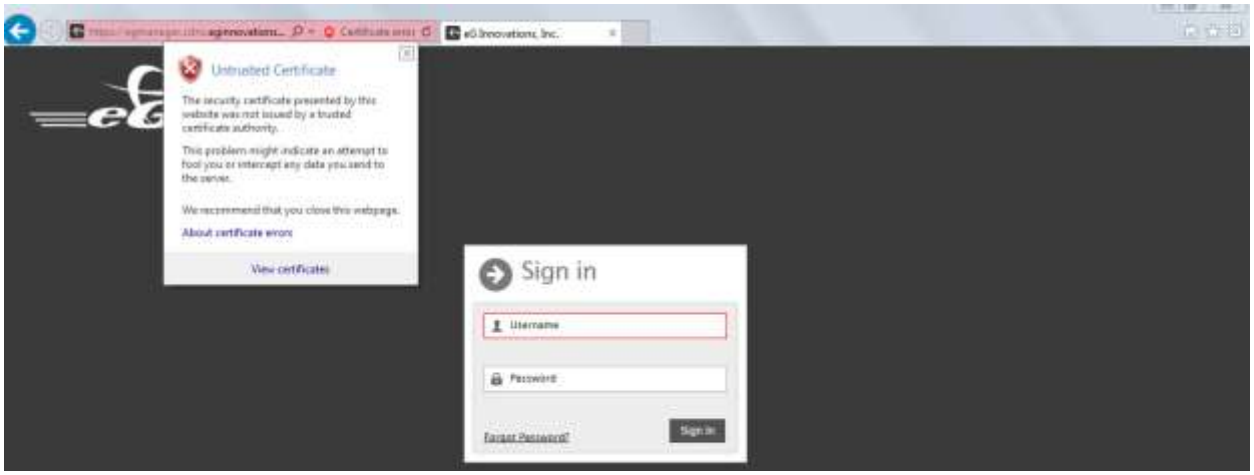
Figure 3.82: Viewing the Certificate information

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 3.83: 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 3.84) to import the certificate to the browser.

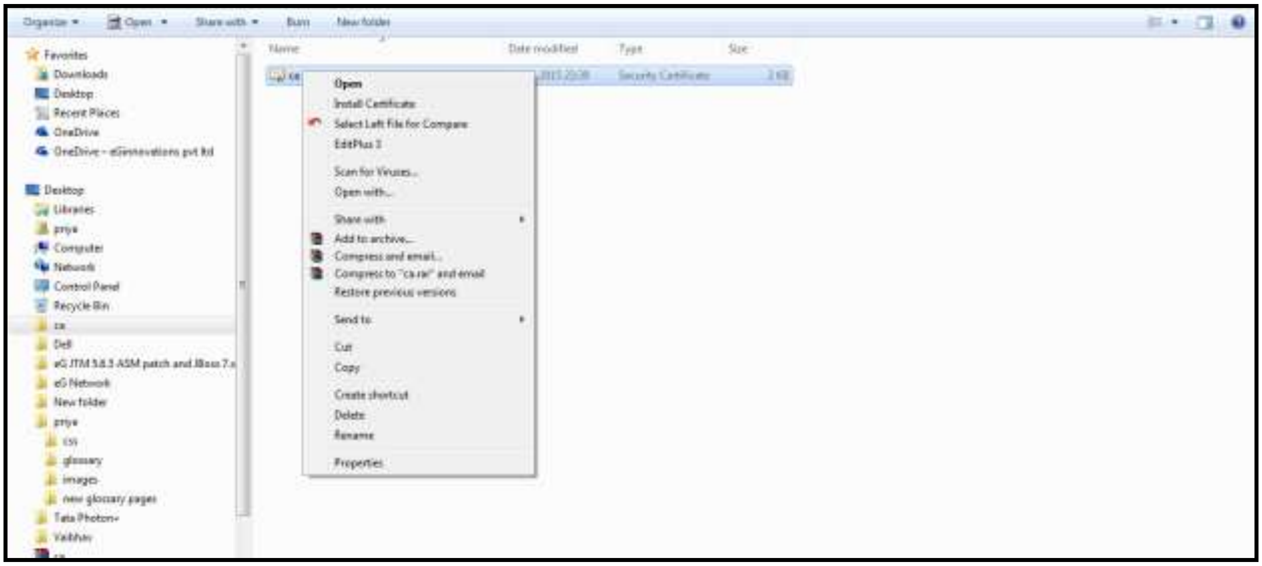
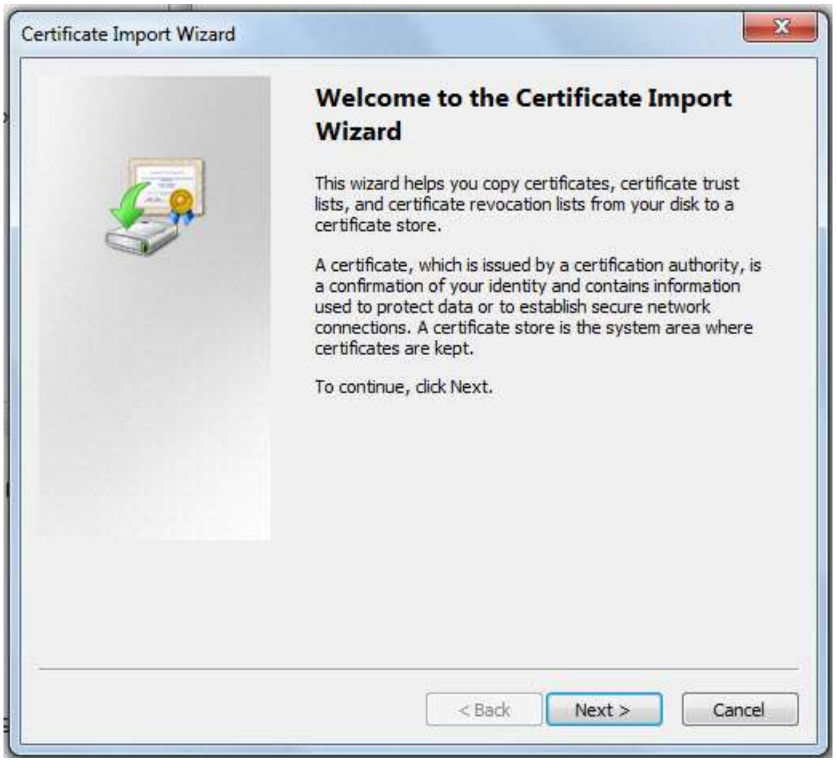


Figure 3.84: Selecting the option to install the certificate on the browser host

3. Figure 3.85 will then appear. Click **Next** here to continue.



Welcome to the Certificate Import Wizard

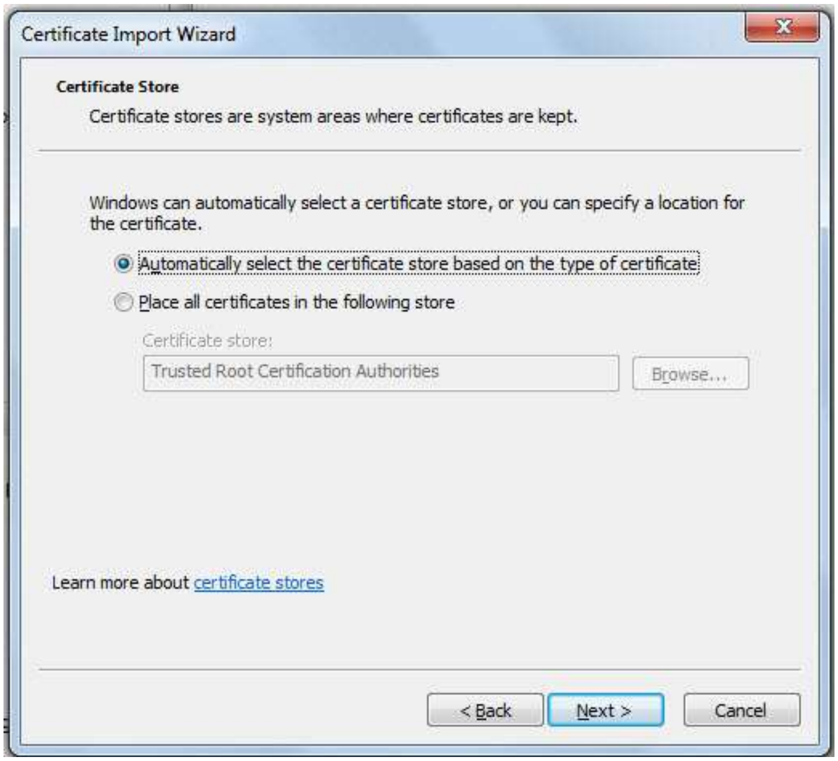
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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 3.85: Welcome screen of the Certificate Import Wizard

4. Figure 3.86 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

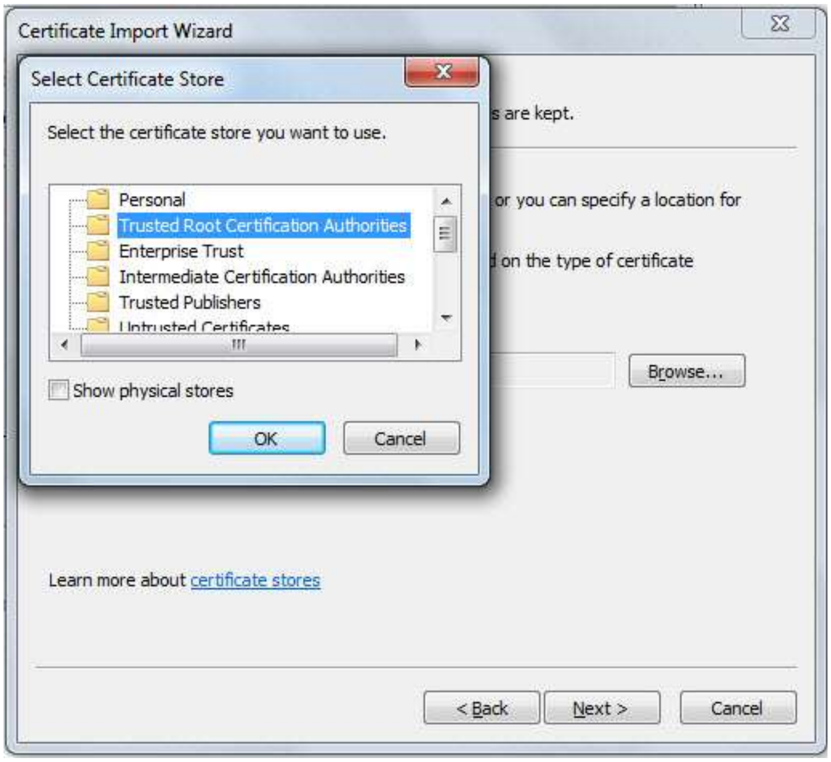
Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

Figure 3.86: Choosing to place the certificate in a specific store

5. From Figure 3.87 that then appears, select the **Trusted Root Certificate Authorities** store and click **OK**.



Certificate Import Wizard

Select Certificate Store

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.

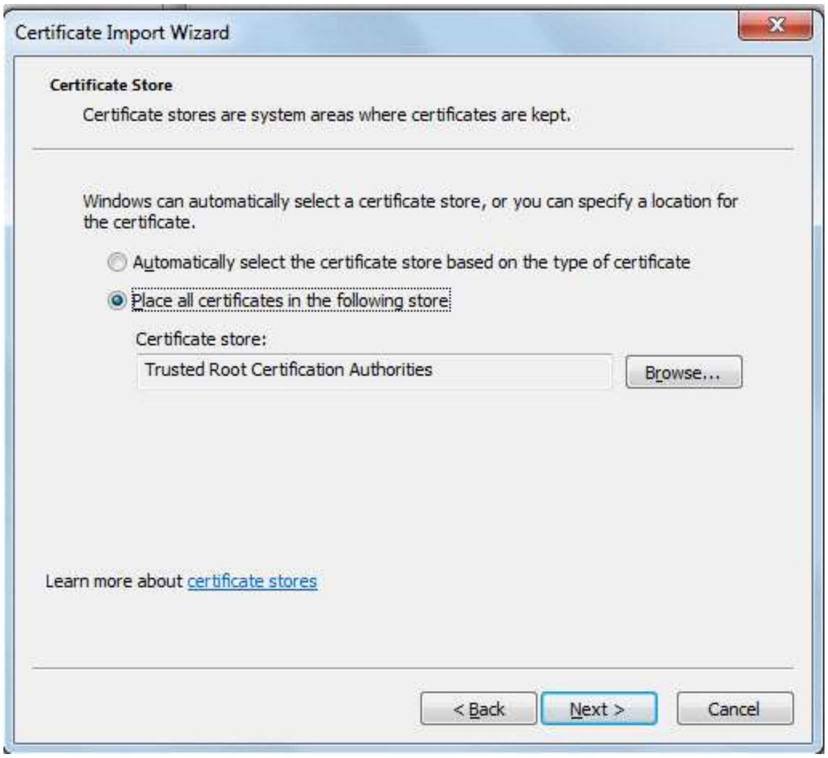
or you can specify a location for

d on the type of certificate

Learn more about certificate stores

Figure 3.87: 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 3.88. Click **Next** in Figure 3.88 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

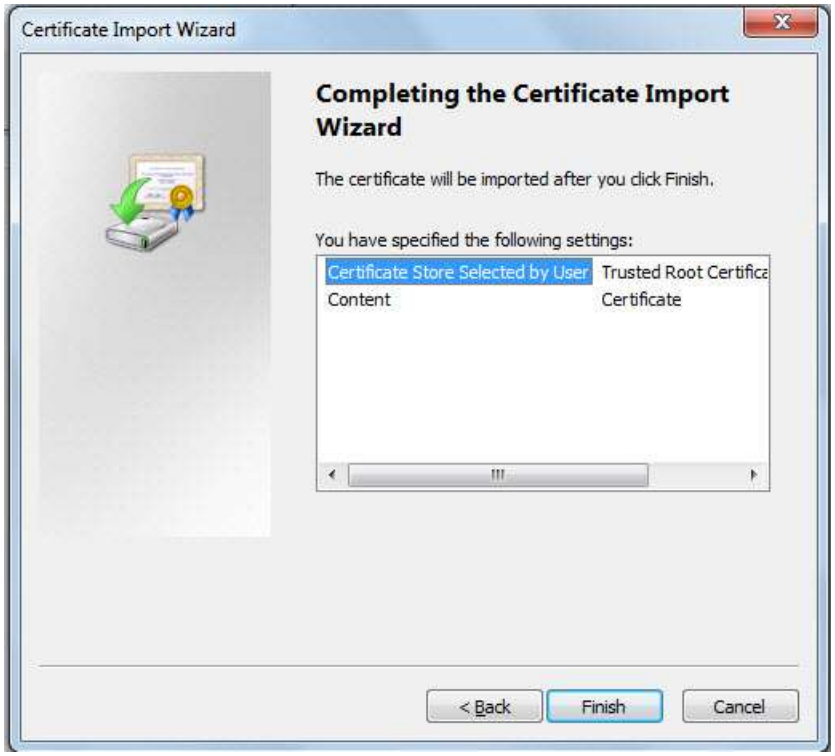
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Figure 3.88: The chosen store displayed

7. A quick summary of your selections will appear in Figure 3.89. Review your specifications and click **Finish** to complete the import.



Certificate Import Wizard

Completing the Certificate Import Wizard

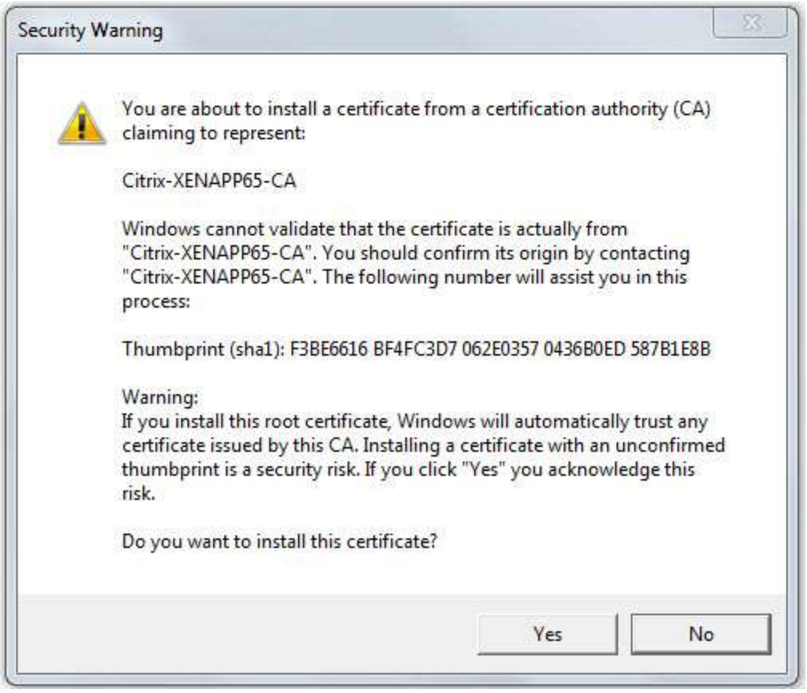
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

Figure 3.89: Finishing the import

8. The following warning message will appear. Click **Yes** in Figure 3.90 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:

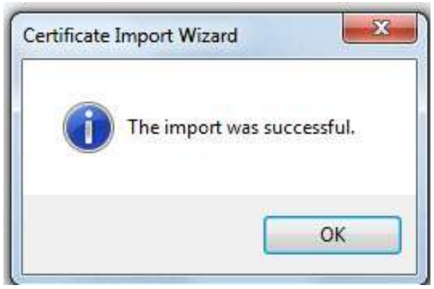
Thumbprint (sha1): F3BE6616 BF4FC3D7 062E0357 0436B0ED 587B1E8B

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 3.90: 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 3.91: 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!

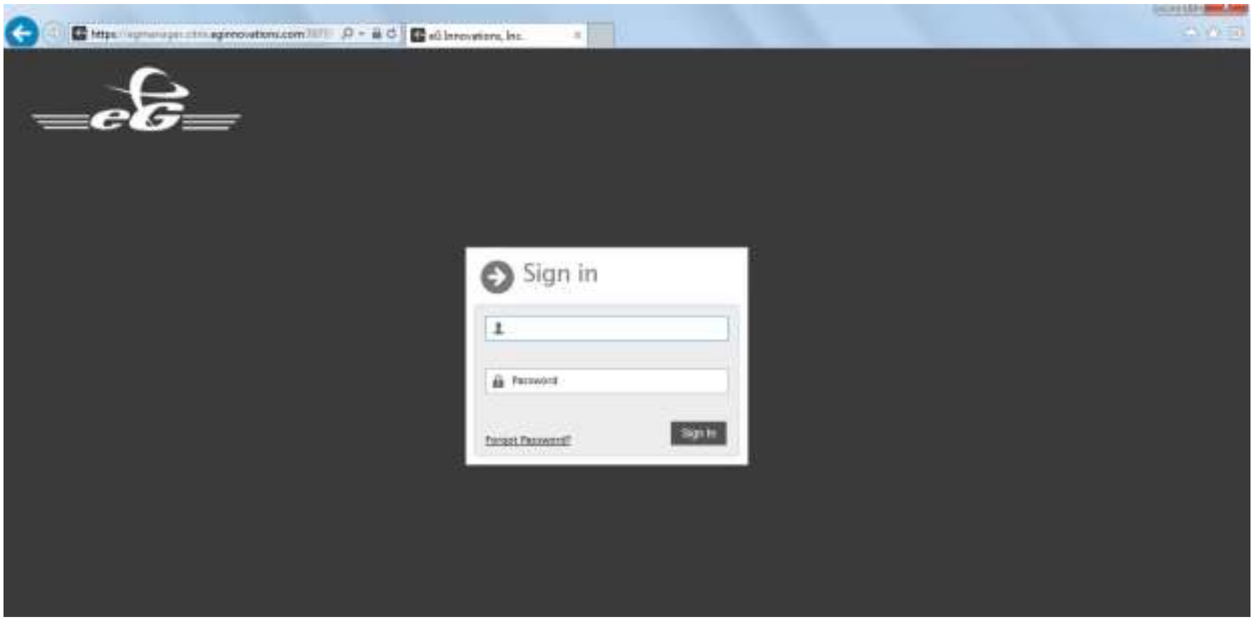


Figure 3.92: The login screen of the eG manager, without the 'Certificate error'

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 Section 3.4.2.4), 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 3.93).

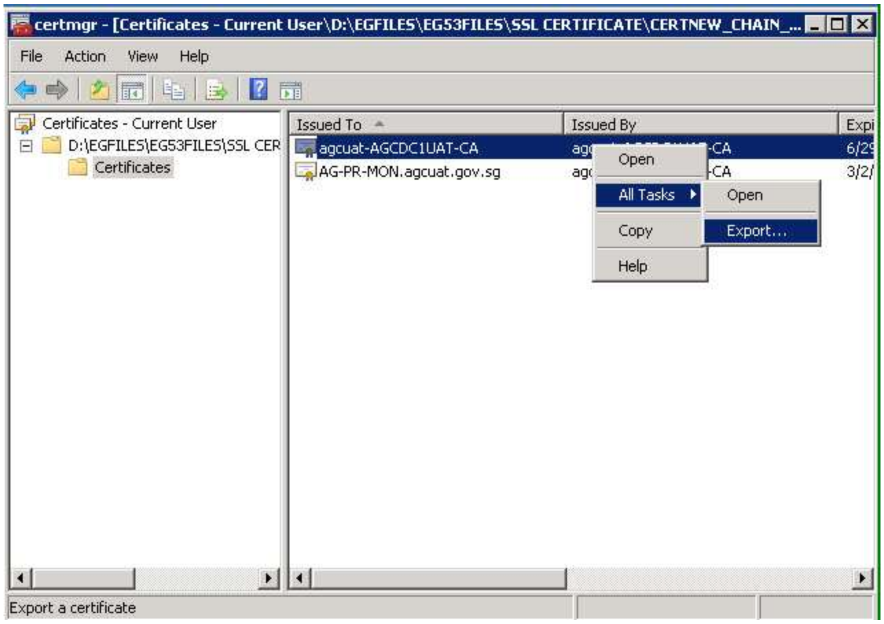


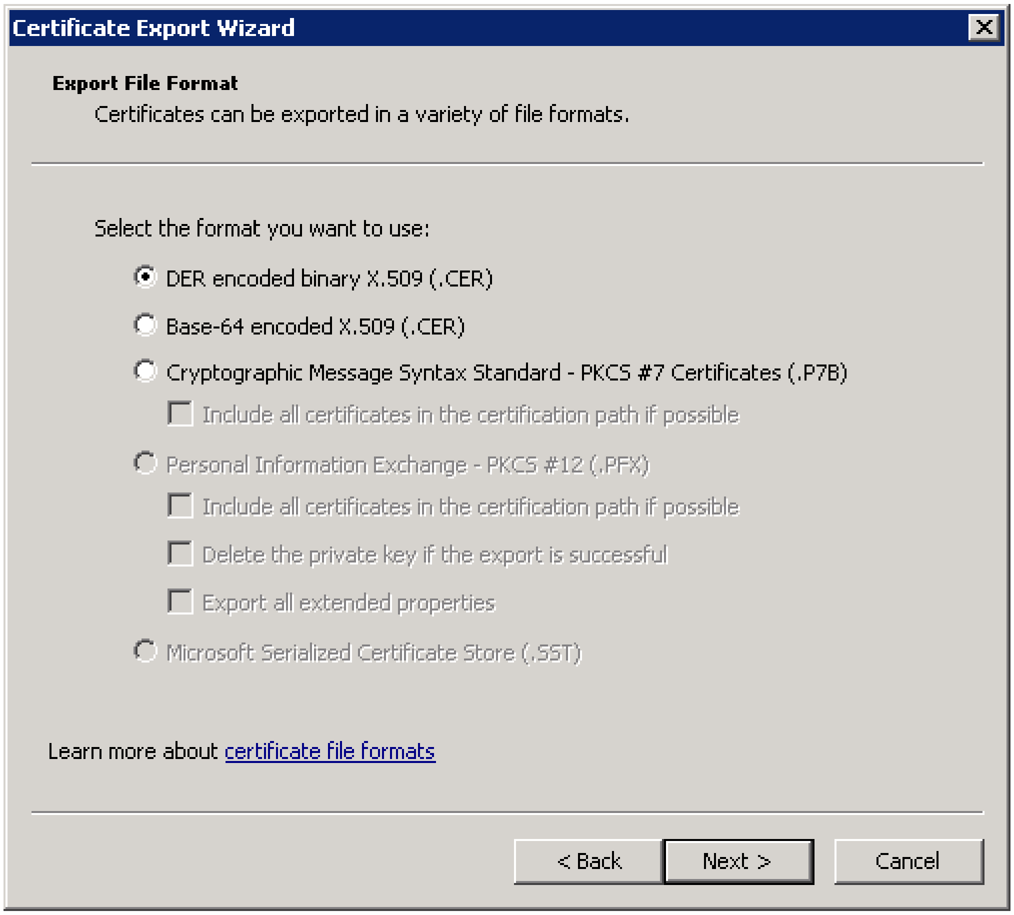
Figure 3.93: The Certificates window

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 3.93).

6. A wizard will appear. Click **Next** in the wizard to proceed.

7. Figure 3.94 will then appear. Select the **DER encoded binary X.509 (.CER)** option in Figure 3.94 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 3.94: Converting the certificate into PEM format

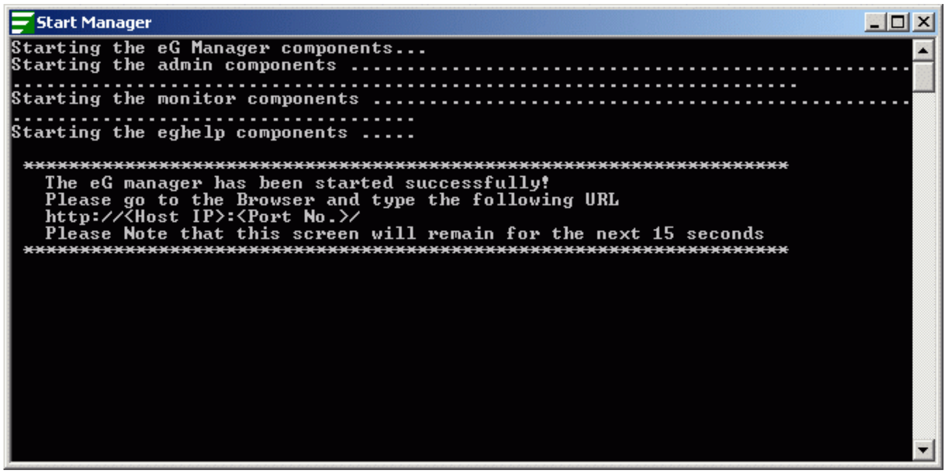
8. You will now be prompted for a **File name**. Provide a name for the converted digital certificate, and click **Next.**

3.5 Starting the eG Manager

3.5.1 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:



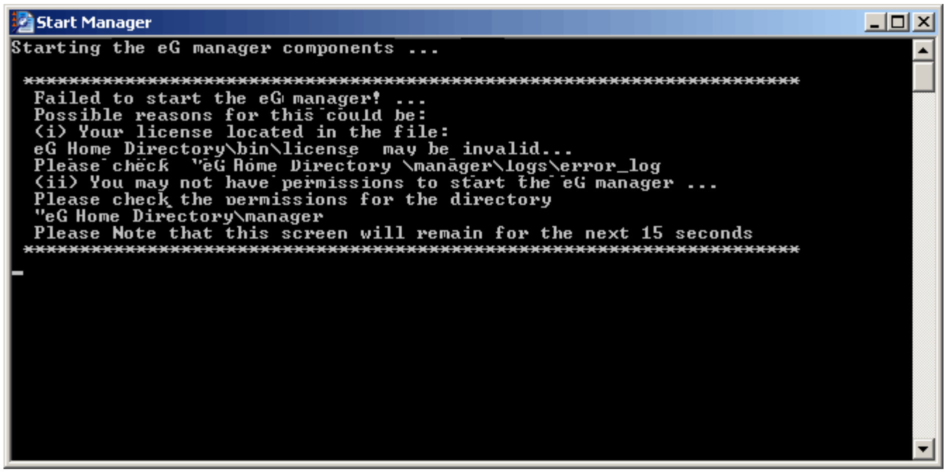
```
Starting the eG Manager components...
Starting the admin components ..................................................
.......................................................................
Starting the monitor components ................................................
....................................
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 3.95: 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 3.96: Message indicating that the manager has not been started successfully

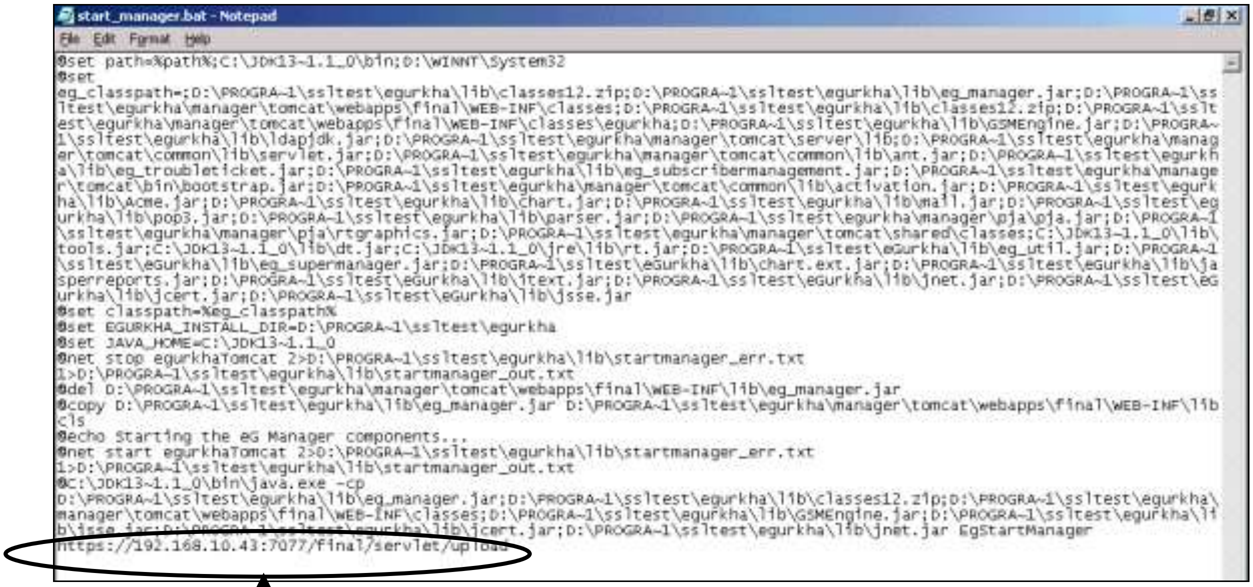
Please check the **<EG_HOME_DIR>\manager\logs\error_log** file to find out the reasons due which the manager failed to start.

3.5.2 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 3.97) 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 3.97).



```
@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\egurkha\lib\startmanager_err.txt
1>D:\PROGRA~1\ssltest\egurkha\lib\startmanager_out.txt
@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 3.97: SSL-enabling the startmanager script

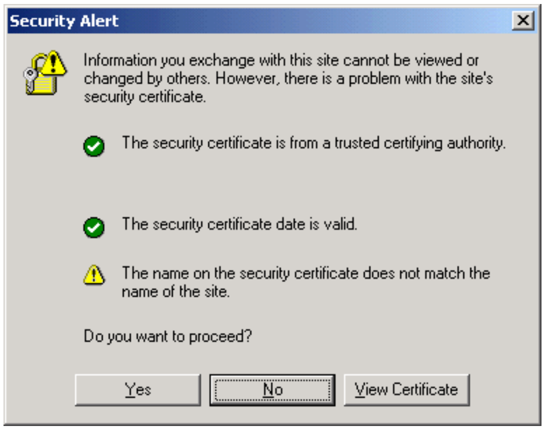
SSL-enabling the start manager script by making the indicated change

2. Finally, start the eG manager as discussed in Section 3.4.

3.6 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 3.98). 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.



Security Alert

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 3.98: 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.

3.7 Increasing the Memory of the eG Manager

The eG manager runs as a Java process. The maximum heap memory that can be allocated to a 32-bit eG manager process is limited to 1.5 GB. The maximum heap memory allocation to a 64-bit eG manager process on the other hand, is limited to 3 GB.

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, 2 GB (i.e., 2048 MB), change these specifications as indicated below:

```
@set XMX=2048
@set XMS=2048
```

5. Finally, save the file.

3.8 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 3.99).

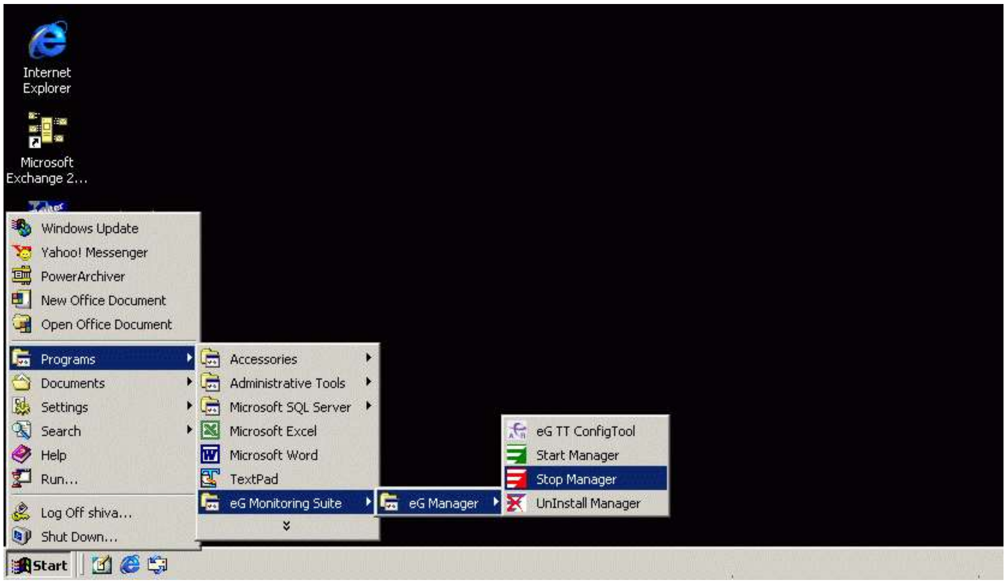


Figure 3.99: Stopping the eG manager

If, for some reason, the IIS web server hosting the eG manager stops running, then you can configure the Tomcat server to fill in for the IIS web server that is non-operational, and continue to work with the eG manager. To achieve this, do the following:

1. Once the IIS web server goes down, proceed to delete the **egurkha** web site that is automatically created on the IIS web server upon installing the eG Enterprise manager. To do so, select the **Internet Services Manager** option (in Windows 2003, this will be the **Internet Information Services (IIS) Manager** option) from the Start -> Programs -> Administrative Tools menu of the IIS web server.

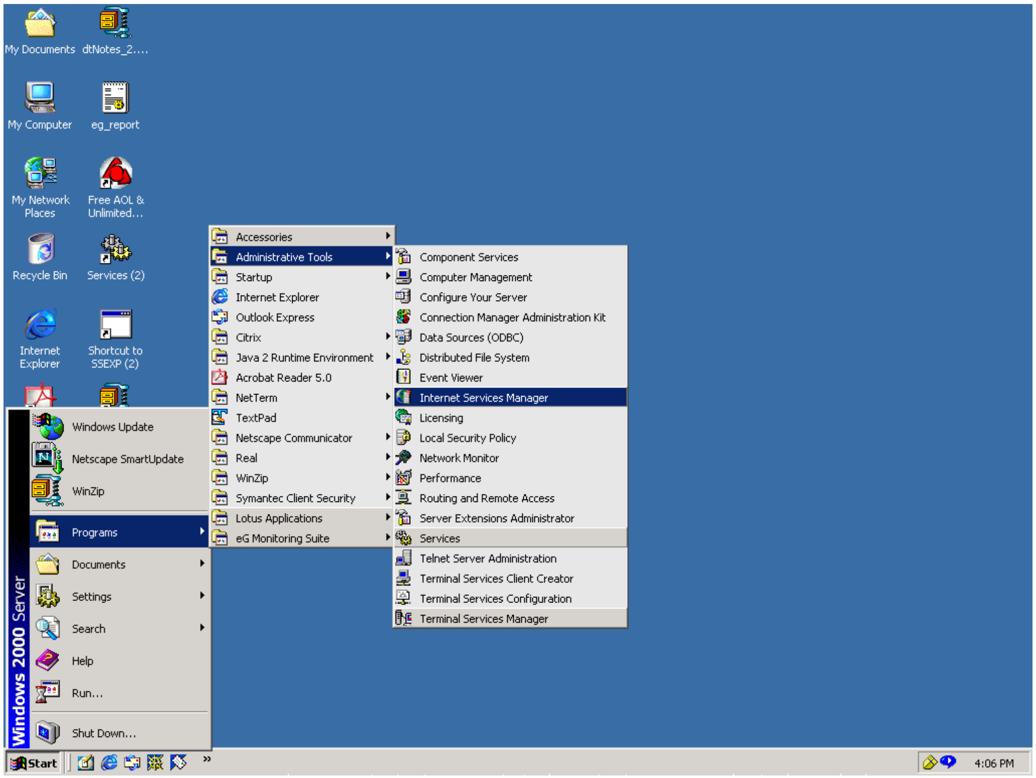


Figure 3.100: Selecting the Internet Information Services (IIS) Manager option

2. From the window that appears, select the **egurkha** web site, right-click on it, and choose the **Delete** option (see Figure 3.101).

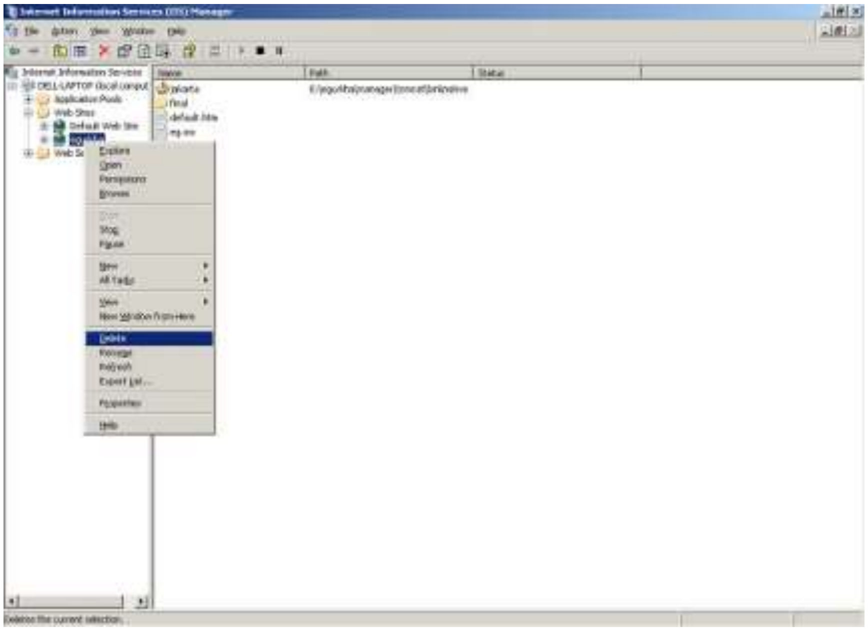
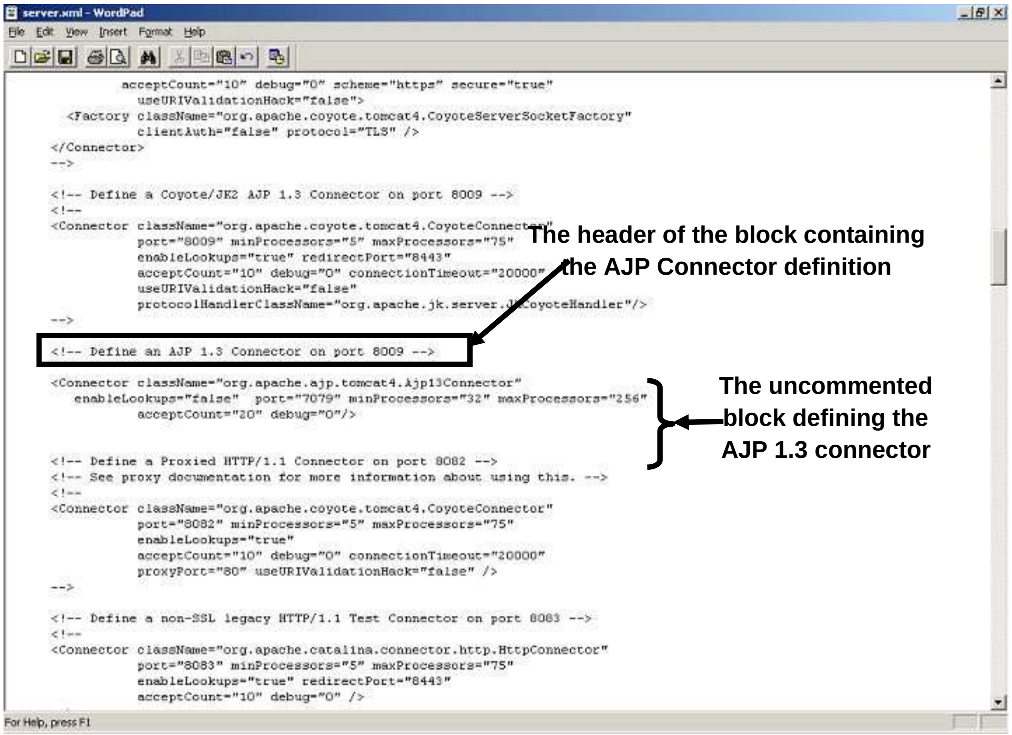


Figure 3.101: Deleting the **egurkha** web site

3. Next, to configure the Tomcat server so that it functions as the web server, edit the **server.xml** file in the

<EG_INSTALL_DIR>\manager\tomcat\conf directory on the eG manager host.

4. In the **server.xml** file, locate the block where the **AJP 1.3 Connector** is defined. By default, this block will be uncommented as indicated by Figure 3.102.



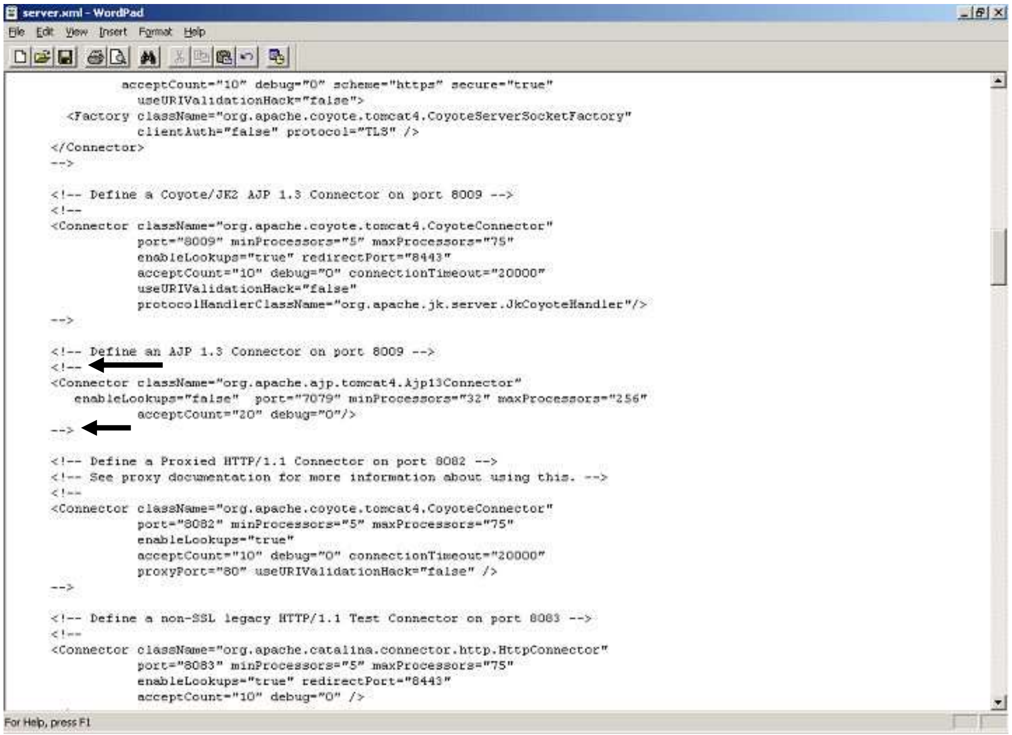
```
              acceptCount="10" debug="0" scheme="https" secure="true"
                useURIValidationHack="false">
    <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
                clientAuth="false" protocol="TLS" />
  </Connector>
  -->

  <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
  <!--
  <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
             port="8009" minProcessors="5" maxProcessors="75"
             enableLookups="true" redirectPort="8443"
             acceptCount="10" debug="0" connectionTimeout="20000"
             useURIValidationHack="false"
             protocolHandlerClassName="org.apache.jk.server.JkCoyoteHandler"/>
  -->

  <!-- Define an AJP 1.3 Connector on port 8009 -->

  <Connector className="org.apache.ajp.tomcat4.Ajp13Connector"
     enableLookups="false"  port="7079" minProcessors="32" maxProcessors="256"
             acceptCount="20" debug="0"/>


  <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
  <!-- See proxy documentation for more information about using this. -->
  <!--
  <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
             port="8082" minProcessors="5" maxProcessors="75"
             enableLookups="true"
             acceptCount="10" debug="0" connectionTimeout="20000"
             proxyPort="80" useURIValidationHack="false" />
  -->

  <!-- Define a non-SSL legacy HTTP/1.1 Test Connector on port 8083 -->
  <!--
  <Connector className="org.apache.catalina.connector.http.HttpConnector"
             port="8083" minProcessors="5" maxProcessors="75"
             enableLookups="true" redirectPort="8443"
             acceptCount="10" debug="0" />
```

The header of the block containing the AJP Connector definition

The uncommented block defining the AJP 1.3 connector

Figure 3.102: The uncommented block in the server.xml file containing the AJP Connector definition

5. In order to disable the AJP connector, comment the block by inserting the **<!- -** symbol at the beginning of the block (i.e., just below the block header), and the **- ->** symbol at the end of the block, as depicted by Figure 3.103.



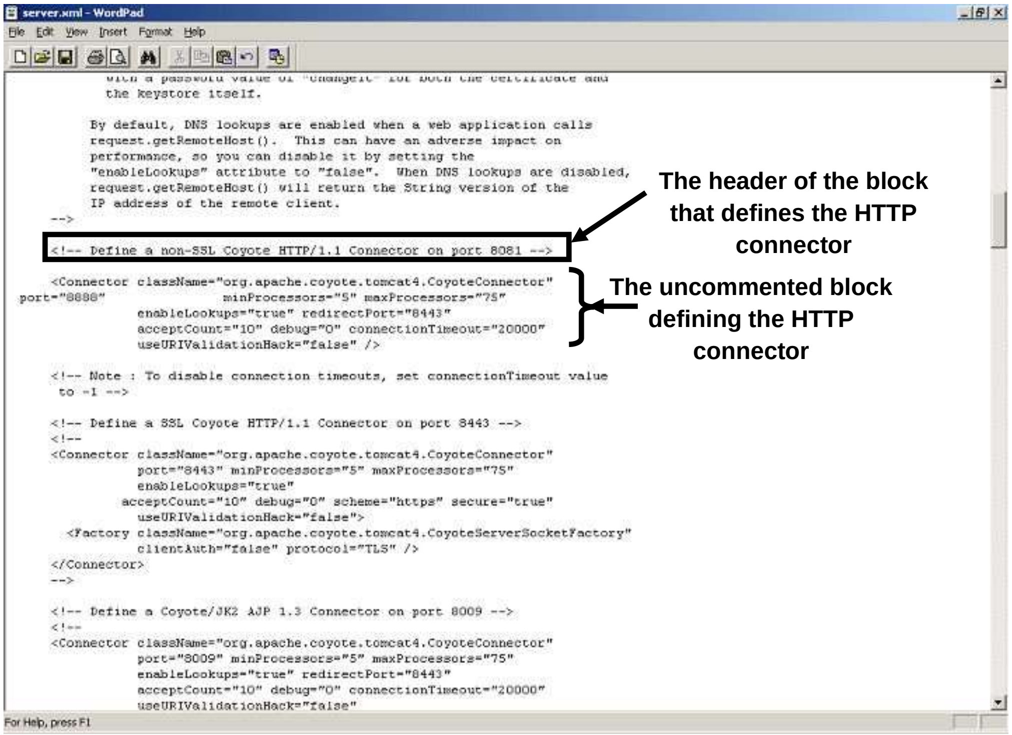
```
            acceptCount="10" debug="0" scheme="https" secure="true"
              useURIValidationHack="false">
    <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
              clientAuth="false" protocol="TLS" />
  </Connector>
  -->

  <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
  <!--
  <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
              port="8009" minProcessors="5" maxProcessors="75"
              enableLookups="true" redirectPort="8443"
              acceptCount="10" debug="0" connectionTimeout="20000"
              useURIValidationHack="false"
              protocolHandlerClassName="org.apache.jk.server.JkCoyoteHandler"/>
  -->

  <!-- Define an AJP 1.3 Connector on port 8009 -->
  <!--
  <Connector className="org.apache.ajp.tomcat4.Ajp13Connector"
     enableLookups="false"  port="7079" minProcessors="32" maxProcessors="256"
              acceptCount="20" debug="0"/>
  -->

  <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
  <!-- See proxy documentation for more information about using this. -->
  <!--
  <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
              port="8082" minProcessors="5" maxProcessors="75"
              enableLookups="true"
              acceptCount="10" debug="0" connectionTimeout="20000"
              proxyPort="80" useURIValidationHack="false" />
  -->

  <!-- Define a non-SSL legacy HTTP/1.1 Test Connector on port 8083 -->
  <!--
  <Connector className="org.apache.catalina.connector.http.HttpConnector"
              port="8083" minProcessors="5" maxProcessors="75"
              enableLookups="true" redirectPort="8443"
              acceptCount="10" debug="0" />
```

Figure 3.103: Commenting the AJP Connector block

6. Next, proceed to open any of the HTTP connector ports by uncommenting the corresponding connector definition block (by default, this block will be commented). To uncomment the block, remove the **<!- -** symbol at the beginning of the block (i.e., just below the block header), and the **- ->** symbol at the end of the block, as depicted by Figure 3.104.

Note

If the eG manager is SSL-enabled, then you will have to open the SSL HTTP/1.1 definition. For a non-SSL eG manager, open the non-SSL HTTP/1.1 definition.



```
          with a password value of "changeit" for both the certificate and
          the keystore itself.

        By default, DNS lookups are enabled when a web application calls
        request.getRemoteHost().  This can have an adverse impact on
        performance, so you can disable it by setting the
        "enableLookups" attribute to "false".  When DNS lookups are disabled,
        request.getRemoteHost() will return the String version of the
        IP address of the remote client.
    -->

    <!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->

    <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8888"                minProcessors="5" maxProcessors="75"
               enableLookups="true" redirectPort="8443"
               acceptCount="10" debug="0" connectionTimeout="20000"
               useURIValidationHack="false" />

    <!-- Note : To disable connection timeouts, set connectionTimeout value
     to -1 -->

    <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
               port="8443" minProcessors="5" maxProcessors="75"
               enableLookups="true"
             acceptCount="10" debug="0" scheme="https" secure="true"
               useURIValidationHack="false">
      <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
               clientAuth="false" protocol="TLS" />
    </Connector>
    -->

    <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
    <!--
    <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
               port="8009" minProcessors="5" maxProcessors="75"
               enableLookups="true" redirectPort="8443"
               acceptCount="10" debug="0" connectionTimeout="20000"
               useURIValidationHack="false"
```

The header of the block that defines the HTTP connector

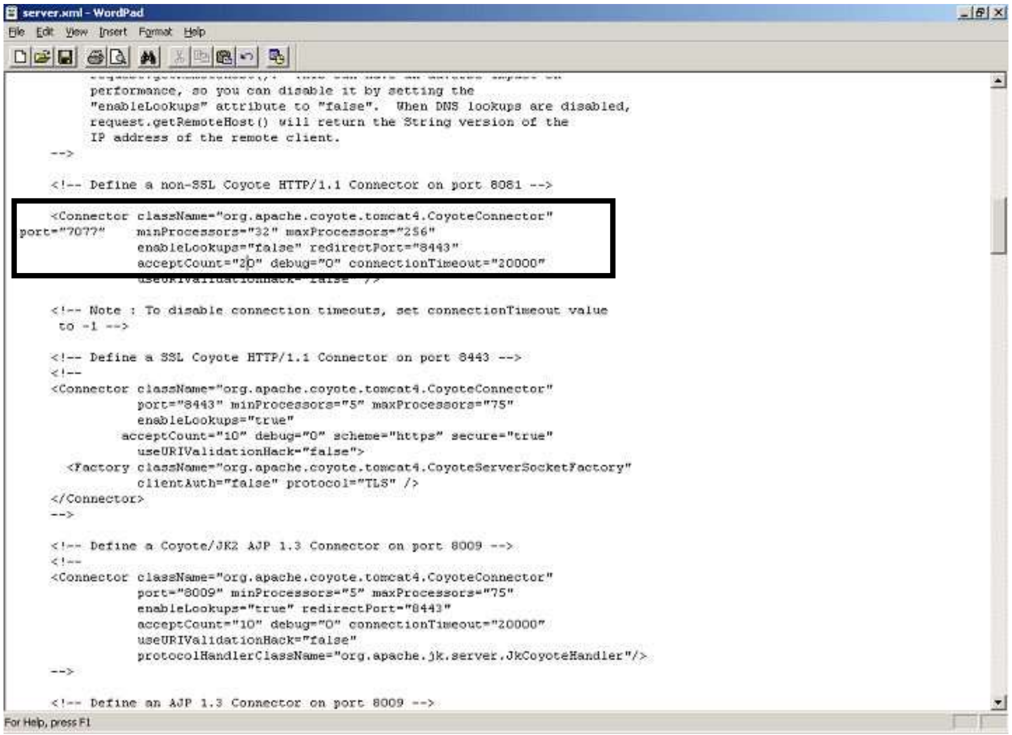
The uncommented block defining the HTTP connector

Figure 3.104: Uncommenting the block containing the HTTP Connector port definition

7. Next, proceed to make the following changes to the HTTP connector block that was just uncommented:

   - Change *port* to 7077
   - Change *minprocessors* to 32
   - Set *maxprocessors* to a value that is half the RAM size of the eG manager host - i.e., for a RAM size of 512, *maxprocessors* will be 256
   - Change *enableLookups* to false
   - Change *acceptcount* to 20
   - Change *connectionTimeout* to 20000

   Figure 3.105 depicts the aforesaid changes.



```
          performance, so you can disable it by setting the
          "enableLookups" attribute to "false".  When DNS lookups are disabled,
          request.getRemoteHost() will return the String version of the
          IP address of the remote client.
     -->

     <!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8081 -->

     <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="7077"      minProcessors="32" maxProcessors="256"
                 enableLookups="false" redirectPort="8443"
                 acceptCount="20" debug="0" connectionTimeout="20000"
                 useURIValidationHack="false" />

     <!-- Note : To disable connection timeouts, set connectionTimeout value
      to -1 -->

     <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
     <!--
     <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
                 port="8443" minProcessors="5" maxProcessors="75"
                 enableLookups="true"
               acceptCount="10" debug="0" scheme="https" secure="true"
                 useURIValidationHack="false">
       <Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
                 clientAuth="false" protocol="TLS" />
     </Connector>
     -->

     <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
     <!--
     <Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
                 port="8009" minProcessors="5" maxProcessors="75"
                 enableLookups="true" redirectPort="8443"
                 acceptCount="10" debug="0" connectionTimeout="20000"
                 useURIValidationHack="false"
                 protocolHandlerClassName="org.apache.jk.server.JkCoyoteHandler"/>
     -->

     <!-- Define an AJP 1.3 Connector on port 8009 -->
```

Figure 3.105: Changes made to the HTTP/1.1 connector block

8. Finally, save the **server.xml** file.
9. Restart the Tomcat server.
10. Start the eG manager.
11. While connecting to the eG manager, use the URL: **http://<eG_manager_IP>:<port>/final/admin/default.htm**. In case of an SSL-enabled manager: **https://<eG_manager_IP>:<SSL_port>/final/admin/default.htm**.

3.9 Recommended Browser Settings for the eG Manager

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

- Internet Explorer 10, 11, or Edge
- Mozilla Firefox v18 or above
- Chrome v28 or above

No additional plugins 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 sub-sections below are in place.

3.9.1 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.

3.9.1.1 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 3.106).

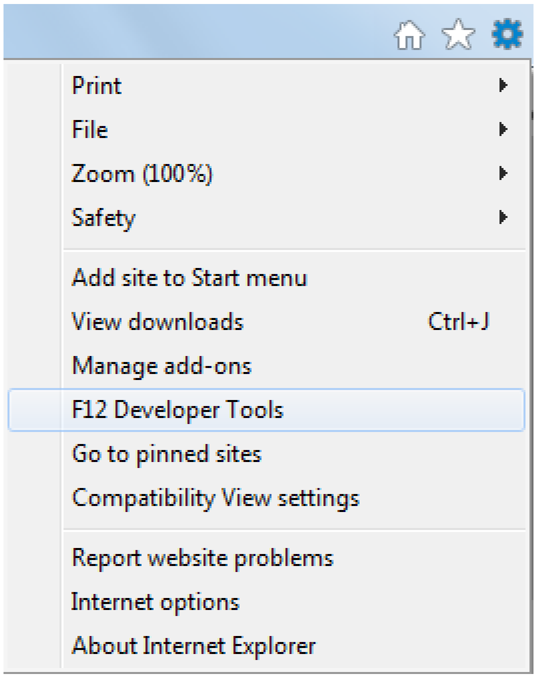
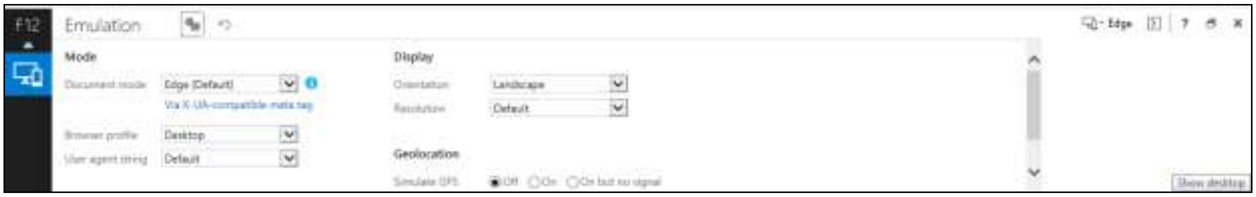


Figure 3.106: Launching the Developer Tools

3. When Figure 3.107 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 3.107: Changing the Document mode

3.9.1.2 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 3.108).

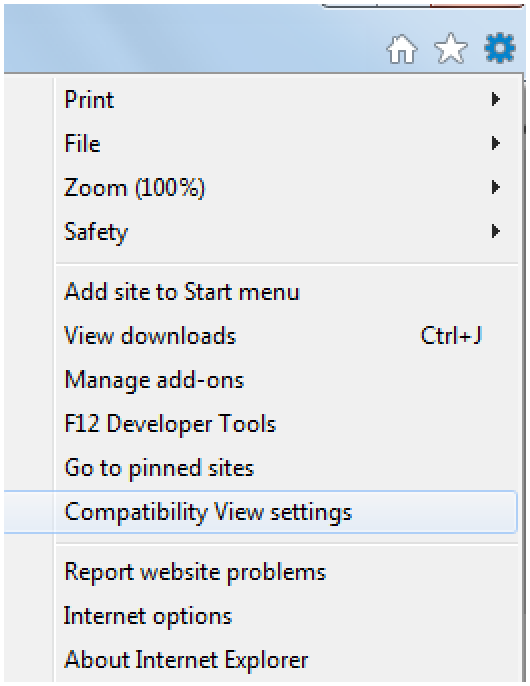
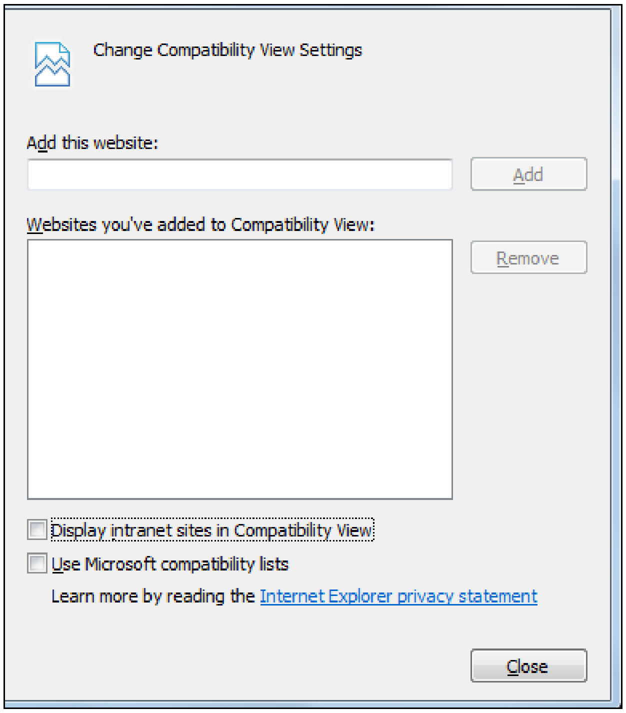


Figure 3.108: Accessing the Compatibility View Settings dialog

2. In Figure 3.109 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:

Websites you've added to Compatibility View:

□ Display intranet sites in Compatibility View

□ Use Microsoft compatibility lists

Learn more by reading the Internet Explorer privacy statement

Figure 3.109: 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 3.109.

3.9.1.3 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 3.110).

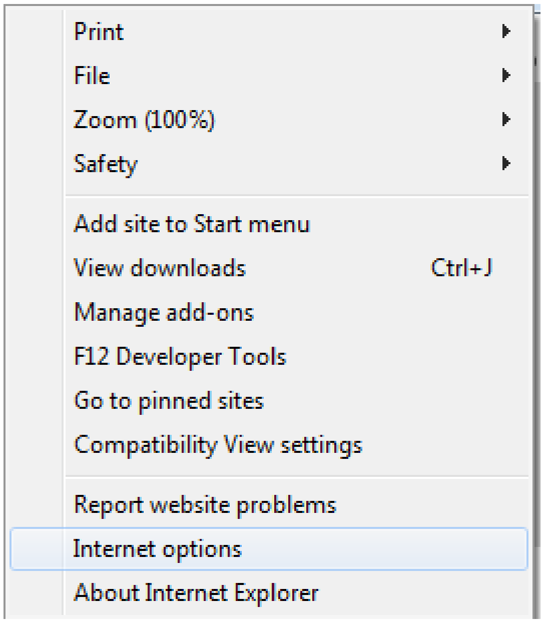
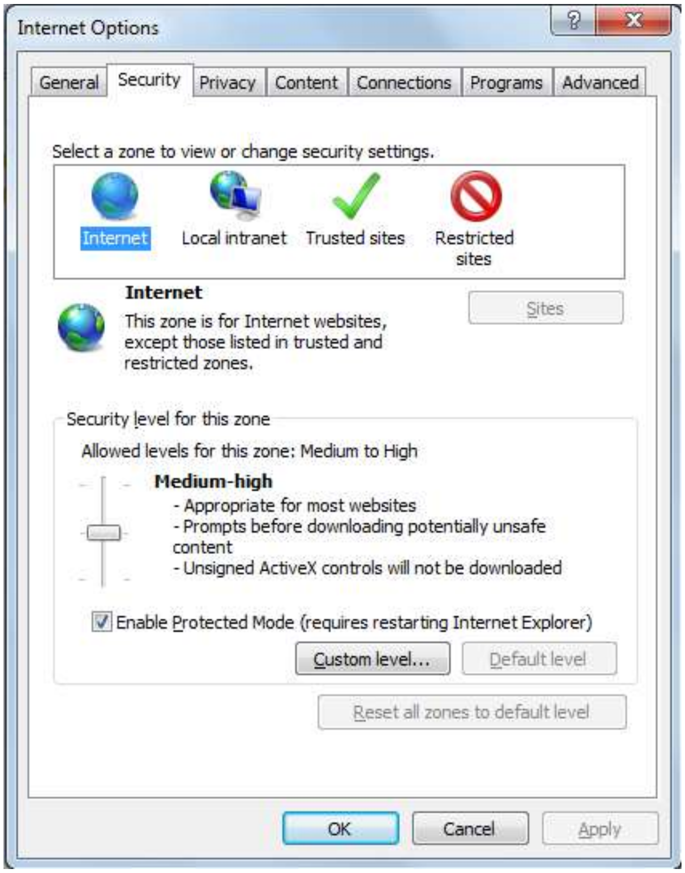


Figure 3.110: Selecting the Internet Options option from the Tools menu

2. Figure 3.111 will then appear. Select the **Security** tab page in Figure 3.111 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

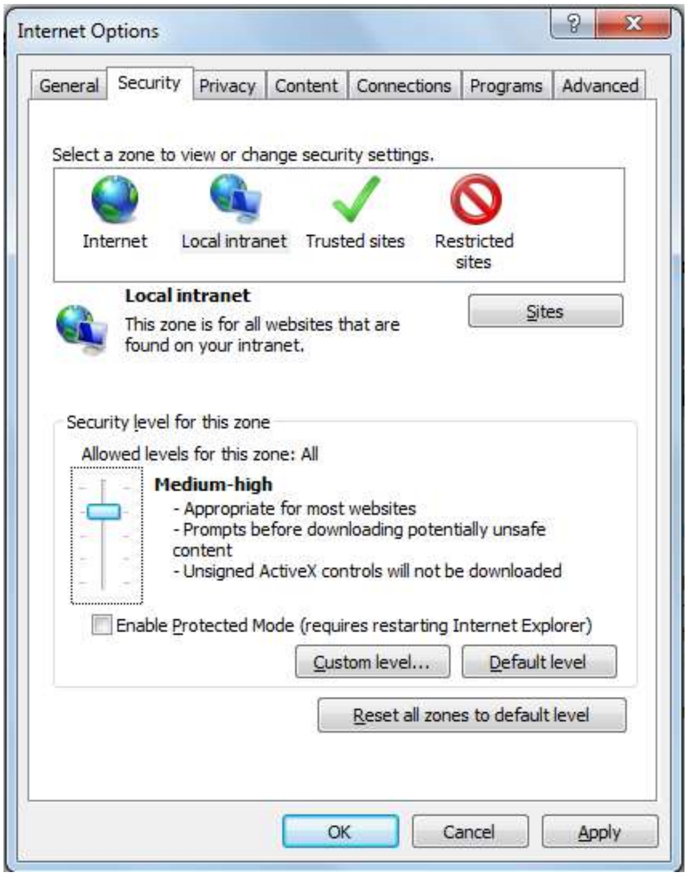
Medium-high

- 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 3.111: Changing the security settings for the Internet zone

3. Use the slider in the **Security level for this zone** section to set the security level at *Medium* or *Medium-high*.
4. Then, pick the **Local intranet** zone and set *Medium* or *Medium-high* as its security level (see Figure 3.112).



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

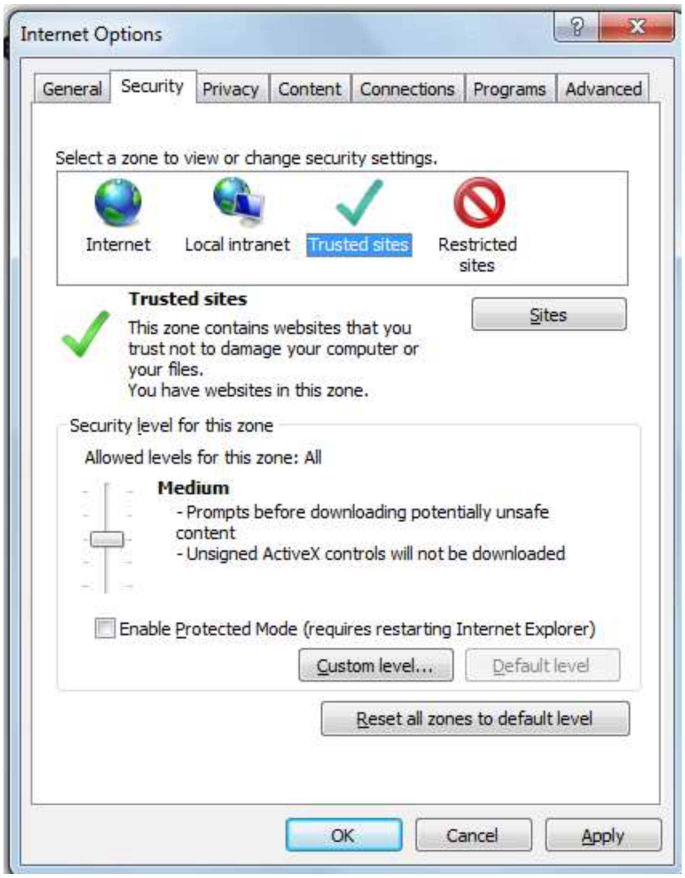
Medium-high

- 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 3.112: Changing the security level of the Local intranet zone

5. Then, select the **Trusted sites** zone and set *Medium* or *Medium-high* as its security level (see Figure 3.113).



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

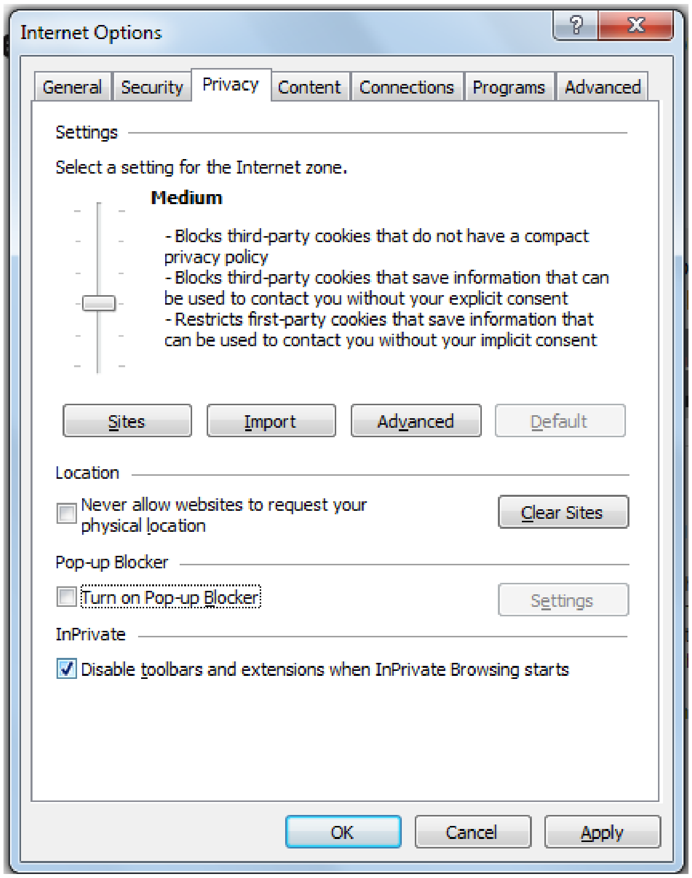
Allowed levels for this zone: All

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

□ Enable Protected Mode (requires restarting Internet Explorer)

Figure 3.113: Changing the security settings of the Trusted sites zone

6. 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 3.114).



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 3.114: Changing privacy settings

7. 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 3.114. If you want pop-ups to be allowed for the eG manager alone, then follow the steps detailed in Section 3.9.1.4

8. Finally, click the **Apply** and **OK** buttons in Figure 3.114 to save the changes.

3.9.1.4 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 3.115), and select the **Pop-up Blocker settings** option therein.

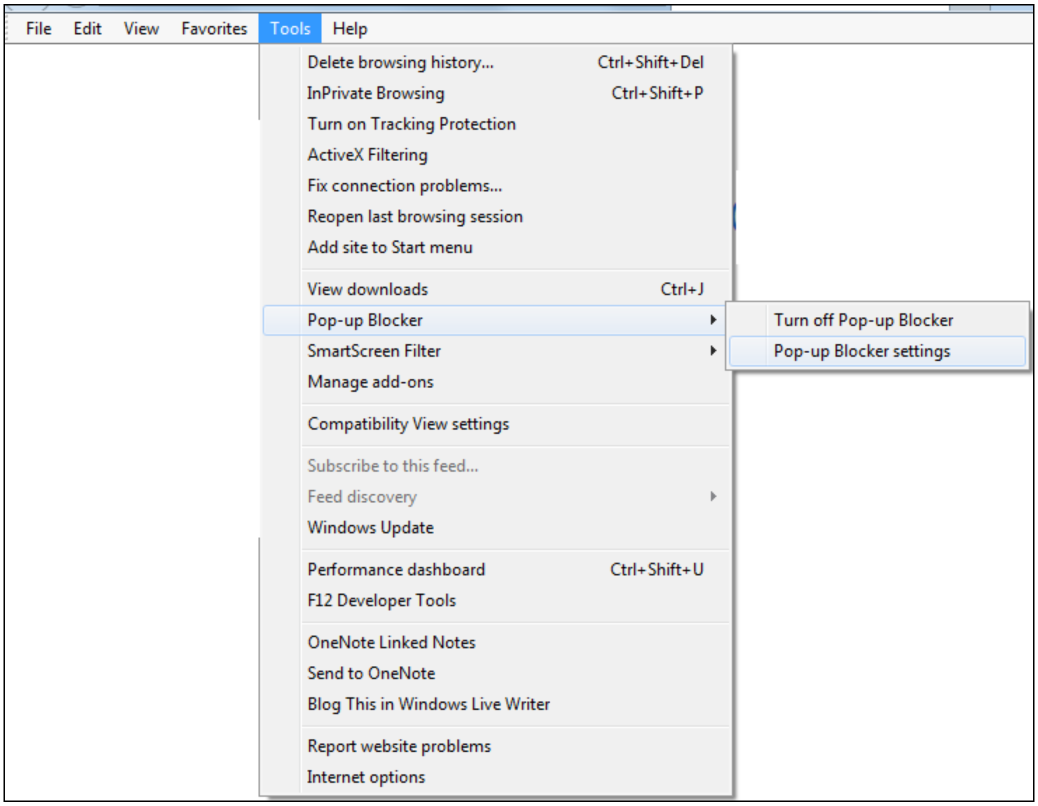
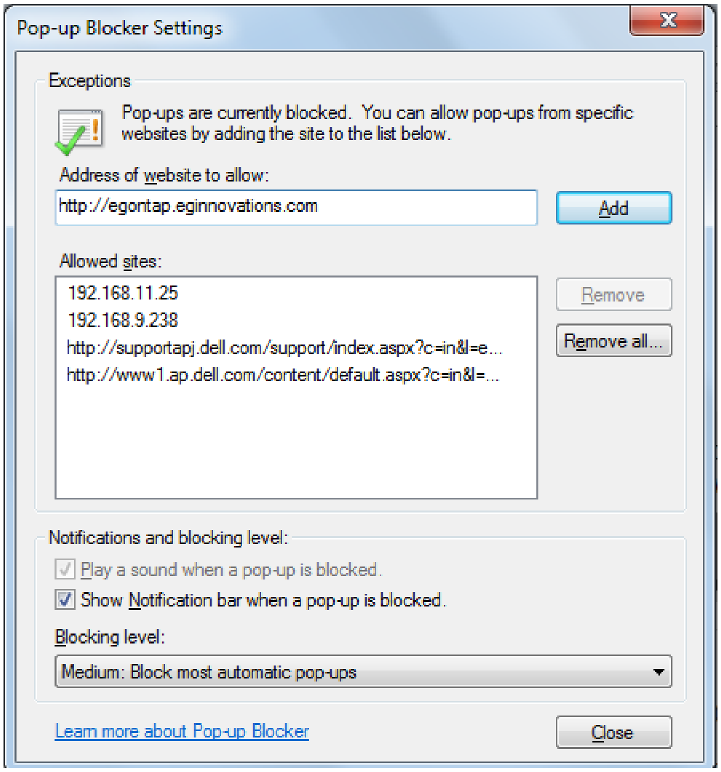


Figure 3.115: Selecting the Pop-up Blocker menu

2. Figure 3.116 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 3.116 to add that URL to the **Allowed sites** list.



Pop-up Blocker Settings

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

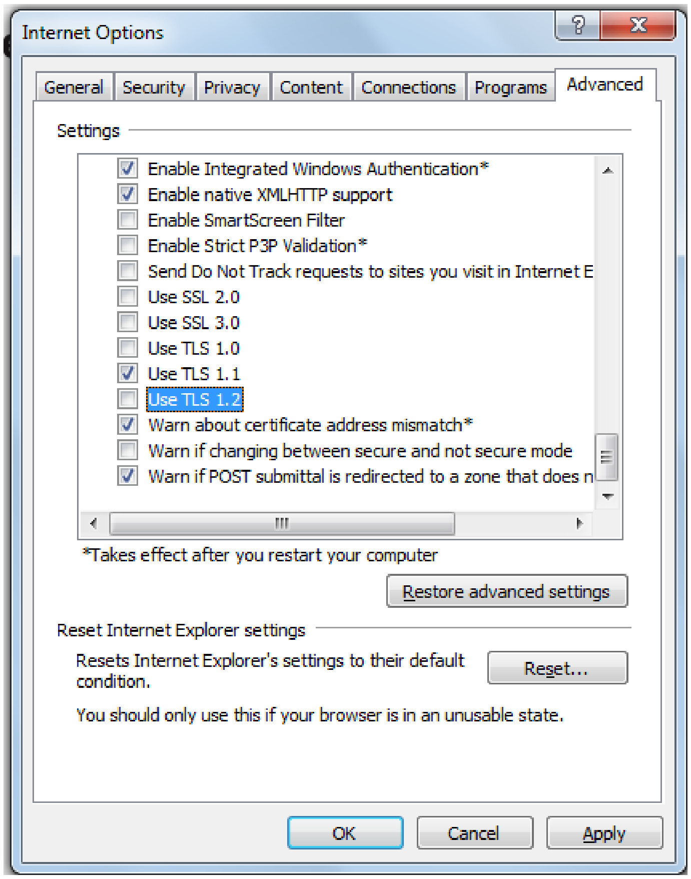
Figure 3.116: Allowing pop-up for the eG manager

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

3.9.1.5 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 3.106).
2. When Figure 3.107 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 3.117: 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 3.117 to save the changes.

3.9.2 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.

3.9.2.1 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 3.118).

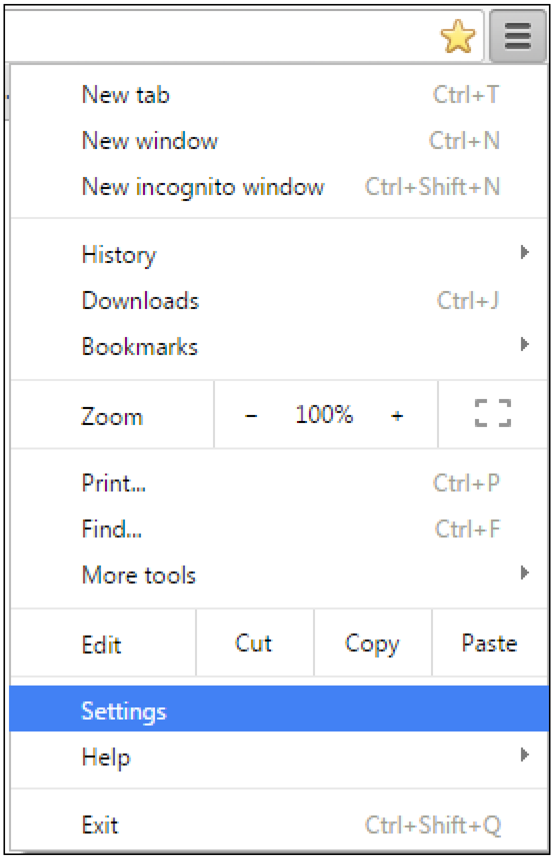


Figure 3.118: Selecting the Settings option from the Chrome menu

2. Scroll down the **Settings** page that then appears until you find the **Show advanced settings** link (see Figure 3.119). Then, click on the link.

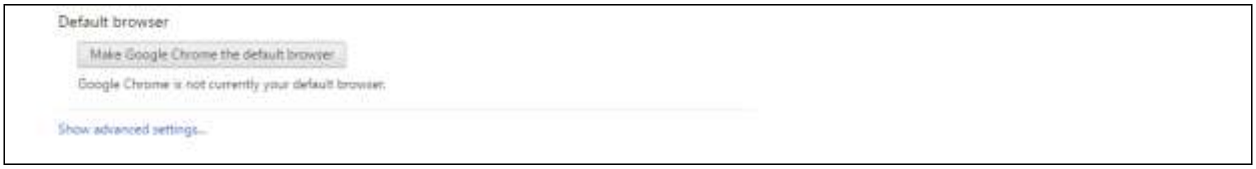
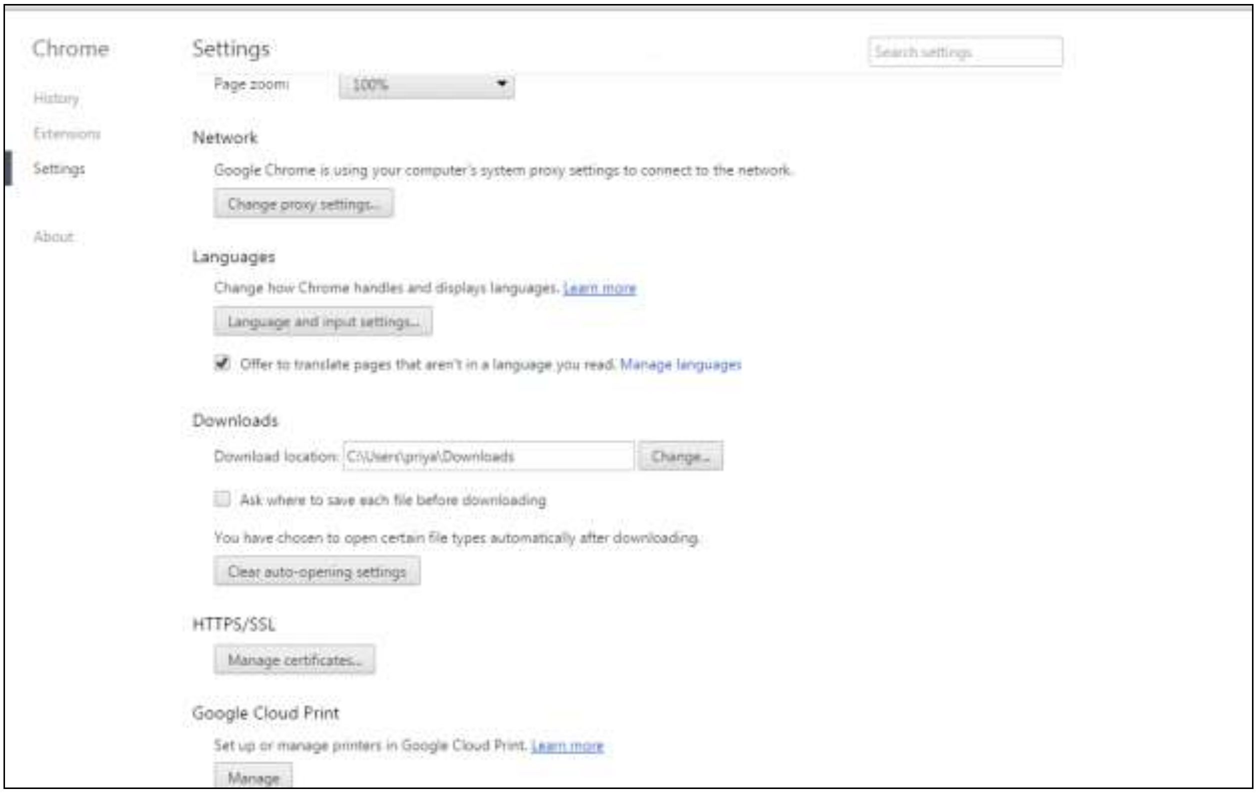

Default browser
Make Google Chrome the default browser
Google Chrome is not currently your default browser.
Show advanced settings...

Figure 3.119: 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.



Page zoom: 100%

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

Change how Chrome handles and displays languages.

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

Download location: C:\Users\priya\Downloads

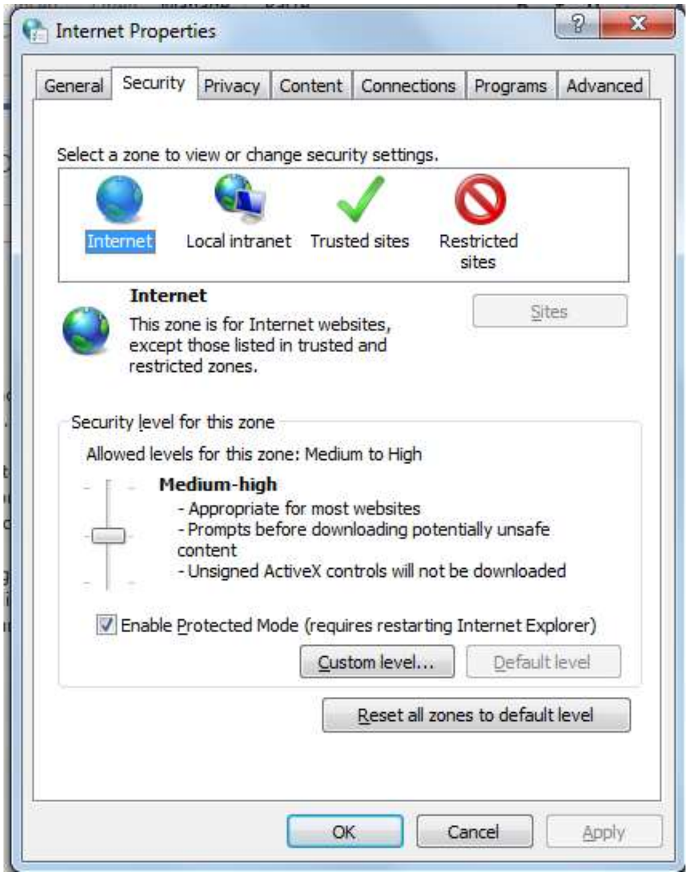
□ Ask where to save each file before downloading

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

Set up or manage printers in Google Cloud Print.

Figure 3.120: 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 3.121).



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

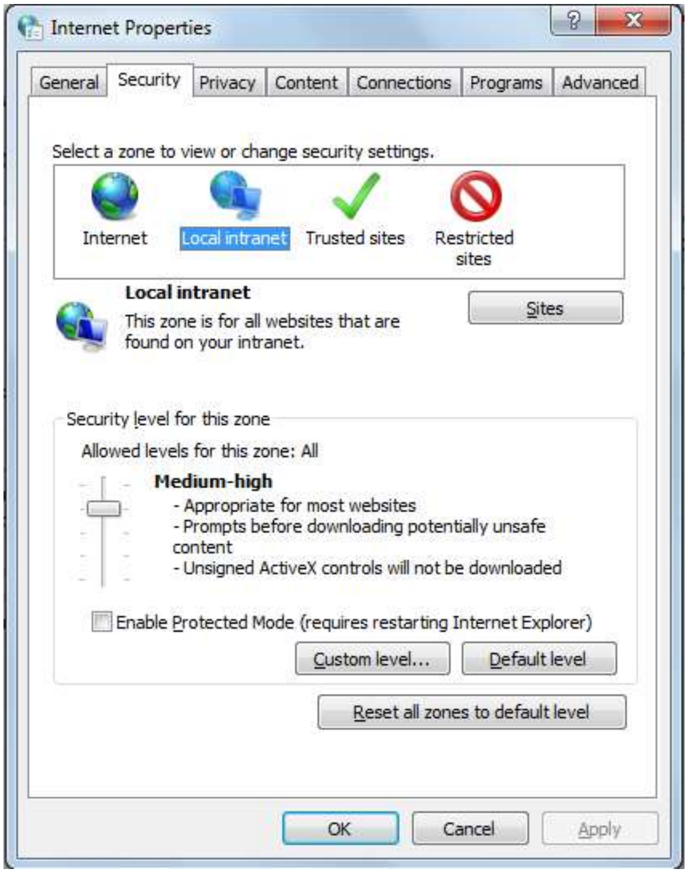
Medium-high

- 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 3.121: 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 3.122).



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

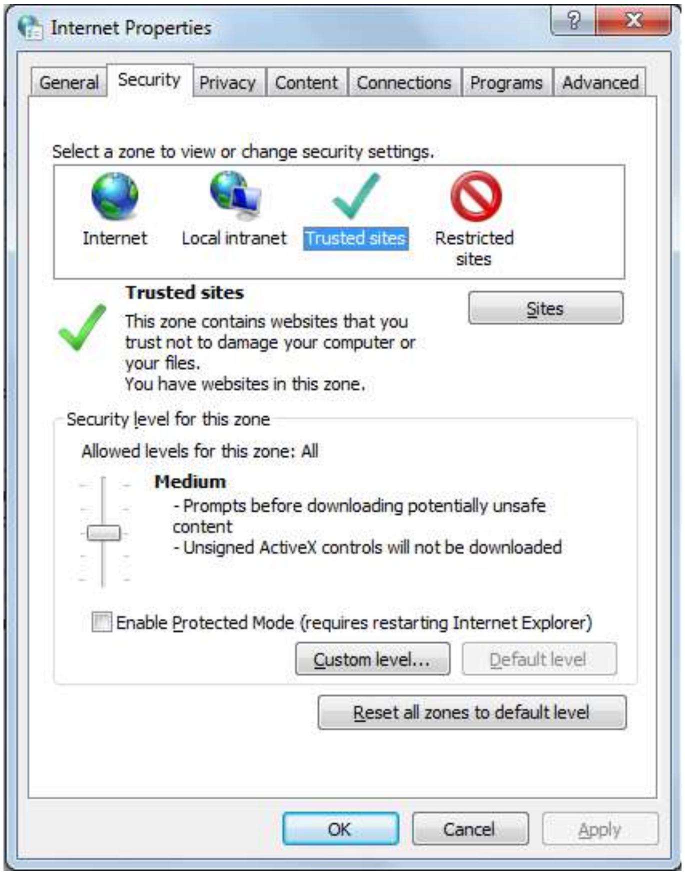
Medium-high

- 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 3.122: 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 3.123).



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

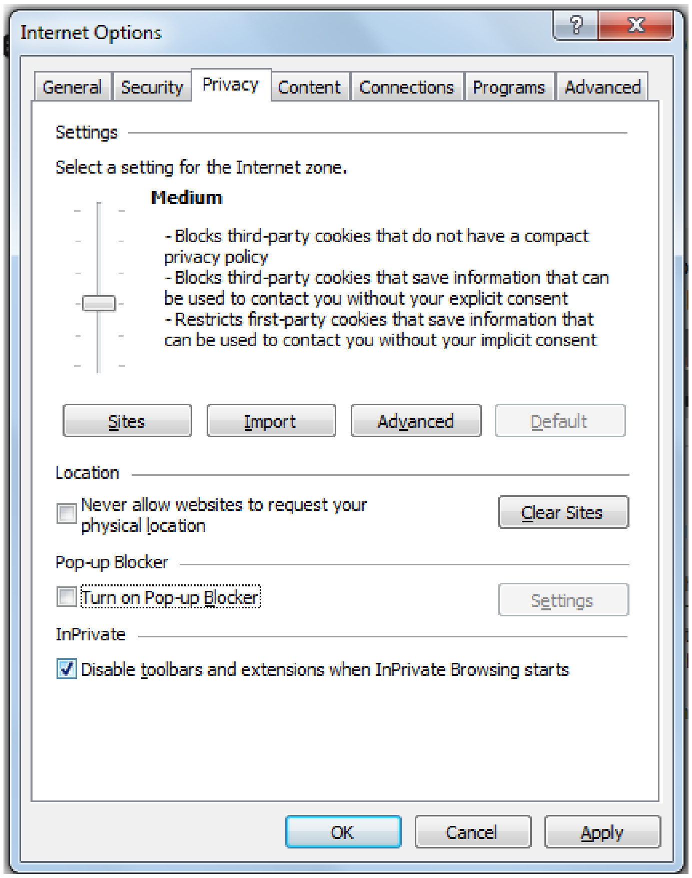
Medium

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

☐ Enable Protected Mode (requires restarting Internet Explorer)

Figure 3.123: 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 3.124).



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

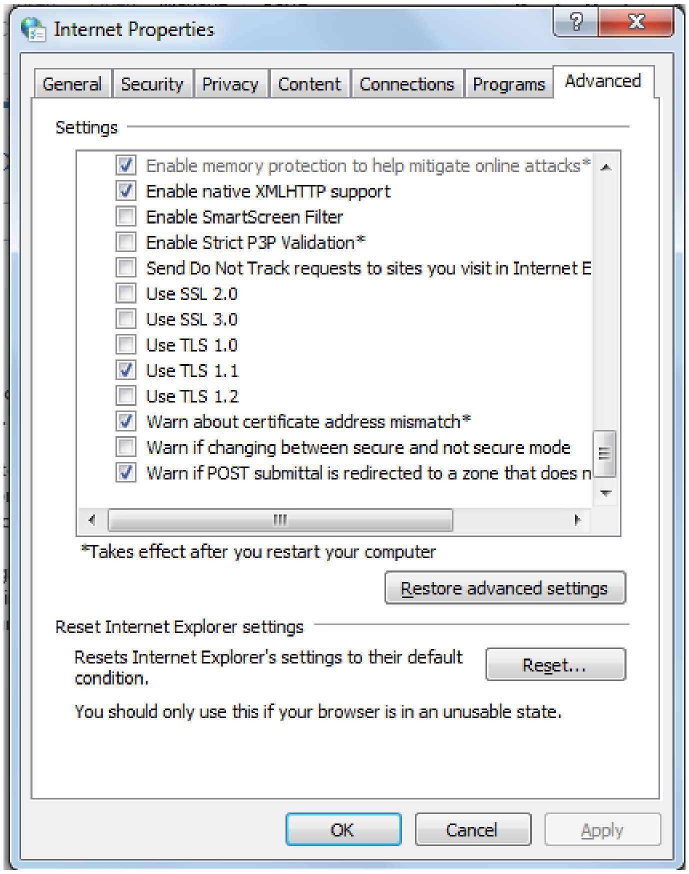
Figure 3.124: Changing privacy settings

9. Finally, click the **Apply** and **OK** buttons in Figure 3.124 to save the changes.

3.9.2.2 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 3.118).
2. Scroll down the **Settings** page that then appears until you find the **Show advanced settings** link (see Figure 3.119). 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 3.125: 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.

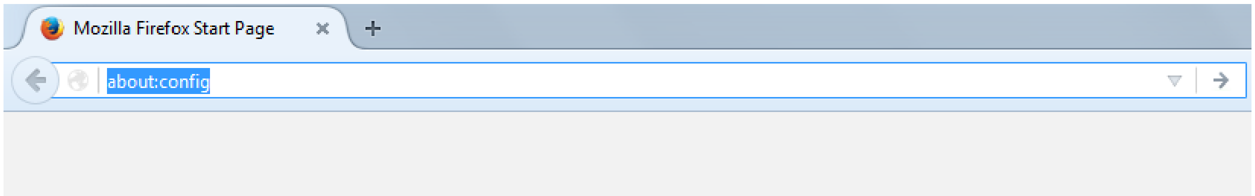
6. Finally, click the **Apply** and **OK** buttons in Figure 3.125 to save the changes.

3.9.3 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.

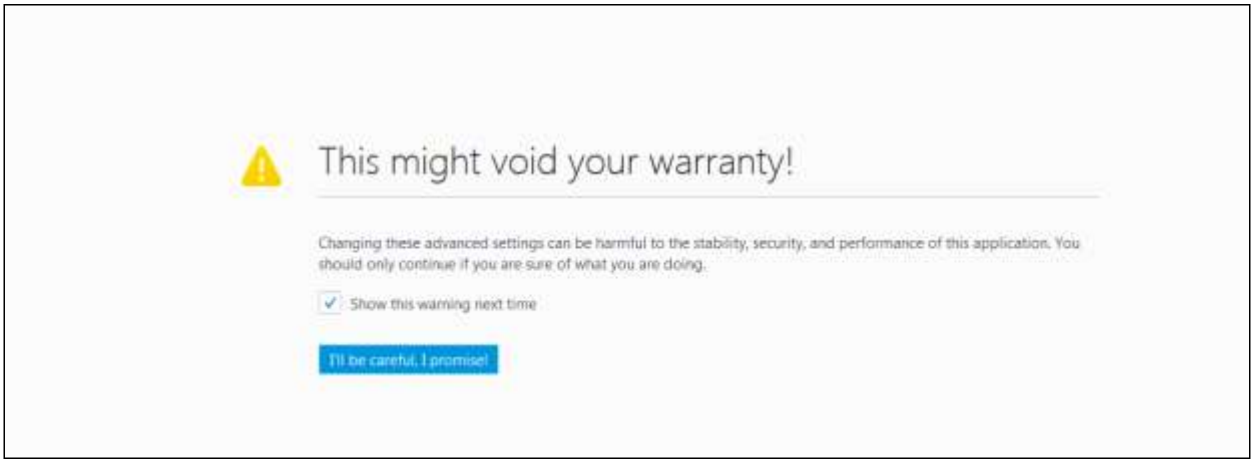
2. In the **Search** bar of the browser, type *about:config*.



about:config

Figure 3.126: Typing about:config in the Search bar

3. The warning message depicted by Figure 3.126 will then appear.



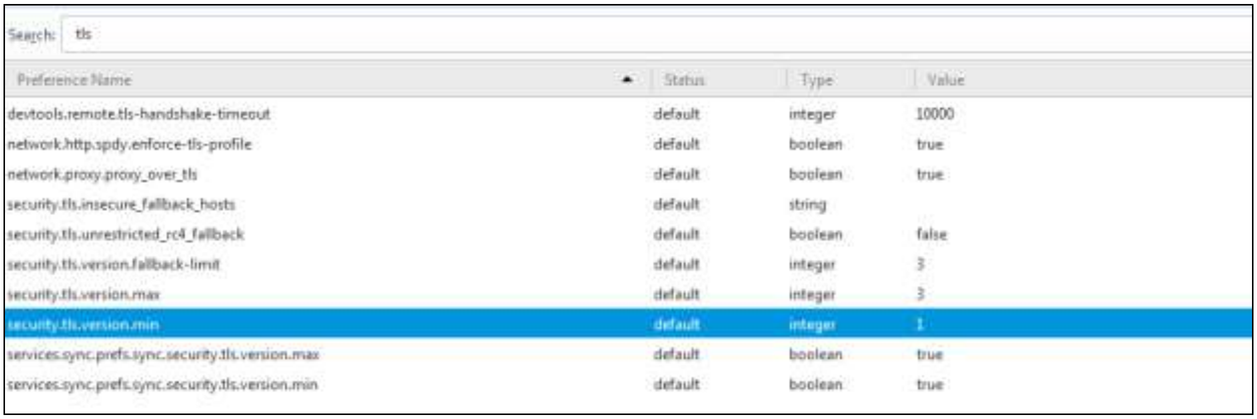
This might void your warranty!

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 3.127: The warning message that appears in the Firefox browser

4. Click the **I'll be careful, I promise!** button in Figure 3.127. Figure 3.128 will appear. Here, select the **security.tls.version.min** preference.

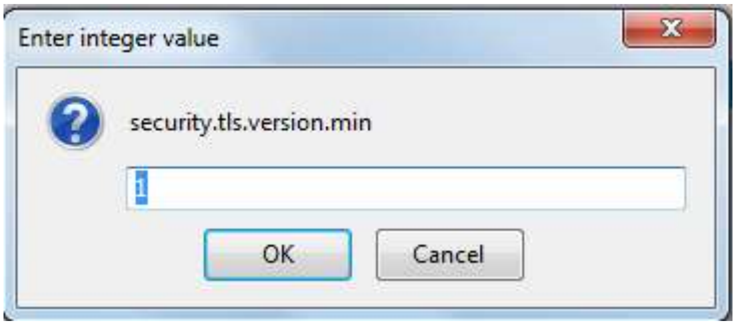


Search: tls

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 3.128: 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 3.129 will appear. Type **1** in the text box that appears next, and click the **OK** button therein (see Figure 3.129).



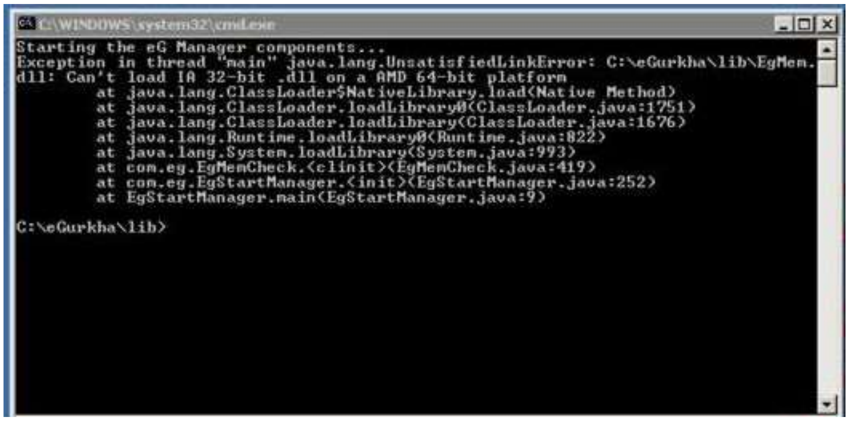
security.tls.version.min

1

Figure 3.129: Setting the value of the security.tls.version.min preference

3.10 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 3.130: 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.

3.11 Pre-requisites for Installing the eG Agent on Windows Environments

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

- 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 compatability of the filters before deployment.

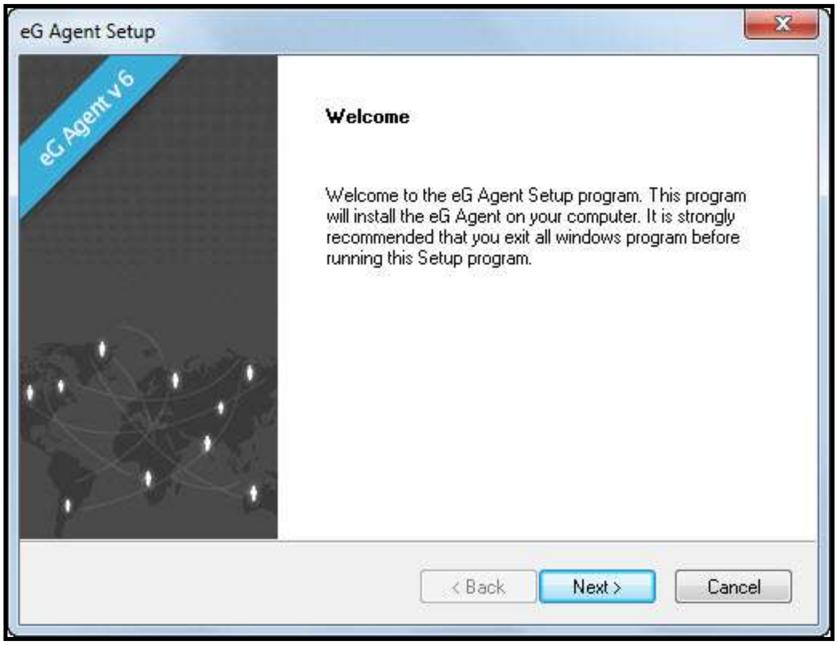
3.12 Installing and Configuring the eG Agent on Windows

The standard eG agent software for Windows is provided as a self-extracting set-up program called **eGAgent_win2008.exe**, which should be used to install the eG agent on a Windows 2008 / Windows Vista/ Windows 7 host. Likewise, you will have to use the program called **eGAgent_win2012.exe** to install the eG agent on a Windows 8 / Windows 10 host. By default, the eG agent is a 32-bit application. For agent deployments on 64-bit Windows 2008 / Windows Vista / Windows 7 hosts therefore, use the **eGAgent_win2008_x64.exe**. To install the eG agent on a 64-bit Windows 8 / Windows 2012/ Windows 10 host on the other hand, use the **eGAgent_win2012_x64.exe**. Similarly, to install on a 64-bit Windows 2016 host, use the **eGAgent_win2016_x64.exe**.

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, run the corresponding **exe**. The Welcome screen (see Figure 3.131) 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.

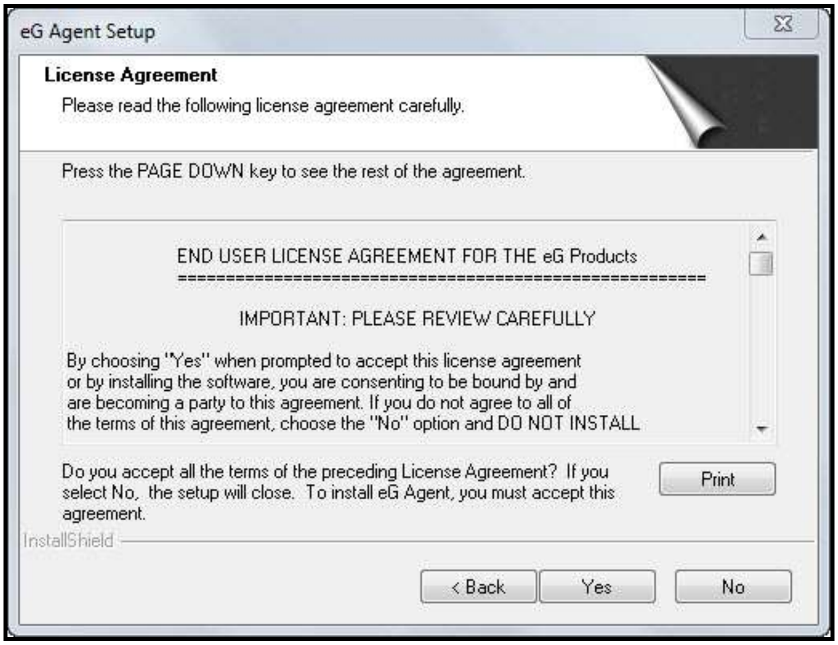


Welcome

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 3.131: Welcome screen of the eG agent setup program

2. Now, the user can view the eG license agreement (see Figure 3.132). 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.



License Agreement

Please read the following license agreement carefully.

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

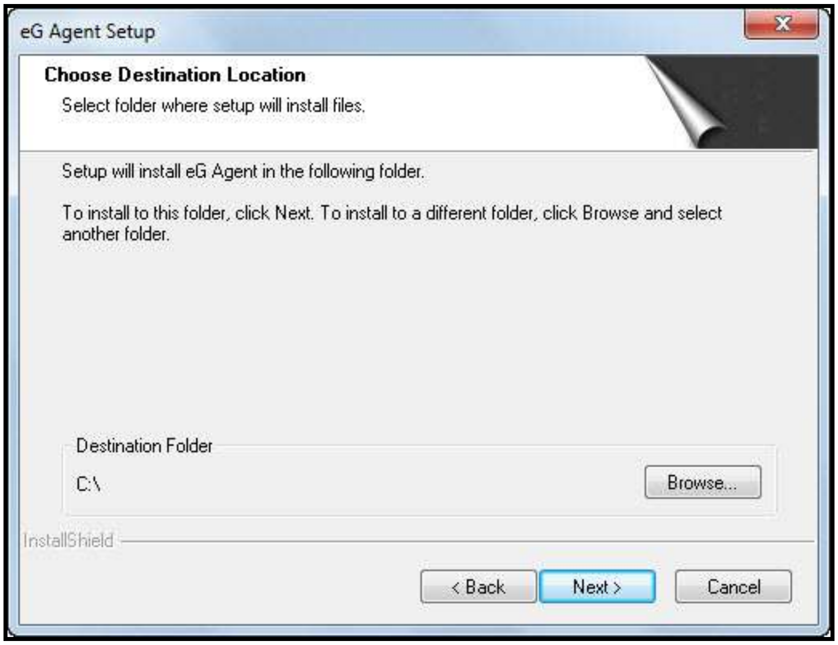
```
END USER LICENSE AGREEMENT FOR THE eG Products
==================================================

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
are becoming a party to this agreement. If you do not agree to all of
the terms of this agreement, choose the "No" option and DO NOT INSTALL
```

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 3.132: License agreement for the eG agent

3. The next step depicted by Figure 3.133 prompts the user to select the destination location for the eG agent if

he/she chooses not to install the agent in the default folder. If the eG manager resides on the host where the agent is being installed, the Setup program will place the agent in the same location as the manager. In this case, the screen depicted by Figure 3.133 will not appear.



eG Agent Setup

Choose Destination Location

Select folder where setup will install files.

Setup will install eG Agent in the following folder.

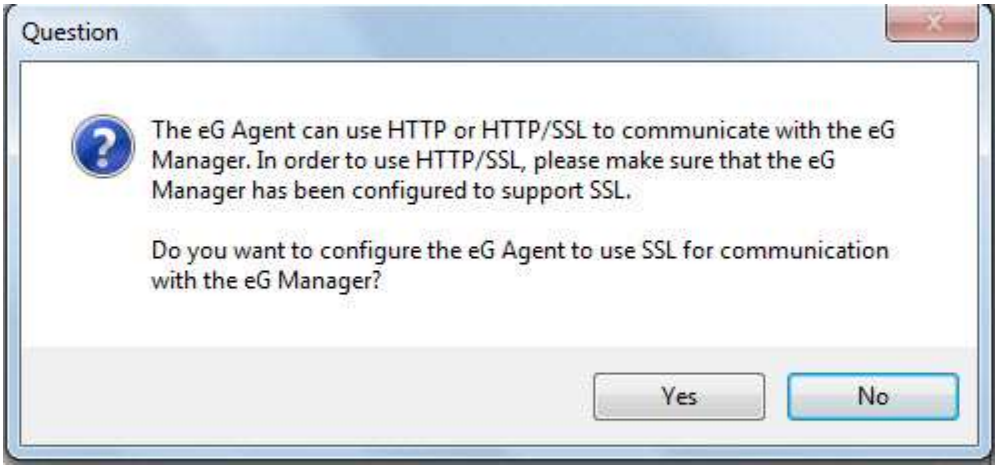
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\

Figure 3.133: Location of the eG agent

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 3.134). Click on the **Yes** button to confirm SSL support for the agent.



Question

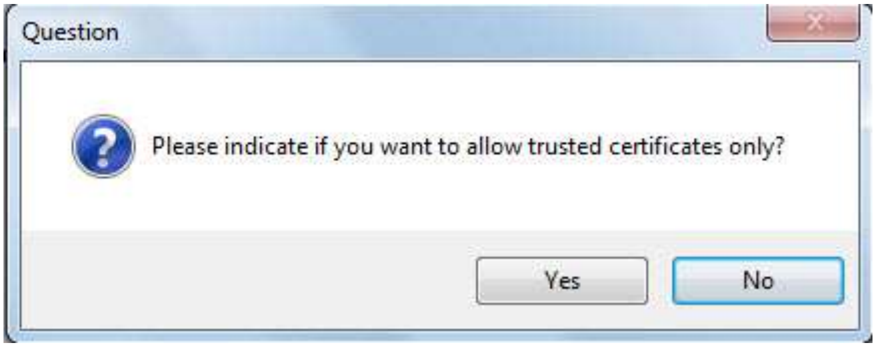
The eG Agent can use HTTP or HTTP/SSL to communicate with the eG Manager. In order to use HTTP/SSL, please make sure that the eG Manager has been configured to support SSL.

Do you want to configure the eG Agent to use SSL for communication with the eG Manager?

Figure 3.134: A message box requesting the user's confirmation to enable SSL support for the eG agent

5. Now, Figure 3.135 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.

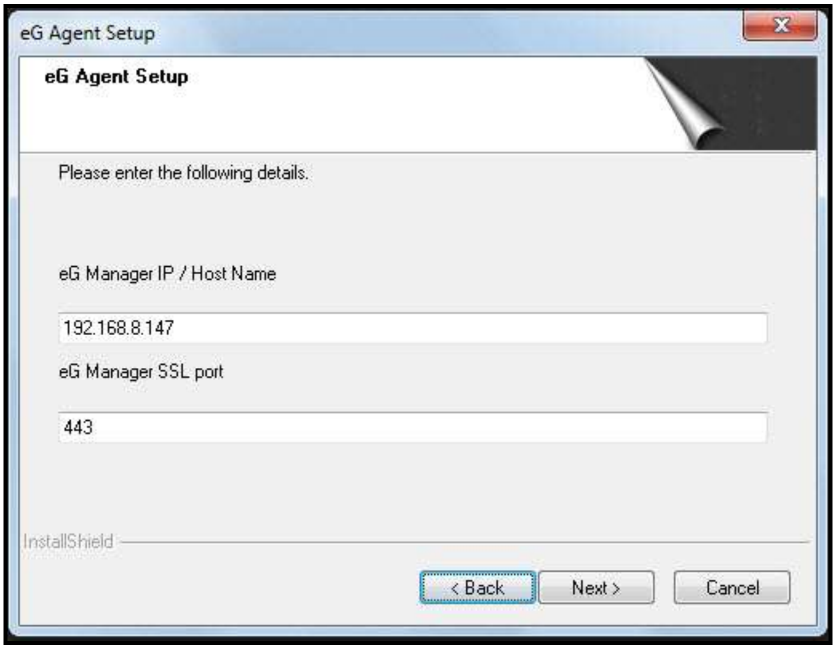


Question

Please indicate if you want to allow trusted certificates only?

Figure 3.135: A message box requesting your confirmation to allow only trusted certificates

6. Clicking on either button (in Figure 3.135) will reveal Figure 3.136 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

192.168.8.147

eG Manager SSL port

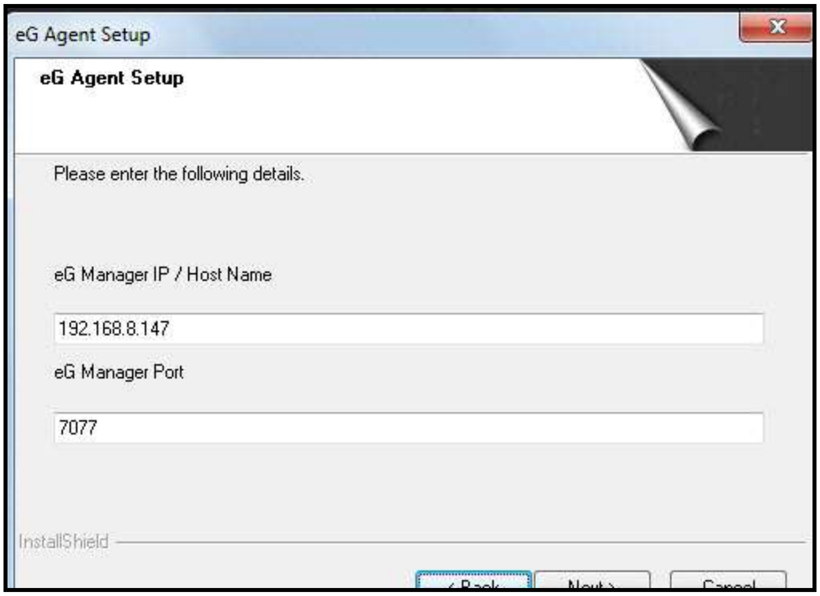
443

Figure 3.136: Specifying the IP/hostname and SSL port of the eG manager

Note

If you have chosen to allow only trusted certificates, then ensure that the IP/hostname provided in Figure 3.136 matches that of the certificate. Then, follow the procedure detailed in Section 3.13 once the agent installation is complete.

7. If you select the **No** button in Figure 3.136, then setup will attempt to configure the agent's operational environment with the details of the eG manager that the agent should communicate with. For this purpose, the setup process prompts the user for the hostname (or IP address) and the port number of the eG manager (see Figure 3.137). However, 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

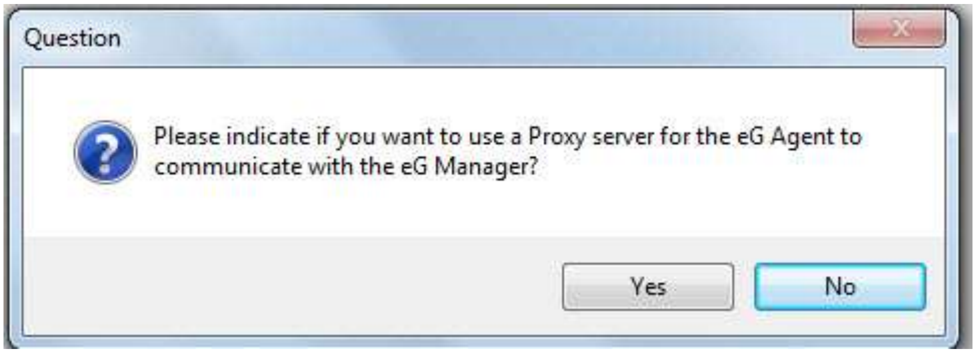
192.168.8.147

eG Manager Port

7077

Figure 3.137: 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 3.138. The default option is **No**.

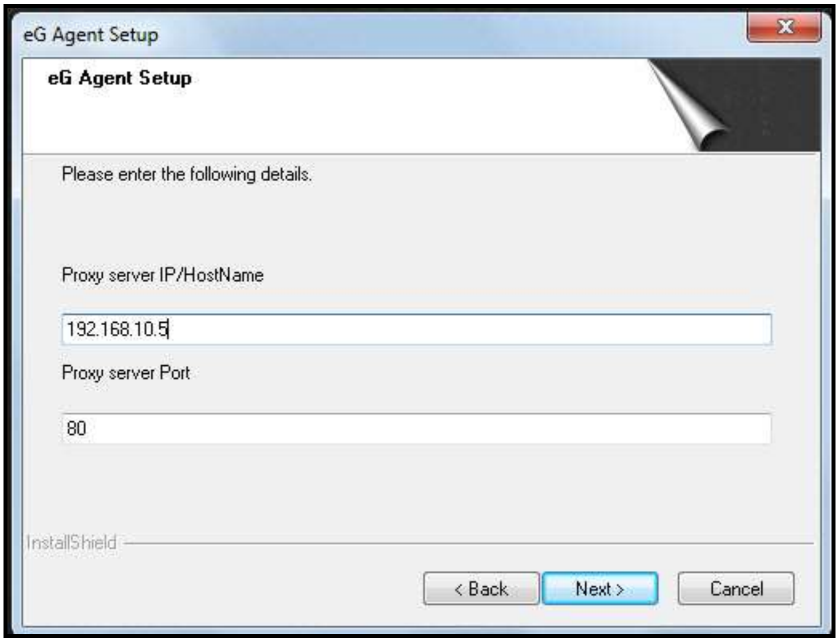


Question

Please indicate if you want to use a Proxy server for the eG Agent to communicate with the eG Manager?

Figure 3.138: 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 3.139. 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

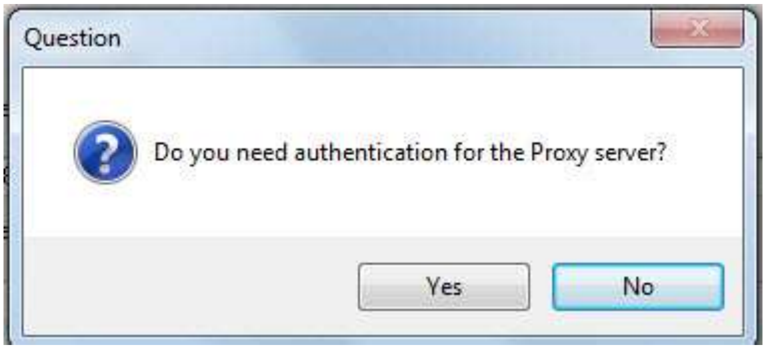
192.168.10.5

Proxy server Port

80

Figure 3.139: 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 3.140). The default option is **No**.



Question

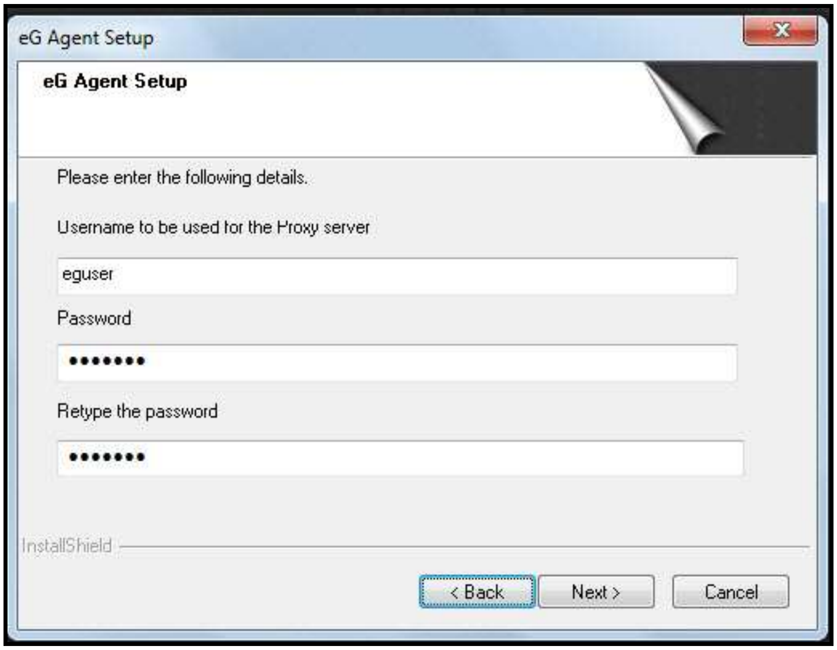
Do you need authentication for the Proxy server?

Figure 3.140: Setup seeking the confirmation regarding authentication of the proxy server

Note

To get the eG agent to communicate via an ISA proxy server to the eG manager, follow the steps discussed in Section 3.20.

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 3.141.



Please enter the following details.

Username to be used for the Proxy server

eguser

Password

•••••••

Retype the password

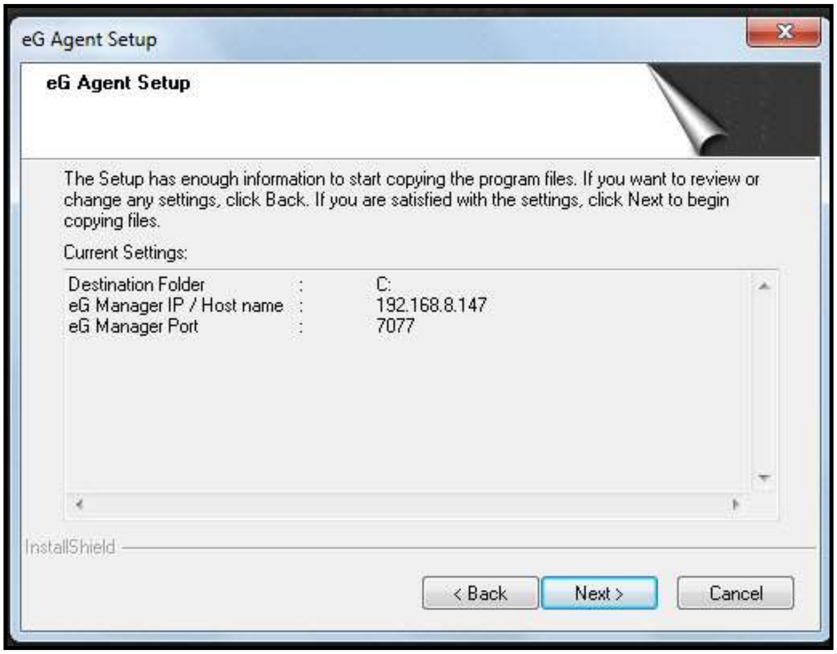
•••••••

Figure 3.141: 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.

The next step displays all the details that have been provided so far by the user as in Figure 3.142.



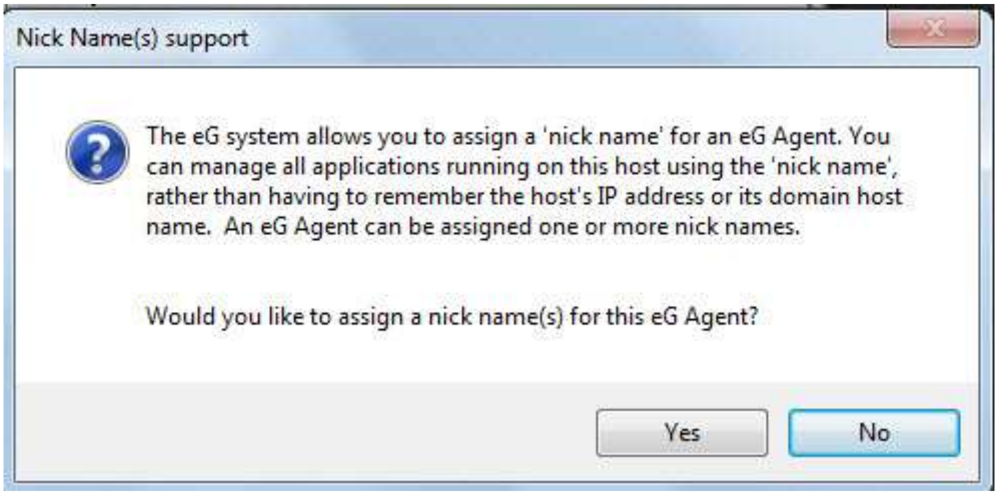
The Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Destination Folder          :        C:
eG Manager IP / Host name   :        192.168.8.147
eG Manager Port             :        7077
```

Figure 3.142: Information specified by the user at the various stages of the setup process

1. 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 3.143 provides the user the option of specifying a nick name.

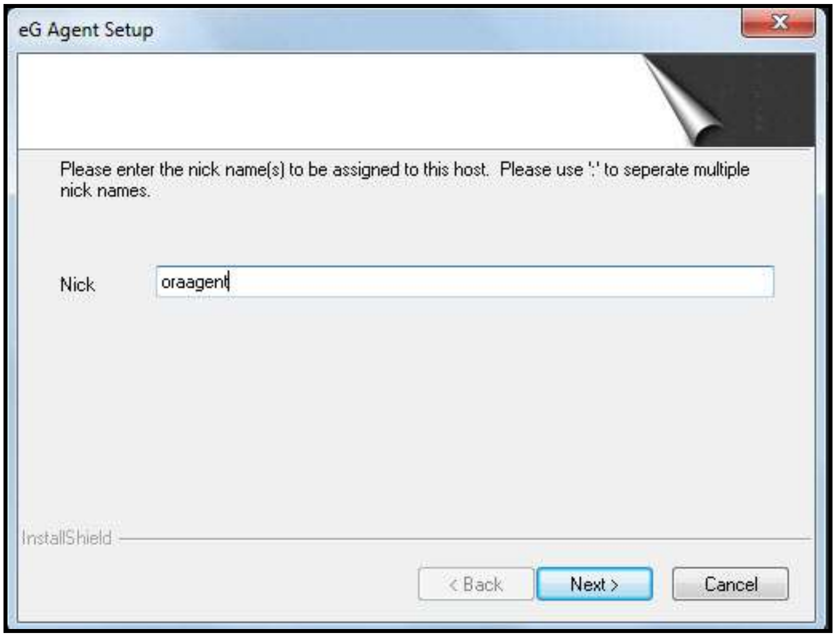


The eG system allows you to assign a 'nick name' for an eG Agent. You can manage all applications running on this host using the 'nick name', rather than having to remember the host's IP address or its domain host name. An eG Agent can be assigned one or more nick names.

Would you like to assign a nick name(s) for this eG Agent?

Figure 3.143: Setup requesting the user’s confirmation to assign a nick name for the eG agent

2. Clicking on the **Yes** button will then require the user to specify the nick name (see Figure 3.144).



eG Agent Setup

Please enter the nick name(s) to be assigned to this host. Please use ':' to seperate multiple nick names.

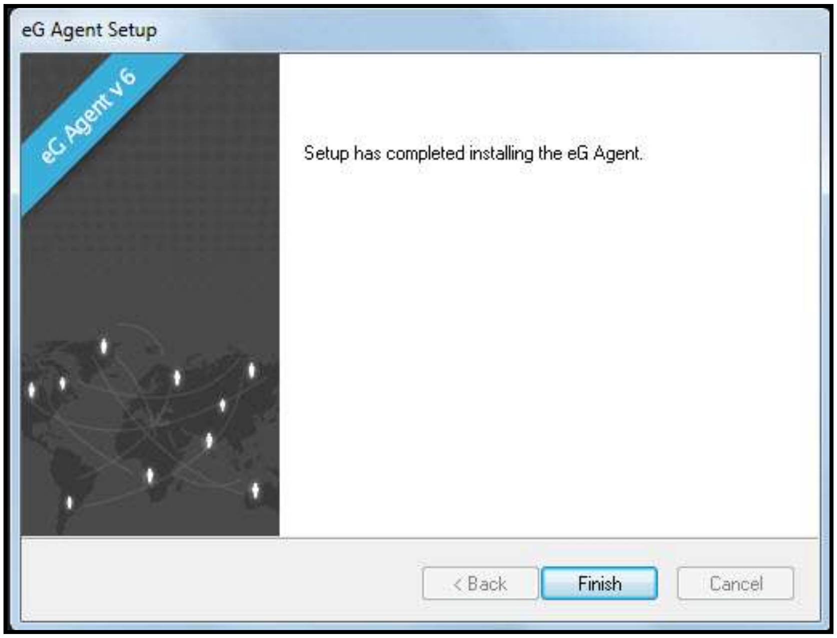
Nick oraagent

Figure 3.144: 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.

3. If the configuration process succeeds, the following screen will be displayed (see Figure 3.145). Clicking on the **Finish** button will exit the Setup.



Setup has completed installing the eG Agent.

Figure 3.145: The completion of the eG agent setup

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\SecurePipeServ ers\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**

3.13 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.

3.13.1 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 3.4.1.1 or 3.4.2.1 of this document).** 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 3.4.1.1 or 3.4.2.1 of this document).** 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 3.4.1.1 or 3.4.2.1 of this document)**.

- **-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.

3.13.2 Importing the SSL Certificate into the JRE of the eG Agent

To achieve this, do the following:

1. 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%

2. 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 3.4.1.1 or 3.4.2.1 of this document, 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**.

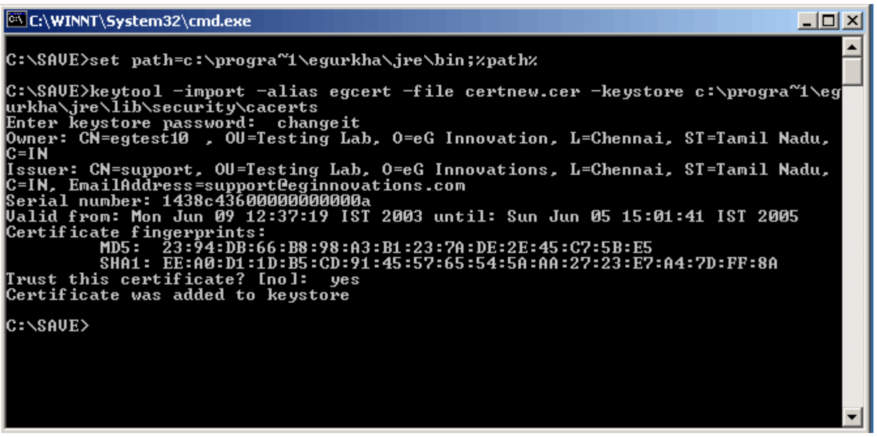
   - **-file** : the full path to the **.cer** file that was created in **Section 3.13.1**

   - **-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 3.4.1.1 or 3.4.2.1 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 3.4.1.1 or 3.4.2.1, as the case may be)**. For the default certificate bundled with the eG manager, the password should be *eginnovations.*

3. Finally, the command will request your confirmation to make the imported certificate a trusted one. Enter **yes** to trust the certificate.

4. If the processing was successful, then a message stating that the *"Certificate was added to keystore"* will appear. Figure 5 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 1: The process of importing and trusting the manager certificate

- Now, start the agent.

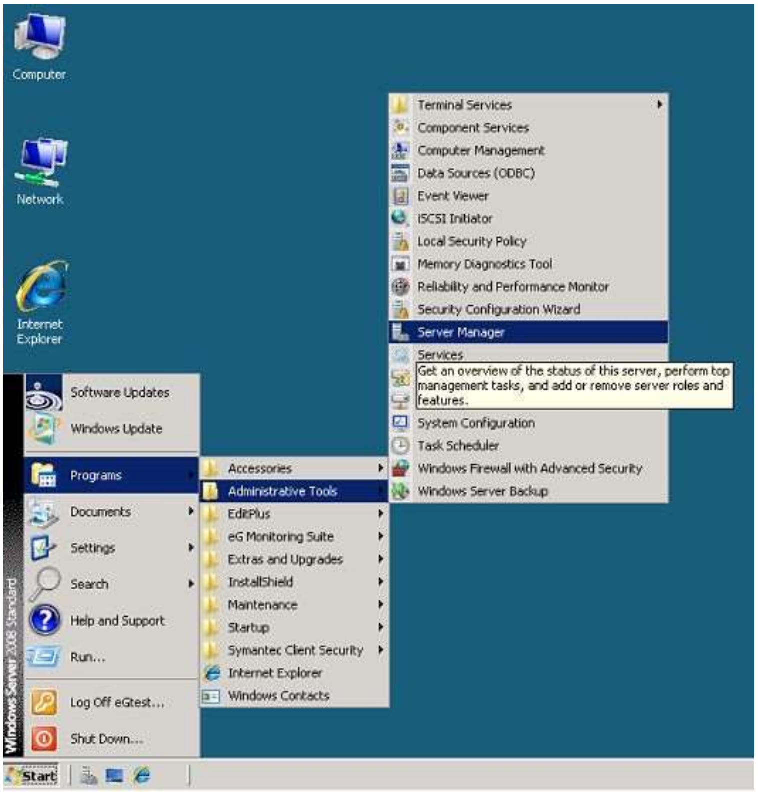
3.14 Configuring the eG Agent to Monitor an IIS Web Server

The eG agent can monitor an IIS web server only if the **Web Server** role is configured on the target Windows server.

Typically, for an IIS web server to function on a Windows 2008/2012/2016 server, a **Web Server Role** should be configured on the server. The **Web Server** role lets you share information with users on the Internet, an intranet, or an extranet. If such a role does not exist on a Windows 2008/2012/2016 server, then, you cannot monitor the transactions to the IIS web server on that host; this is because, the ISAPI filter required for transaction monitoring cannot be installed on these servers without the **Web Server** role.

To configure this **Web Server** role on a Windows 2008/2012/2016 server, follow the steps detailed below:

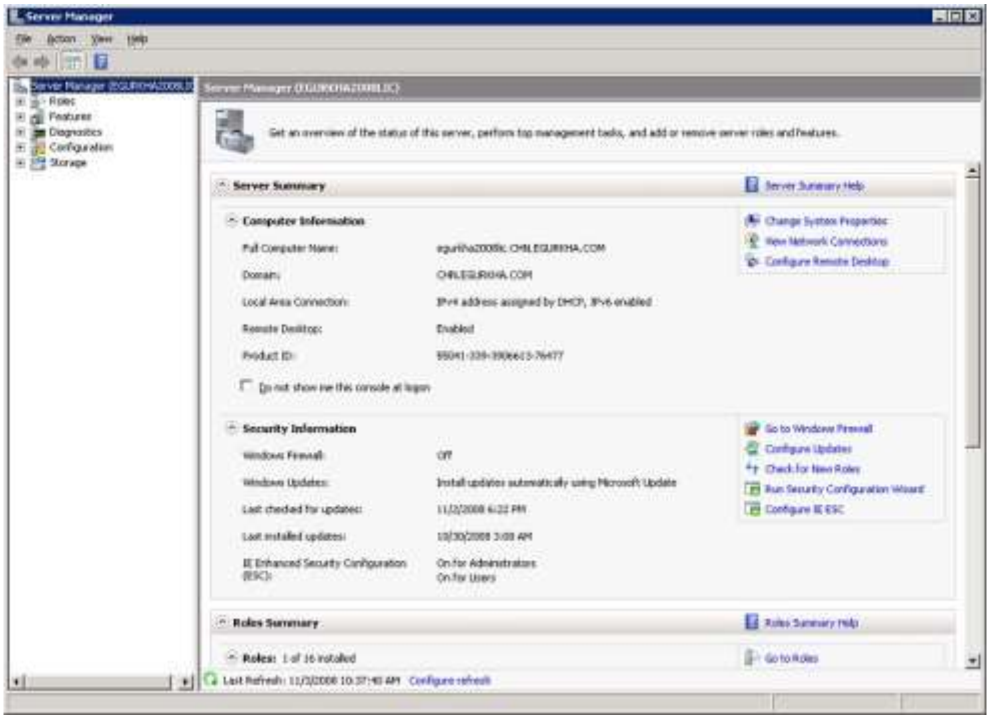
1. Login to the Windows server as a local/domain administrator.
2. Open the **Server Manager** console by following the menu sequence, Start -> Programs -> Administrative Tools -> Server Manager (see Figure 3.146).



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Figure 3.146: Opening the Server Manager

3. The **Server Manager** console then appears (see Figure 3.147).



Server Manager (EGURKHA2008LC)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

Computer Information

Full Computer Name: egurkha2008lc.CHNLEGURKHA.COM

Domain: CHNLEGURKHA.COM

Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled

Remote Desktop: Enabled

Product ID: 55041-339-3906613-76477

☐ Do not show me this console at logon

Security Information

Windows Firewall: Off

Windows Updates: Install updates automatically using Microsoft Update

Last checked for updates: 11/2/2008 6:22 PM

Last installed updates: 10/30/2008 3:00 AM

IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

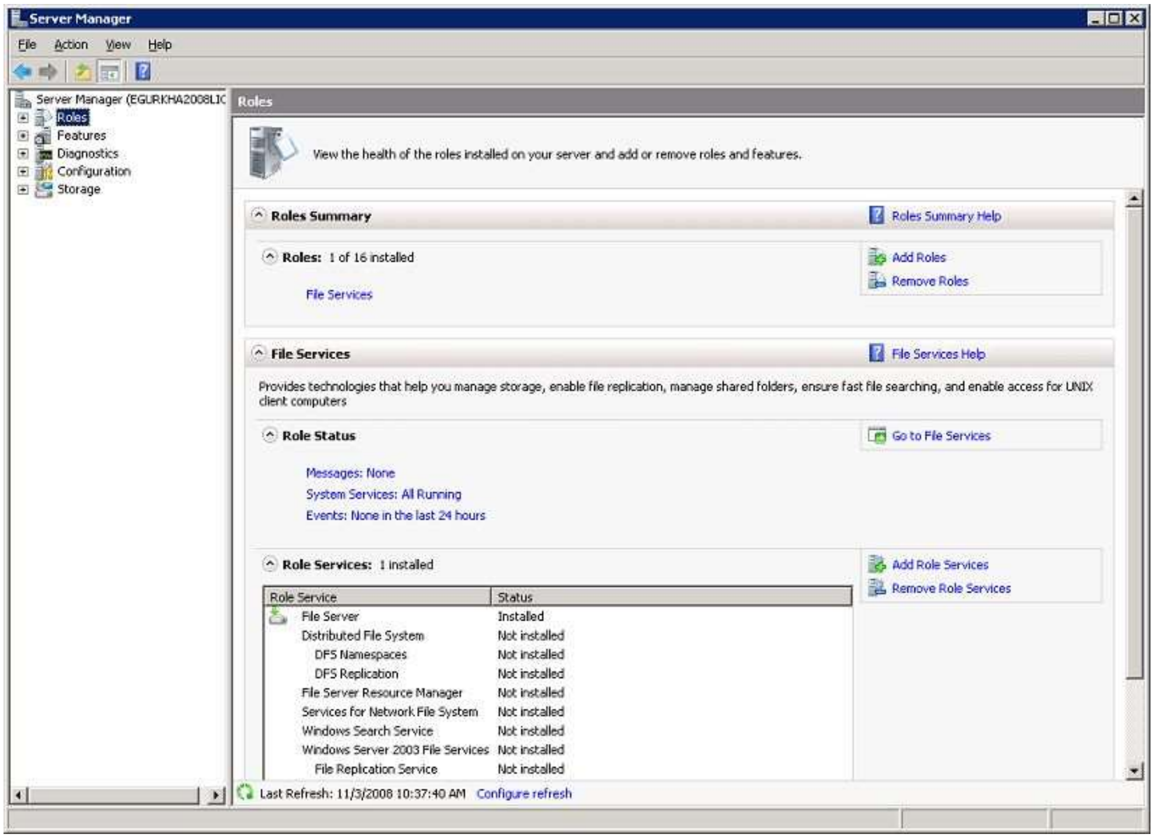
Roles Summary

Roles: 1 of 16 installed

Last Refresh: 11/3/2008 10:37:40 AM

Figure 3.147: The Server Manager console

4. In the **Server Manager** console, click on the **Roles** node in the tree-structure in the left panel of the console. The information in the right-panel will change to display a **Roles Summary** and related details. To add a new role, click on the **Add Roles** option in the right panel pf Figure 3.148.



Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary — Roles Summary Help

Roles: 1 of 16 installed — Add Roles, Remove Roles

File Services

File Services — File Services Help

Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Role Status — Go to File Services

Messages: None
System Services: All Running
Events: None in the last 24 hours

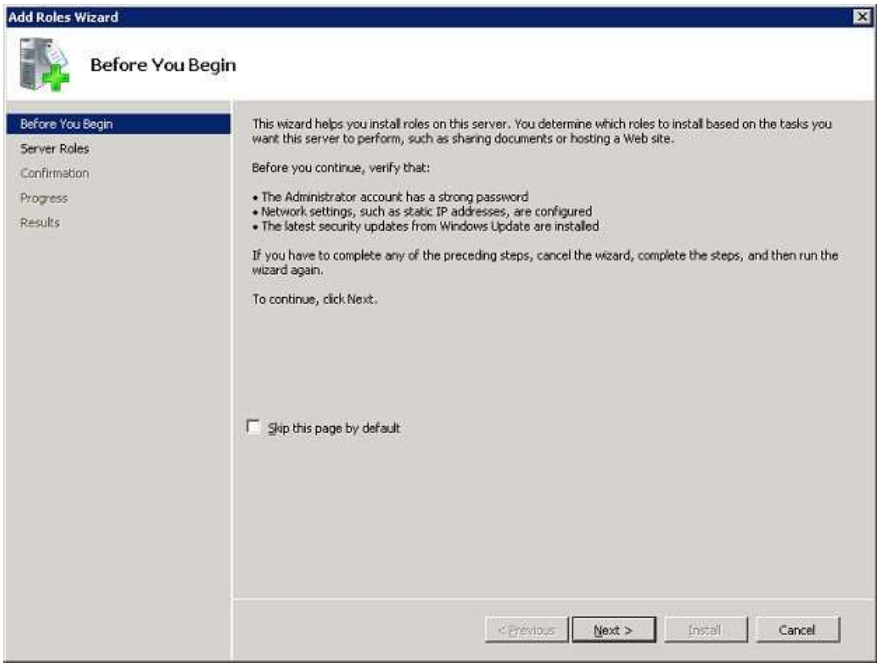
Role Services: 1 installed — Add Role Services, Remove Role Services

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed
Services for Network File System	Not installed
Windows Search Service	Not installed
Windows Server 2003 File Services	Not installed
File Replication Service	Not installed

Last Refresh: 11/3/2008 10:37:40 AM Configure refresh

Figure 3.148: Clicking on the Roles node in the tree-structure

5. This will invoke the **Add Roles Wizard**. Click on the **Next** button in the welcome screen of Figure 3.149 to proceed with the role creation.



This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

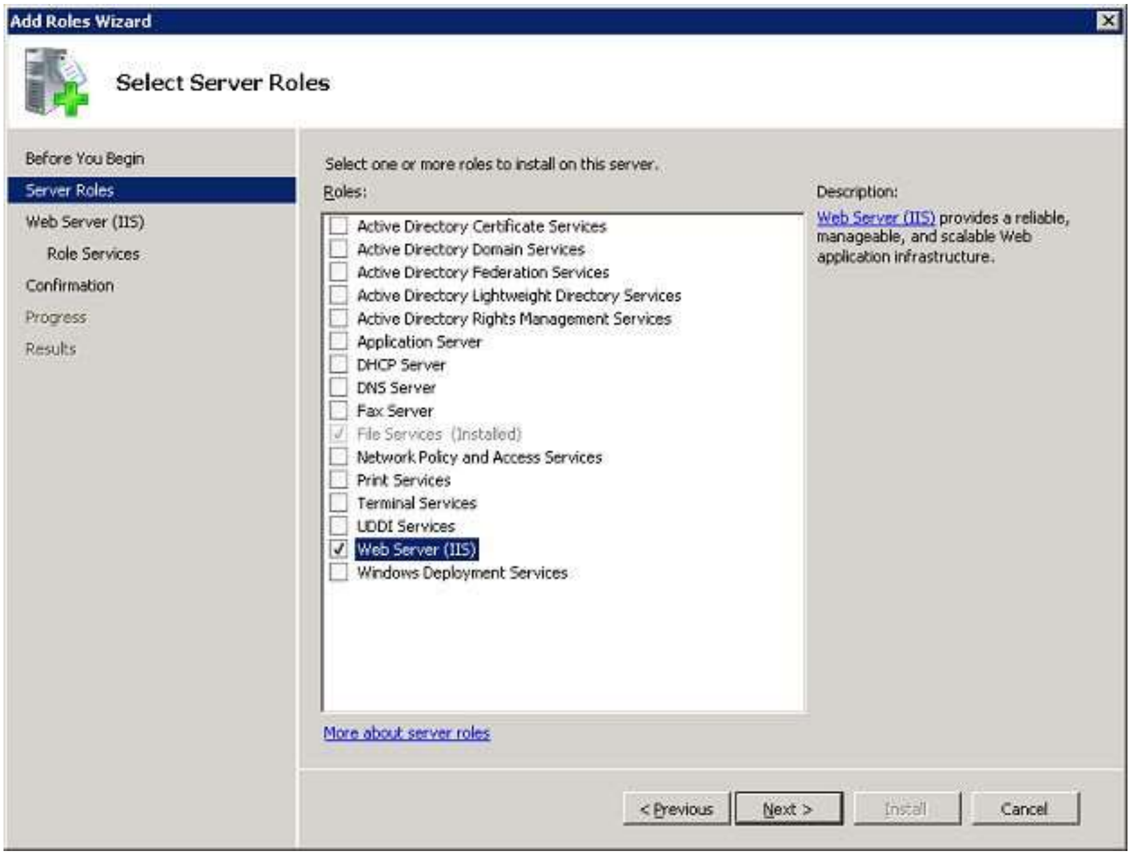
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Figure 3.149: Clicking on the Next button in the welcome screen of the Add Roles Wizard

6. The next step of the wizard prompts you to pick one/more roles to install on the Windows 2008/2012 server. Select the **Web Server (IIS)** role depicted by Figure 3.150 to install it. Then, click the **Next** button to proceed.



Select one or more roles to install on this server.

Roles:

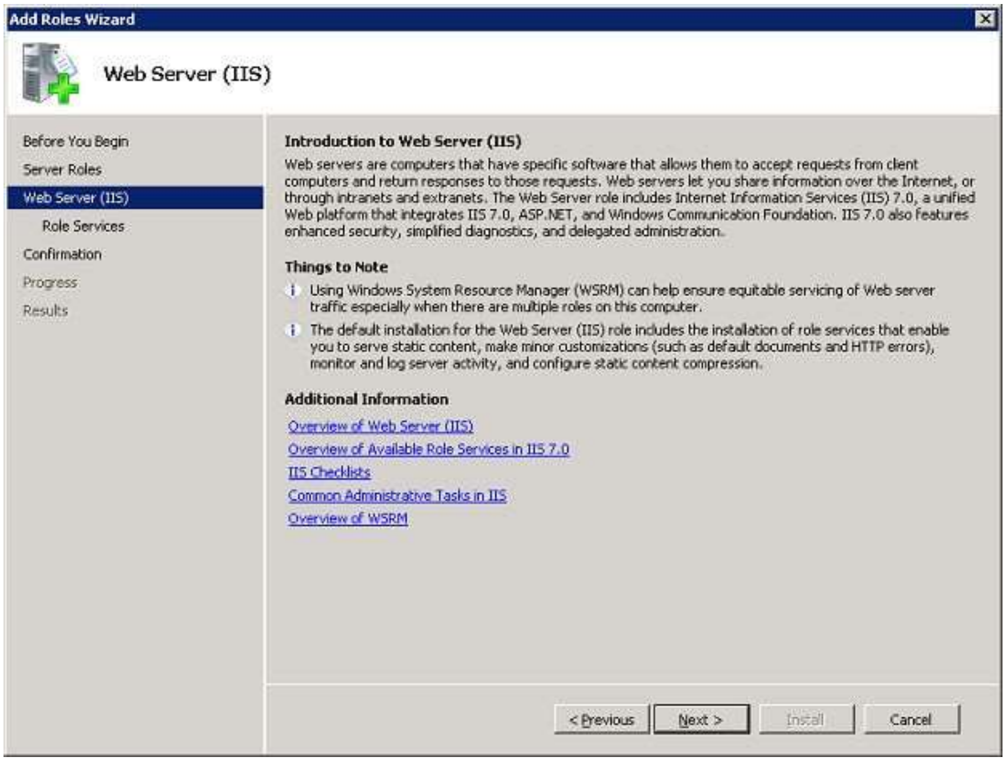
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ☑ File Services (Installed)
- □ Network Policy and Access Services
- □ Print Services
- □ Terminal Services
- □ UDDI Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services

Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 3.150: Selecting the Web Server (IIS) role

7. Then, when Figure 3.151 appears, click on the **Next** button to switch to the next step of the role installation.



Introduction to Web Server (IIS)

Web servers are computers that have specific software that allows them to accept requests from client computers and return responses to those requests. Web servers let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 7.0, a unified Web platform that integrates IIS 7.0, ASP.NET, and Windows Communication Foundation. IIS 7.0 also features enhanced security, simplified diagnostics, and delegated administration.

Things to Note

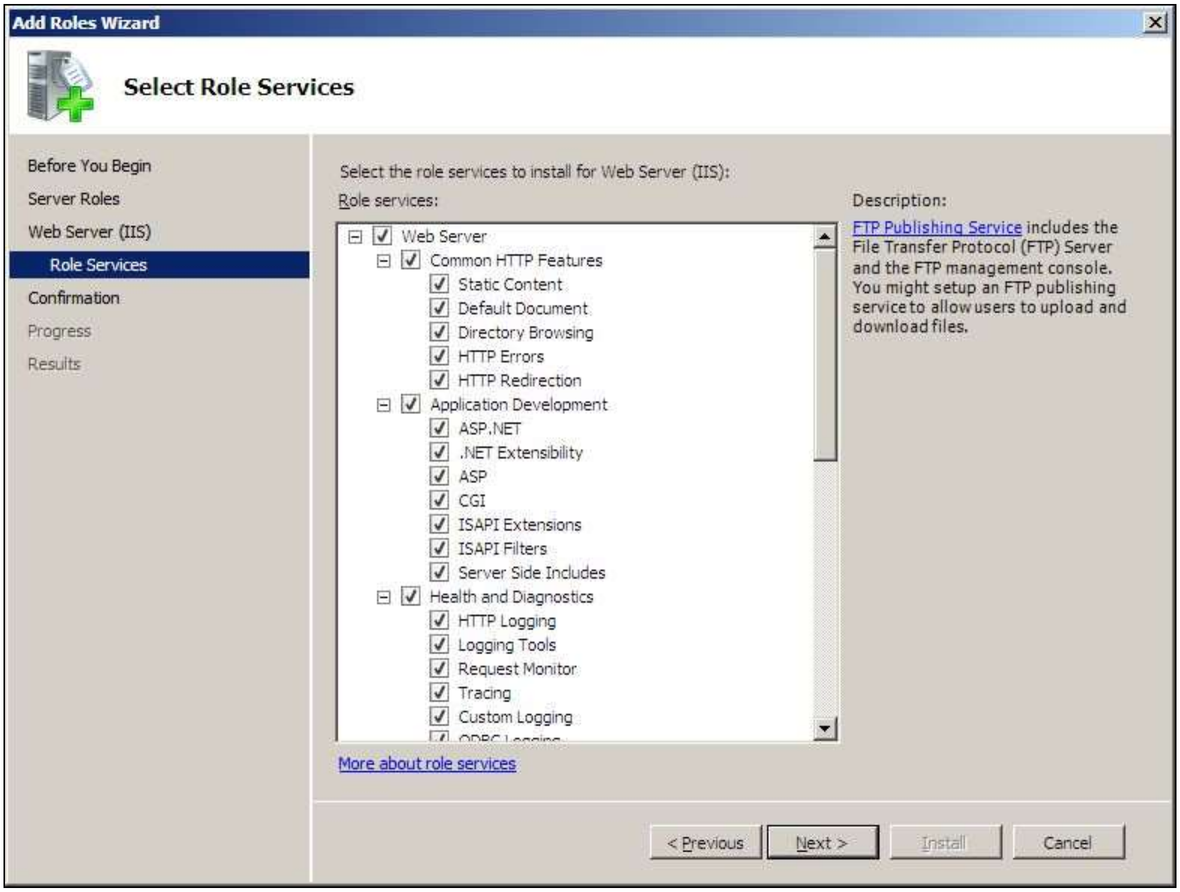
- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Additional Information

Overview of Web Server (IIS)
Overview of Available Role Services in IIS 7.0
IIS Checklists
Common Administrative Tasks in IIS
Overview of WSRM

Figure 3.151: An introduction to the web server role

8. The next step will prompt you to choose the role services. Select all the listed services and click the **Next** button to proceed. **Make sure that the IIS Management Scripts and Tools feature in particular is installed and enabled for the 'Web Server' role.**



Add Roles Wizard

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ HTTP Redirection
  - ☑ Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - ☑ ASP
    - ☑ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - ☑ Server Side Includes
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - ☑ Logging Tools
    - ☑ Request Monitor
    - ☑ Tracing
    - ☑ Custom Logging
    - ☑ ODBC Logging

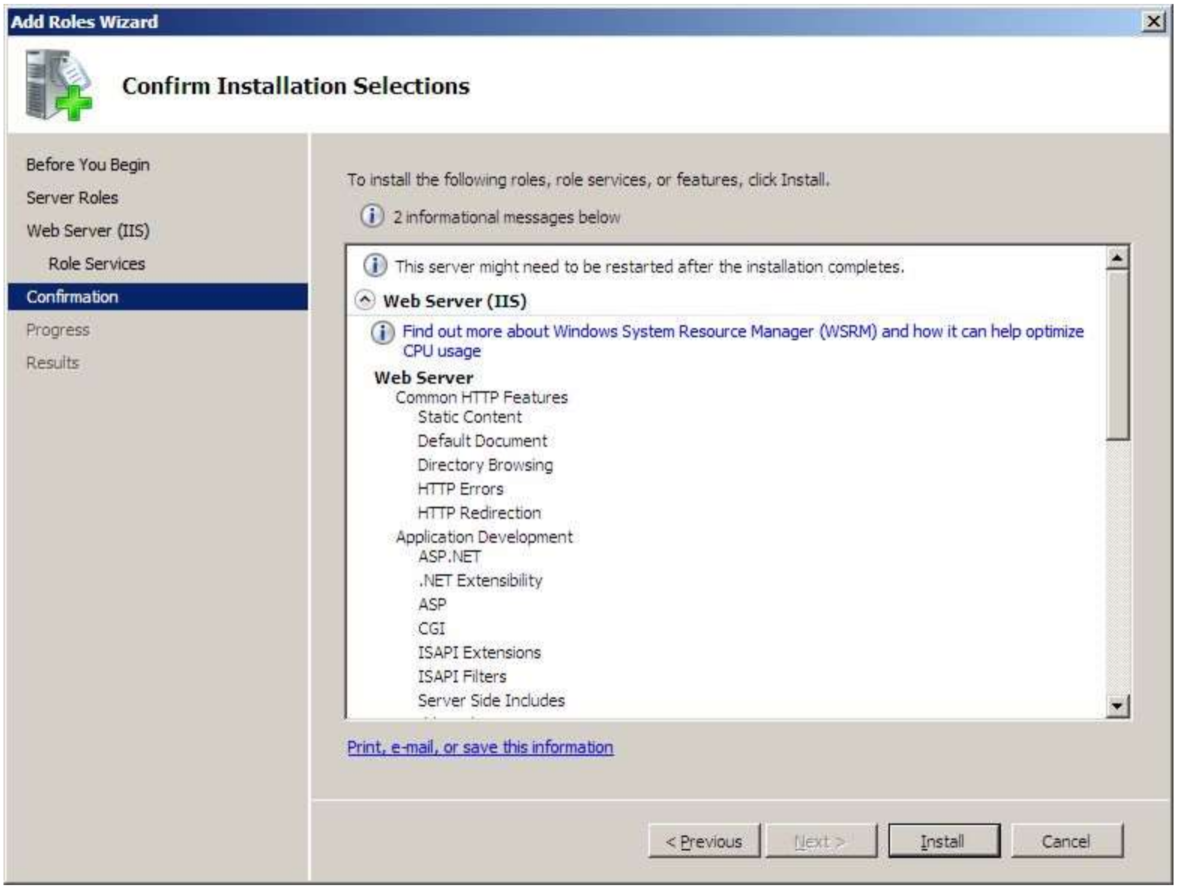
Description:

FTP Publishing Service includes the File Transfer Protocol (FTP) Server and the FTP management console. You might setup an FTP publishing service to allow users to upload and download files.

More about role services

Figure 3.152: Selecting the required role services

9. The screen that appears subsequently provides a summary of your specifications. After reviewing your selections, you can confirm installation of the chosen web server role by clicking on the **Install** button in Figure 3.153.



To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

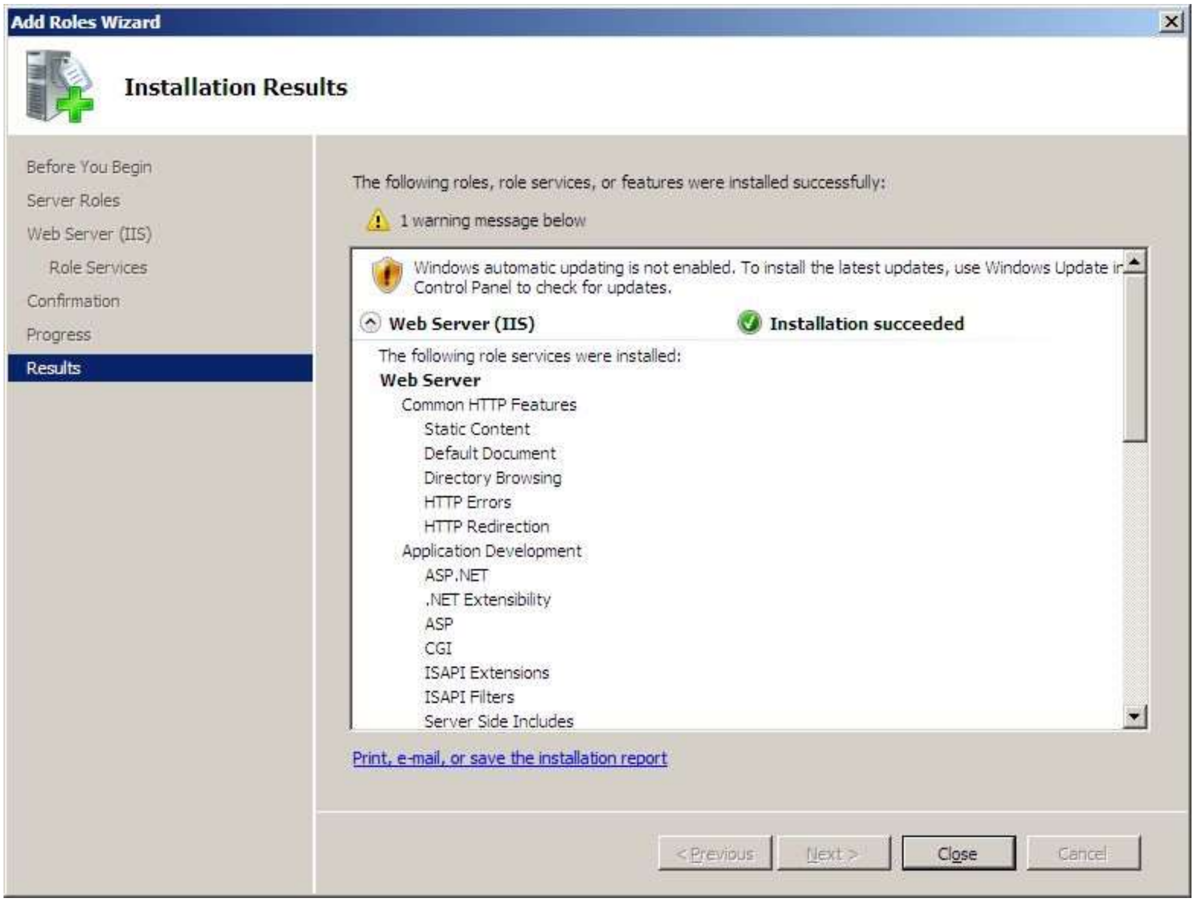
Web Server (IIS)

Find out more about Windows System Resource Manager (WSRM) and how it can help optimize CPU usage

Web Server
Common HTTP Features
Static Content
Default Document
Directory Browsing
HTTP Errors
HTTP Redirection
Application Development
ASP.NET
.NET Extensibility
ASP
CGI
ISAPI Extensions
ISAPI Filters
Server Side Includes

Figure 3.153: Installing the web server role

10. Once installation completes successfully, Figure 3.154 will appear confirming the success of the installation.



The following roles, role services, or features were installed successfully:

1 warning message below

Windows automatic updating is not enabled. To install the latest updates, use Windows Update in Control Panel to check for updates.

Web Server (IIS) — Installation succeeded

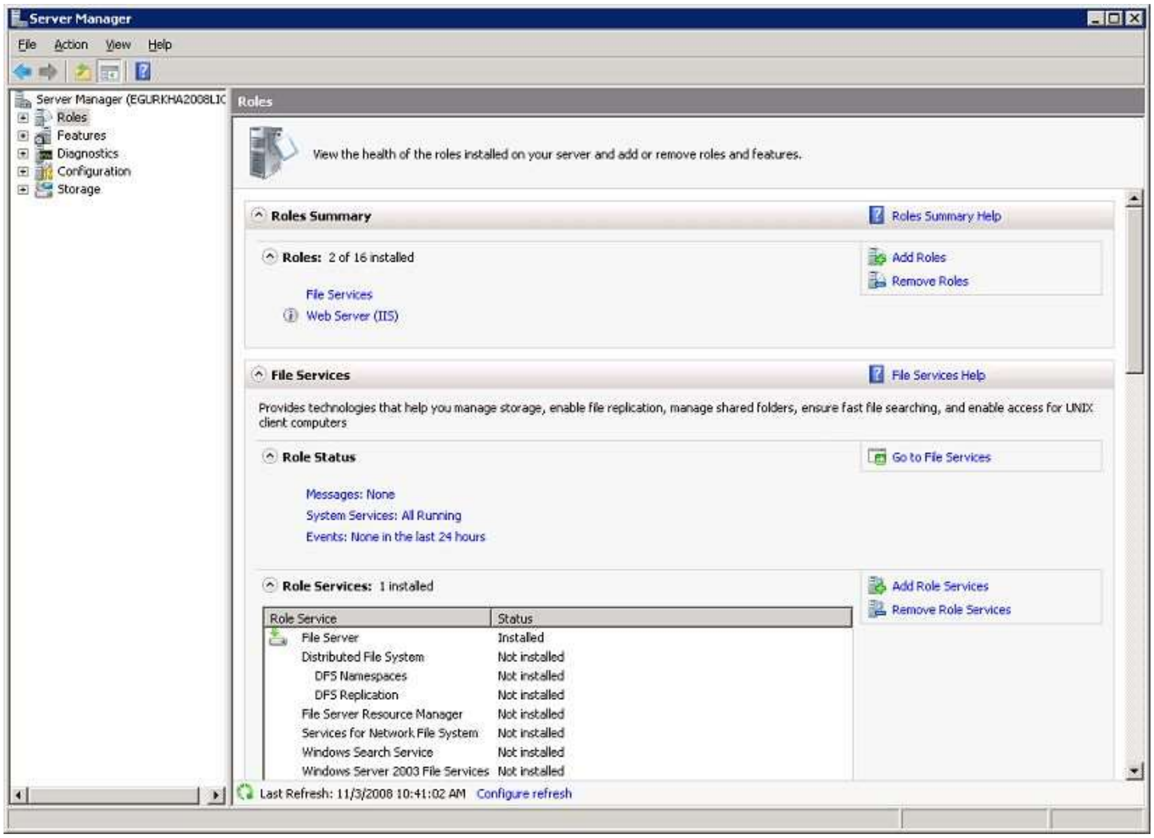
The following role services were installed:

Web Server

- Common HTTP Features
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - HTTP Redirection
- Application Development
  - ASP.NET
  - .NET Extensibility
  - ASP
  - CGI
  - ISAPI Extensions
  - ISAPI Filters
  - Server Side Includes

Figure 3.154: A message indicating that installation was successful

11. Click on the **Close** button in Figure 3.154 to close the wizard. Figure 3.155 will then appear displaying the newly installed role.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 2 of 16 installed

File Services
Web Server (IIS)

Provides technologies that help you manage storage, enable file replication, manage shared folders, ensure fast file searching, and enable access for UNIX client computers

Role Status

Messages: None
System Services: All Running
Events: None in the last 24 hours

Role Services: 1 installed

Role Service	Status
File Server	Installed
Distributed File System	Not installed
DFS Namespaces	Not installed
DFS Replication	Not installed
File Server Resource Manager	Not installed
Services for Network File System	Not installed
Windows Search Service	Not installed
Windows Server 2003 File Services	Not installed

Last Refresh: 11/3/2008 10:41:02 AM

Figure 3.155: The Roles page in the right panel displaying the Web Server (IIS) role that was just installed

3.15 Cofiguring the eG Agent to Monitor the Web Site Transactions on an IIS Web Server

Note

eG cannot monitor Web transactions to web sites operating on an IIS web server 8.x.

To perform web site transaction monitoring on an IIS web server executing on Windows 2008/2012/2016, you need to install and configure **Advanced Logging** on the target IIS web server, soon after you create the **Web Server** role on the Windows server.

IIS Advanced Logging provides enhanced data collection and real-time server and client-side logging capabilities. It can be managed by using IIS Manager and other tools that can work with the IIS configuration system.

The Advanced Logging feature supports complex Web and media delivery scenarios that demand flexibility and control. These scenarios may require custom logging fields, real-time access to data, greater control over what gets logged and when, extensibility for new sources of data, the ability to consolidate log data posted by clients and correlate it to server data, the option of sharing data from various sources and storing it in multiple logs, capturing system-state information, inclusion of canceled requests in logs, and even logging multiple times per request.

In order to monitor the web transactions to IIS, the eG agent requires that the **Advanced Logging** be installed and configured on IIS.

The steps in this regard have been discussed below:

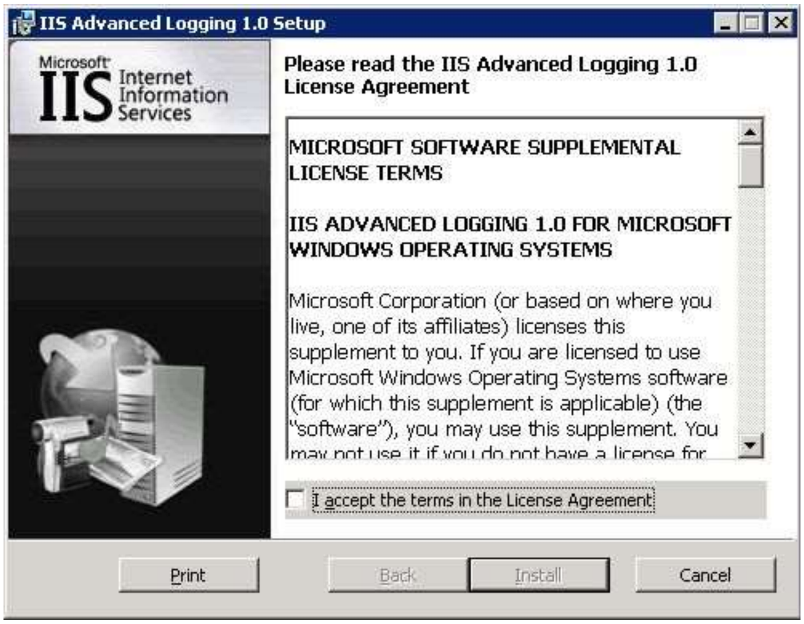
1. Login to the IIS host.

2. Download the executable that installs the **Advanced Logging** feature from any of the following URLs, depending upon whether the IIS installation is a 32-bit one or a 64-bit one:

32-bt/64-bit	URL
32-bit	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=4d110e78-95cb-4764-959c-b8afc33df496&displaylang=en
64-bit	http://www.microsoft.com/downloads/en/details.aspx?FamilyID=793051A8-36A0-4342-BDFE-47A6B0E3488F

3. Once the download is complete, go to the directory to which the executable was downloaded and double-click on it.

4. Figure 3.156 will then appear. Accept the license by selecting the **I accept the terms in the License Agreement** check box, and click on the **Install** button to proceed with the installation.


IIS Advanced Logging 1.0 Setup
Microsoft IIS Internet Information Services
Print
Back
Install
Cancel

Please read the IIS Advanced Logging 1.0 License Agreement

MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

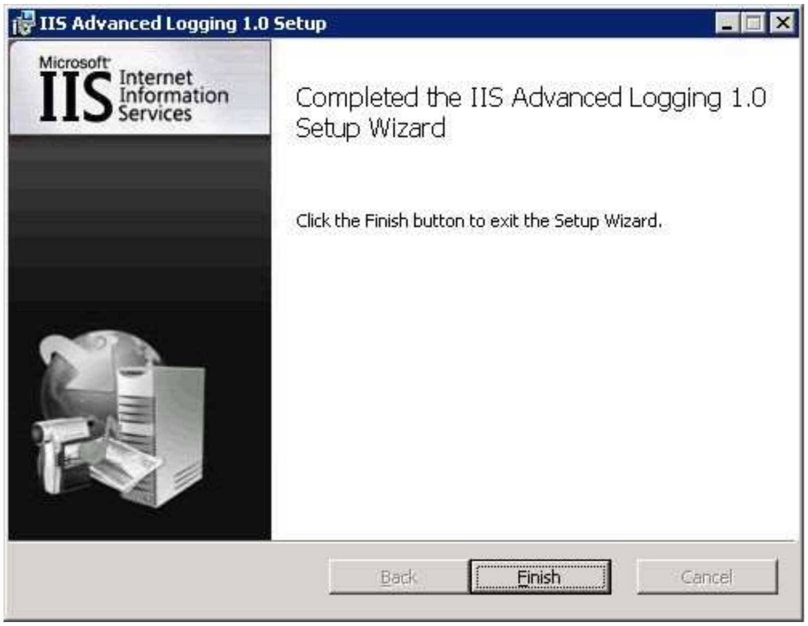
IIS ADVANCED LOGGING 1.0 FOR MICROSOFT WINDOWS OPERATING SYSTEMS

Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows Operating Systems software (for which this supplement is applicable) (the "software"), you may use this supplement. You may not use it if you do not have a license for

□ I accept the terms in the License Agreement

Figure 3.156: Accepting the license agreement

5. Once the installation ends, Figure 3.157 will appear indicating the successful installation of the **Advanced Logging** feature. Click the **Finish** button to exit the wizard.


IIS Advanced Logging 1.0 Setup
Microsoft
IIS Internet Information Services
Back
Finish
Cancel

Completed the IIS Advanced Logging 1.0 Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 3.157: Finishing the installation

6. Next, proceed to configure the Advanced Logs. For that, first, open the **Internet Information Services (IIS) Manager** console using the menu sequence: Start -> Programs -> Administrative Tools -> Internet Information Services (IIS) Manager. Figure 3.158 will then appear.

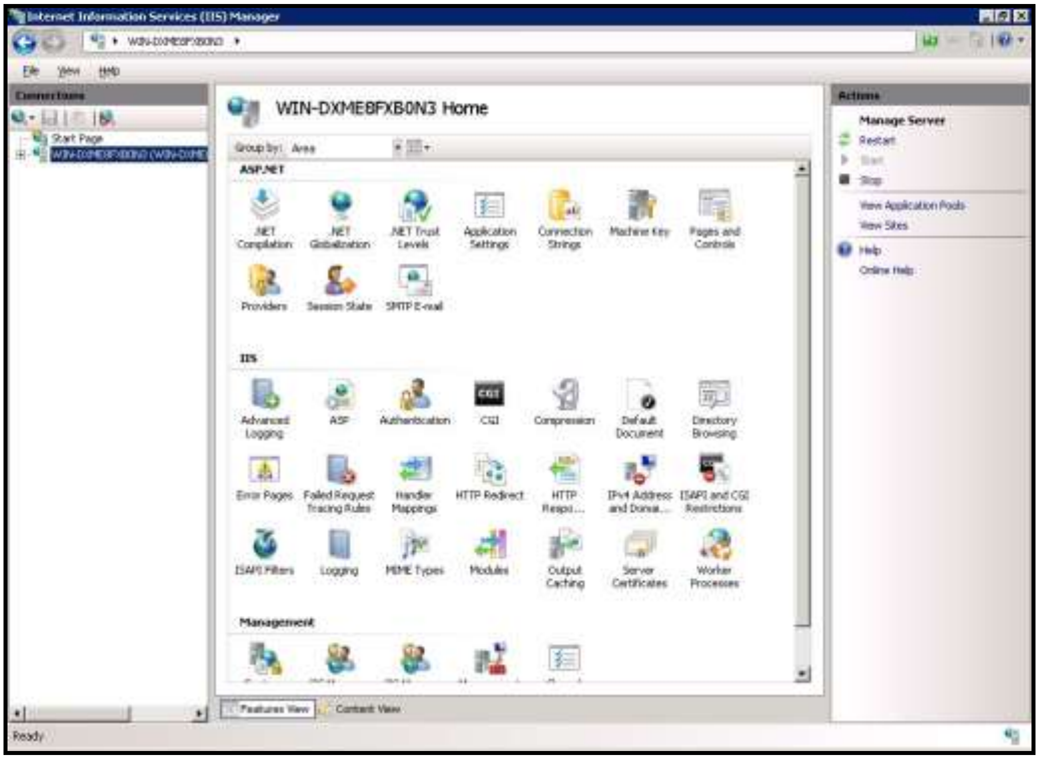
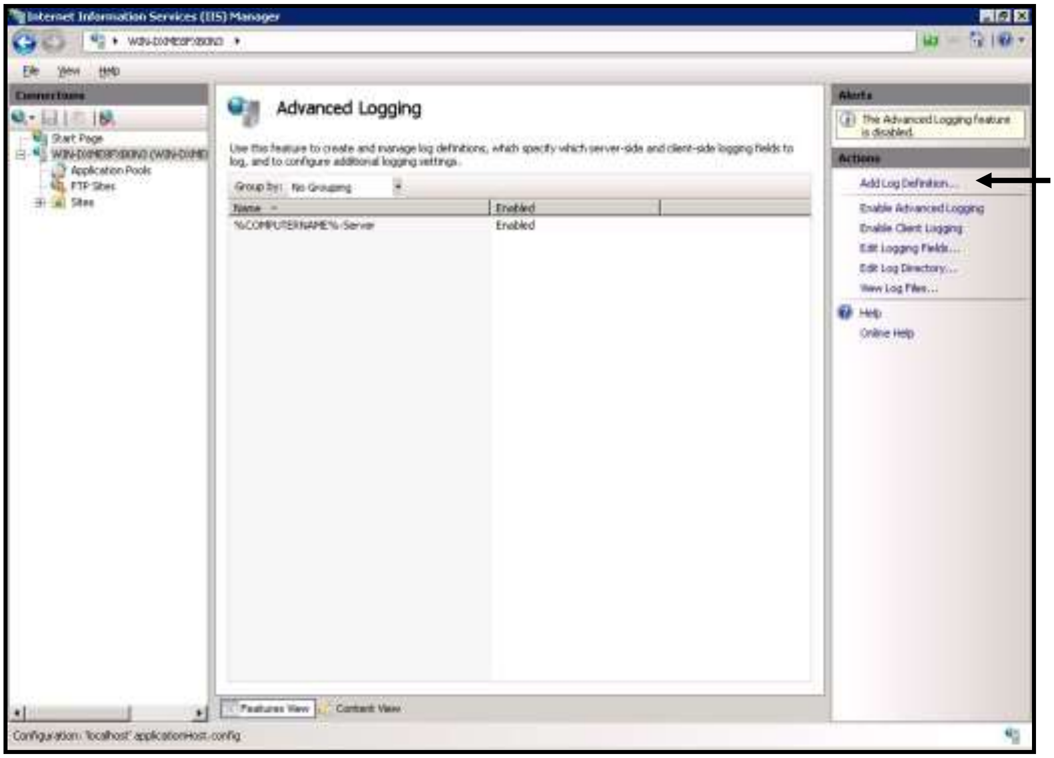


Figure 3.158: The Internet Information Services (IIS) Manager console

7. Click on the node representing the IIS web server host in the tree-structure in the left panel of the console. The

right panel will change to display a variety of options. In the **IIS** section of the right panel, click on the **Advanced Logging** option. Figure 3.159 will then appear. In the **Actions** list in the right panel, click on the **Add Log Definition** option (as indicated by Figure 3.159) to add a new log definition.



Advanced Logging

Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

Group by: No Grouping

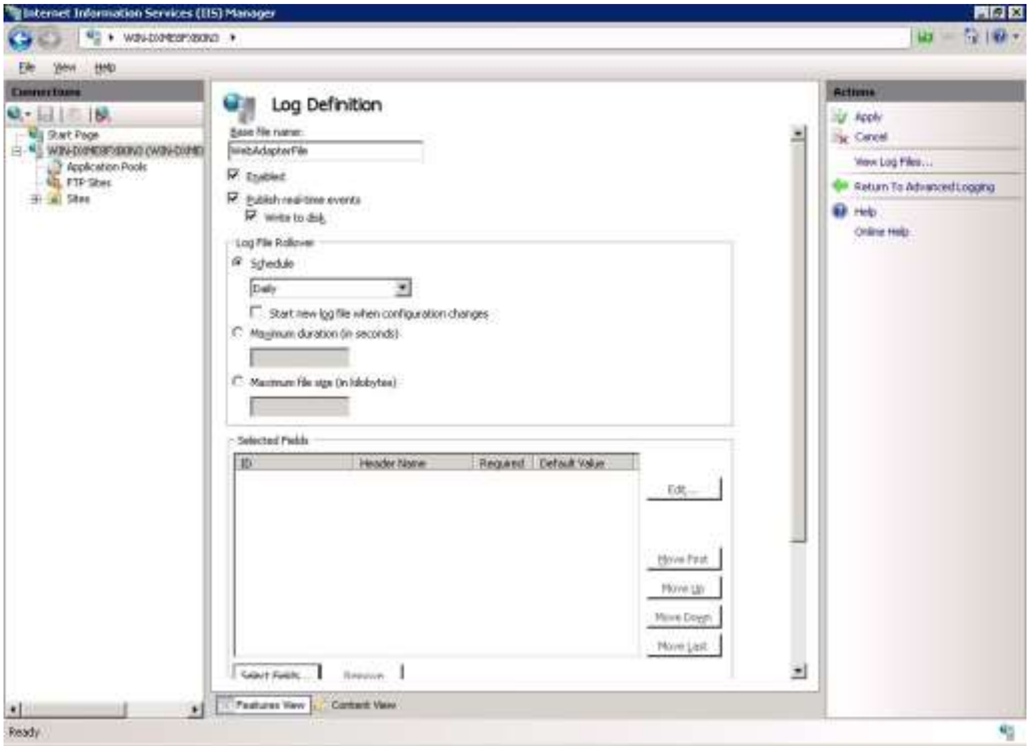
Name	Enabled
%COMPUTERNAME%-Server	Enabled

The Advanced Logging feature is disabled.

Configuration: 'localhost' applicationHost.config

Figure 3.159: Viewing the list of log definitons that pre-exist

8. In the **Log Definition** page that appears, specify **WebAdapterFile** as the **Base file name**. Check the **Enabled** option, the **Publish real-time events** option, and the **Write to disk** sub-option.



Log Definition

Base file name: WebAdapterFile

☑ Enabled

☑ Publish real-time events

☑ Write to disk

Log File Rollover

● Schedule

Daily

□ Start new log file when configuration changes

○ Maximum duration (in seconds)

○ Maximum file size (in kilobytes)

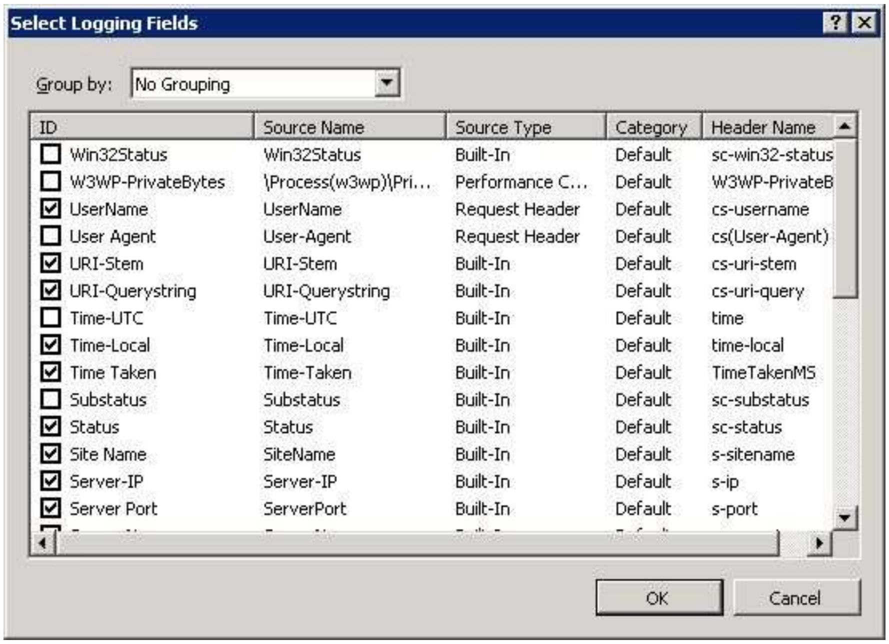
Selected Fields

ID	Header Name	Required	Default Value

Figure 3.160: Adding a new log file definition

9. Then, click on the **Select Fields** button at the bottom of the **Log Definition** page to select he server-side and client-side logging fields to be logged in the specified log file. Doing so will invoke Figure 3.161, from which you wil have to select the following fields:

    - UserName
    - URI-Stem
    - URI-QueryString
    - Time-Local
    - Time Taken
    - Status
    - Server-IP
    - Server Port
    - Server Name
    - Site Name
    - CPU-utilization
    - Bytes Sent
    - Bytes Received
    - Host
    - Client Ip
    - Date-local

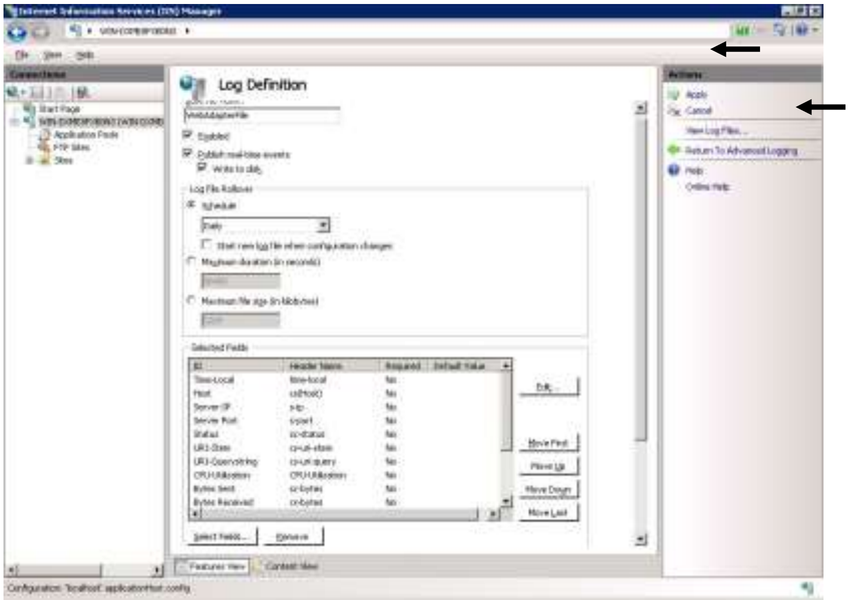


ID	Source Name	Source Type	Category	Header Name
□ Win32Status	Win32Status	Built-In	Default	sc-win32-status
□ W3WP-PrivateBytes	\Process(w3wp)\Pri...	Performance C...	Default	W3WP-PrivateB
☑ UserName	UserName	Request Header	Default	cs-username
□ User Agent	User-Agent	Request Header	Default	cs(User-Agent)
☑ URI-Stem	URI-Stem	Built-In	Default	cs-uri-stem
☑ URI-Querystring	URI-Querystring	Built-In	Default	cs-uri-query
□ Time-UTC	Time-UTC	Built-In	Default	time
☑ Time-Local	Time-Local	Built-In	Default	time-local
☑ Time Taken	Time-Taken	Built-In	Default	TimeTakenMS
□ Substatus	Substatus	Built-In	Default	sc-substatus
☑ Status	Status	Built-In	Default	sc-status
☑ Site Name	SiteName	Built-In	Default	s-sitename
☑ Server-IP	Server-IP	Built-In	Default	s-ip
☑ Server Port	ServerPort	Built-In	Default	s-port

Figure 3.161: Selecting the logging fields to be logged

10. Click on the **OK** button in Figure 3.161 to confirm the selection. When this is done, the **Selected Fields** section of the **Log Definition** page will get updated with your selection (see Figure 3.162). Use the **Move First**, **Move Up**, **Move Down**, and **Move Last** buttons adjacent to your selection to re-arrange the sequence of the logging fields. The desired sequence is as follows:

- Time-Local
- Host
- Server-IP
- Server Port
- Status
- URI-stem
- URI-QueryString
- CPU-utilization
- Bytes Sent
- Bytes Received
- Time Taken
- Server Name
- Site Name
- User Name
- Client Ip
- Date-local



WebAdapterFile

☑ Enabled

☑ Publish real-time events

☑ Write to disk

Log File Rollover

● Schedule: Daily

□ Start new log file when configuration changes

○ Maximum duration (in seconds)

○ Maximum file size (in kilobytes)

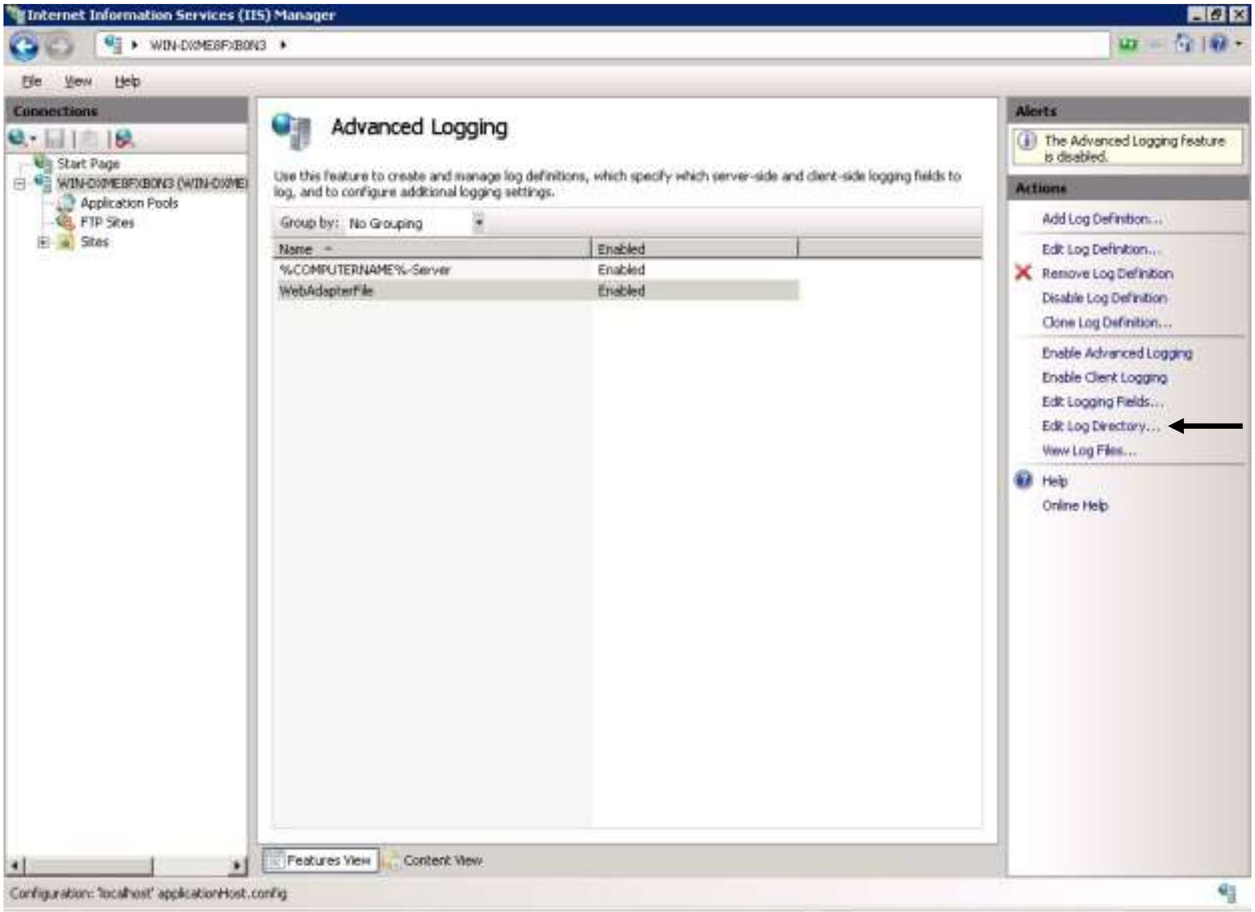
Selected Fields:

ID	Header Name	Required	Default Value
Time-Local	time-local	No	
Host	cs(Host)	No	
Server-IP	s-ip	No	
Server Port	s-port	No	
Status	sc-status	No	
URI-Stem	cs-uri-stem	No	
URI-Querystring	cs-uri-query	No	
CPU-Utilization	CPU-Utilization	No	
Bytes Sent	sc-bytes	No	
Bytes Received	cs-bytes	No	

Configuration: 'localhost' applicationHost.config

Figure 3.162: Re-arranging the sequence of the logging fields

11. Then, apply the changes by clicking on the **Apply** button indicated by Figure 3.162 above. Once the changes are saved, click on the **Return to Advanced Logging** option indicated by Figure 3.162 above. Figure 3.163 will then appear. In the right panel of Figure 3.163, you will find that the newly added **WebAdapterFile** is appended to the list of log file definitions that pre-exist.



Advanced Logging

Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

Group by: No Grouping

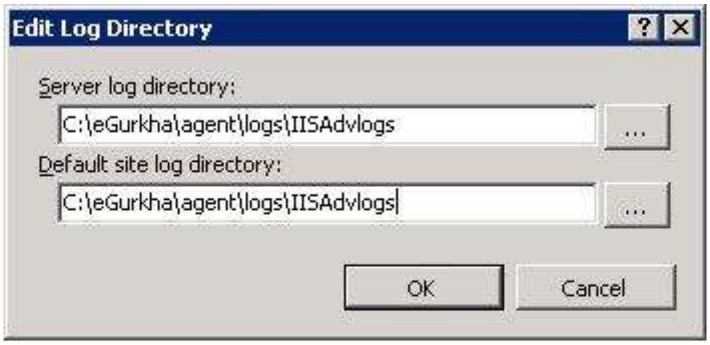
Name	Enabled
%COMPUTERNAME%-Server	Enabled
WebAdapterFile	Enabled

The Advanced Logging feature is disabled.

Configuration: 'localhost' applicationHost.config

Figure 3.163: The newly added log definition displayed in the list of log files that pre-exist

12. Now, select the **WebAdapterFile** entry in Figure 3.163 and click on the **Edit Log Directory** option in the **Actions** list, as indicated by Figure 3.163. When Figure 3.164 appears, change the default values of the **Server log directory** and **Default site log directory** text boxes to **<EG_INSTALL_DIR>\agent\logs\IISAdvlogs** directory. Then, click the **OK** button therein.

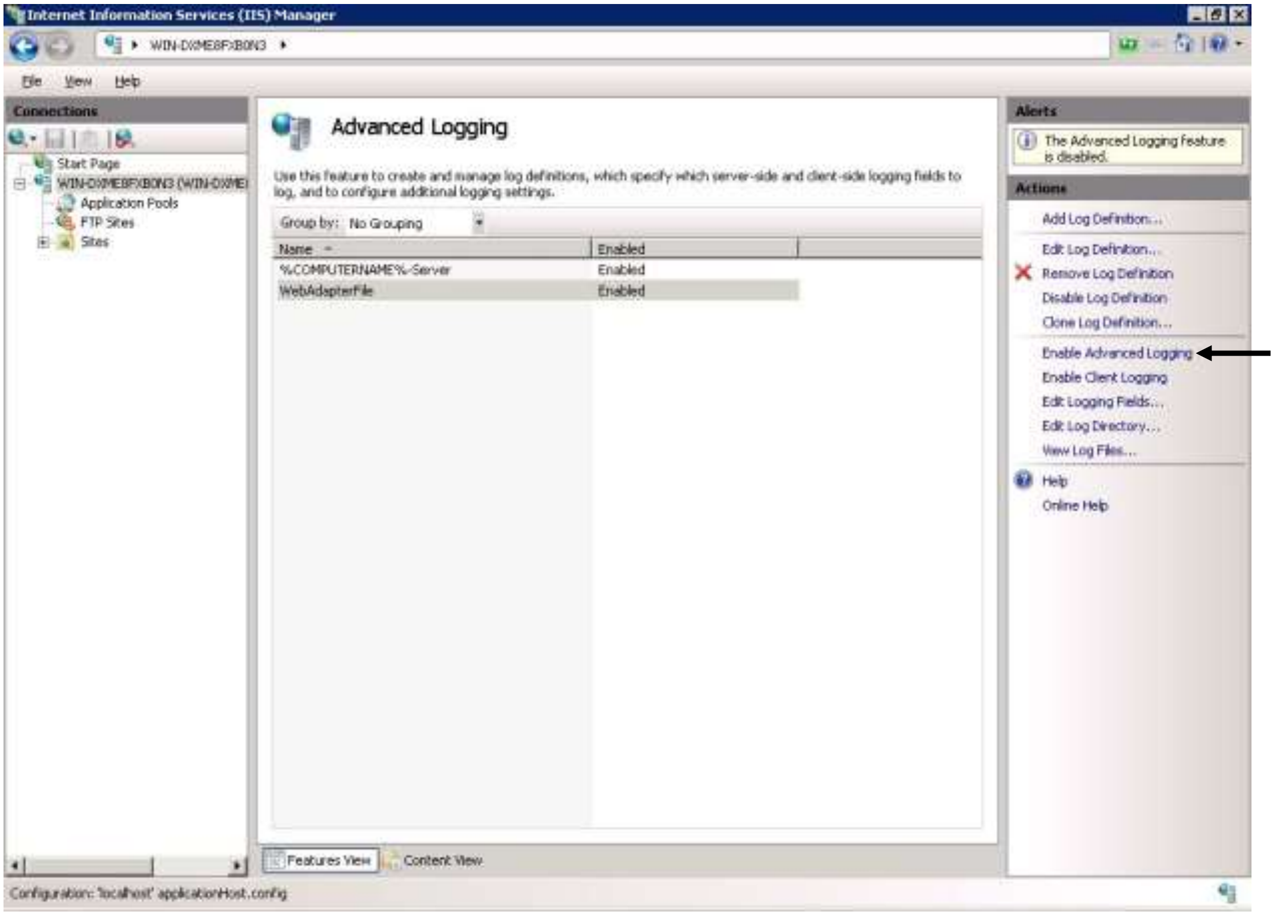


Server log directory: C:\eGurkha\agent\logs\IISAdvlogs

Default site log directory: C:\eGurkha\agent\logs\IISAdvlogs

Figure 3.164: Changing the server log and default site log directories

13. This will lead you to Figure 3.165. Click on the **Enable Advanced Logging** option in the **Actions** list of Figure 3.165 to enable advanced logging.



Advanced Logging

Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

Group by: No Grouping

Name	Enabled
%COMPUTERNAME%-Server	Enabled
WebAdapterFile	Enabled

The Advanced Logging feature is disabled.

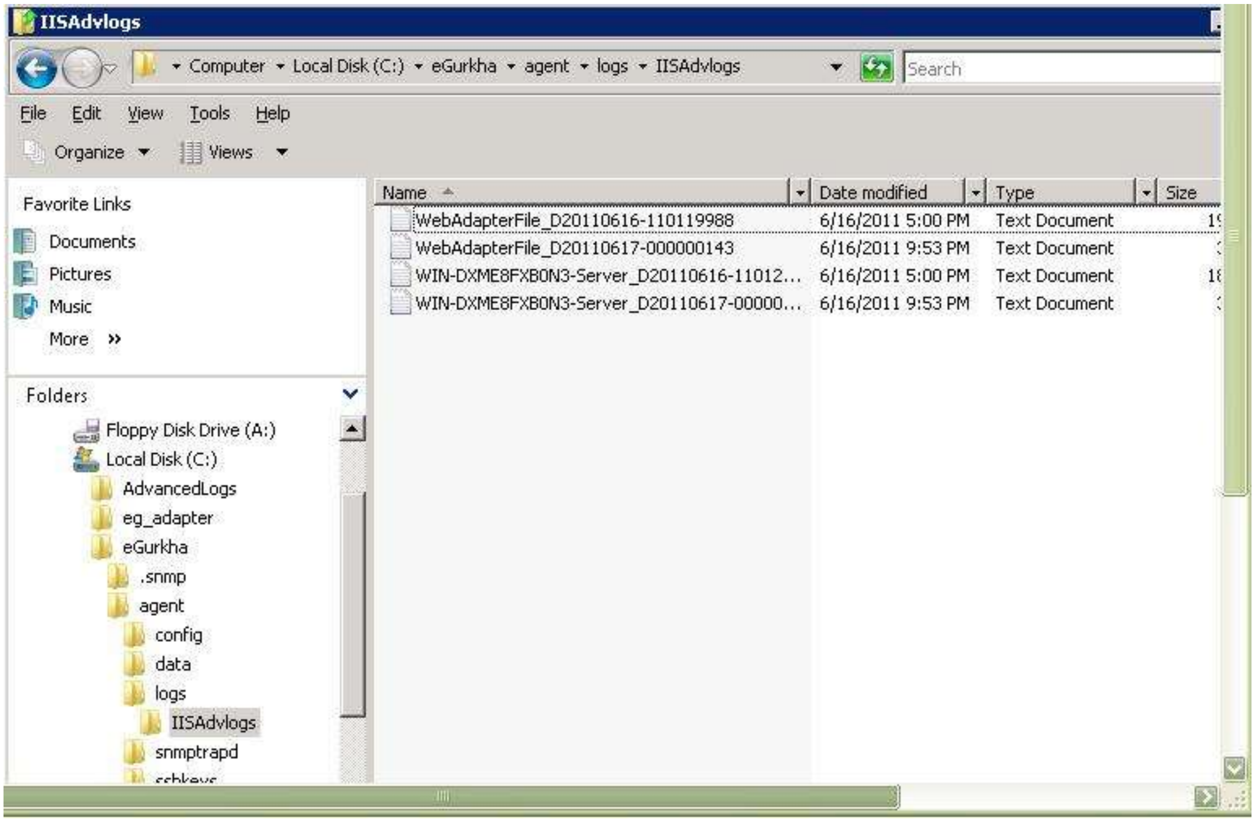
Configuration: 'localhost' applicationHost.config

Figure 3.165: Enabling advanced logging

14. Next, restart IIS for the changes to take effect.

15. If you now want to view the advanced log files, first open the **Internet Information Services (IIS) Manager** console using the menu sequence: Start -> Programs -> Administrative Tools -> Internet Information Services (IIS) Manager. Then, in the tree structure that appears, click on the node representing the IIS web server host. Next, from the options displayed in the right panel, click on **Advanced Logging**. Figure 3.165 will then appear.

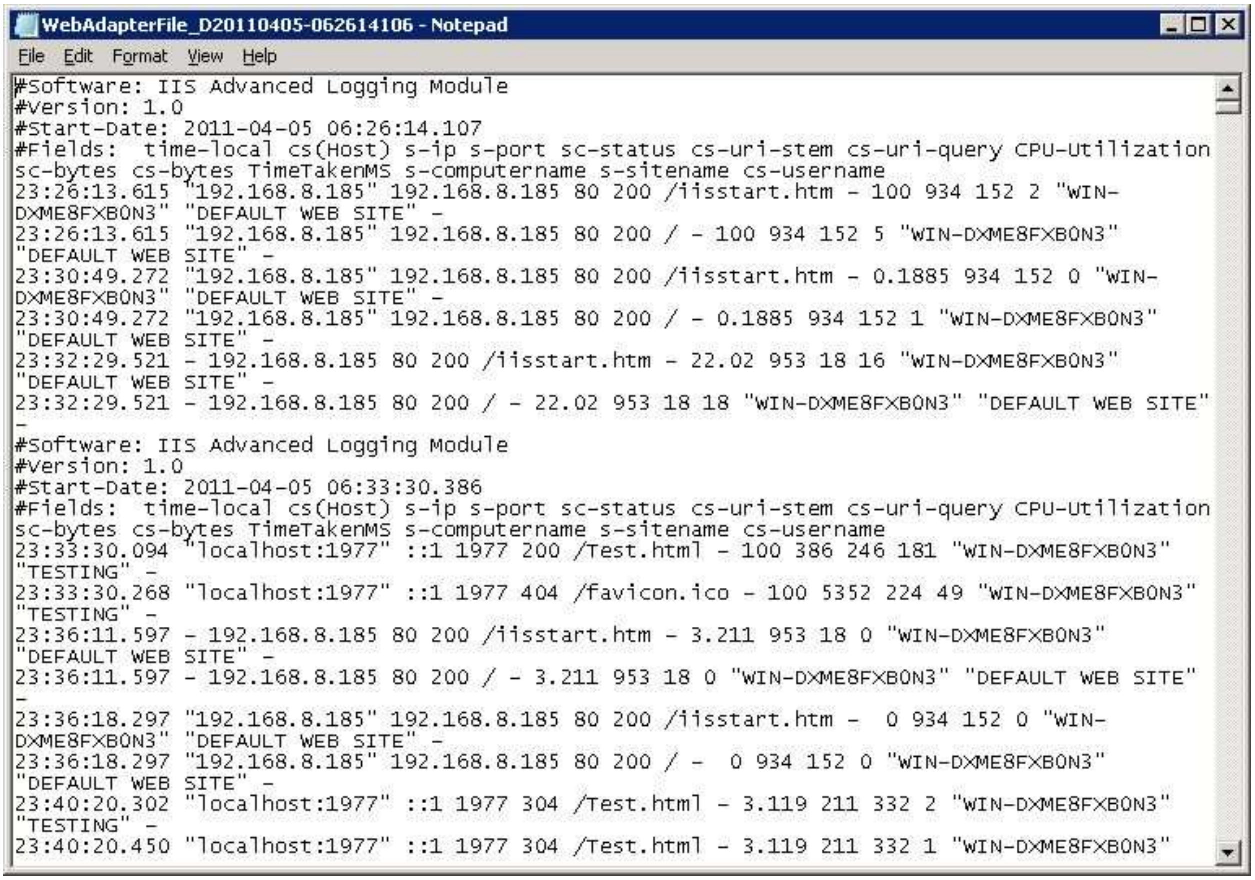
16. Select the **WebAdapterFile** entry in Figure 3.165 and click on the **View Log Files** option in the **Actions** list. This will invoke Figure 3.166, where all the log files saved to the **<EG_INSTALL_DIR>\agent\logs\IISAdvlogs** directory will be displayed.



Name	Date modified	Type	Size
WebAdapterFile_D20110616-110119988	6/16/2011 5:00 PM	Text Document	1
WebAdapterFile_D20110617-000000143	6/16/2011 9:53 PM	Text Document	
WIN-DXME8FXB0N3-Server_D20110616-11012...	6/16/2011 5:00 PM	Text Document	18
WIN-DXME8FXB0N3-Server_D20110617-00000...	6/16/2011 9:53 PM	Text Document	

Figure 3.166: List of log files saved to the AdvancedLogs directory

17. To view a log file, click on any of the log files in the list of Figure 3.166. The chosen log file will then open in Notepad as depicted by Figure 3.167.


WebAdapterFile_D20110405-062614106 - Notepad
File Edit Format View Help

```
#Software: IIS Advanced Logging Module
#Version: 1.0
#Start-Date: 2011-04-05 06:26:14.107
#Fields:  time-local cs(Host) s-ip s-port sc-status cs-uri-stem cs-uri-query CPU-Utilization
sc-bytes cs-bytes TimeTakenMS s-computername s-sitename cs-username
23:26:13.615 "192.168.8.185" 192.168.8.185 80 200 /iisstart.htm - 100 934 152 2 "WIN-
DXME8FXBON3" "DEFAULT WEB SITE" -
23:26:13.615 "192.168.8.185" 192.168.8.185 80 200 / - 100 934 152 5 "WIN-DXME8FXBON3"
"DEFAULT WEB SITE" -
23:30:49.272 "192.168.8.185" 192.168.8.185 80 200 /iisstart.htm - 0.1885 934 152 0 "WIN-
DXME8FXBON3" "DEFAULT WEB SITE" -
23:30:49.272 "192.168.8.185" 192.168.8.185 80 200 / - 0.1885 934 152 1 "WIN-DXME8FXBON3"
"DEFAULT WEB SITE" -
23:32:29.521 - 192.168.8.185 80 200 /iisstart.htm - 22.02 953 18 16 "WIN-DXME8FXBON3"
"DEFAULT WEB SITE" -
23:32:29.521 - 192.168.8.185 80 200 / - 22.02 953 18 18 "WIN-DXME8FXBON3" "DEFAULT WEB SITE"
-
#Software: IIS Advanced Logging Module
#Version: 1.0
#Start-Date: 2011-04-05 06:33:30.386
#Fields:  time-local cs(Host) s-ip s-port sc-status cs-uri-stem cs-uri-query CPU-Utilization
sc-bytes cs-bytes TimeTakenMS s-computername s-sitename cs-username
23:33:30.094 "localhost:1977" ::1 1977 200 /Test.html - 100 386 246 181 "WIN-DXME8FXBON3"
"TESTING" -
23:33:30.268 "localhost:1977" ::1 1977 404 /favicon.ico - 100 5352 224 49 "WIN-DXME8FXBON3"
"TESTING" -
23:36:11.597 - 192.168.8.185 80 200 /iisstart.htm - 3.211 953 18 0 "WIN-DXME8FXBON3"
"DEFAULT WEB SITE" -
23:36:11.597 - 192.168.8.185 80 200 / - 3.211 953 18 0 "WIN-DXME8FXBON3" "DEFAULT WEB SITE"
-
23:36:18.297 "192.168.8.185" 192.168.8.185 80 200 /iisstart.htm -  0 934 152 0 "WIN-
DXME8FXBON3" "DEFAULT WEB SITE" -
23:36:18.297 "192.168.8.185" 192.168.8.185 80 200 / -  0 934 152 0 "WIN-DXME8FXBON3"
"DEFAULT WEB SITE" -
23:40:20.302 "localhost:1977" ::1 1977 304 /Test.html - 3.119 211 332 2 "WIN-DXME8FXBON3"
"TESTING" -
23:40:20.450 "localhost:1977" ::1 1977 304 /Test.html - 3.119 211 332 1 "WIN-DXME8FXBON3"
```

Figure 3.167: Viewing the log file

Note

Sometimes, even after choosing to log the **Username**, the advanced logs may continue to display only a '-' (hyphen) against the **Username** field. To ensure that the **Username** is correctly logged, do the following:

- On the IIS 7/8 host, edit the **C:\Windows\System32\inetsrv\config\applicationHost.config** file in an editor.
- Locate the following line in the file:

```
<field id="UserName" sourceName="UserName"
sourceType="RequestHeader" logHeaderName="cs-username"
category="Default" loggingDataType="TypeLPCSTR" />
```

- Change the entry in **Bold** in step 2 above, as indicated below:

```
<field id="UserName" sourceName="UserName"
sourceType="BuiltIn" logHeaderName="cs-username"
category="Default" loggingDataType="TypeLPCSTR" />
```

- Save the file.

3.16 Configuring the eG Agent to Monitor an Apache Web Server

The eG web adapter can be configured on an Apache web server on Windows, using a manual configuration process only. The same has been discussed below.

To manually configure the eG web adapter on an Apache web server 1.x on Windows, do the following:

1. First, login to the Windows server.
2. Edit the **<APACHE_HOME>\conf\httpd.conf** file to append the following lines:

   AddModule mod_egurkha.c

   LoadModule mod_egurkha modules/mod_egurkha.dll
3. Copy the file **mod_egurkha.dll** from the **<EG_AGENT_INSTALL_DIR>\lib** directory to **<APACHE_HOME>\modules**.
4. Stop and restart the Apache server.

To manually configure the eG web adapter on an Apache web server 2.0 on Windows, do the following:

1. First, login to the Windows server.
2. Edit the **<APACHE_HOME>\conf\httpd.conf** file to append the following line:

   LoadModule egurkha_module modules/mod_egurkha2_0.dll
3. Copy the file **mod_egurkha2_0.dll** from the **<EG_AGENT_INSTALL_DIR>\lib** directory to **<APACHE_HOME>\modules**.
4. Stop and restart the Apache server.

To manually configure the eG web adapter on an Apache web server 2.2 on Windows, do the following:

1. First, login to the Windows server.
2. Edit the **<APACHE_HOME>\conf\httpd.conf** file to append the following line:

   LoadModule egurkha_module modules/mod_egurkha2_2.dll
3. Copy the file **mod_egurkha2_2.dll** from the **<EG_AGENT_INSTALL_DIR>\lib** directory to **<APACHE_HOME>\modules**.
4. Stop and restart the Apache server.

3.17 Configuring the eG Agent to Monitor an IBM HTTP Server

To manually configure the eG web adapter on an IBM HTTP server 1.x on Windows, do the following:

1. First, login to the Windows server.
2. Edit the **<IBM_HTTPSERVER_HOME>\conf\httpd.conf** file to append the following line:

   LoadModule ibm_egurkha_module modules/ibm_mod_egurkha.dll
3. Copy the file **ibm_mod_egurkha.dll** from the **<EG_AGENT_INSTALL_DIR>\lib** directory to **<IBM_HTTPSERVER_HOME>\modules**.

4. Stop and restart the IBM HTTP server.

To manually configure the eG web adapter on an IBM HTTP web server 2.x on Windows, do the following:

1. First, login to the Windows server.
2. Edit the **<IBM_HTTPSERVER_HOME>\conf\httpd.conf** file to append the following line:

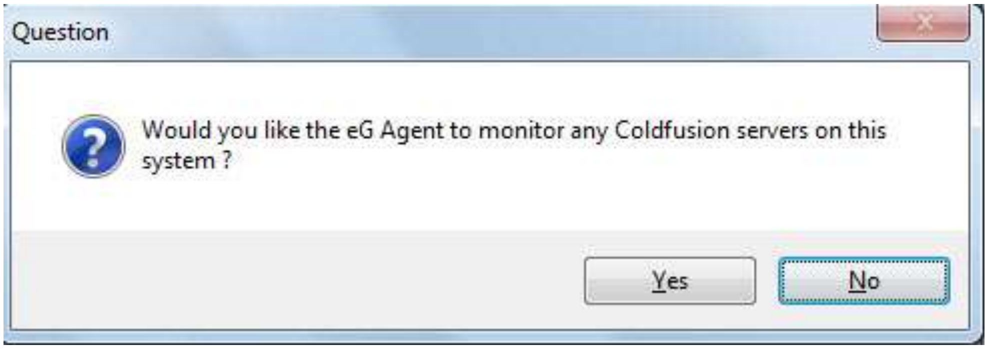
   LoadModule ibm_ egurkha_module modules/ibm_mod_egurkha.dll

3. Copy the file **ibm_mod_egurkha2_0.dll** from the **<EG_AGENT_INSTALL_DIR>\lib** directory to **<IBM_HTTPSERVER_HOME>\modules**.
4. Rename the **<IBM_HTTPSERVER_HOME>\modules\ibm_mod_egurkha2_0.dll** to **ibm_mod_egurkha.dll**
5. Stop and restart the IBM HTTP server.

3.18 Configuring the eG Agent to Monitor a ColdFusion Server

For enabling the eG agent to monitor a ColdFusion server, the agent configuration needs to be modified. To achieve this, do the following:

1. Select **Uninstall Agent** from the options available under the eG Monitoring Suite -> eG Agent menu. From the screen that appears next, select the **Modify** option and click the **Next >** button.
2. The setup then provides an option for the user to configure a Coldfusion application server in his environment for monitoring as in Figure 3.168. The default option is **No**.

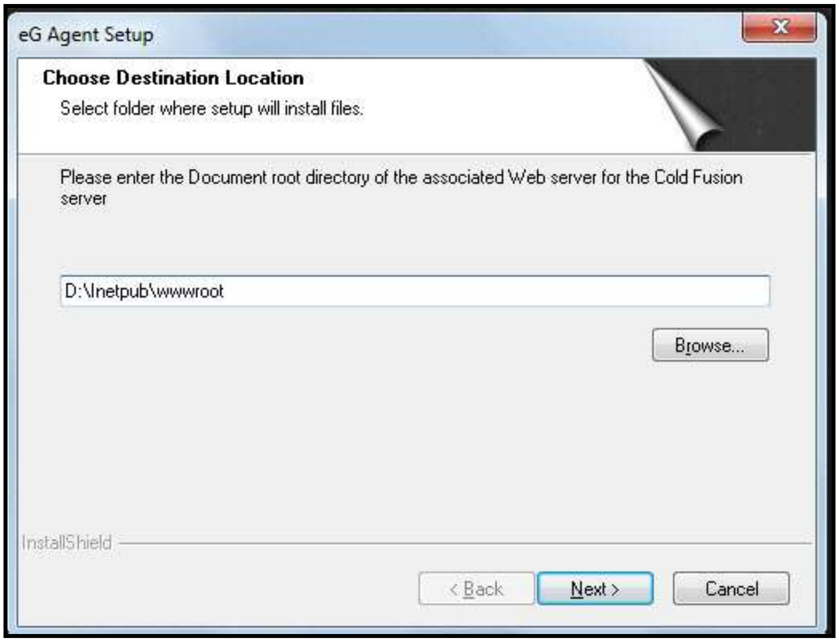


Question

Would you like the eG Agent to monitor any Coldfusion servers on this system ?

Figure 3.168: Setup providing an option to configure a Coldfusion server for monitoring

3. If the user desires to configure a Coldfusion server at this stage, he/she needs to specify the document root of the associated web server as in Figure 3.169.



eG Agent Setup

Choose Destination Location

Select folder where setup will install files.

Please enter the Document root directory of the associated Web server for the Cold Fusion server

D:\Inetpub\wwwroot

Figure 3.169: Setup requesting for the document directory of the web server used with the Coldfusion server

3.19 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 3.170).

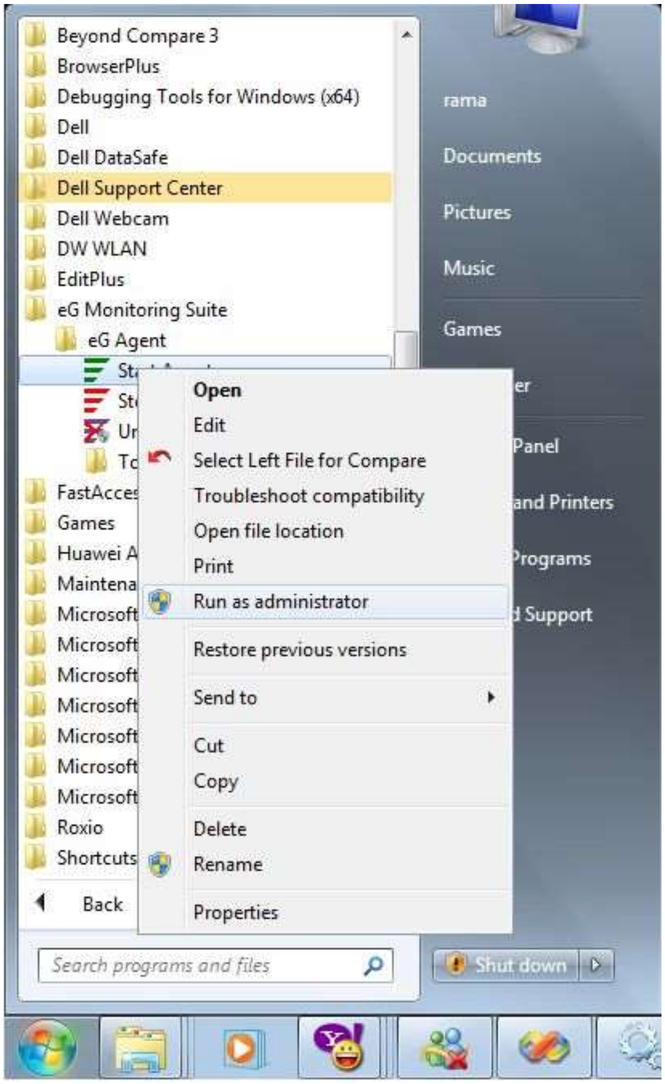


Figure 3.170: Starting an eG agent on Windows 2008

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 3.171. This implies that the command that is issued at the command prompt soon after, will be executed with administrator privileges.

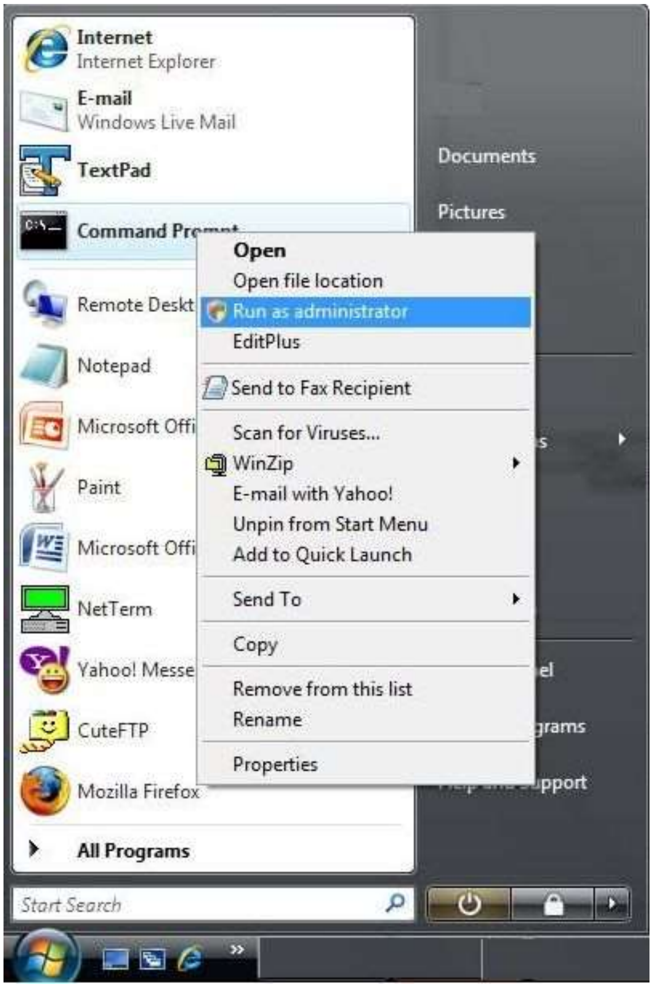
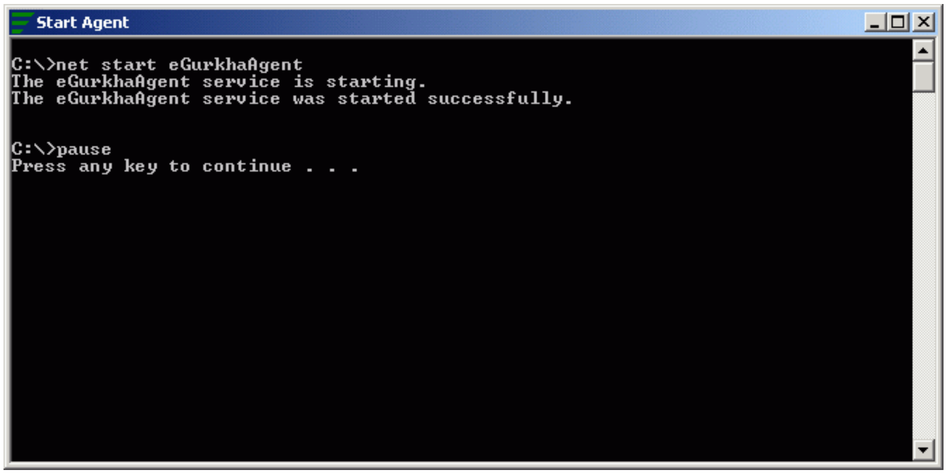


Figure 3.171: Starting the eG agent on Windows Vista

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 3.172: Message indicating that the agent has started successfully.

3.19.1 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 3.173).

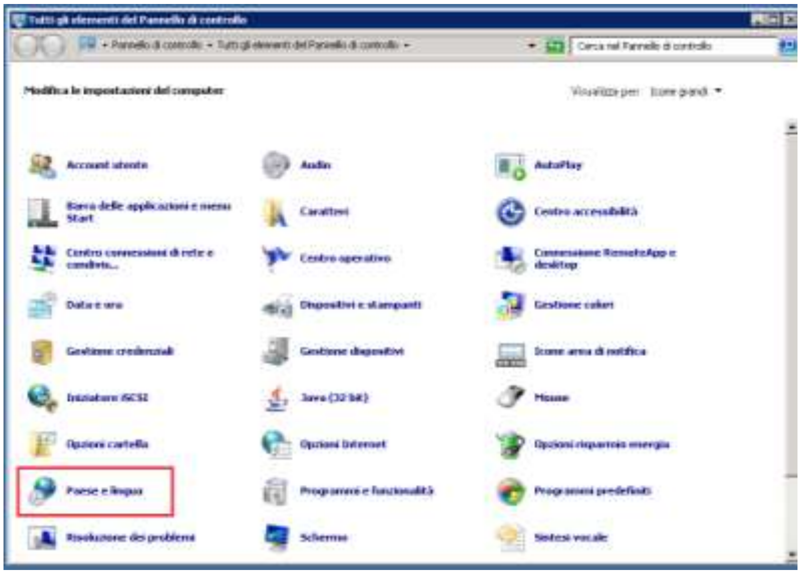
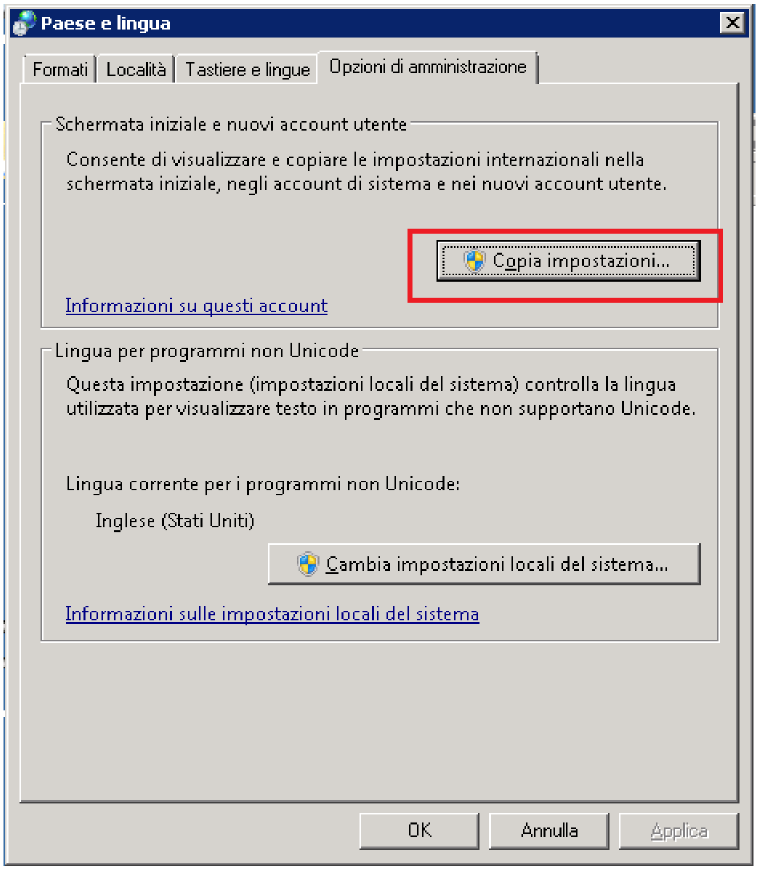


Figure 3.173: The Control Panel

2. Figure 3.174 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.



Paese e lingua
Formati
Località
Tastiere e lingue
Opzioni di amministrazione
Copia impostazioni...
Informazioni su questi account
Cambia impostazioni locali del sistema...
Informazioni sulle impostazioni locali del sistema
OK
Annulla
Applica

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

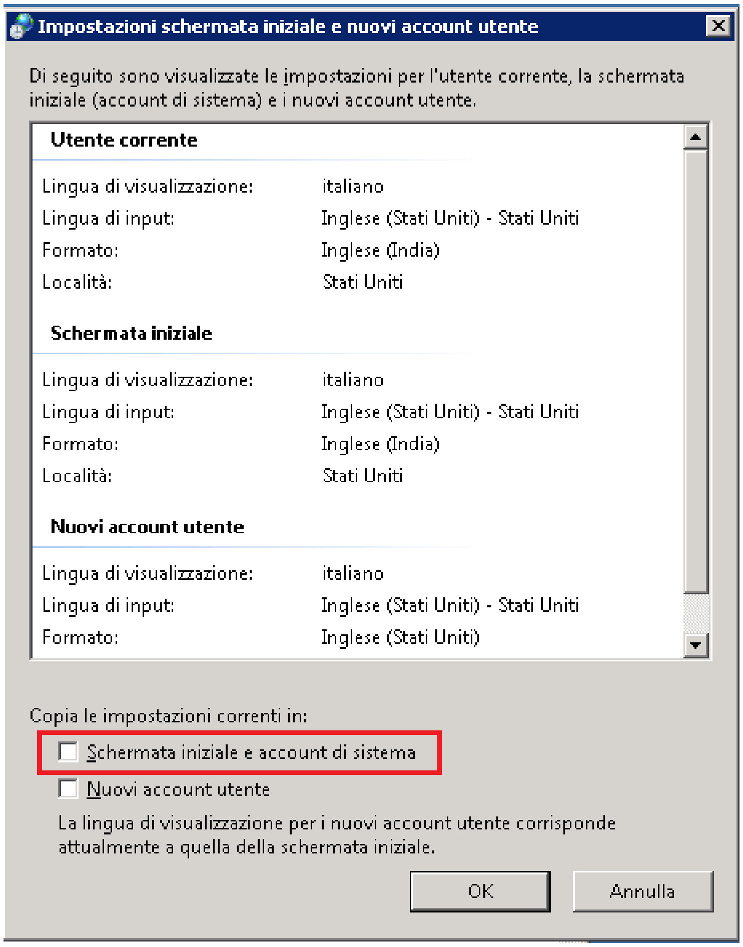
Questa impostazione (impostazioni locali del sistema) controlla la lingua utilizzata per visualizzare testo in programmi che non supportano Unicode.

Lingua corrente per i programmi non Unicode:

Inglese (Stati Uniti)

Figure 3.174: The Administrative tab page

3. When Figure 3.175 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 3.175: Copying the current user's settings to the system accounts

3.20 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.

3.21 Troubleshooting the Failure of the eG Agent

Please 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.

3.22 Performance Impact of the eG Agent

The resource utiliation 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 100 MB. 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 30 – 50 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.

3.23 Increasing the Memory of the eG Agent

The eG agent runs as a Java process. The maximum heap memory that can be allocated to a 32-bit eG agent process is limited to 1.5 GB. The maximum heap memory allocation to a 64-bit eG agent process on the other hand, is limited to 3 GB. 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 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 256 MB of memory to the eG agent, your *–Xmx* specification should be as follows:

-Xmx256M

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).

3.24 Configuring High Availability for the eG Agent Using Windows Cluster Setup (on Windows 2008)

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.

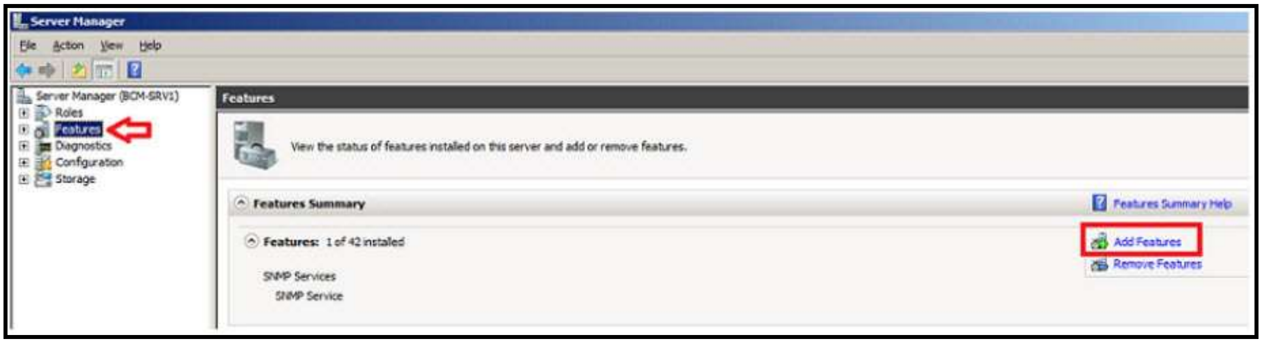
In order to configure a fail-proof agent, follow the broad steps listed below:

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 3.24.1 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 3.24.2 of this document.
8. Configure cluster quorum settings using the procedure discussed in Section 3.24.3.
9. Add eG agent service as a cluster resource, as outlined in Section 3.24.4 of this document.

3.24.1 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 3.176). Then, under **Features Summary**, click **Add Features**.



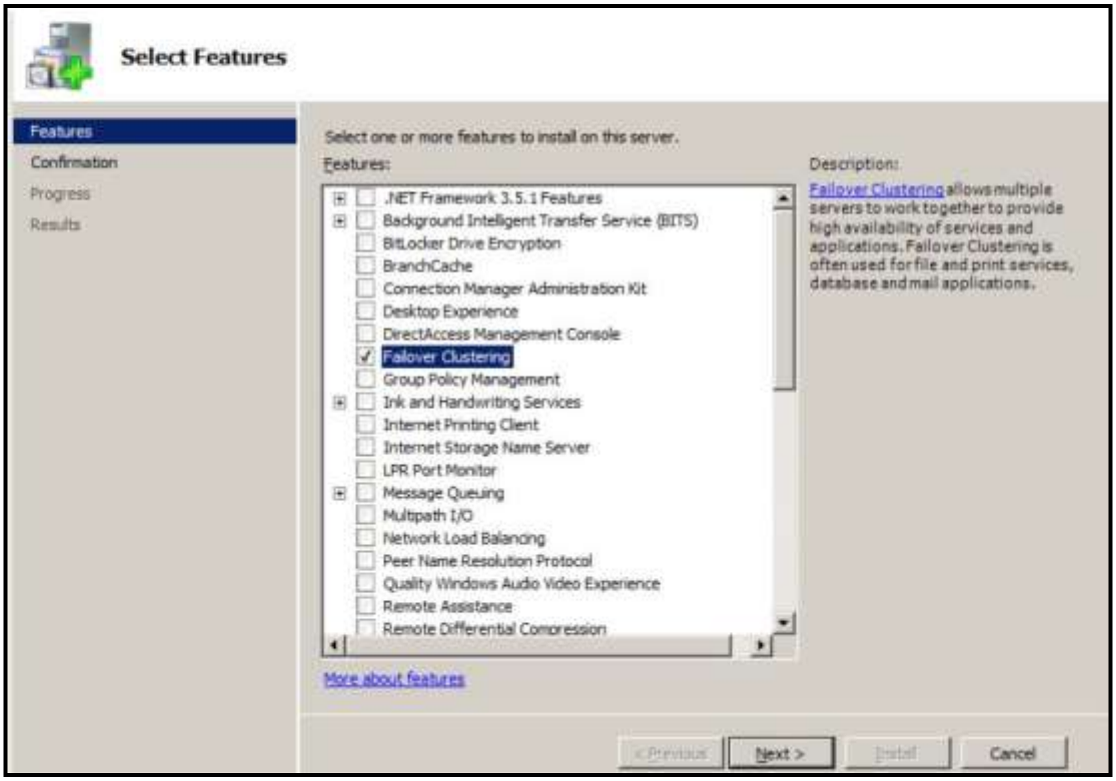
View the status of features installed on this server and add or remove features.

Features: 1 of 42 installed

SNMP Services
SNMP Service

Figure 3.176: 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 3.177).



Select one or more features to install on this server.

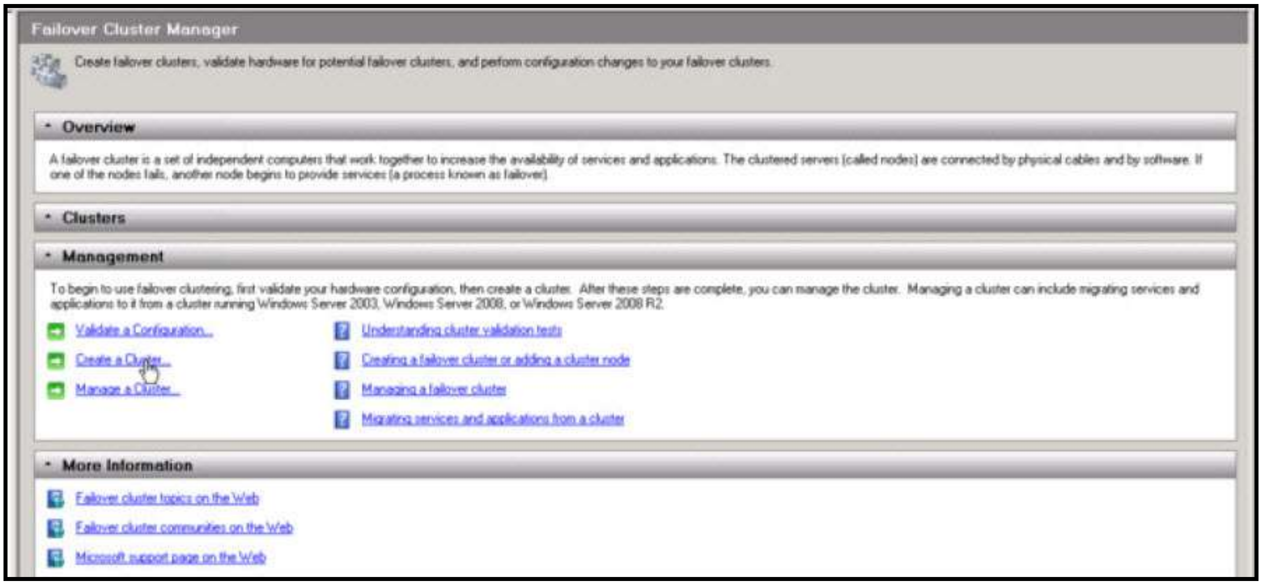
☐ .NET Framework 3.5.1 Features
☐ Background Intelligent Transfer Service (BITS)
☐ BitLocker Drive Encryption
☐ BranchCache
☐ Connection Manager Administration Kit
☐ Desktop Experience
☐ DirectAccess Management Console
☑ Failover Clustering
☐ Group Policy Management
☐ Ink and Handwriting Services
☐ Internet 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

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 3.177: 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 3.178). Then, click on the **Create a Cluster** link therein (see Figure 3.178).


Failover Cluster Manager
Overview
Clusters
Management
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

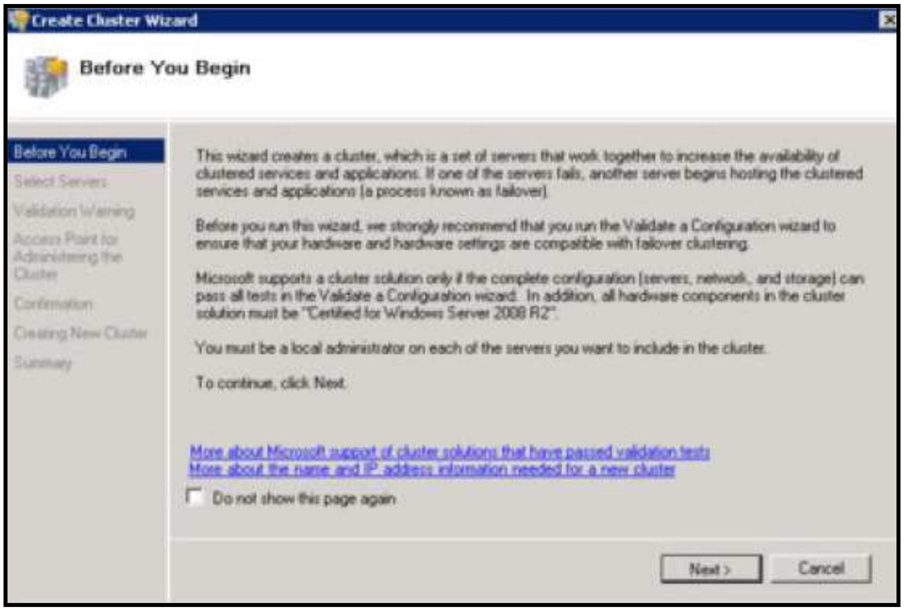
Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

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 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.

Figure 3.178: Creating a failover cluster

8. When Figure 3.179 appears, click on the **Next** button to proceed.


Create Cluster Wizard
Before You Begin
Before You Begin
Select Servers
Validation Warning
Access Point for Administering the Cluster
Confirmation
Creating New Cluster
Summary
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
Next >
Cancel

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".

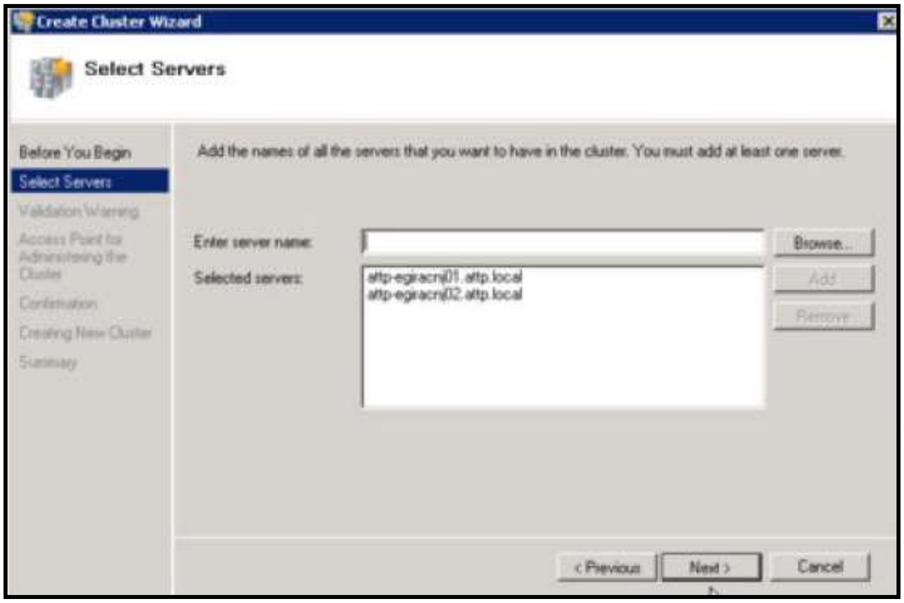
You must be a local administrator on each of the servers you want to include in the cluster.

To continue, click Next.

□ Do not show this page again

Figure 3.179: The Welcome screen of the Create Cluster Wizard

9. Using Figure 3.180 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 3.180 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.



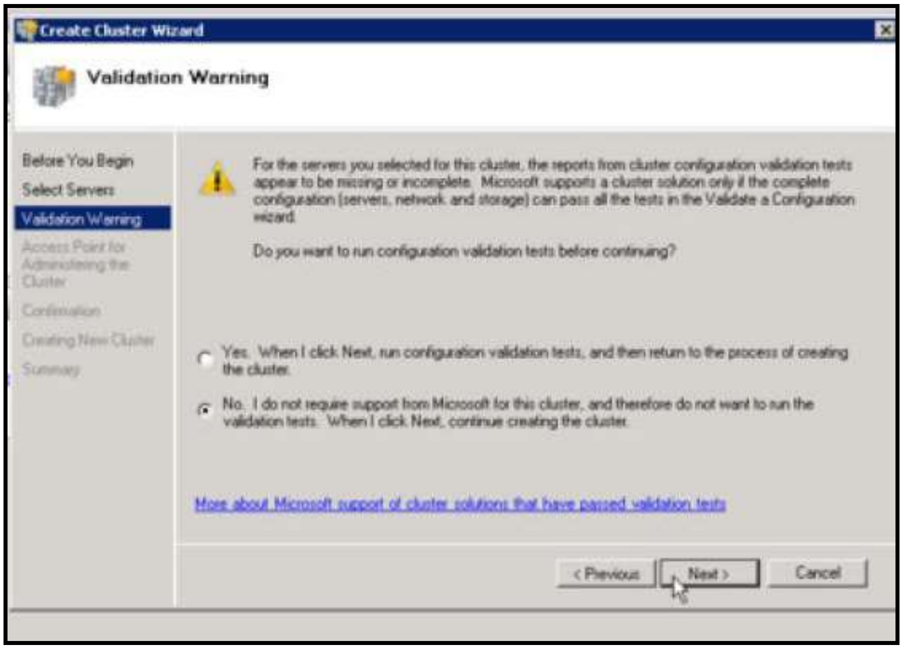
Add the names of all the servers that you want to have in the cluster. You must add at least one server.

Enter server name:

Selected servers: attp-egiracnj01.attp.local
attp-egiracnj02.attp.local

Figure 3.180: Adding nodes to a cluster

10. Skip the validation tests by clicking the **Next** button in Figure 3.181.



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?

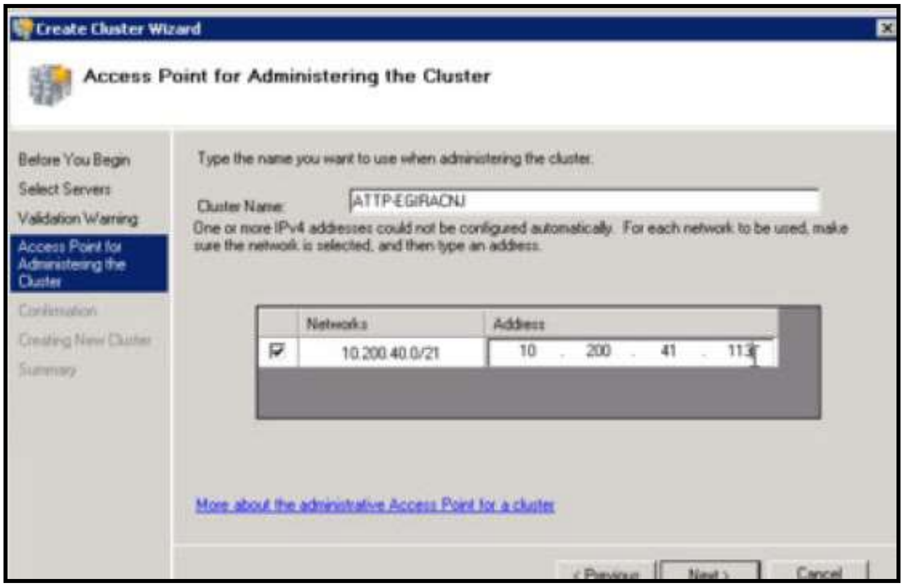
○ Yes. When I click Next, run configuration validation tests, and then return to the process of creating the cluster.

● 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 3.181: Skipping the validation tests

11. Next, provide a name for the cluster and specify its IP address, as depicted by Figure 3.182 below. Then, click the **Next** button.



Type the name you want to use when administering the cluster.

Cluster Name: ATTP-EGIRACNJ

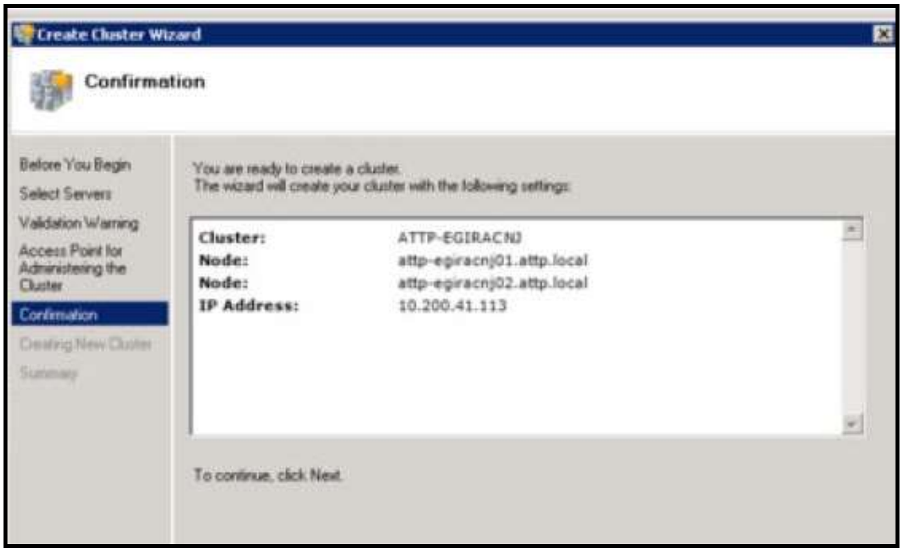
One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.

	Networks	Address
☑	10.200.40.0/21	10 . 200 . 41 . 113

More about the administrative Access Point for a cluster

Figure 3.182: Specifying the name and IP address of the cluster

12. A brief summary of the cluster configuration will then appear, as shown by Figure 3.183. Click **Next** therein to confirm and proceed.



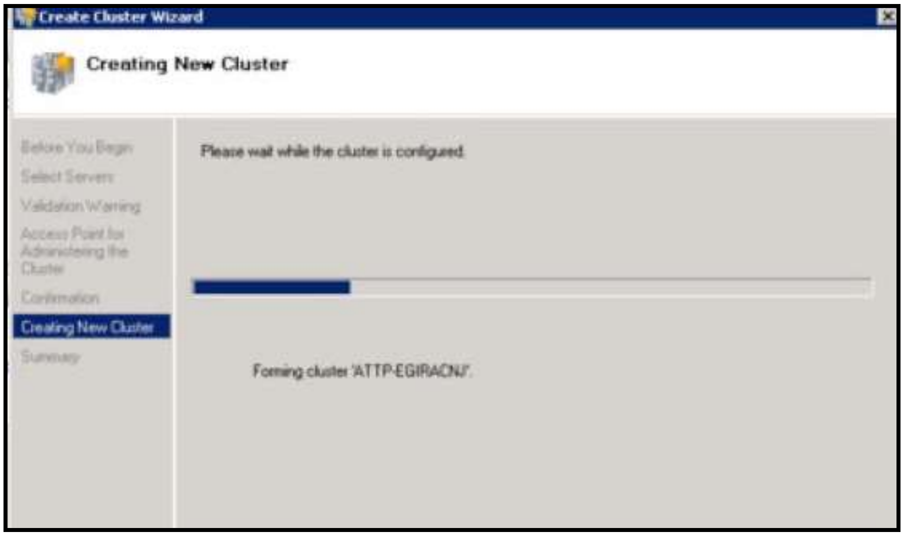
You are ready to create a cluster.
The wizard will create your cluster with the following settings:

```
Cluster:        ATTP-EGIRACNJ
Node:           attp-egiracnj01.attp.local
Node:           attp-egiracnj02.attp.local
IP Address:     10.200.41.113
```

To continue, click Next.

Figure 3.183: Confirming the cluster configuration

13. Cluster creation will then begin (see Figure 3.184).

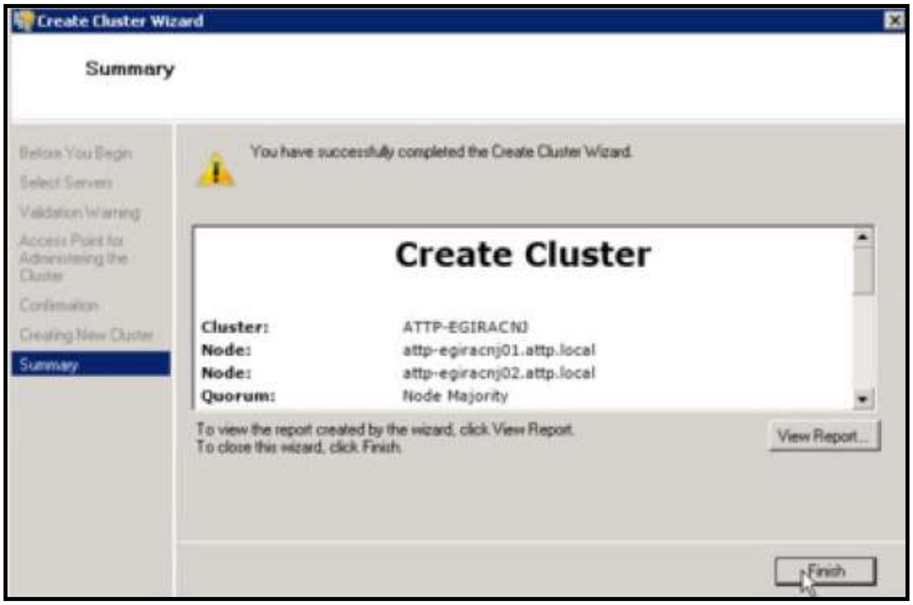


Please wait while the cluster is configured.

Forming cluster 'ATTP-EGIRACNJ'.

Figure 3.184: Cluster creation in progress

14. Once cluster creation completes, Figure 3.185 will appear. Click the **Finish** button therein to end the cluster creation process.



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

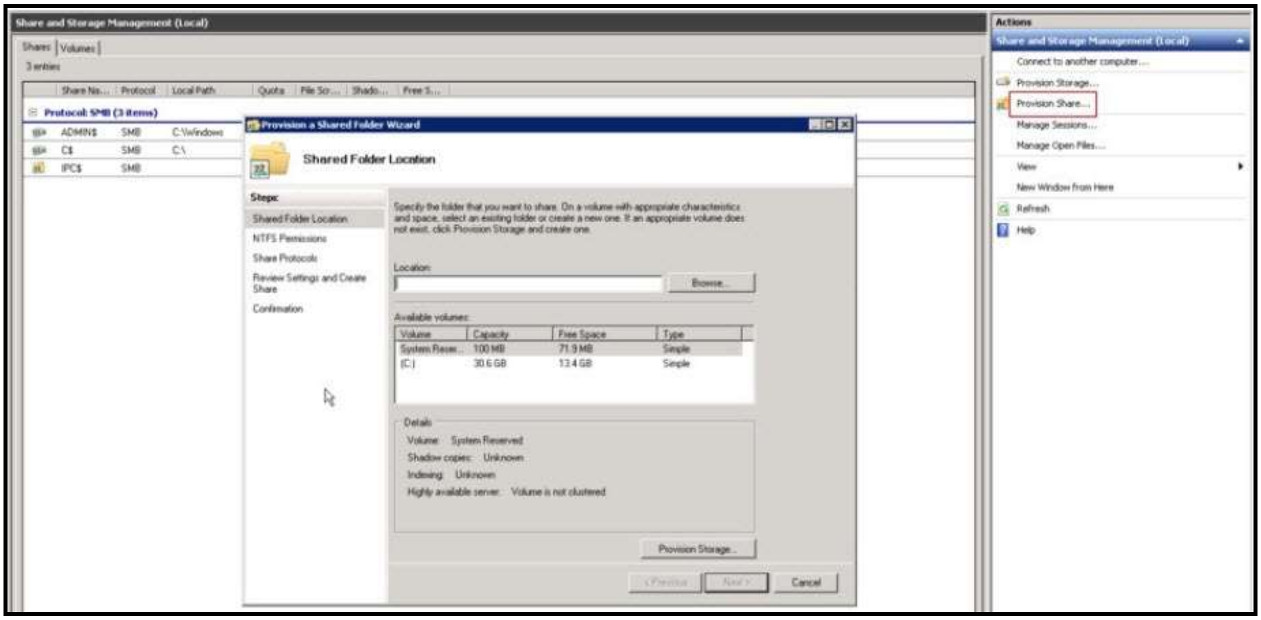
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Figure 3.185: Completion of cluster creation

3.24.2 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 3.186.



Share Na...	Protocol	Local Path	Quota	File Scr...	Shado...	Free S...
Protocol: SMB (3 items)						
ADMIN$	SMB	C:\Windows				
C$	SMB	C:\				
IPC$	SMB					

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:

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

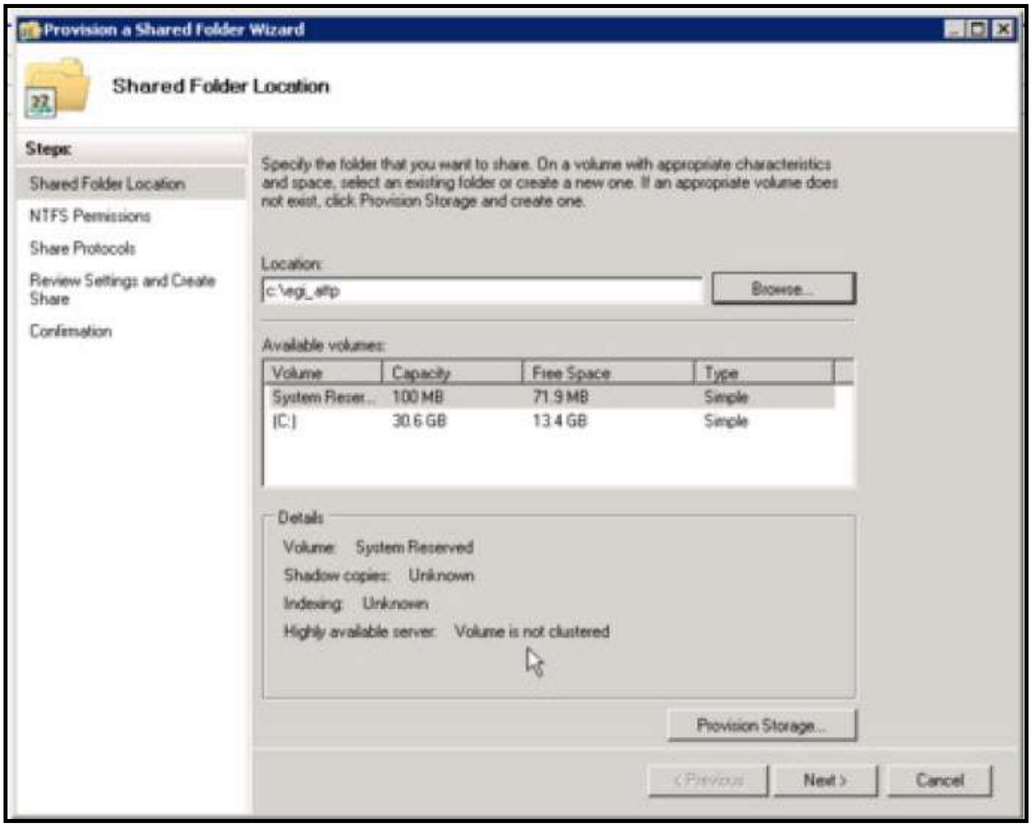
Shadow copies: Unknown

Indexing: Unknown

Highly available server: Volume is not clustered

Figure 3.186: Selecting the Provision Share option

2. In the **Location** text box of Figure 3.187 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_attp

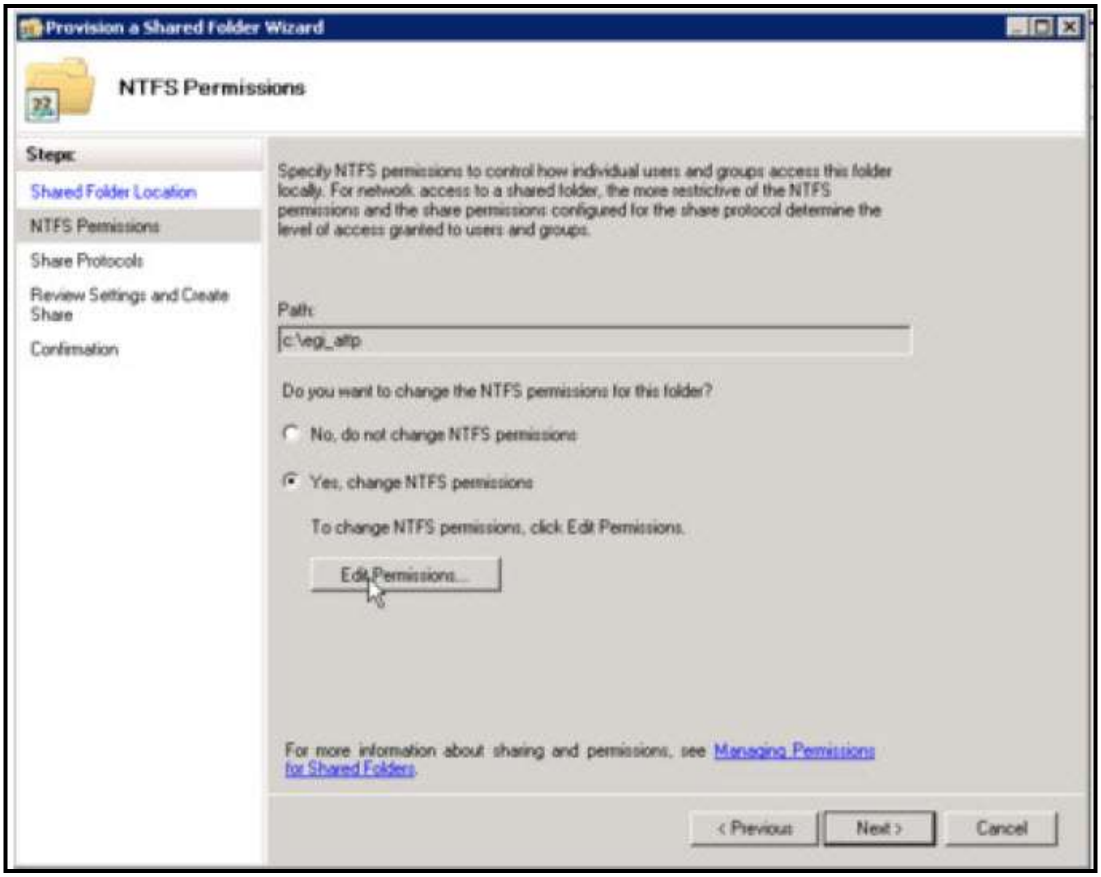
Available volumes:

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 3.187: Selecting the folder to share

3. In the **NTFS Permissions** dialog box that appears next (see Figure 3.188), 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_aftp

Do you want to change the NTFS permissions for this folder?

○ No, do not change NTFS permissions

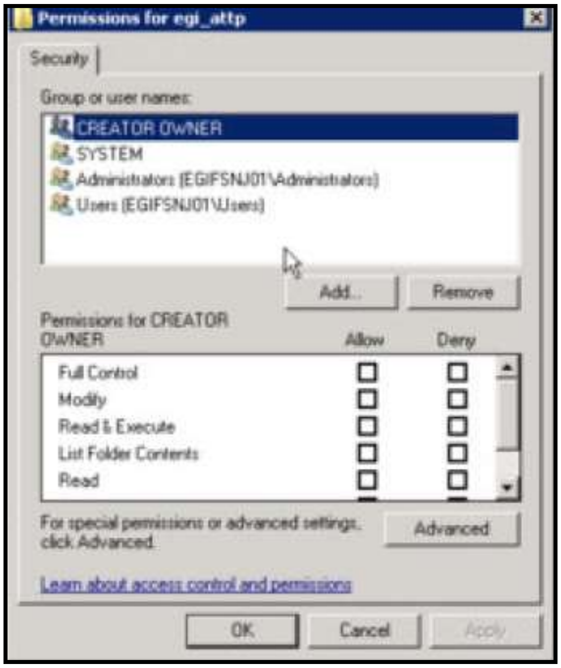
● Yes, change NTFS permissions

To change NTFS permissions, click Edit Permissions.

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.188: Choosing to change the NTFS permissions of the specified folder

4. Doing so invokes Figure 3.189. Click the **Add** button in Figure 3.189.



Group or user names:

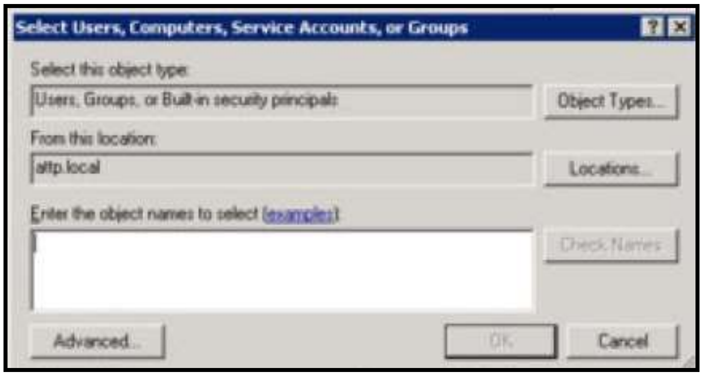
CREATOR OWNER
SYSTEM
Administrators (EGIFSNJ01\Administrators)
Users (EGIFSNJ01\Users)

Permissions for CREATOR OWNER	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	□	□
List Folder Contents	□	□
Read	□	□

For special permissions or advanced settings, click Advanced.

Figure 3.189: Adding a user/group

5. Figure 3.190 will then appear. Click the **Object Types** button in Figure 3.190, select the **Computers** check box in the window that pops up, and click the **OK** button in that window to return to Figure 3.190.



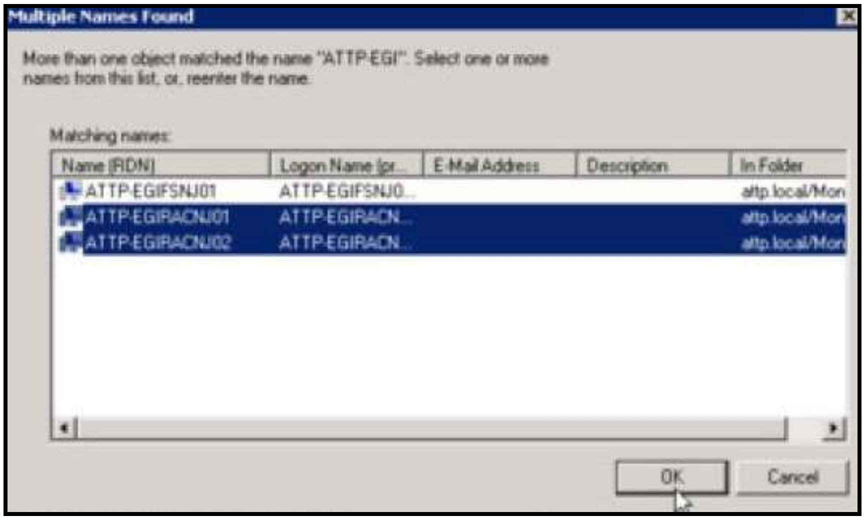
Select this object type:
Users, Groups, or Built-in security principals

From this location:
attp.local

Enter the object names to select (examples):

Figure 3.190: Clicking the Object Types button

6. Now, in the **Enter the object names to select** text area of Figure 3.190, type the name of the cluster you created using the procedure detailed in Section 3.23.1, and click the **Check Names** button. Figure 3.191 will then appear, listing all objects that match the cluster name that you specified.



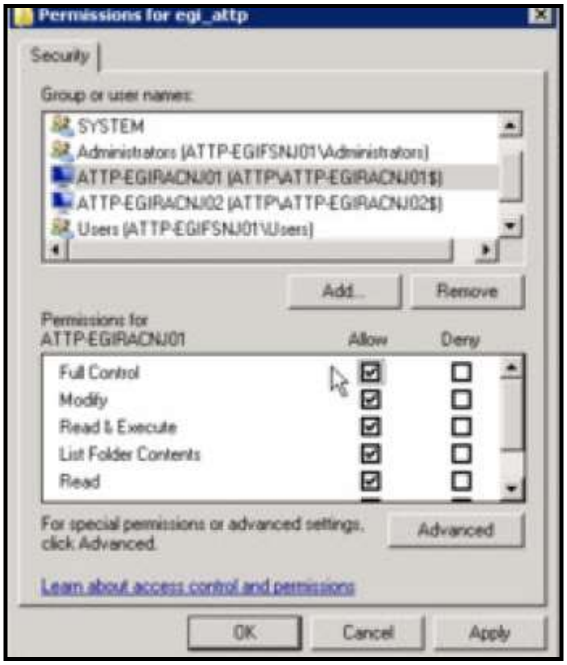
More than one object matched the name "ATTP-EGI". Select one or more names from this list, or, reenter the name.

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

Figure 3.191: A window displaying all objects with names that match the specified cluster name

7. Select the name of the cluster you created from Figure 3.191 and click the **OK** button therein. Figure 3.192 will then appear. From the **Group of user names** list of Figure 3.192, 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:

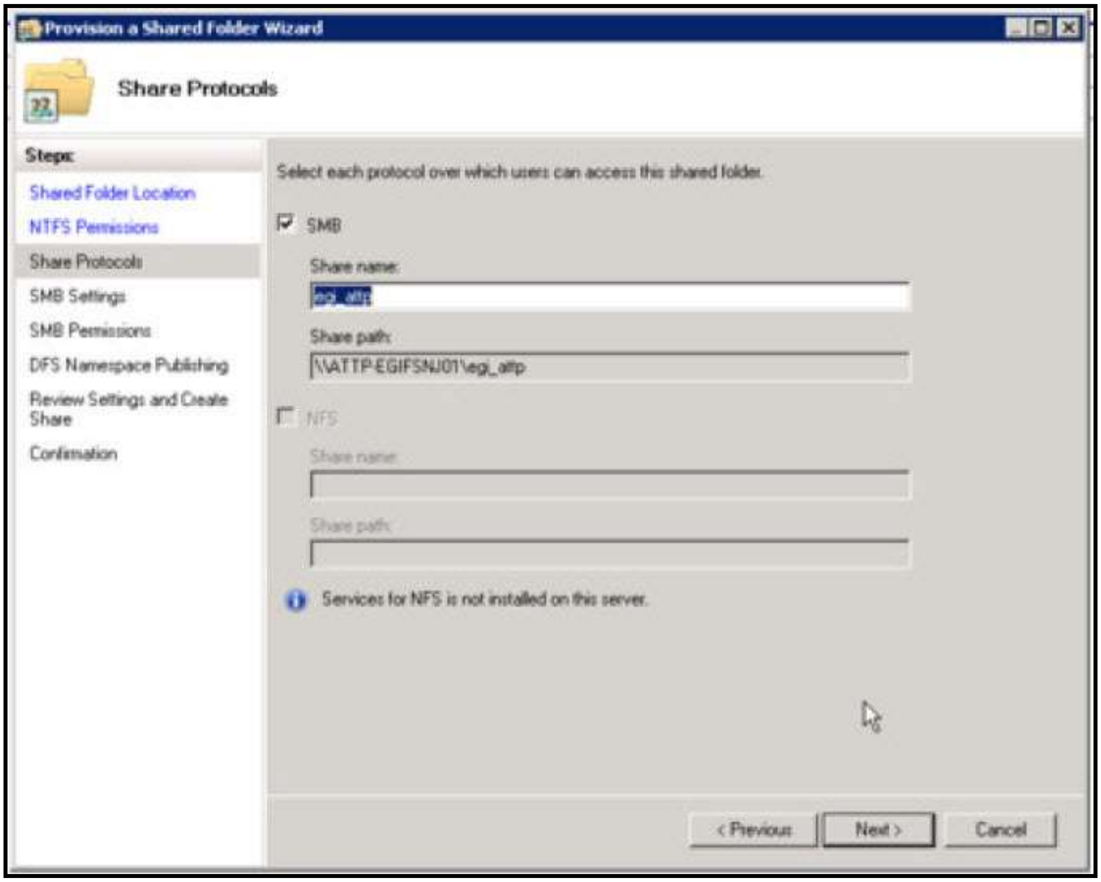
SYSTEM
Administrators (ATTP-EGIFSNJ01\Administrators)
ATTP-EGIRACNJ01 (ATTP\ATTP-EGIRACNJ01$)
ATTP-EGIRACNJ02 (ATTP\ATTP-EGIRACNJ02$)
Users (ATTP-EGIFSNJ01\Users)

Permissions for ATTP-EGIRACNJ01	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□

For special permissions or advanced settings, click Advanced.

Figure 3.192: 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

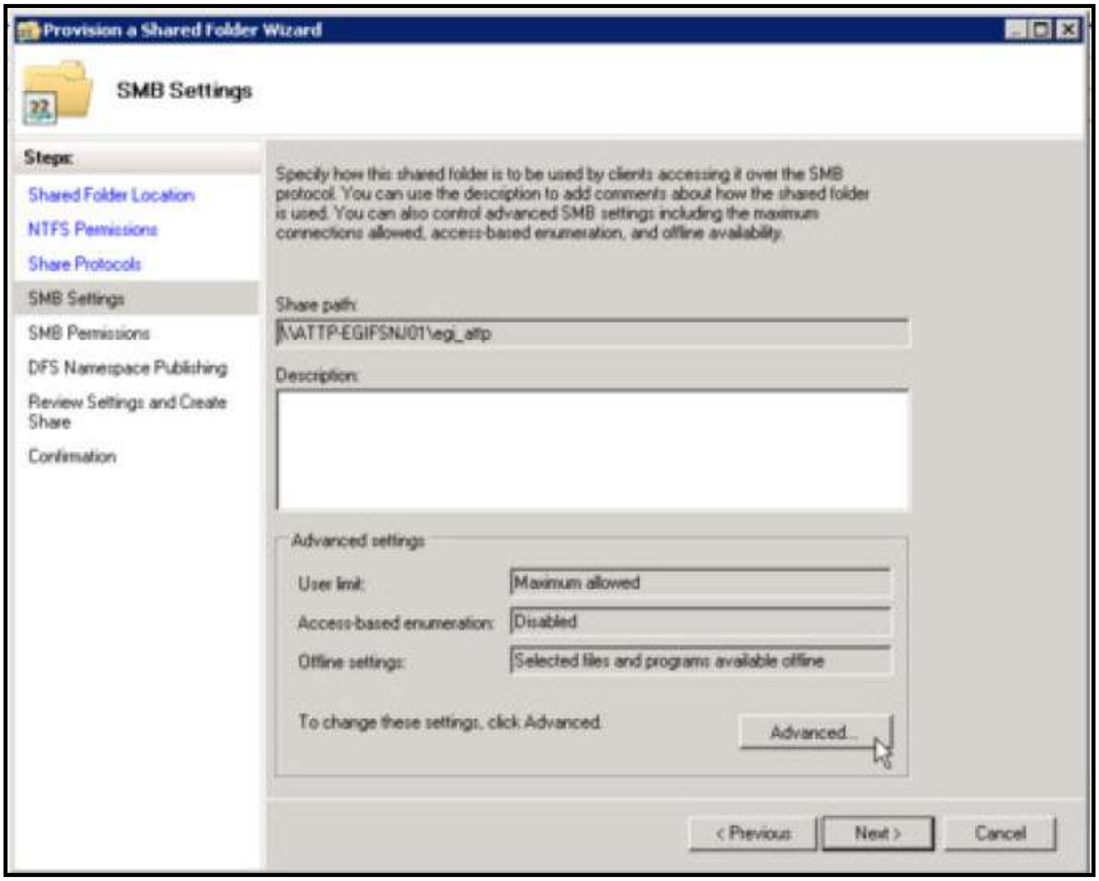
Share name:

Share path:

Services for NFS is not installed on this server.

Figure 3.193: Accepting the default settings of the Share Protocols section

9. This will take you to the **SMB Settings** section (see Figure 3.194). 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

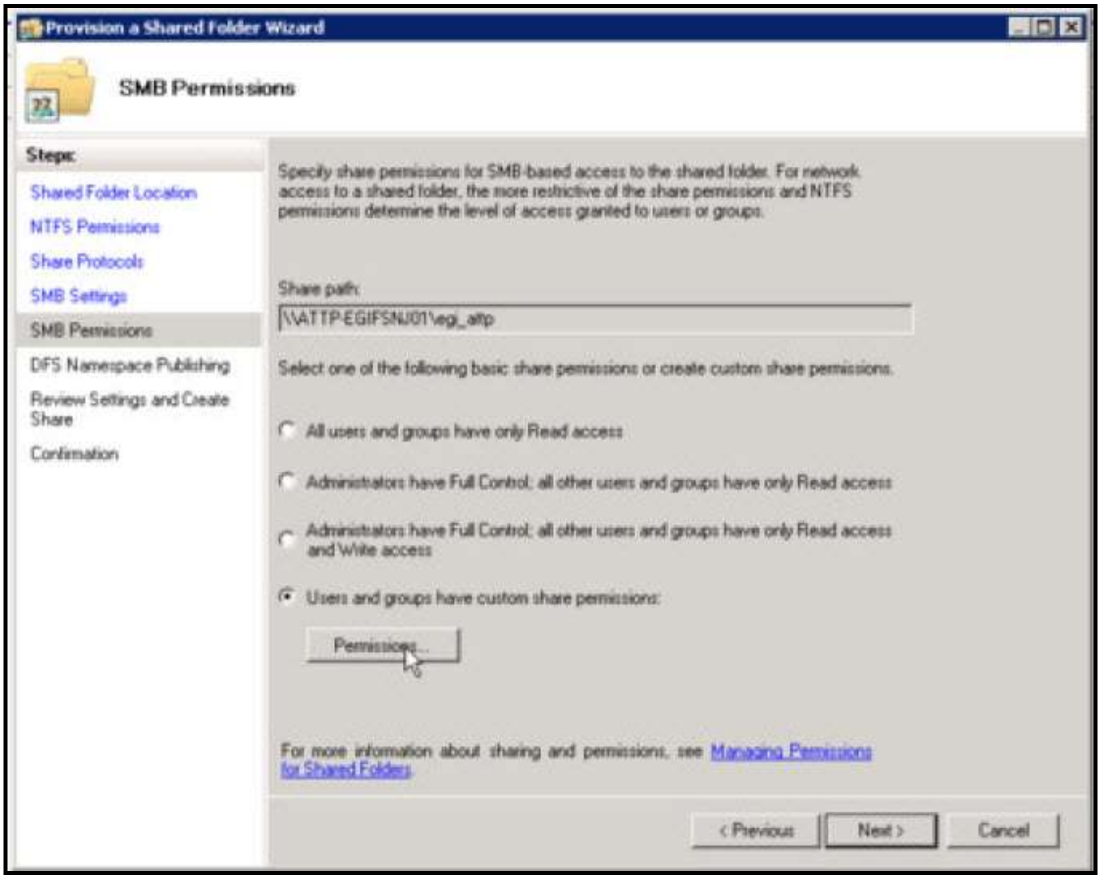
Access-based enumeration: Disabled

Offline settings: Selected files and programs available offline

To change these settings, click Advanced.

Figure 3.194: 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 3.195). Then, click the **Permissions** button in Figure 3.195.



Provision a Shared Folder Wizard

SMB Permissions

Steps:

- Shared Folder Location
- NTFS Permissions
- Share Protocols
- SMB Settings
- SMB Permissions
- DFS Namespace Publishing
- Review Settings and Create Share
- Confirmation

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

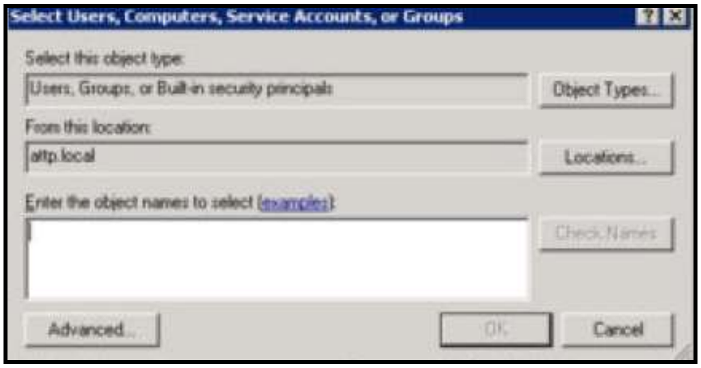
○ Administrators have Full Control; all other users and groups have only Read access and Write access

● Users and groups have custom share permissions:

For more information about sharing and permissions, see Managing Permissions for Shared Folders.

Figure 3.195: Configuring SMP Permissions

11. When Figure 3.196 appears, click the **Object Types** button in Figure 3.196, select the **Computers** check box in the window that pops up, and click the **OK** button in that window to return to Figure 3.196.



Select Users, Computers, Service Accounts, or Groups

Select this object type:

Users, Groups, or Built-in security principals

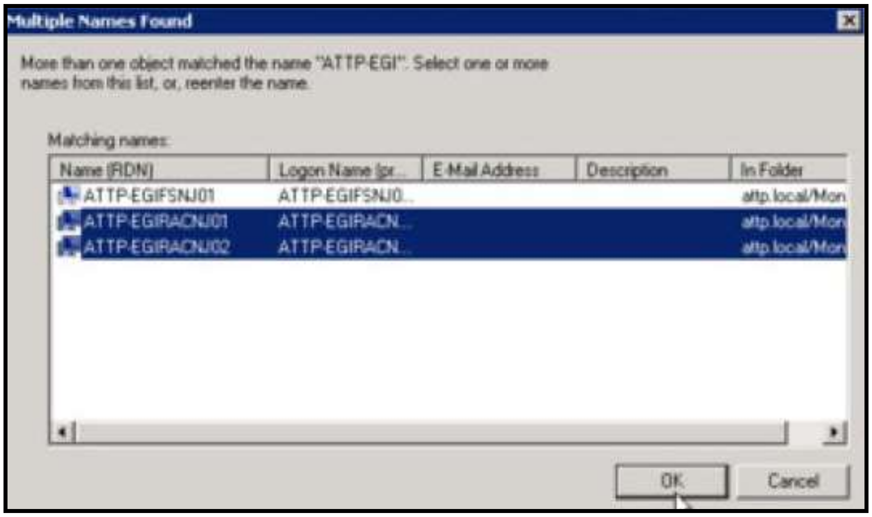
From this location:

attp.local

Enter the object names to select (examples):

Figure 3.196: Clicking the Object Types button

12. Now, in the **Enter the object names to select** text area of Figure 3.196, type the name of the cluster you created using the procedure detailed in Section 3.23.1, and click the **Check Names** button. Figure 3.197 will then appear, listing all objects that match the cluster name that you specified.



Multiple Names Found

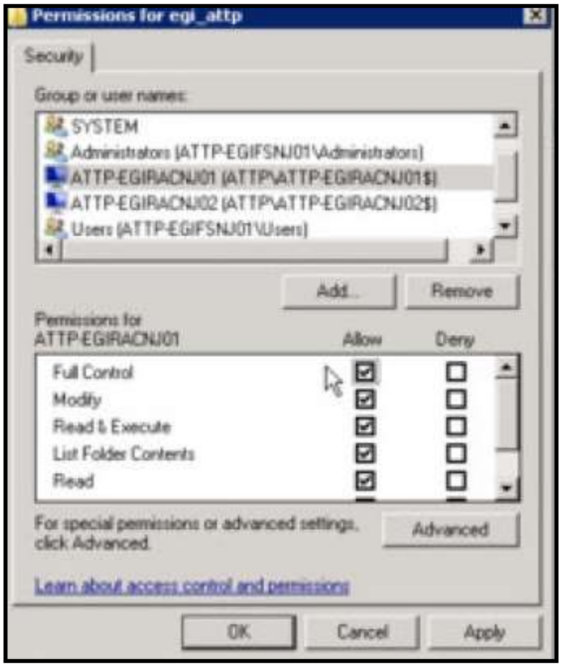
More than one object matched the name "ATTP-EGI". Select one or more names from this list, or, reenter the name.

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

Figure 3.197: A window displaying all objects with names that match the specified cluster name

13. Select the name of the cluster you created from Figure 3.197 and click the **OK** button therein. Figure 3.198 will then appear. From the **Group or user names** list of Figure 3.198, select the cluster name. Then, select the **Allow** check box against **Full Control** permission in the **Permissions for ...** list and click the **OK** button.



Permissions for egi_attp

Security

Group or user names:

- SYSTEM
- Administrators (ATTP-EGIFSNJ01\Administrators)
- ATTP-EGIRACNJ01 (ATTP\ATTP-EGIRACNJ01$)
- ATTP-EGIRACNJ02 (ATTP\ATTP-EGIRACNJ02$)
- Users (ATTP-EGIFSNJ01\Users)

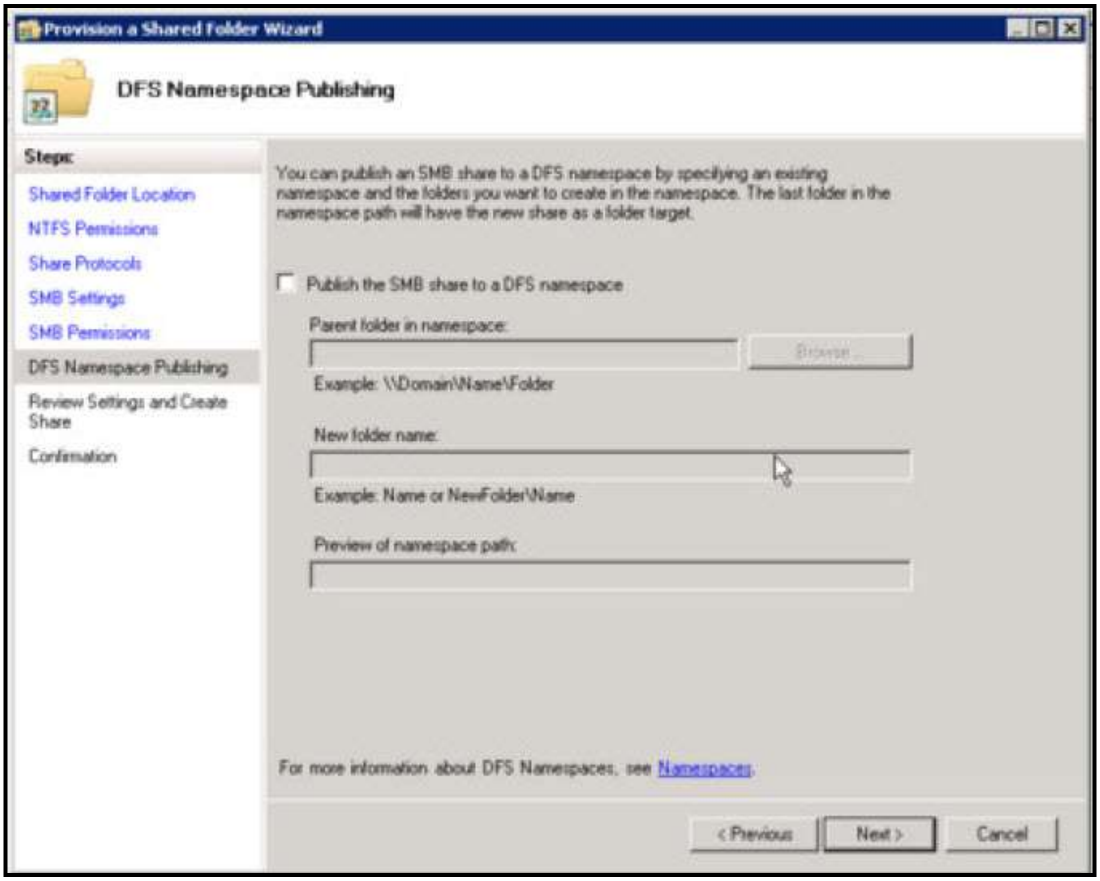
Permissions for ATTP-EGIRACNJ01	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Figure 3.198: Granting Full Control to cluster

14. Once you return to the **SMB Settings** section, click on the **Next** button to move on. Figure 3.199 will then appear. Accept the default settings of Figure 3.199 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:

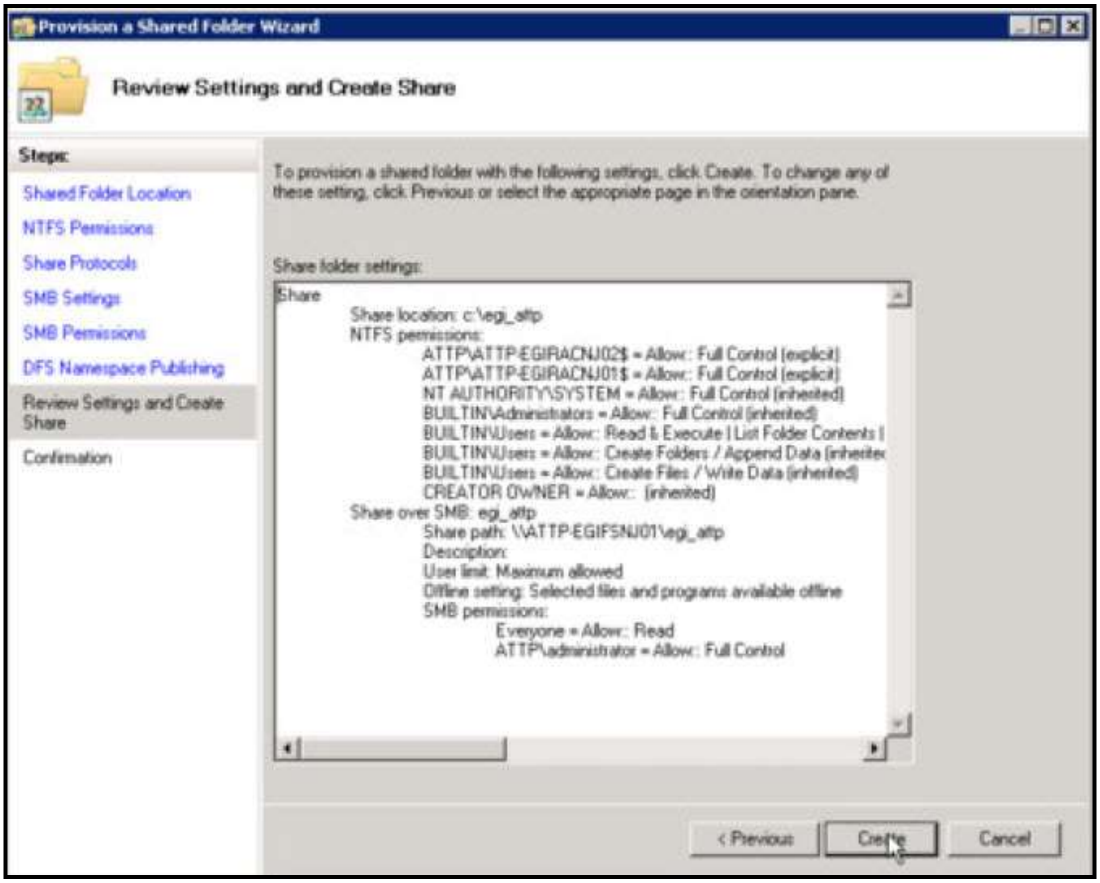
Example: Name or NewFolder\Name

Preview of namespace path:

For more information about DFS Namespaces, see Namespaces.

Figure 3.199: Accepting the default settings of DFS Namespace Publishing section

15. Figure 3.200 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.



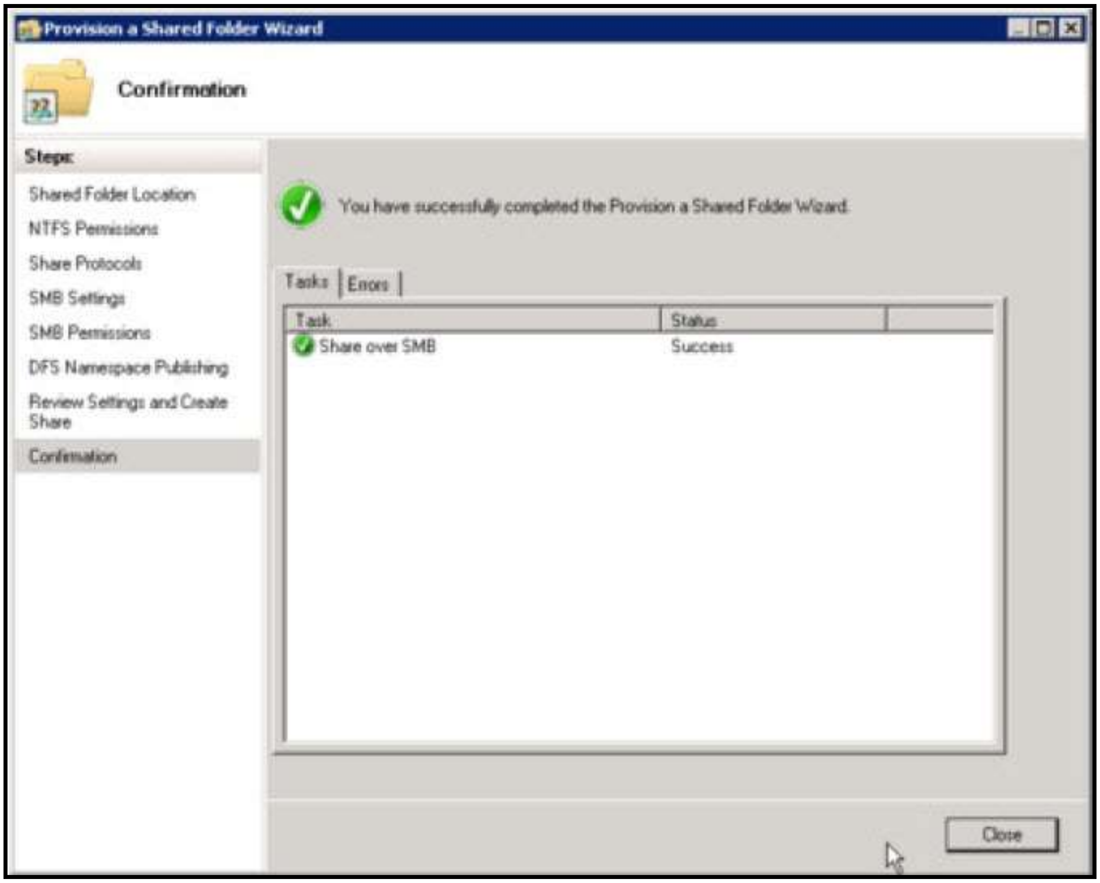
To provision a shared folder with the following settings, click Create. To change any of these setting, click Previous or select the appropriate page in the orientation pane.

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 3.200: Reviewing the share settings

16. If share creation is successful, then Figure 3.201 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 3.201: Successful creation of the file share

3.24.3 Configuring Cluster Quorum Settings

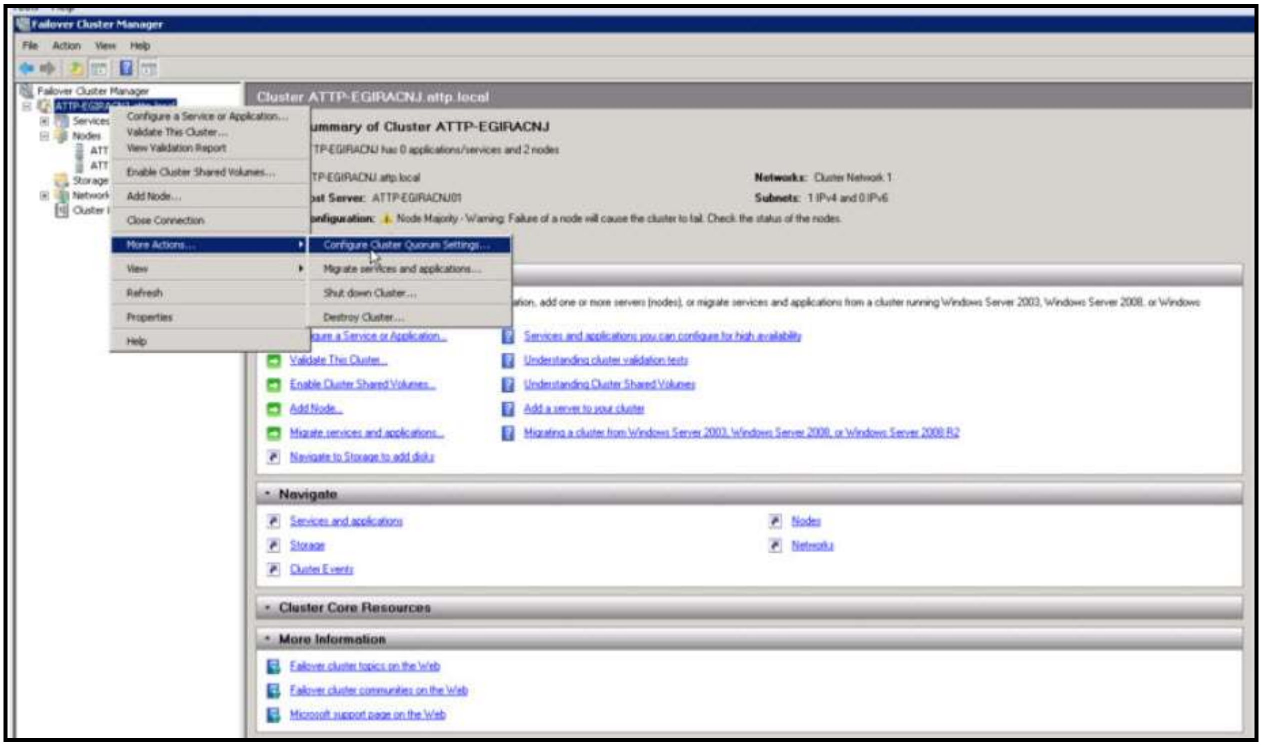
As stated earlier, the quorum for a cluster is the number of elements that must be online for that cluster to continue running.

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.



ummary of Cluster ATTP-EGIRACNJ

TP-EGIRACNJ has 0 applications/services and 2 nodes

TP-EGIRACNJ.attp.local

Networks: Cluster Network 1

ost Server: ATTP-EGIRACNJ01

Subnets: 1 IPv4 and 0 IPv6

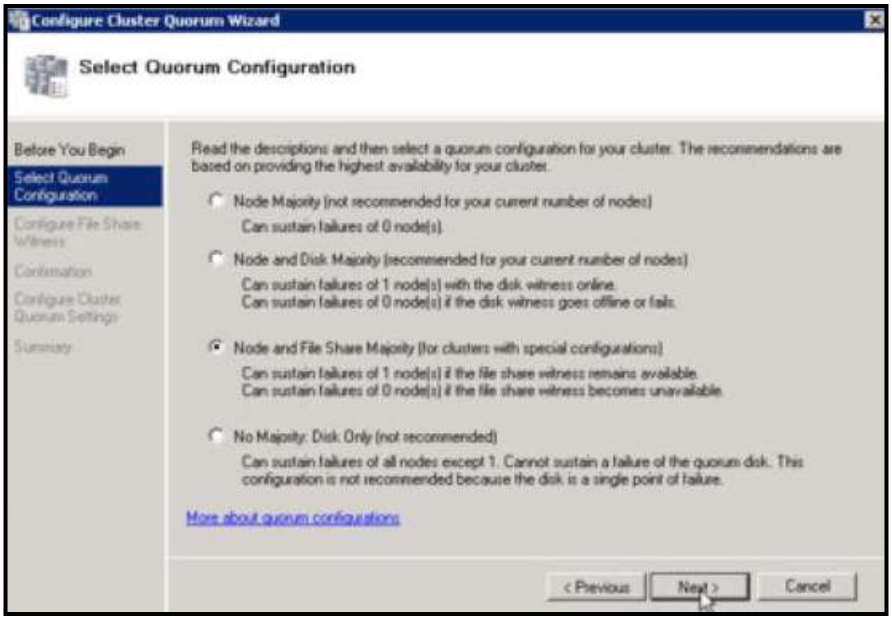
onfiguration: Node Majority - Warning: Failure of a node will cause the cluster to fail. Check the status of the nodes.

ation, add one or more servers (nodes), or migrate services and applications from a cluster running Windows Server 2003, Windows Server 2008, or Windows

Failover Cluster Manager
File
Action
View
Help
Failover Cluster Manager
ATTP-EGIRACNJ.attp.local
Services
Nodes
ATT
ATT
Storage
Network
Cluster
Cluster ATTP-EGIRACNJ.attp.local
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...
gure 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

Figure 3.202: 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 3.203). Then, click the **Next** button therein.



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.

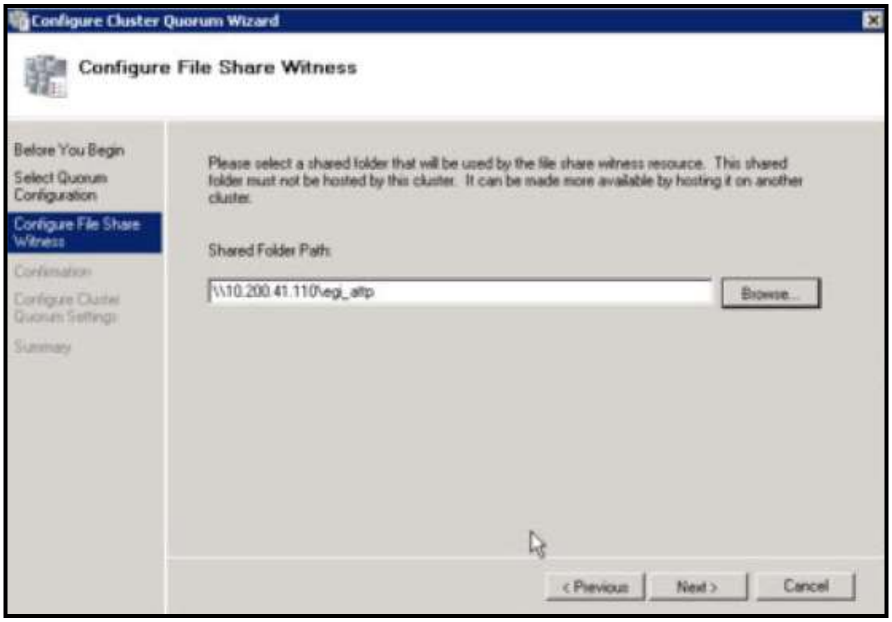
● Node and File Share Majority (for clusters with special configurations)
Can sustain failures of 1 node(s) if the file share witness remains available.
Can sustain failures of 0 node(s) if the file share witness becomes unavailable.

○ 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.

Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
More about quorum configurations
< Previous
Next >
Cancel

Figure 3.203: Selecting the Node and File Sharing Majority option

3. In the **Shared Folder Path** text box of Figure 3.204, enter the full path to the shared folder that you had created earlier on the file share server (refer to Section 3.23.2). Then, click the **Next** button.



Configure Cluster Quorum Wizard

Configure File Share Witness

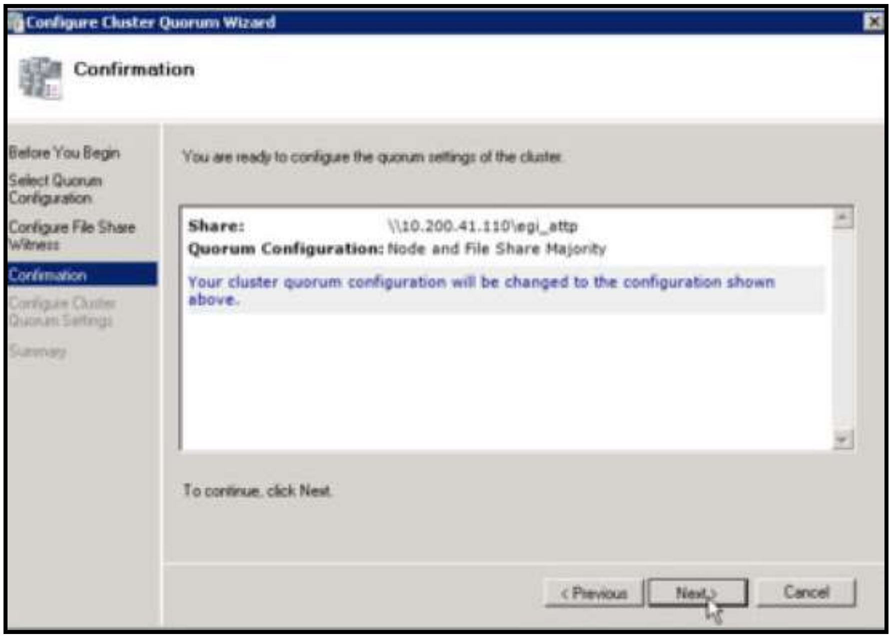
Please select a shared folder that will be used by the file share witness resource. This shared folder must not be hosted by this cluster. It can be made more available by hosting it on another cluster.

Shared Folder Path: \\10.200.41.110\egi_aftp

Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
Browse...
< Previous
Next >
Cancel

Figure 3.204: Entering the full path to the shared folder

4. Review the quorum settings once more in Figure 3.205, and click the **Next** button to proceed with the settings.


Configure Cluster Quorum Wizard
Confirmation
Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
< Previous
Next >
Cancel

You are ready to configure the quorum settings of the cluster.

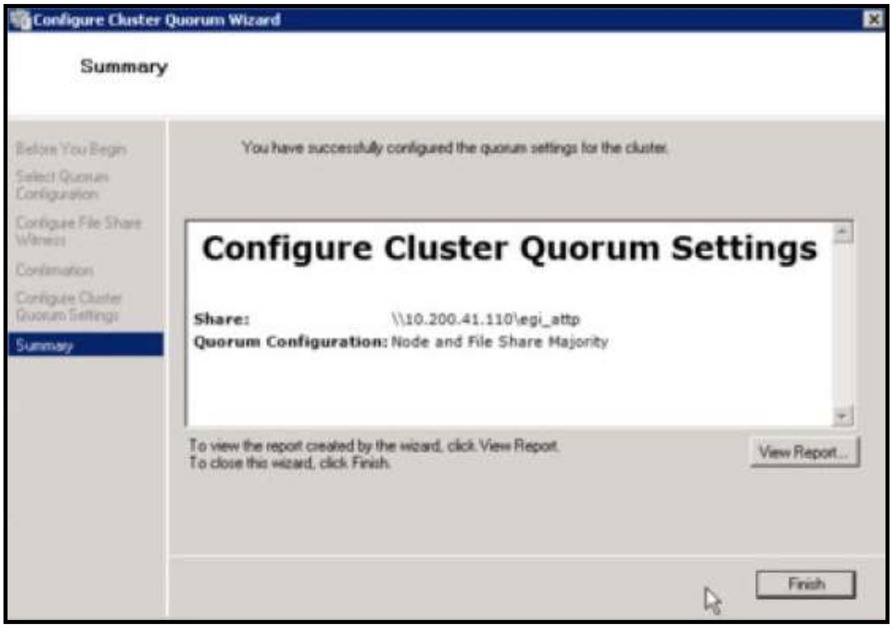
Share: \\10.200.41.110\egi_attp
Quorum Configuration: Node and File Share Majority

Your cluster quorum configuration will be changed to the configuration shown above.

To continue, click Next.

Figure 3.205: Reviewing the quorum settings

5. Click the **Finish** button in Figure 3.206 to end the quorum configuration process.


Configure Cluster Quorum Wizard
Summary
Before You Begin
Select Quorum Configuration
Configure File Share Witness
Confirmation
Configure Cluster Quorum Settings
Summary
View Report...
Finish

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

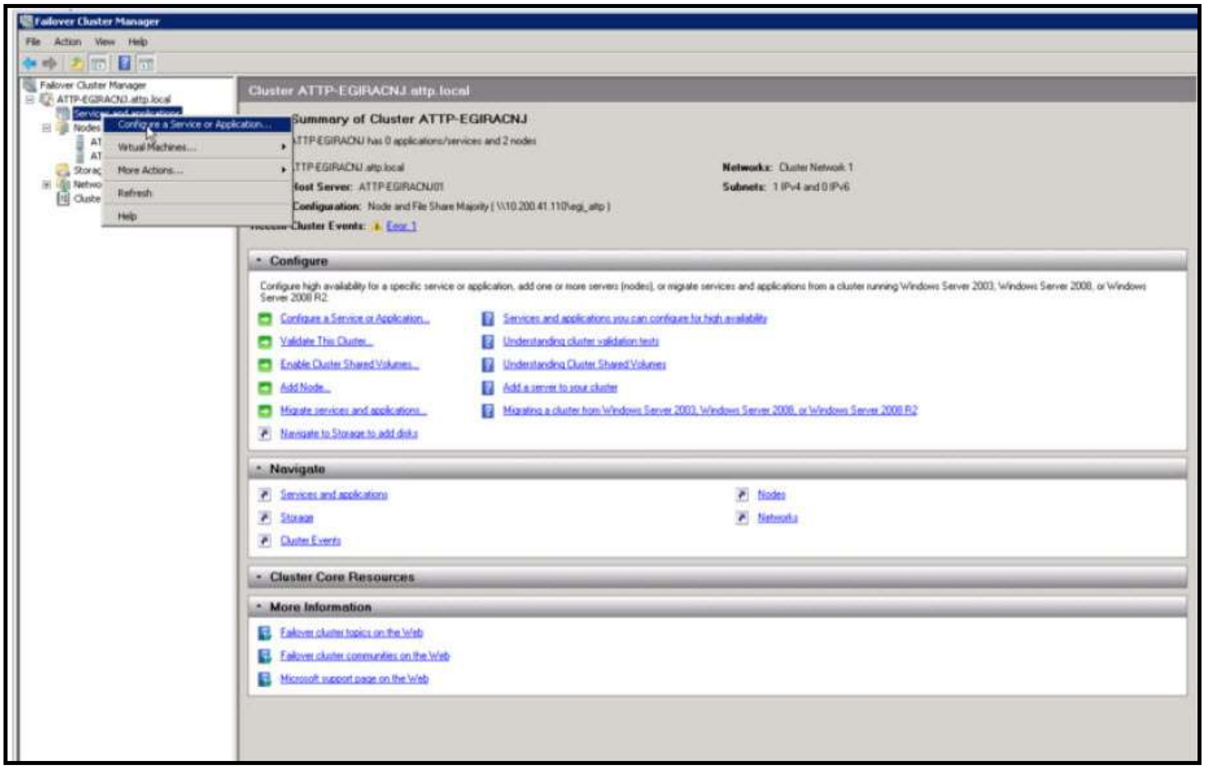
To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Figure 3.206: Completion of quorum configuration

3.24.4 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)

Cluster Events: Error: 1

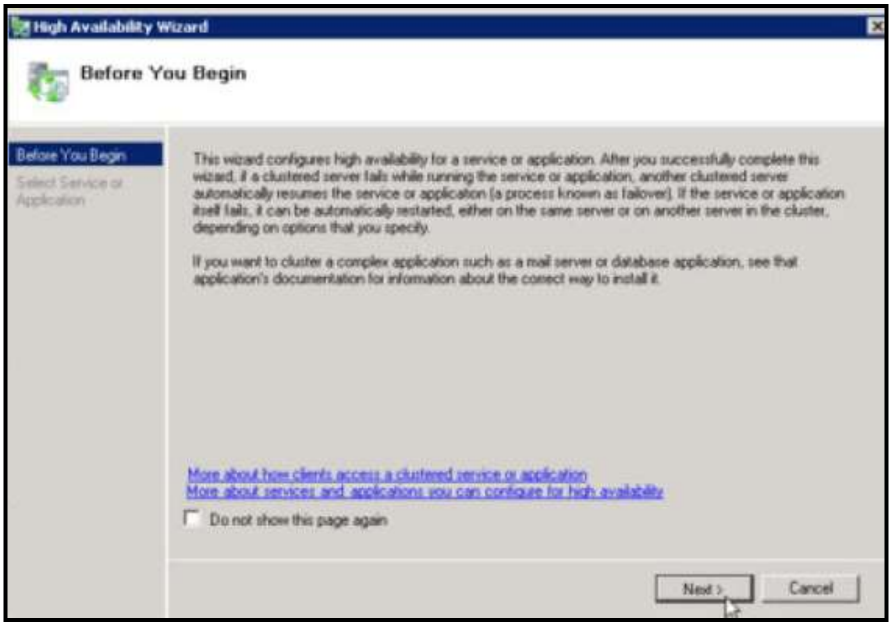
Networks: Cluster Network 1

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 3.207: 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.

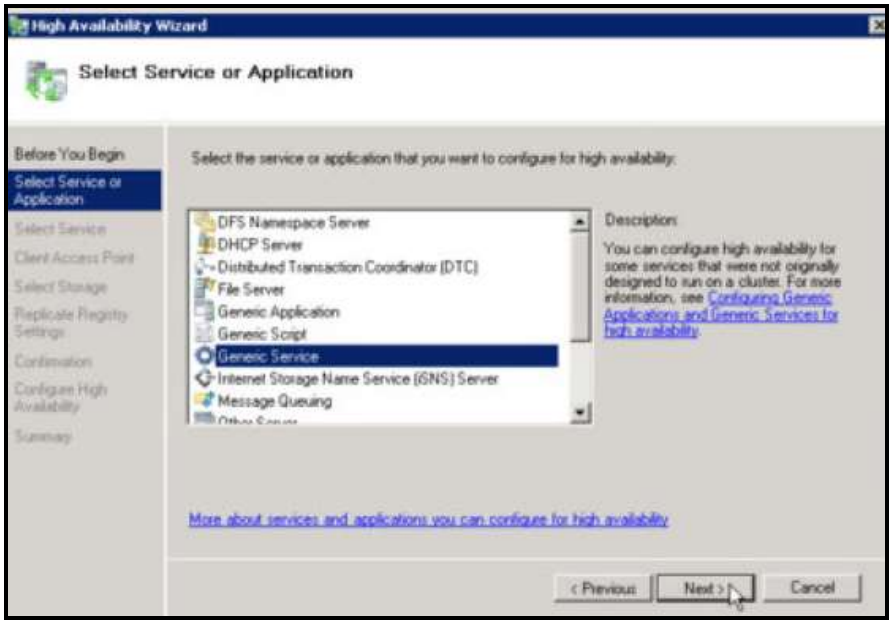

High Availability Wizard
Before You Begin
Before You Begin
Select Service or Application
More about how clients access a clustered service or application
More about services and applications you can configure for high availability
☐ Do not show this page again
Next >
Cancel

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.

Figure 3.208: The welcome screen of the High Availability wizard

3. When Figure 3.209 appears, select the **Generic Service** option and click the **Next** button.

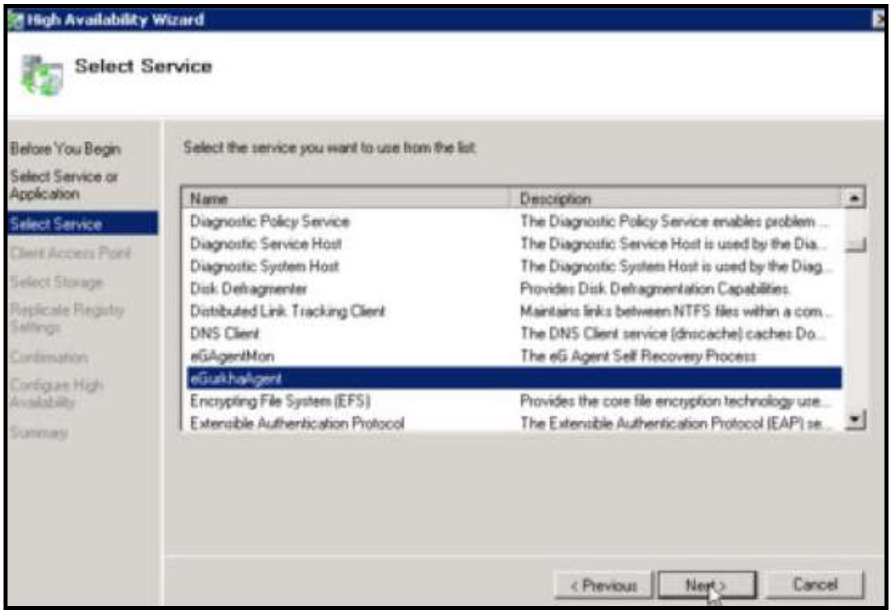

High Availability Wizard
Select Service or Application
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
DFS Namespace Server
DHCP Server
Distributed Transaction Coordinator (DTC)
File Server
Generic Application
Generic Script
Generic Service
Internet Storage Name Service (iSNS) Server
Message Queuing
Other Server
Description:
More about services and applications you can configure for high availability
< Previous
Next >
Cancel

Select the service or application that you want to configure for high availability:

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.

Figure 3.209: Selecting the Generic Service option

4. In Figure 3.210, select the **eGurkhaAgent** service from the list of services displayed therein and click the **Next** button.

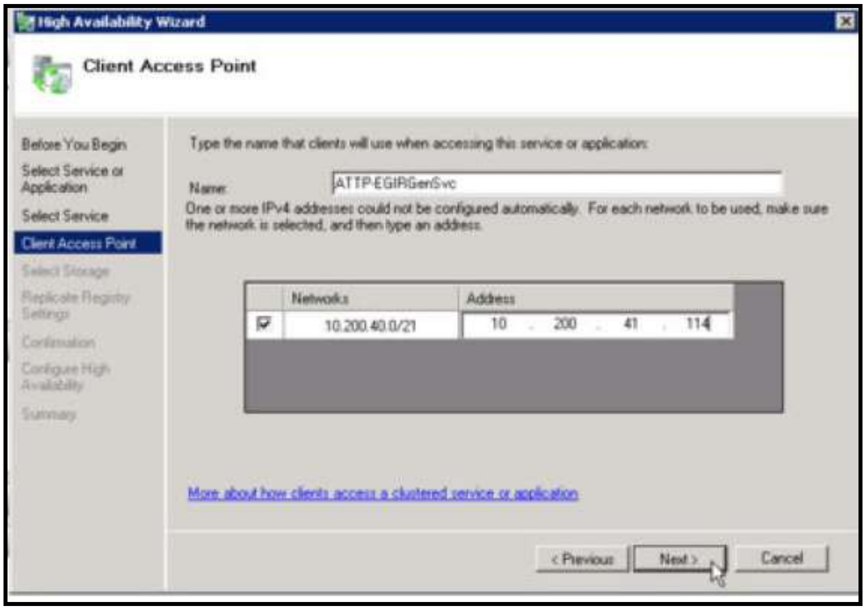


Select the service you want to use from the list:

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...

Figure 3.210: 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 3.211.


High Availability Wizard
Client Access Point
Before You Begin
Select Service or Application
Select Service
Client Access Point
Select Storage
Replicate Registry Settings
Confirmation
Configure High Availability
Summary
More about how clients access a clustered service or application
< Previous
Next >
Cancel

Type the name that clients will use when accessing this service or application:

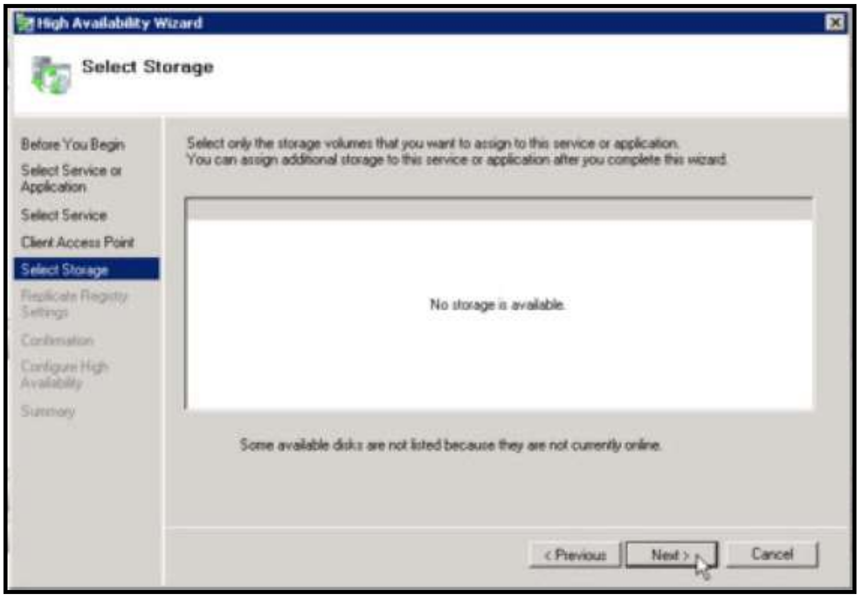
Name: ATTP-EGIRGenSvc

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

Figure 3.211: Entering the network name and IP address using which clients will be accessing the clustered resource

6. When Figure 3.212, click on the **Next** button to move on.



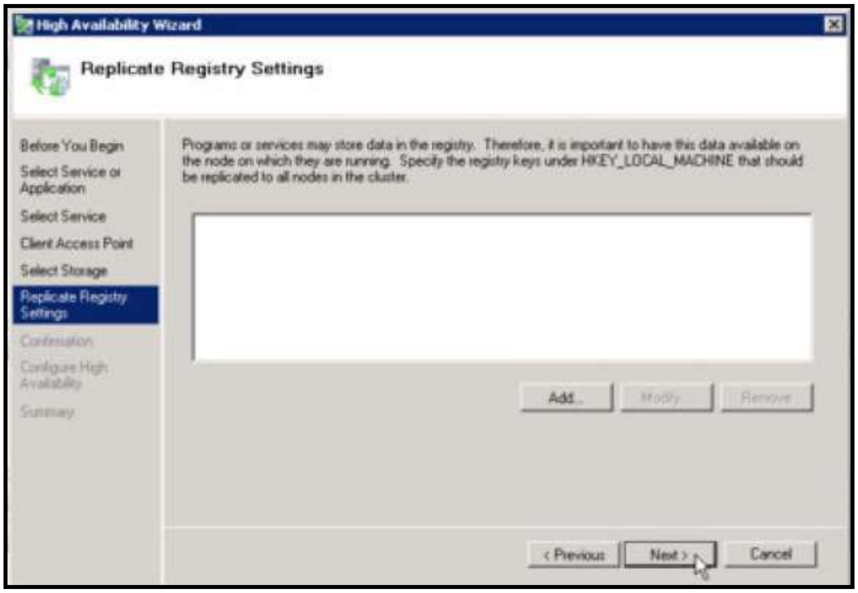
Select only the storage volumes that you want to assign to this service or application.
You can assign additional storage to this service or application after you complete this wizard.

No storage is available.

Some available disks are not listed because they are not currently online.

Figure 3.212: Clicking the Next button in the Select Storage page

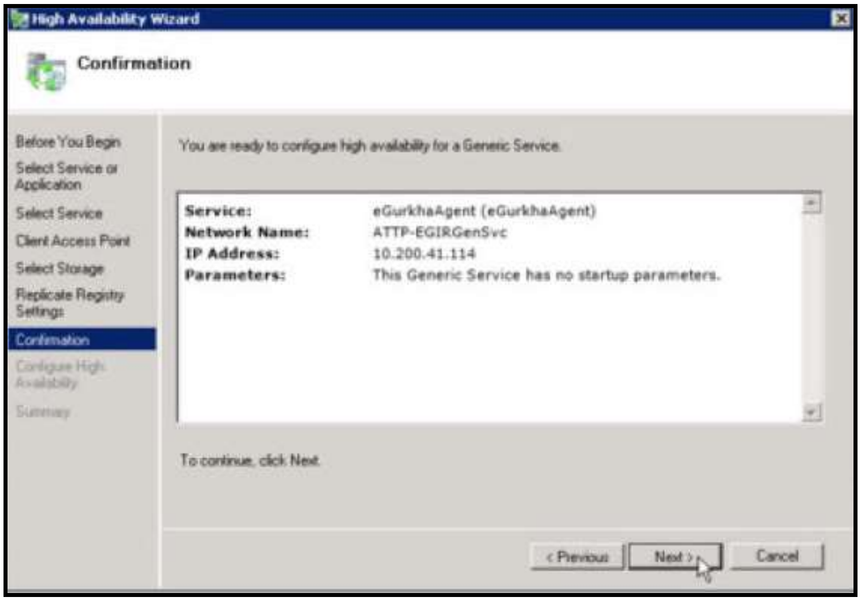
7. To skip the **Replicate Registry Settings** page and move to the next step, click the **Next** button in Figure 3.213.



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.

Figure 3.213: Skipping the Replicate Registry Settings page

8. Once the **Confirmation** page appears (see Figure 3.214), quickly review the service configuration displayed therein, and click the **Next** button to confirm the addition of that service as a clustered resource.



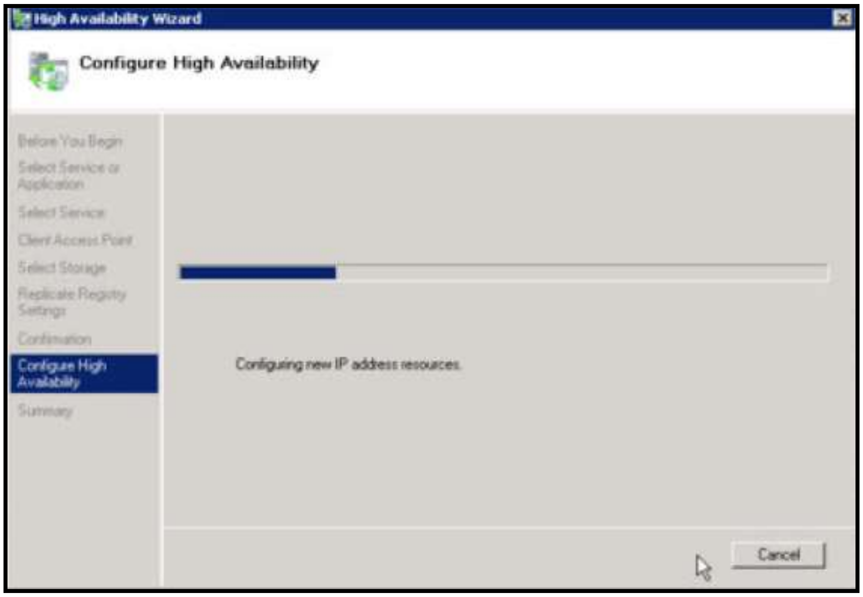
You are ready to configure high availability for a Generic Service.

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.

Figure 3.214: Reviewing the service configuration

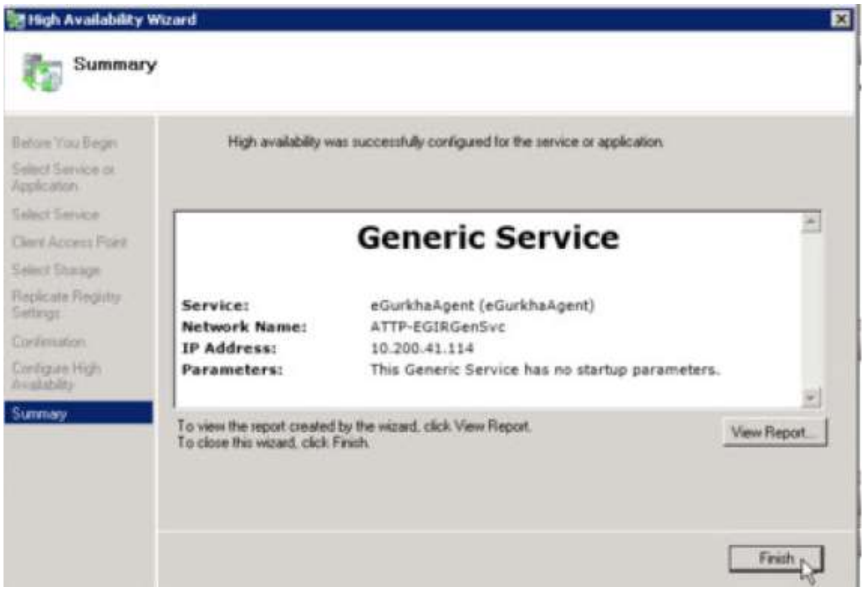
9. Upon confirmation, the cluster manager will then begin configuring the high availability of the **eGurkhaAgent** service (see Figure 3.215).



Configuring new IP address resources.

Figure 3.215: High availability configuration in progress for the eGurkhaAgent service

10. Once the configuration process ends, Figure 3.216 appears confirming the successful completion of the high availability configuration, and displaying the details of the **eGurkhaAgent** service for which high availability was configured.



High availability was successfully configured for the service or application

Generic Service

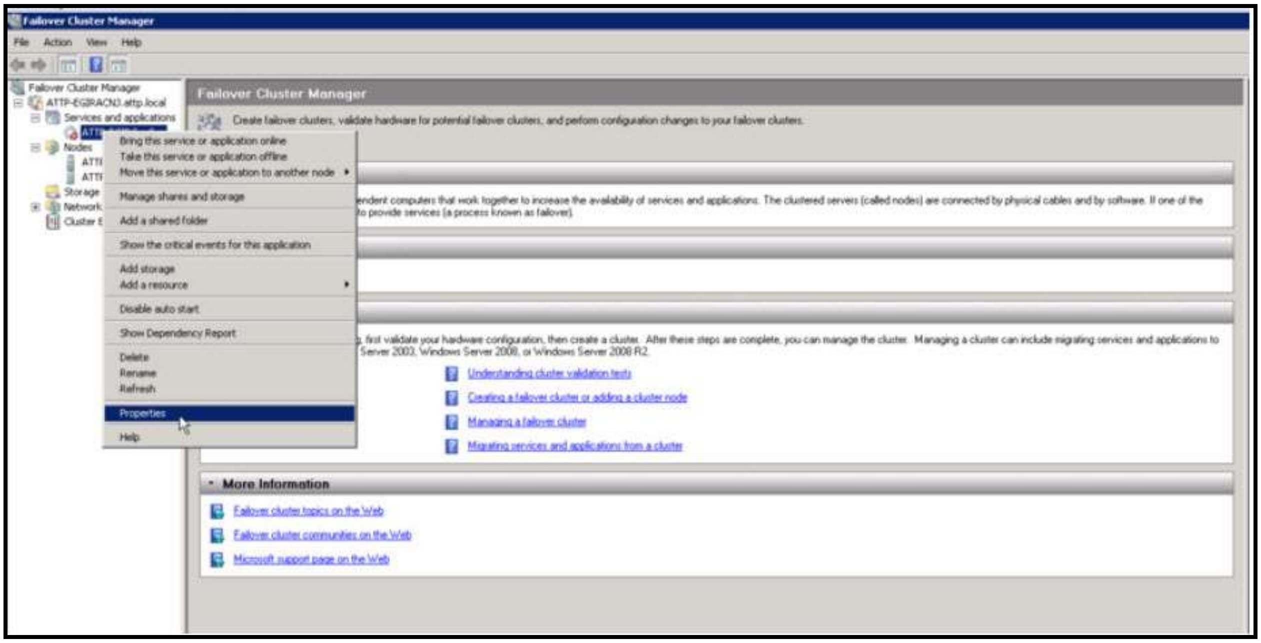
Service: eGurkhaAgent (eGurkhaAgent)
Network Name: ATTP-EGIRGenSvc
IP Address: 10.200.41.114
Parameters: This Generic Service has no startup parameters.

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.

Figure 3.216: A message indicating the successful configuration of high availability for the eGurkhaAgent service

11. Click the **Finish** button in Figure 3.216 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 3.217).


Failover Cluster Manager
File
Action
View
Help
Failover Cluster Manager
ATTP-EGIRACN3.attp.local
Services and applications
ATTP
Nodes
ATTI
ATTI
Storage
Network
Cluster E
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
Failover Cluster Manager
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

Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

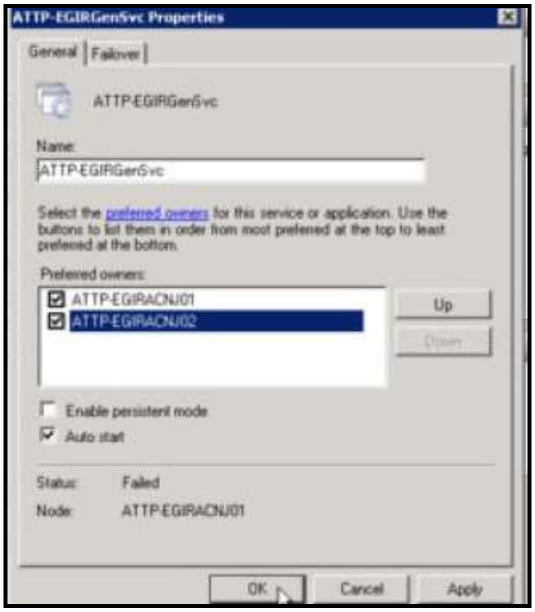
endent computers that work together to increase the availability of services and applications. The clustered servers (called nodes) are connected by physical cables and by software. If one of the to provide services (a process known as failover).

, 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 3.217: Editing the Properties of the eGurkhaAgent service that has been added as a cluster resource

13. Figure 3.218 then appears. In the **General** tab of Figure 3.218, 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 3.218 to save the changes you made.



ATTP-EGIRGenSvc

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:

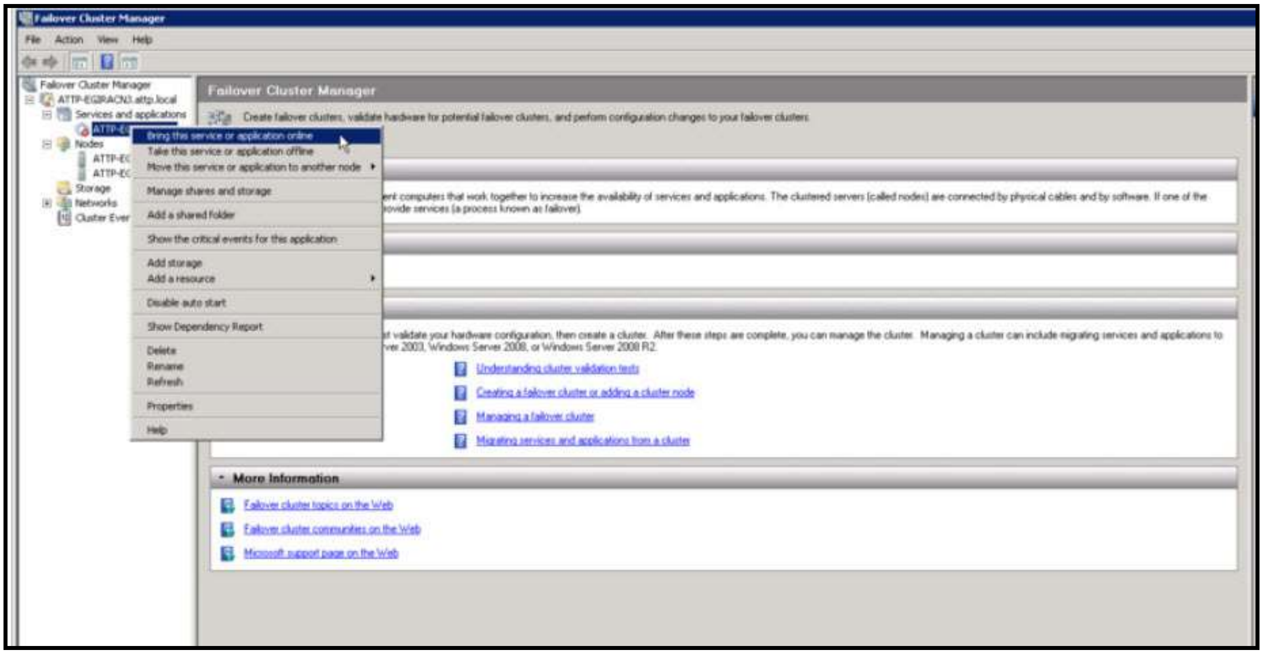
☑ ATTP-EGIRACNJ01
☑ ATTP-EGIRACNJ02

☐ Enable persistent mode
☑ Auto start

Status: Failed
Node: ATTP-EGIRACNJ01

Figure 3.218: 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 3.219).


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
ATTP-EGIRACNJ.attp.local
Services and applications
ATTP-EG
Nodes
ATTP-EG
ATTP-EG
Storage
Networks
Cluster Ever
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
Failover Cluster Manager
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

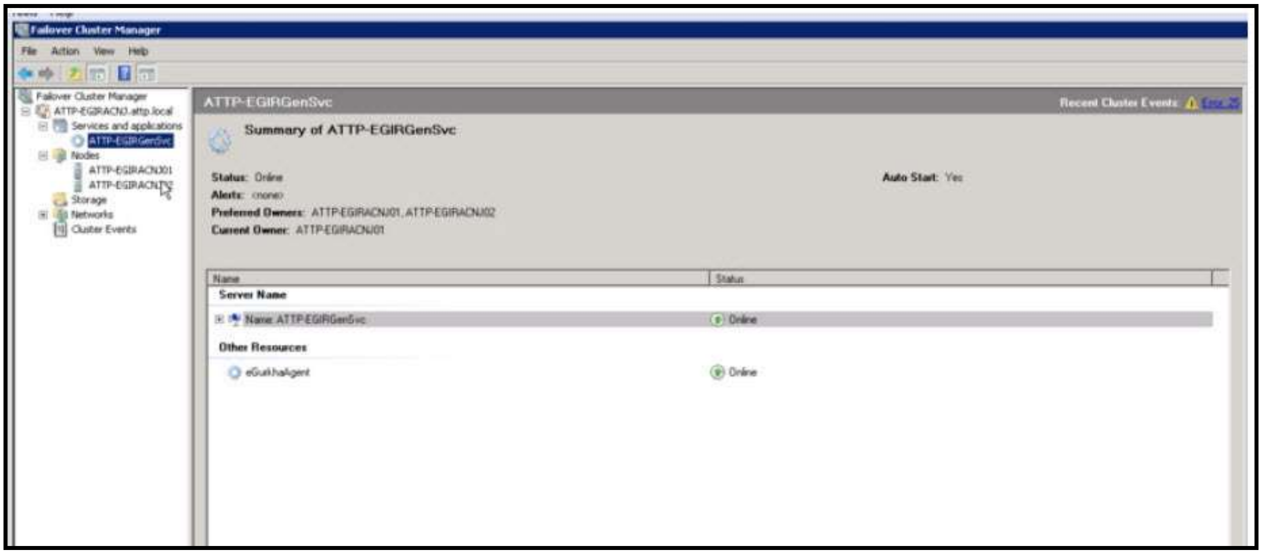
Create failover clusters, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.

ent 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 rovide services (a process known as failover).

t 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 ver 2003, Windows Server 2008, or Windows Server 2008 R2.

Figure 3.219: Bringing the clustered service online

15. Once the service goes online, Figure 3.220 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 3.220: The right panel of the Failover Cluster Manager indicating that the service is online

3.24.5 Manually Configuring an Apache Server

To configure an apache server manually, do the following:

1. Change the Apache configuration file. For that, first open the **httpd.conf** file, which is located at

<APACHE_ROOT>/conf/httpd.conf. Then, enter the following lines at the end of the file:

LoadModule egurkha_module libexec/mod_egurkha.dll

AddModule mod_egurkha.c

2. Copy the dll file **mod_egurkha.dll** from **<EG_ROOT>/lib/** to <**APACHE_ROOT>/libexec/**.
3. Create an **apache_root.txt** file at <**EG_ROOT>/agent/config** directory and type the following:

   server=<APACHE_ROOT>

   For example, if the root directory of the Apache server is **C:\Program Files\Apache group\Apache**, then:

   server= C:\Program Files\Apache group\Apache
4. Restart the Apache server.

3.25 Stopping the eG Agent

To stop the agent on a Windows 2003/XP host, click the **Start** button on the task bar. From thereon, select Programs > eG Monitoring Suite > eG Agent > Stop Agent.

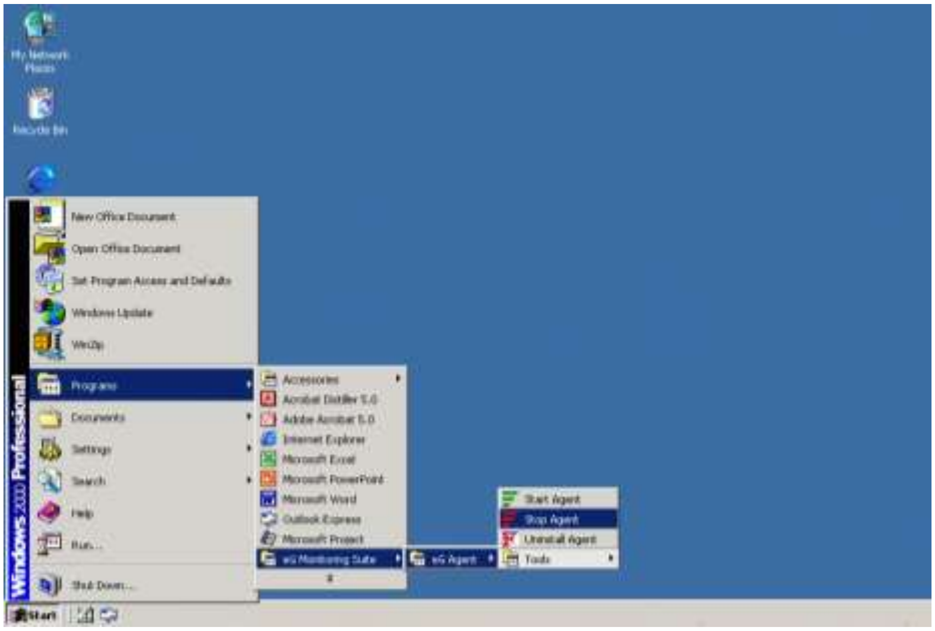


Figure 3.221: Stopping the eG agent

In case of Windows Vista however, only a user with "administrator" privileges can stop the agent. Therefore, before attempting to start 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 3.224. This implies that the command that is issued at the command prompt soon after, will be run with administrator privileges.

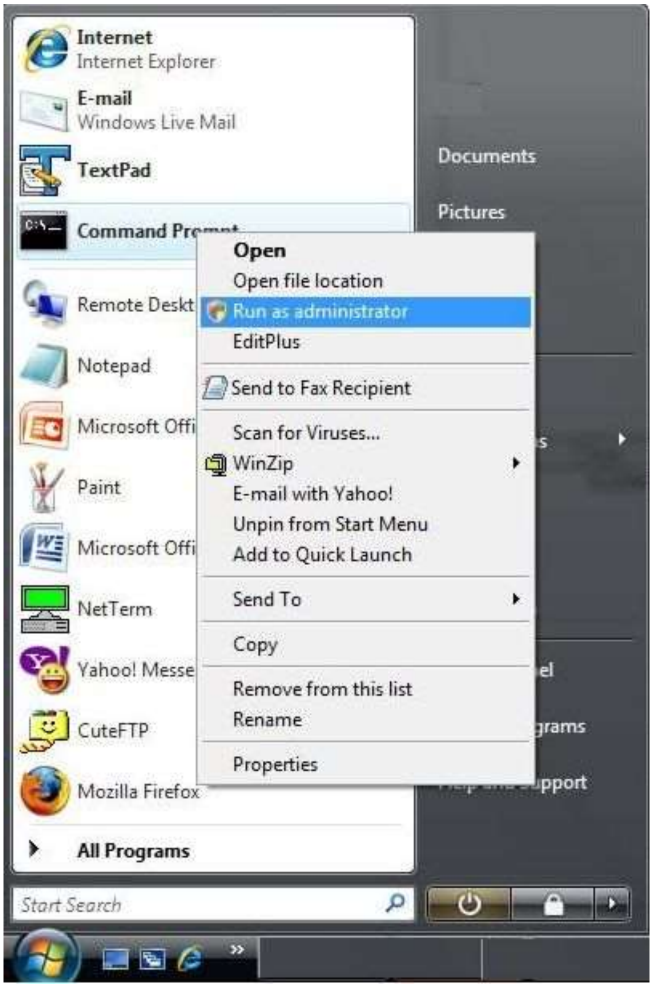


Figure 3.222: Stopping the eG agent on Windows Vista

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 3.223.

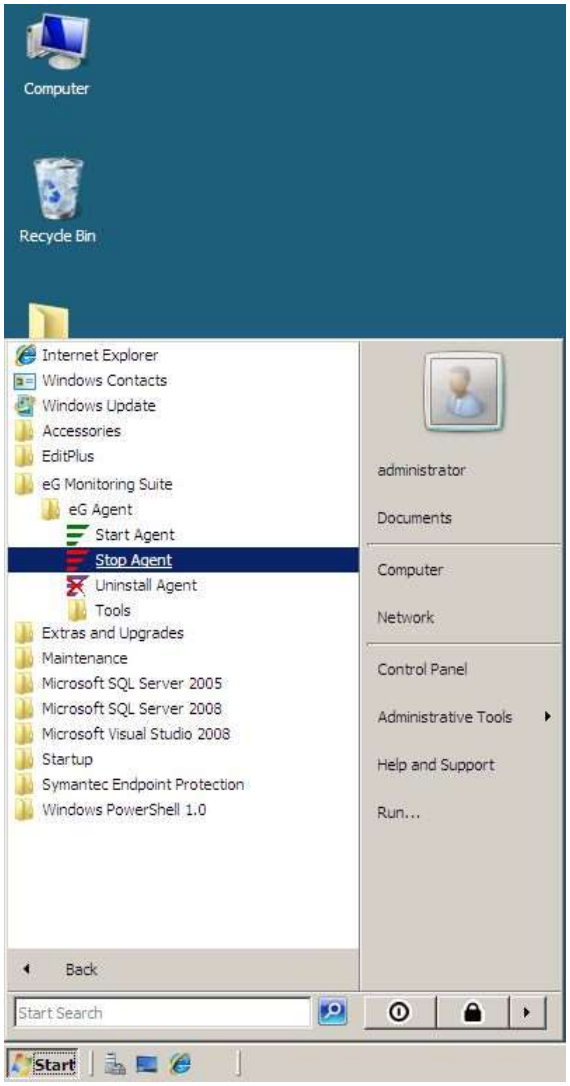
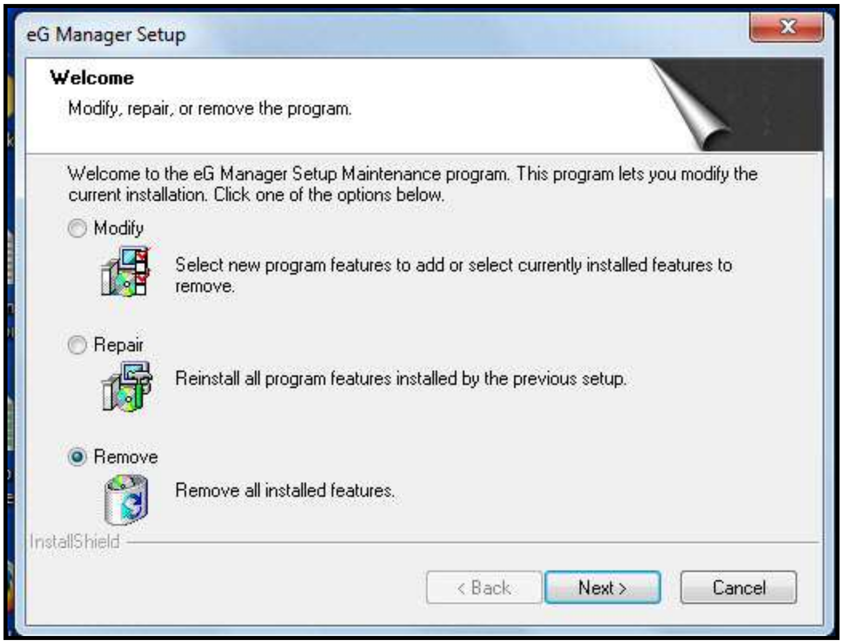


Figure 3.223: Stopping an eG agent on Windows 2008

3.26 Uninstalling the eG Manager

1. It is essential to stop the manager 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 3.224 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

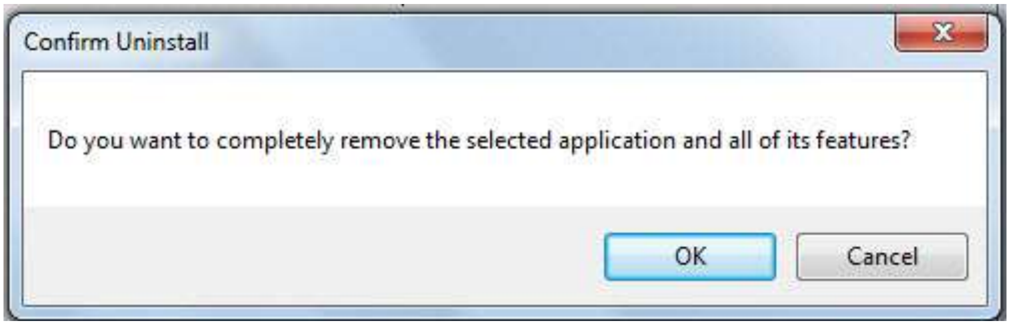
Reinstall all program features installed by the previous setup.

● Remove

Remove all installed features.

Figure 3.224: Uninstalling the eG manager

3. This process requires the confirmation of the user to remove the package and its related components as in Figure 3.225. Click the **OK** button.



Confirm Uninstall

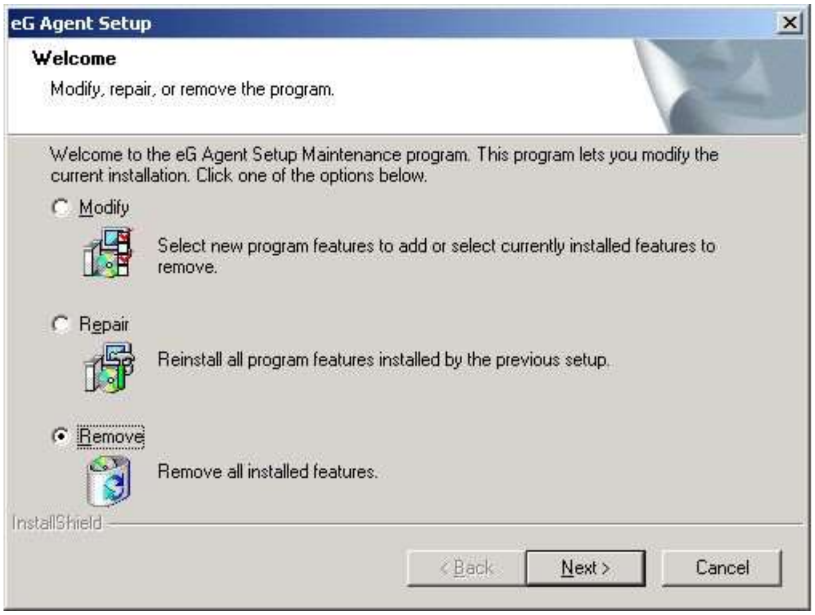
Do you want to completely remove the selected application and all of its features?

Figure 3.225: Uninstall process seeking the confirmation of the user to delete the eG manager

3.27 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 3.226 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

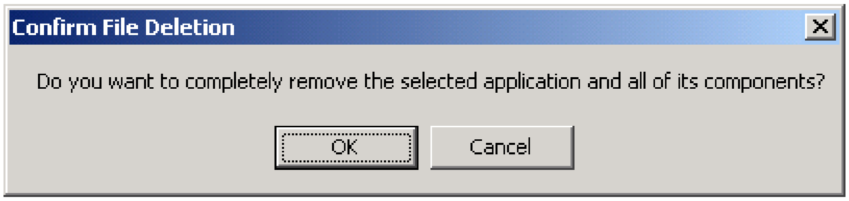
Reinstall all program features installed by the previous setup.

● Remove

Remove all installed features.

Figure 3.226: Uninstalling the eG agent

3. This process requires the confirmation of the user to remove the package and its related components as in Figure 3.227. Click the **OK** button.



Confirm File Deletion

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

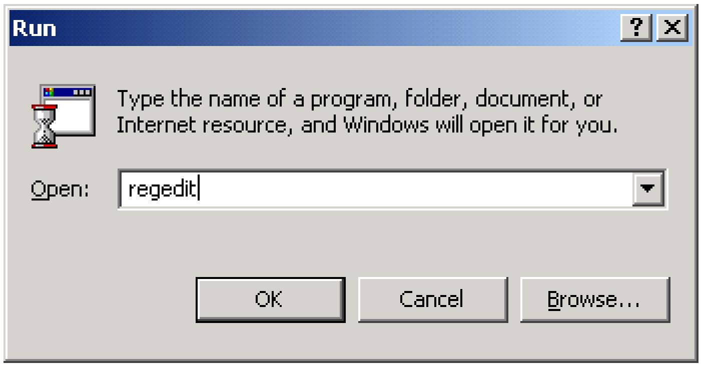
Figure 3.227: Uninstall process seeking the confirmation of the user to delete the eG agent

3.28 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 3.228).

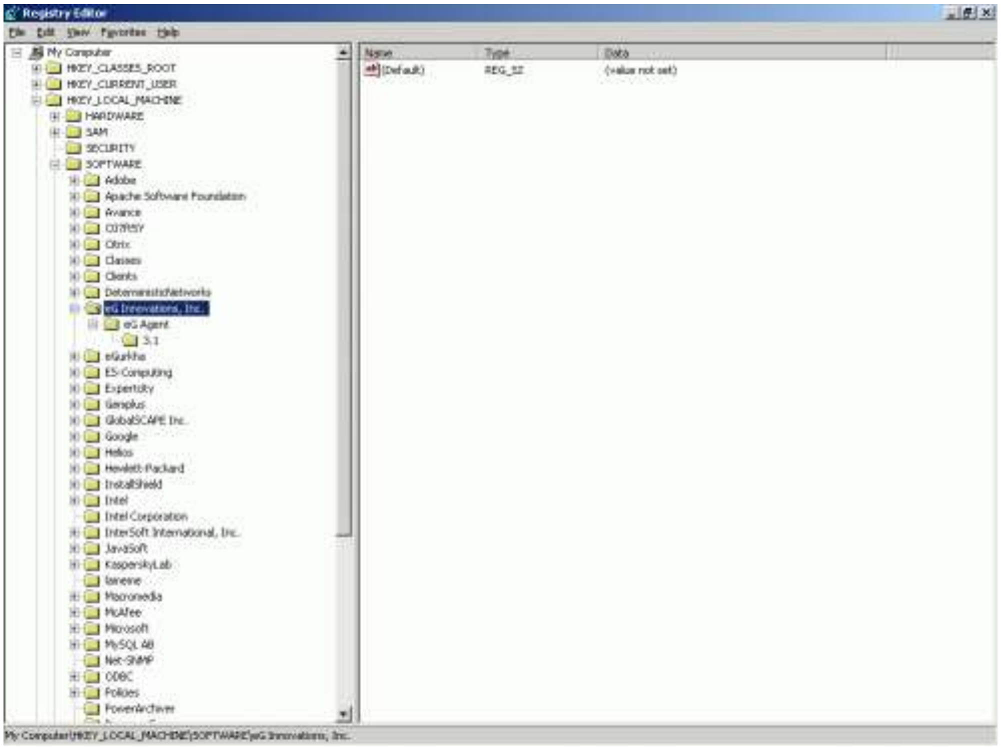


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

Figure 3.228: Opening the Windows registry

3. In the **Registry Editor** (see Figure 3.228) that opens, look for the **eG Innovations, Inc.** entry in the **My Computer\HKEY_LOCAL_MACHINE\SOFTWARE** node sequence (see Figure 3.229).

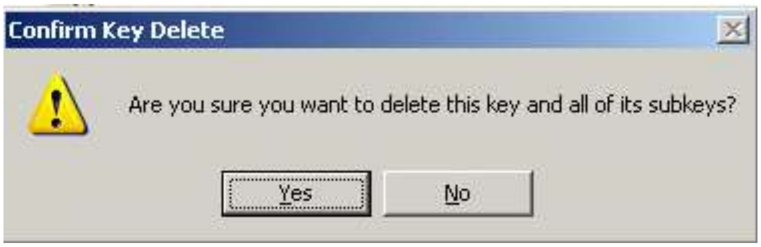


Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\eG Innovations, Inc.

Figure 3.229: Selecting the eG Innovations, Inc. entry

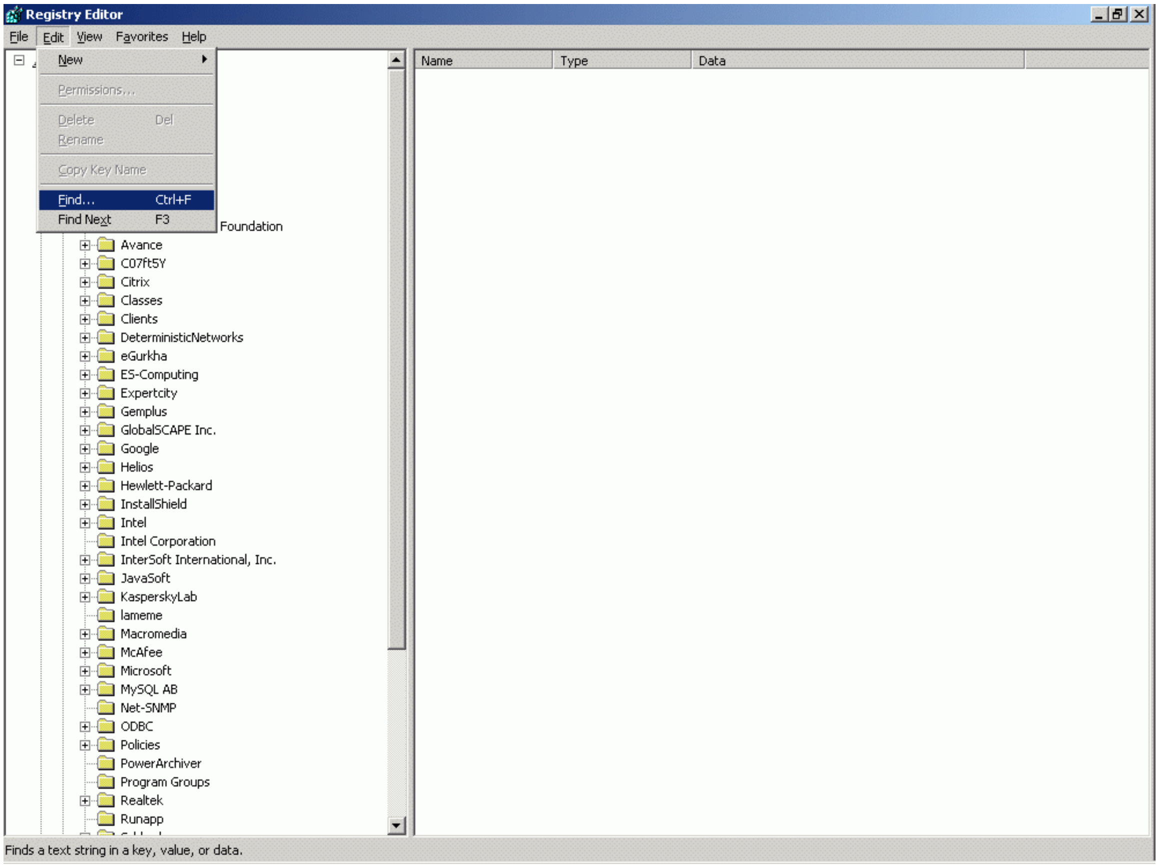
4. Delete the selected entry by pressing the **Delete** key on the keyboard, and confirm deletion by clicking the **OK** button in Figure 3.230 that appears.



Are you sure you want to delete this key and all of its subkeys?

Figure 3.230: Confirming deletion of the selected key

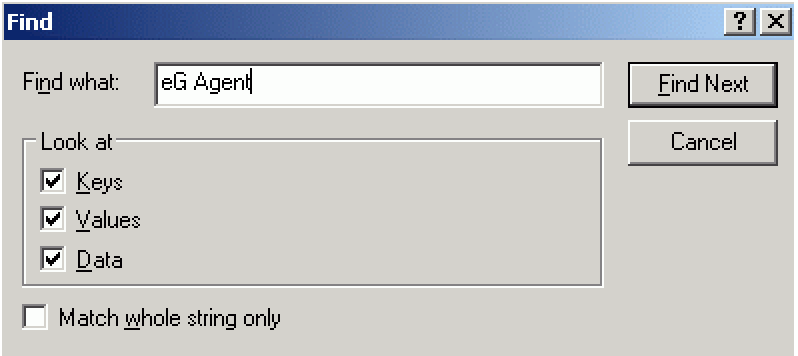
5. Then, place the cursor on the **My Computer** key at the top of the registry tree (see Figure 3.229) and then proceed to choose the **Find** option from the **Edit** menu (see Figure 3.231).



Finds a text string in a key, value, or data.

Figure 3.231: Selecting the Find option

6. When the **Find** dialog box appears (see Figure 3.232), specify **eG Agent** as the string to search for.



Find what: eG Agent

Look at

☑ Keys

☑ Values

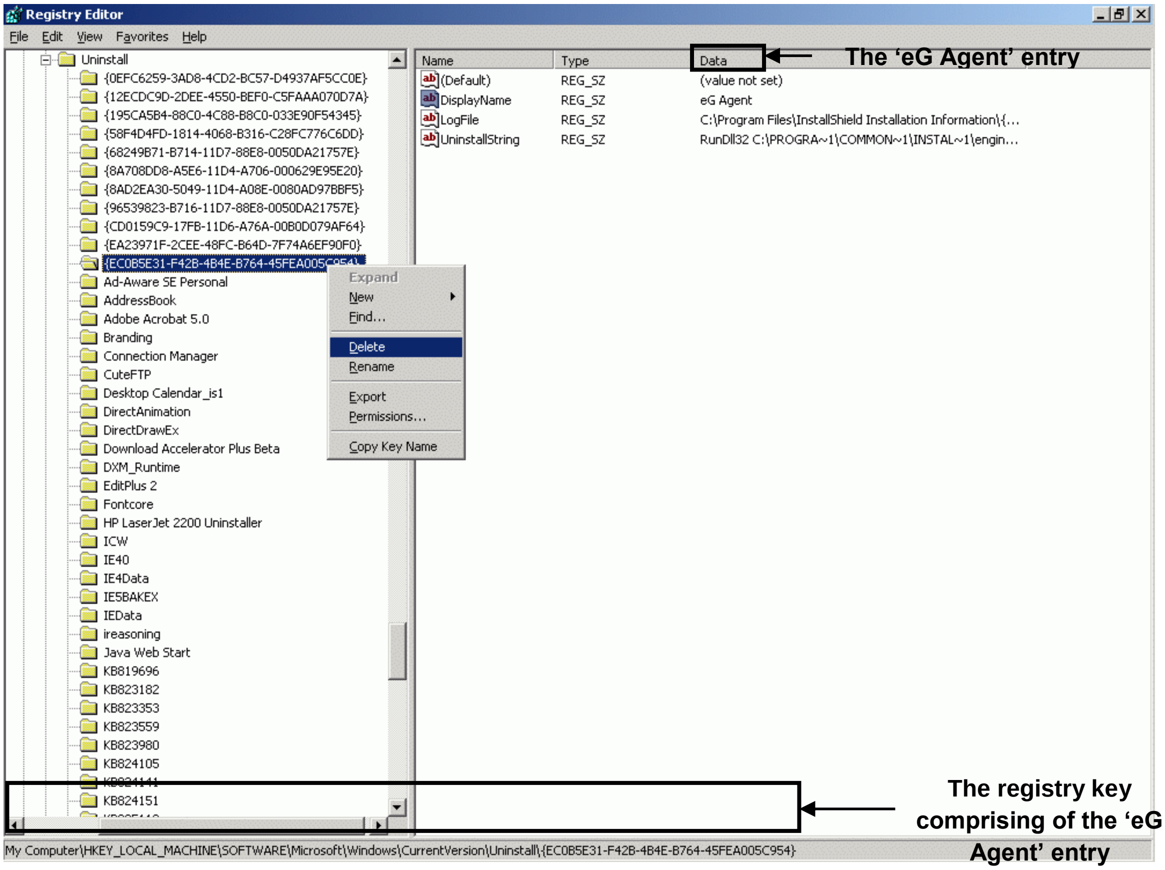
☑ Data

□ Match whole string only

Figure 3.232: Finding the string ‘eG Agent’

7. Then, click the **Find Next** button in Figure 3.232 to trigger the search.

8. Continue searching until the **eG Agent** entry present under the key indicated by Figure 3.233 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}

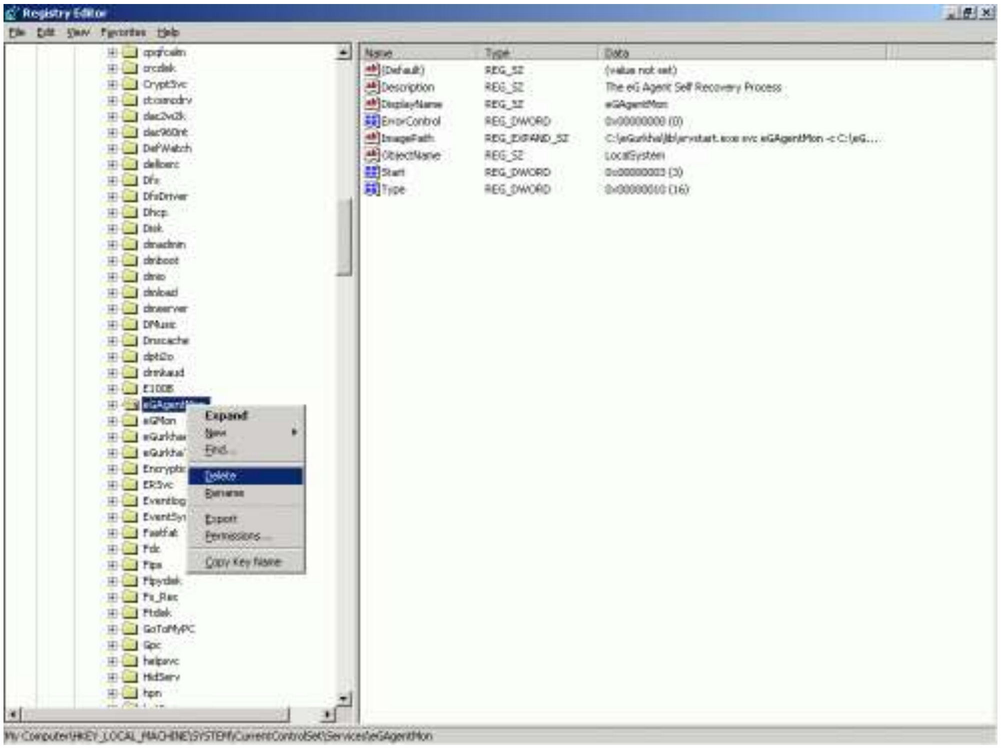
The ‘eG Agent’ entry

The registry key comprising of the ‘eG Agent’ entry

Figure 3.233: 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 3.233, right-clicking on it, and choosing the **Delete** option from the shortcut menu that appears (see Figure 3.233). 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 3.234).

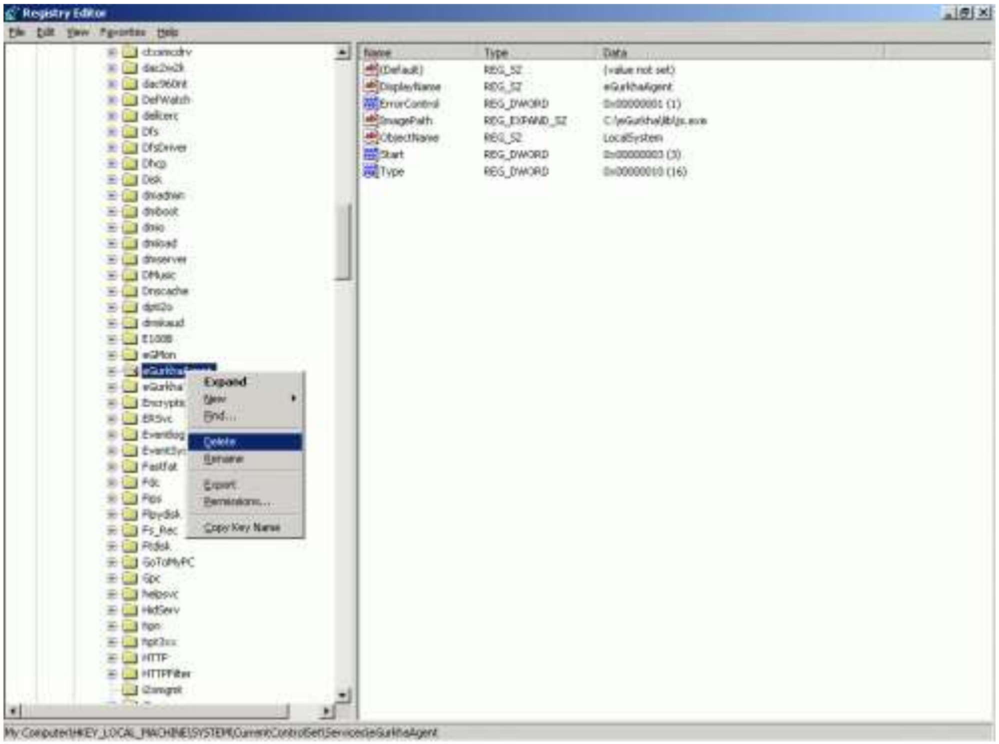


Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	The eG Agent Self Recovery Process
DisplayName	REG_SZ	eGAgentMon
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	C:\eGurkha\lib\srvstart.exe svc eGAgentMon -c C:\eG...
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eGAgentMon

Figure 3.234: Deleting the eGAgentMon key

11. Similarly, delete the **My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\eGurkhaAgent** key (see Figure 3.235).



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 3.235: Deleting the eGurkhaAgent key

12. Likewise, delete the **My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\eGurkhaAgent** 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 3.236).

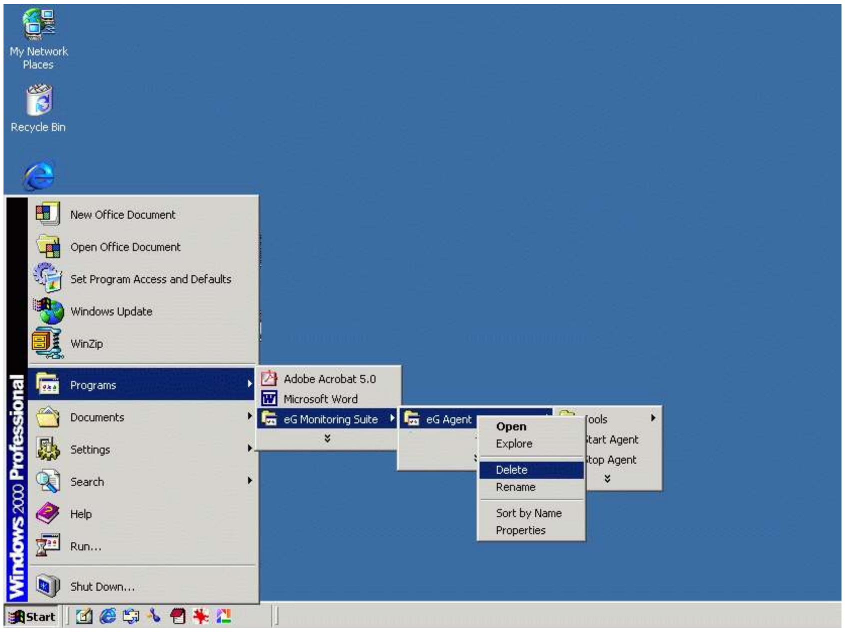


Figure 3.236: Deleting the eG Agent start menu options

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.

3.29 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>.**

4

Configuring Double-byte Support for eG Enterprise

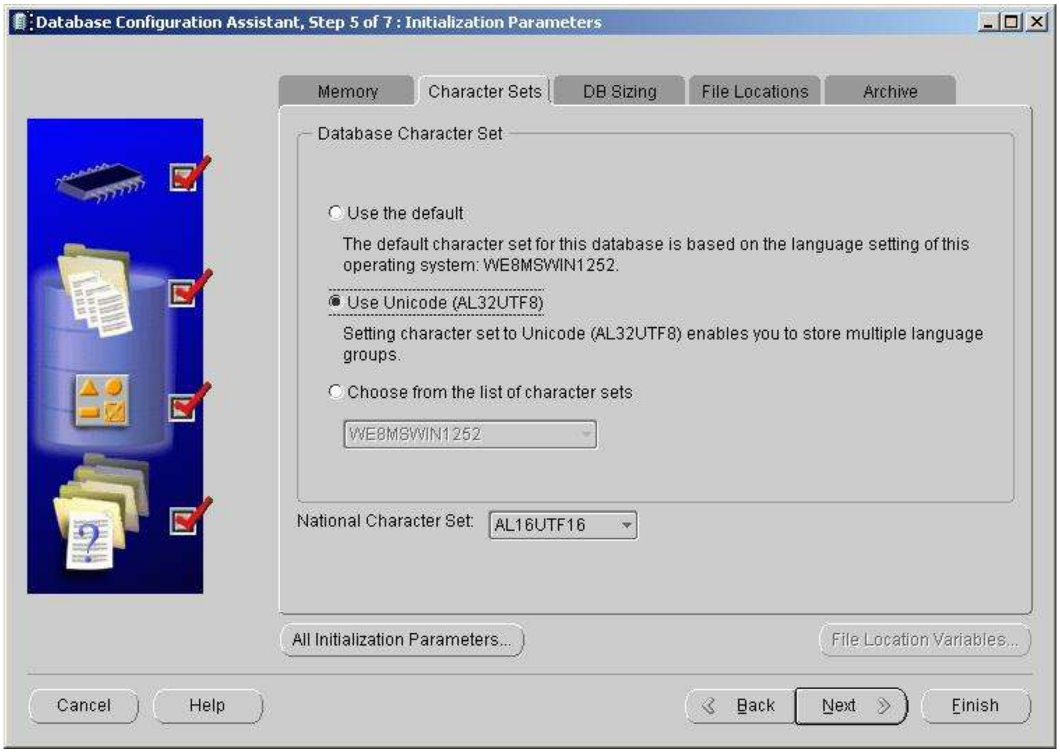
eG Enterprise embeds the ability to store and display data in any language that the user wants. Each user connecting to an eG manager can thus view data in a language that he/she prefers.

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

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

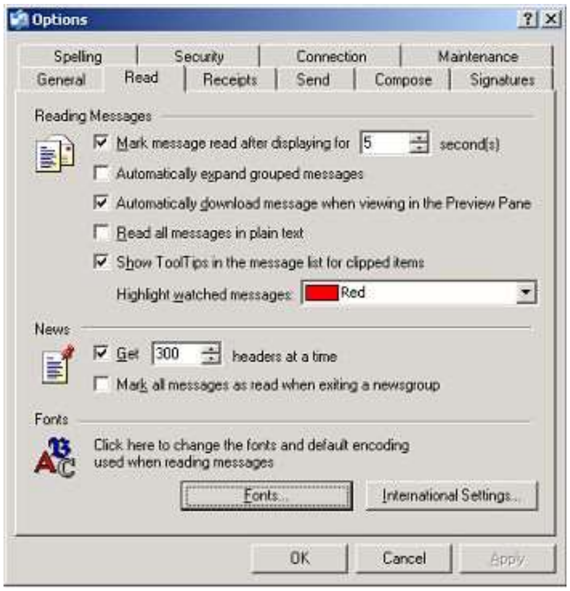
WE8MSWIN1252

National Character Set: AL16UTF16

Figure 4.1: 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.



Options

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

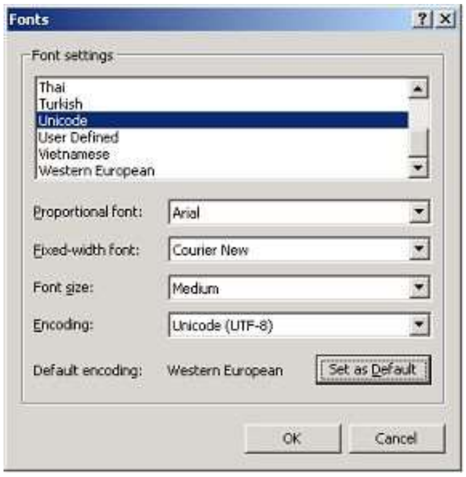
□ Mark all messages as read when exiting a newsgroup

Fonts

Click here to change the fonts and default encoding used when reading messages

Figure 4.2: 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.



Fonts

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 4.3: 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.

5

Backing up and Restoring eG Enterprise

This chapter outlines the procedures involved in backing up and restoring eG Enterprise on Windows and Unix environments.

5.1 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.

5.2 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:
   - 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.
   - 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:
   - 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.
   - 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.

5.3 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.

5.4 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 5.1 and 5.2, depending upon the operating system of the eG manager.
- If the database alone is to be restored, then follow step 5.3 only
- If both have to be restored, then alone follow steps 5.1 through 5.3.
- Restart the system after this process before attempting to start the manager and/or the agent

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.

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).

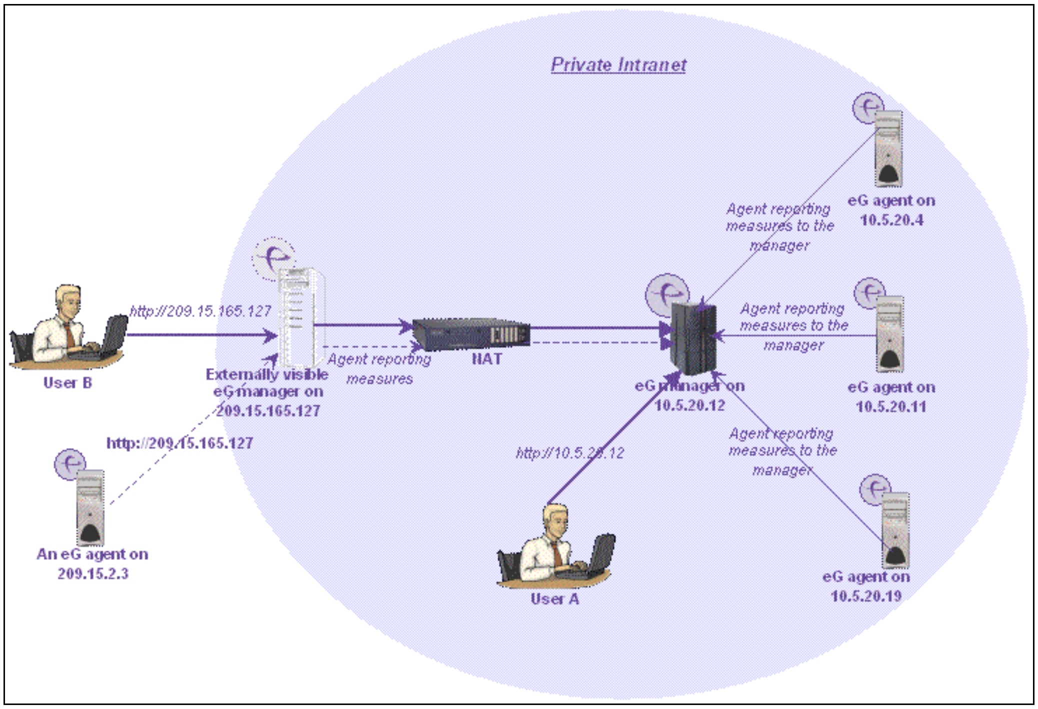


Figure 6.1: Manager behind a NAT

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 6.1represent 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).

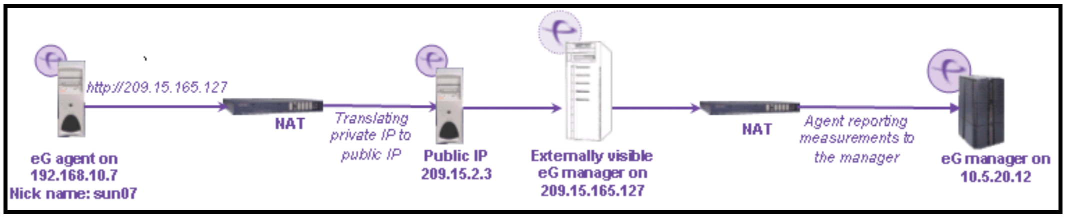

http://209.15.165.127
NAT
Translating private IP to public IP
Public IP 209.15.2.3
Externally visible eG manager on 209.15.165.127
NAT
Agent reporting measurements to the manager
eG agent on 192.168.10.7 Nick name: sun07
eG manager on 10.5.20.12

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).

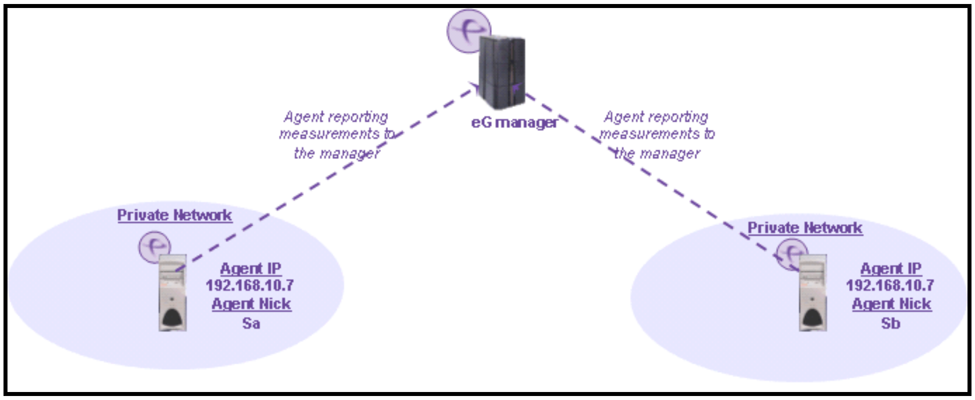


Figure 6.3: Managing agents in multiple private networks

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 futher, 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.

- 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.

7

Configuring the eG Manager to Send SMS Alerts

IT infrastructures that support mission-critical services need to be up and running 24x7. Timely, precise alerting by a monitoring solution can provide adequate notice for an IT manager to react immediately and to avert potential crisis situations.

The eG Enterprise Suite is capable of alerting users to issues anytime, anywhere! Besides providing users to the eG monitoring console with a list of open problems in the **CURRENT ALARMS** window, the eG Enterprise system can also send out email alerts of issues to configured mailboxes, and SMS alerts to configured mobile phones/pagers. To send SMS alerts, the eG manager can be configured to use any of the following mechanisms:

- **By configuring an SMTP mail server to send SMS alerts to specified mail numbers** - The eG manager will be able to send SMS via any SMTP mail server in the target environment. Administrators can even use the same mail server that has been configured for sending email alerts, for this purpose.
- **By integrating the eG manager with NowSMS Lite** - The NowSMS Lite is a software gateway that allows sending of SMS messages using a GSM (GRPS/EDGE/3G) modem. The eG manager can integrate with the NowSMS Lite software so that, eG alarms can be forwarded as SMS alerts to configured mobile phones. This way, operators only see alerts relating to networks, servers, applications, and services under their purview. Employing a patented automatic triage technology, the eG manager prioritizes alerts - so the root-cause of problems are differentiated from the effects - and forwards them instantly to the NowSMS server for delivery to users' mobile phones.
- **By integrating the eG manager with the eG SMS Manager component** - The eG SMS manager is a key component of eG Enterprise, which when integrated with the eG manager, generates personalized alerts to the mobile phones of IT operations staff.
- **By integrating the eG manager with Air2Web** - Air2Web offers a Content Gateway platform using which SMS/MMS/WebPush messages can be sent to any mobile phone anywhere in the world. In environments where this gateway is configured in-house, and in environments that subscribe to the Air2Web's gateway services, the eG manager can be integrated with the gateway service, so that SMS alerts can be instantly sent to mobile phones without modems, SMS subscriptions, or components like the eG SMS manager.
- **By integrating the eG manager with PageGate** - PageGate software allows for network paging or network wide alphanumeric paging and text messaging from any combination of the following modules: web, email, commandline/ascii, serial, TAP-in and (GUI) windows workstations. The eG manager can be integrated with PageGate, so that the alarms generated by the eG manager are sent as SMS' to pagers via PageGate.

The sections to come discuss both these options in great detail.

7.1 Configuring an SMTP Mail Server to Send SMS Alerts

The key pre-requisite for this is to use an SMTP mail server that is capable of sending SMS messages to mobile phones. You can even use the mail server configured for email alerting for this purpose.

Once you have such a mail server, then do the following to configure that mail server to send SMS alerts:

1. Login to the eG manager host.
2. Edit the **eg_services.ini** file in the **<EG_INSTALL_DIR>\manager\config** directory (on Windows; on Unix, this will be the **/opt/egurkha/manager/config** directory).
3. Look for the **[SMTP_SMS_ALERTS]** section in the file. This section will contain the following entries by default.

```
SMTP_SMS_ALERTS]
SendSMSAlertsOverSMTP=false
mail.smtp.host=smtp.myserver.com
mail.smtp.port=25
mail.smtp.auth=false
mail.smtp.starttls.enable=false
mail.smtp.auth.username=john
mail.smtp.auth.password=password
from.email=sender@myserver.com
to.email=$mobilenumber@myserver.com
```

4. To enable SMS alerting over SMTP, first set the **SendSMSAlertsOverSMTP** flag to **true**.
5. Then, against the **mail.smtp.host** parameter, enter the fully qualified host name of the SMTP mail server that you want to use for sending the SMS alerts.
6. Next, enter the port at which this mail server listens against **mail.smtp.port**.
7. If your mail server requires authentication, then set the **mail.smtp.auth** flag to **true**. If this is done, then provide a valid user name and password to authenticate against **mail.smtp.auth.username** and **mail.smtp.auth.password** parameters, respectively.
8. When the eG manager generates an alarm, then the corresponding alarm information will be sent as an email from the **from.email** that you specify. This email alert will be received by the **to.email** that you configure. The format of the **to** email ID should be: **$mobilenumber@<domainname>**. For instance, your specification can be **$mobilenumber@abc.com**.

   $mobilenumber is a variable name, and should not be changed. At runtime, this variable will be replaced by the mobile numbers that you configure in the eG administrative interface for SMS alerting.
9. Finally, save the file.

The next time the eG manager detects a problem condition, the manager sends the details of that problem as an email alert to each of the email IDs that correspond to the mobile numbers that you have configured in the eG administrative interface. Upon receipt of an email, the **to** email ID then converts that email into an SMS and routes it to the corresponding mobile number.

7.2 Integrating the eG Manager with NowSMS Lite

The NowSMS Lite is a software gateway that allows sending of SMS messages using a GSM (GRPS/EDGE/3G) modem. It allows clients to submit SMS messages for delivery via the GSM modem, using HTTP interface that supports HTTP GET meth

You can integrate the eG manager with NowSMS Lite so that:

- the alerts generated by the eG manager are automatically converted into SMS format and forwarded to the NowSMS server through a HTTP interface;
- the SMS alerts received by the NowSMS server are then delivered to configured mobile phones using a GSM modem connected via serial port or USB.

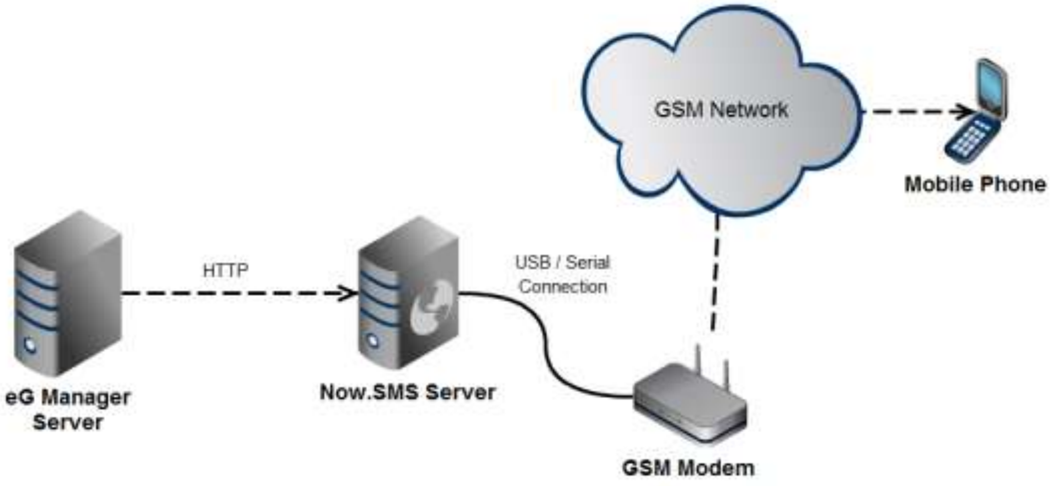


Figure 7.1: How the eG manager - NowSMS Lite integration works

7.2.1 Pre-requisites for Integrating eG Manager with NowSMS Lite

The following pre-requisites should be fulfilled before attempting to integrate the eG manager with NowSMS Lite:

- ○ Make sure that a licensed NowSMS Lite software, purchased from NowMobile.com Limited, is installed and fully operational in the target environment;
- ○ The server/desktop hosting NowSMS Lite should fulfill the following requirements:
  - ○ Should support a USB device driver for the GSM modem (if the modem is USB based). The driver must be explicitly obtained from the modem vendor and installed.
  - ○ Should support a serial port device driver (if the modem is serial port based). This driver will be typically installed and available in Windows OS by default.
  - ○ The environment should comprise of a GSM Modem that supports an "extended AT command set" for sending/receiving SMS messages, as defined in the ETSI GSM 07.05 and and 3GPP TS 27.005 specifications; the recommended GSM modems for this integration are:
    - ○ Wavecom Fastrack M1306B
    - ○ Sierra Wireless – AirLink Fasttrack Xtend

- The other requirements pertaining to GSM modems include:
    - A GSM modem can be a dedicated modem device with a serial or USB connection.
    - The GSM modem has to be placed in a location where the signal strength is good. Measure the signal strength by connecting to the modem using HyperTerminal utility available in Windows and issue the below command:

      AT+CSQ

      The output format of the command will be in the below format:

      +CSQ <rssi>,<ber>

      In the output, <rssi> represents the received signal strength indicator and <ber> denotes the channel bit error rate.

      While the **<rss>** value of 15 and above indicates strong signal strength, a value below 10 will not guarantee SMS delivery.

      The output **+CSQ 99,99** indicates the modem is not registered with the mobile network.

      Note

      The Windows 2008 server does not come with the Hyperterminal utility. The utility can be copied from any of the existing Windows 2003 servers and executed on the Windows 2008 server. Files related to this utility are **hpertrm.exe** and **hypertrm.dll**.

- Mobile SIM card with valid subscription for outgoing SMS;
- The eG license should enable the **SMS Alerting** capability.

7.2.2 Verifying the Proper Setup of the NowSMS Lite Software

Once the NowSMS Lite is installed and setup, check whether SMS can be sent using its web interface. For this purpose, open the browser from the eG manager host, and launch the following URL:

http://<NowSmsServer>:<NowSmsPort>/?PhoneNumber=<MobileNumberforReceivingSMSAlerts>&Text=<TestMessage>

A sample URL will be:

http://192.168.1.25:8800/?PhoneNumber=9840098011&Text=eGAlarms

If the **PhoneNumber** configured in the URL receives the SMS alert with the configured **Text**, it is a clear indicator that the web interface of the NowSMS Lite software is functioning without a glitch.

7.2.3 Configuring the eG Manager to Work with NowSMS Lite

Once the NowSMS lite is setup, eG manager can be configured to send out SMS alerts using the web interface of NowSMS lite.

To achieve this, do the following:

1. Edit the **eg_services.ini** file in the **<EG MANAGER INSTALL>\manager\config** directory.
2. Define a URL against the **NowSmsUrl** parameter in the **[SMS_SERVER]** section of the file in the format shown below.

   NowSmsUrl=http://<NowSmsServer>:<NowSmsPort>/?PhoneNumber=&Text=

   A sample configuration is shown below:-

   [SMS_SETTINGS]

   NowSmsUrl=http://192.168.1.25:8800/?PhoneNumber=&Text=
3. Once the **NowSmsUrl** is set, save the file.

7.3 Integrating the eG Manager with the eG SMS Manager

7.3.1 Architecture of the eG SMS Manager

As and when problems occur in the environment, the eG manager generates alarms to monitor users. If a monitor user has been configured to receive the alarm information via SMS, then the eG manager forwards the alarms to the eG SMS manager. The eG SMS manager then transmits the alarm information to the monitor user’s mobile phone, using a GSM (Global System for Mobile communication) 7.07 compliant modem. Figure 7.2 depicts how the eG SMS manager works.

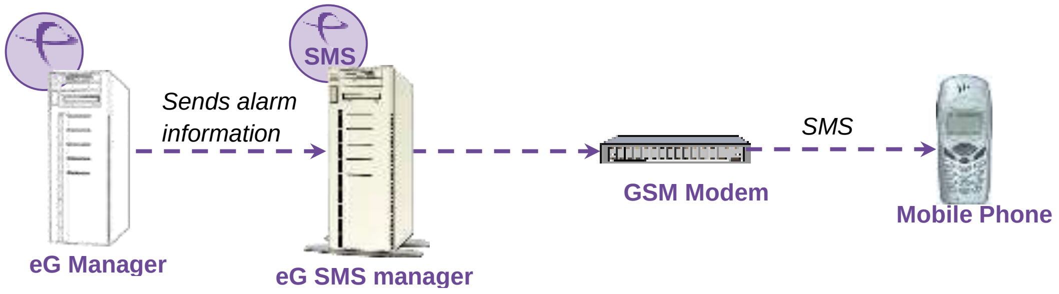


Figure 7.2: How the eG SMS Manager works

7.3.2 Installing the eG SMS manager

This section outlines the prerequisites and the prcedure for installing the eG SMS manager.

7.3.2.1 Installation Prerequisites

Software Prerequisites

Windows 2000 Professional (or) Windows 2003 server (or) Windows XP Professional, with a serial port interface

Hardware Prerequisites

128 MB RAM

A GSM 7.07 compliant modem

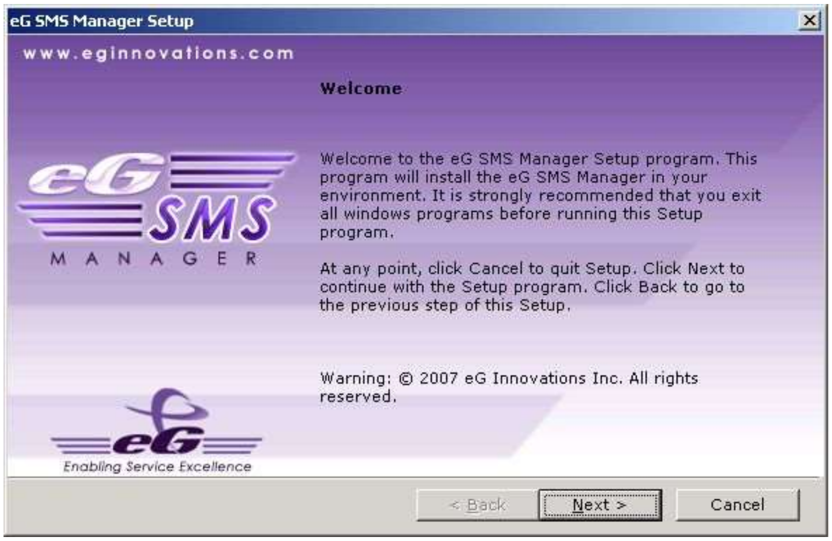
Others

Subscription to a mobile phone operator's SMS service

7.3.2.2 Installation Procedure

To install the eG SMS manager, do the following:

1. Insert the eG product CD into your CD drive.
2. Double-click on the **eGSMSMgr.exe** file in the CD drive to initiate the installation process.
3. When setup commences, the **Welcome** screen will appear (see Figure 7.3). Click on the **Next >** button here to continue.



Welcome

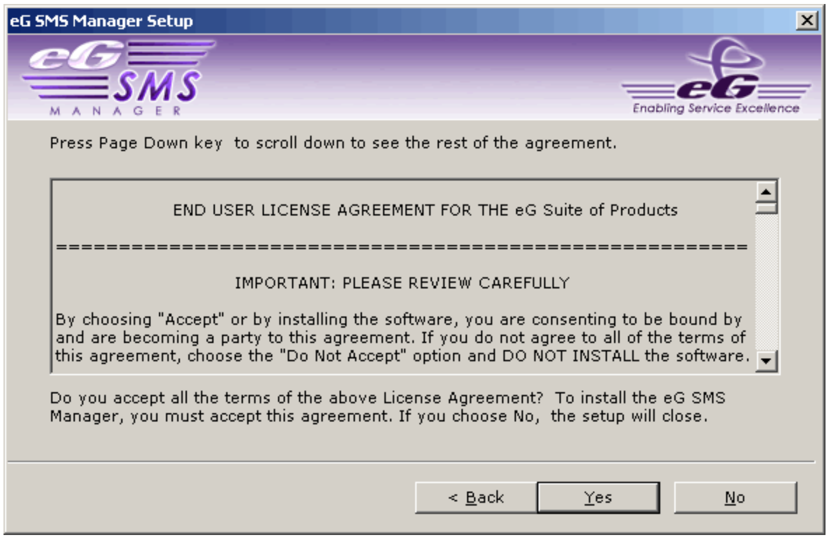
Welcome to the eG SMS Manager Setup program. This program will install the eG SMS Manager in your environment. It is strongly recommended that you exit all windows programs before running this Setup program.

At any point, click Cancel to quit Setup. Click Next to continue with the Setup program. Click Back to go to the previous step of this Setup.

Warning: © 2007 eG Innovations Inc. All rights reserved.

Figure 7.3: The Welcome screen of the eG SMS manager setup

4. Next, the eG SMS manager's license agreement appears (see Figure 7.4). Click on the **Yes** button to accept the agreement or **No** to exit the setup.



Press Page Down key to scroll down to see the rest of the agreement.

END USER LICENSE AGREEMENT FOR THE eG Suite of Products

===

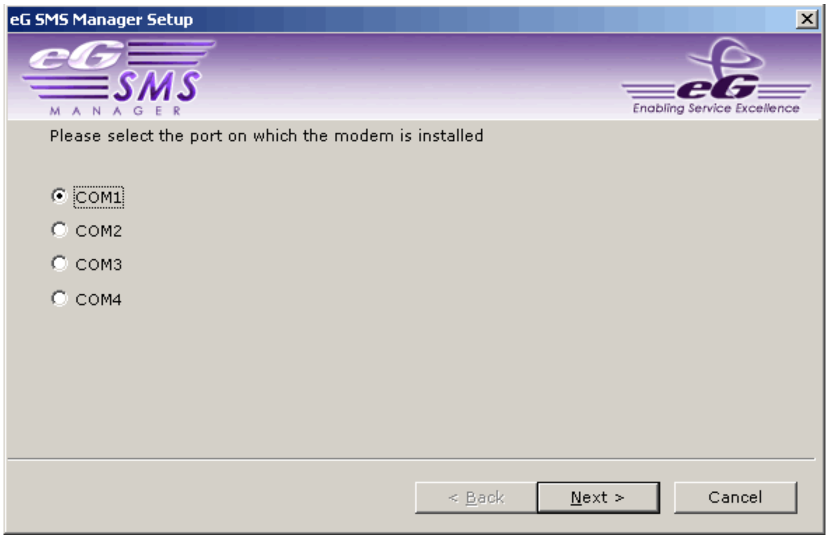
IMPORTANT: PLEASE REVIEW CAREFULLY

By choosing "Accept" or by installing the software, you are consenting to be bound by and are becoming a party to this agreement. If you do not agree to all of the terms of this agreement, choose the "Do Not Accept" option and DO NOT INSTALL the software.

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

Figure 7.4: Accepting the license agreement

5. Upon accepting the license agreement, you will be required to select the port on which the GSM modem has been installed (see Figure 7.5). Then, click the **Next >** button to proceed with the setup.

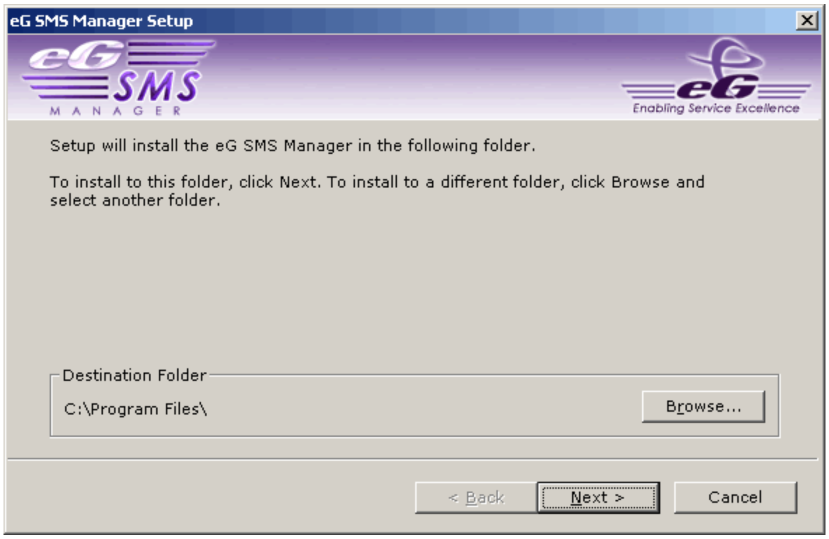


Please select the port on which the modem is installed

● COM1
○ COM2
○ COM3
○ COM4

Figure 7.5: Selecting the port on which the GSM modem has been installed

6. Next, you will be required to specify the path to the directory in which the eG SMS manager is to be installed (see Figure 7.6). Then, click on the **Next >** button to continue.



eG SMS Manager Setup

Setup will install the eG SMS Manager in the following folder.

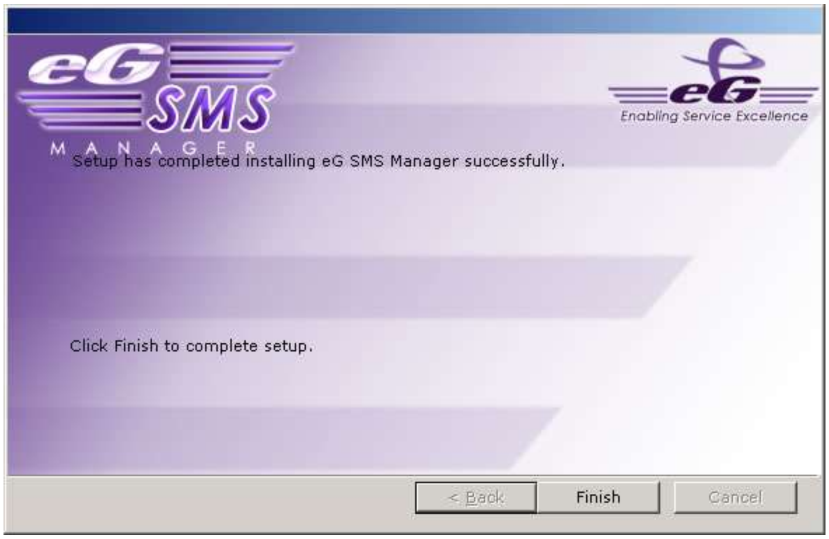
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\

Figure 7.6: Specifying the installation directory of the eG SMS manager

7. Upon completion of the installation, click on the **Finish** button in Figure 7.7 to quit the setup.



Setup has completed installing eG SMS Manager successfully.

Click Finish to complete setup.

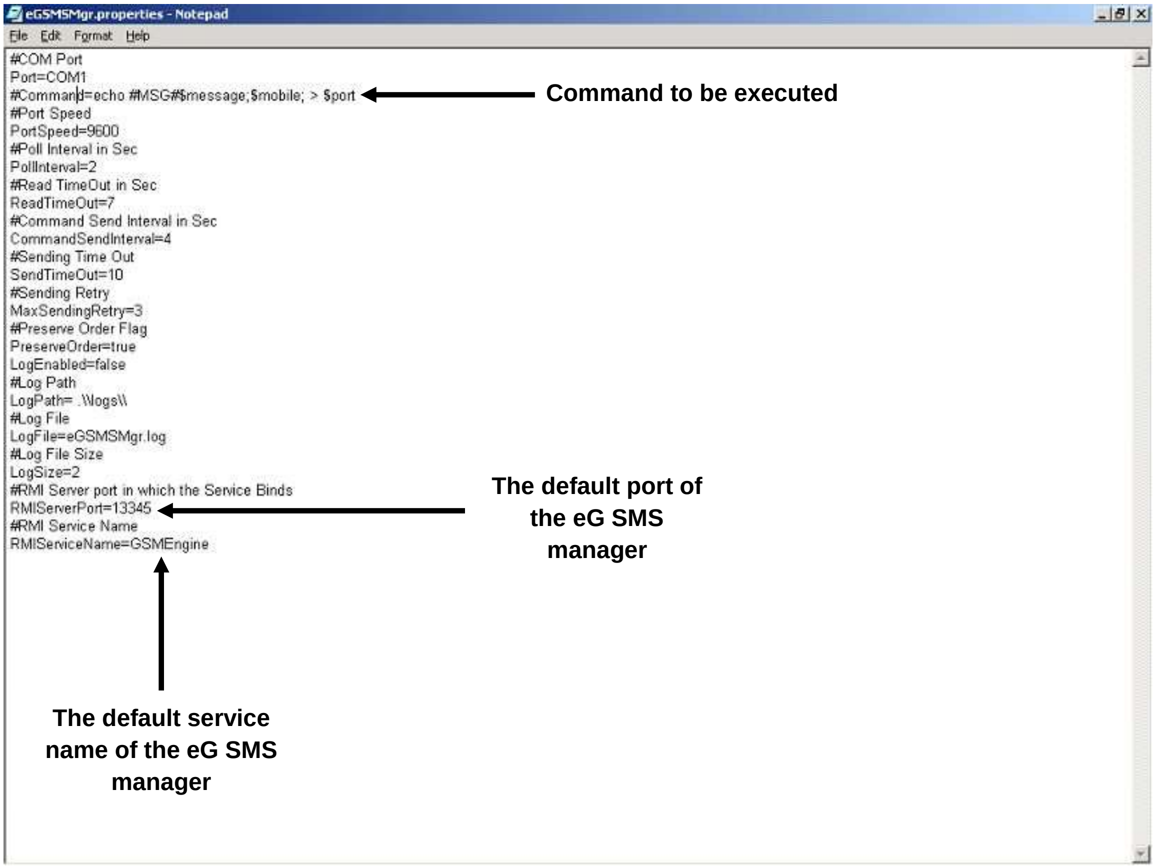
Figure 7.7: Completion of the installation

7.3.3 Configuring the eG Manager to work with the eG SMS manager

Once the eG SMS manager is installed, you need to configure the eG manager to interact smoothly with the eG SMS manager. This configuration will ensure that the eG manager promptly forwards the alarms it generates to the eG SMS manager.

To configure the eG manager, do the following:

1. Open the **eGSMSMgr.properties** file (using Notepad) from the install directory of the eG SMS manager (see Figure 7.8).


eGSMSMgr.properties - Notepad
File Edit Format Help
Command to be executed
The default port of the eG SMS manager
The default service name of the eG SMS manager

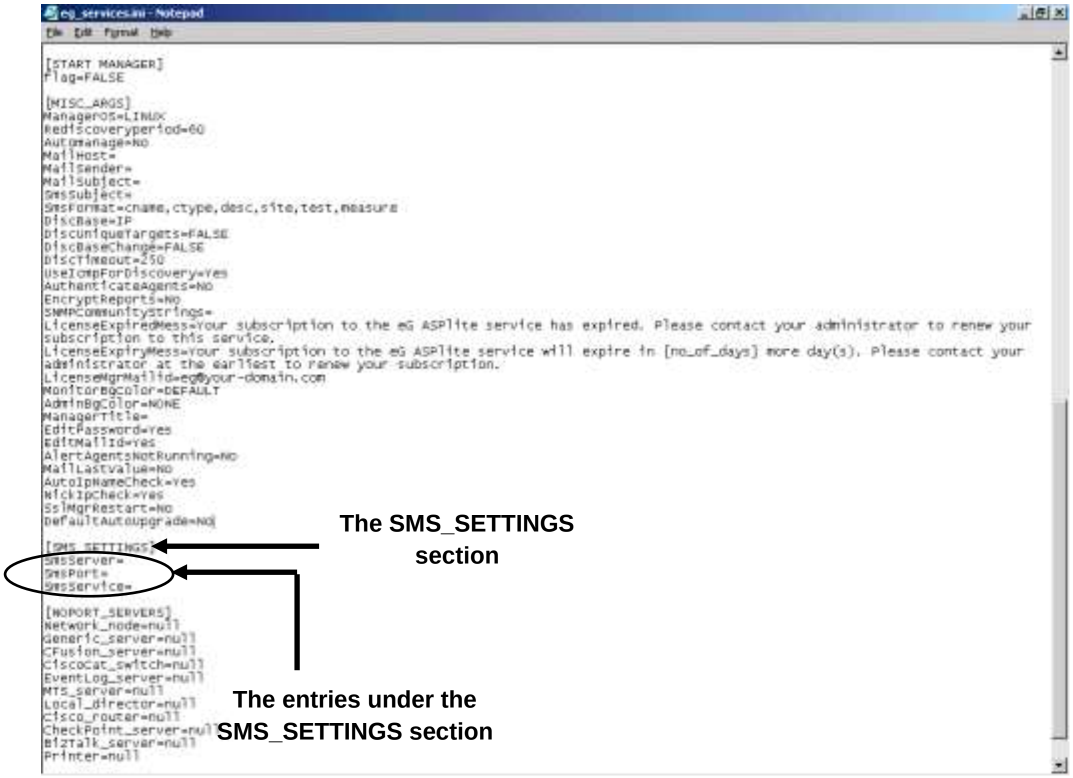
```
#COM Port
Port=COM1
#Command=echo #MSG#$message;$mobile; > $port
#Port Speed
PortSpeed=9600
#Poll Interval in Sec
PollInterval=2
#Read TimeOut in Sec
ReadTimeOut=7
#Command Send Interval in Sec
CommandSendInterval=4
#Sending Time Out
SendTimeOut=10
#Sending Retry
MaxSendingRetry=3
#Preserve Order Flag
PreserveOrder=true
LogEnabled=false
#Log Path
LogPath= .\\logs\\
#Log File
LogFile=eGSMSMgr.log
#Log File Size
LogSize=2
#RMI Server port in which the Service Binds
RMIServerPort=13345
#RMI Service Name
RMIServiceName=GSMEngine
```

Figure 7.8: The contents of the eGSMSMgr.properties file

2. As indicated by Figure 7.8, note that the **egSMSMgr.properties** file consists of the default **RMIServerPort** and the **RMIServiceName** values. These values can be changed, if required.

3. Also, note that a **Command** parameter exists in the **eGSMSMgr.properties** file of Figure 7.8. In some environments, GSM modems may support a command line interface through which SMS messages can be sent. The eG SMS manager can be configured to use the command line interface using the **Command** specification in the **eGSMSMgr.properties** file of Figure 7.8. By default, the **Command** specification is disabled in the **eGSMSMgr.properties** file. A sample command specification has been provided in this file for your benefit. In this example, the command is: *echo #MSG#$message;$mobile; > $port*. When the SMS message is sent by the eG SMS manager, it replaces *$message* with the actual message to be sent, *$mobile* represents the mobile number to which the SMS should be sent, and *$port* is the port number that should be used for sending the SMS message.

4. Now, open the **eg_services.ini** file in the **<EG_INSTALL_DIR>/manager/config** directory (see Figure 7.9).



```
[START MANAGER]
flag=FALSE

[MISC_ARGS]
ManagerOS=LINUX
Rediscoveryperiod=60
Automanage=No
MailHost=
MailSender=
MailSubject=
SmsSubject=
SmsFormat=cname,ctype,desc,site,test,measure
DiscBase=IP
DiscUniqueTargets=FALSE
DiscBaseChange=FALSE
DiscTimeout=250
UseIcmpForDiscovery=Yes
AuthenticateAgents=No
EncryptReports=No
SNMPCommunityStrings=
LicenseExpiredMess=Your subscription to the eG ASPlite service has expired. Please contact your administrator to renew your
subscription to this service.
LicenseExpiryMess=Your subscription to the eG ASPlite service will expire in [no_of_days] more day(s). Please contact your
administrator at the earliest to renew your subscription.
LicenseMgrMailId=eg@your-domain.com
MonitorBgColor=DEFAULT
AdminBgColor=NONE
ManagerTitle=
EditPassword=Yes
EditMailId=Yes
AlertAgentsNotRunning=No
MailLastValue=No
AutoIpNameCheck=Yes
NickIpCheck=Yes
SslMgrRestart=No
DefaultAutoUpgrade=No

[SMS_SETTINGS]
SmsServer=
SmsPort=
SmsService=

[NOPORT_SERVERS]
Network_node=null
Generic_server=null
CFusion_server=null
CiscoCat_switch=null
EventLog_server=null
MTS_server=null
Local_director=null
Cisco_router=null
CheckPoint_server=null
BizTalk_server=null
Printer=null
```

Figure 7.9: The contents of the eg_services.ini file

5. Figure 7.9 indicates that the following entries exist under the **SMS_SETTINGS** section of the **eg_services.ini** file:

```
SmsServer =
SmsPort =
SmsService =
```

To configure the eG manager to work with the eG SMS manager, valid values need to be provided for the above. Therefore, against **SmsServer**, enter the IP/hostname of the server hosting the eG SMS manager. Then, against the **SmsPort** entry in Figure 7.9, specify the **RMIServerPort** value available in the **eGMSMgr.properties** file of Figure 7.9. Similarly, against the **SmsService** entry, enter the **RMIServiceName** displayed in the **eGSMSMgr.properties** file of Figure 7.9.

Note

If for some reason you change the default port and service name settings in the **eGSMSMgr.properties** file, then ensure that the changes are reflected in the **eg_services.ini** file also.

6. Once this is done, save the **eg_services.ini** file.

That concludes the process of configuring the eG manager. Now, proceed to start the eG SMS manager.

7.3.4 Starting the eG SMS Manager

To start the eG SMS manager, follow the menu sequence: Start -> Programs -> eG Monitoring Suite -> eG SMS Manager -> Start SMS Manager (see Figure 7.10).

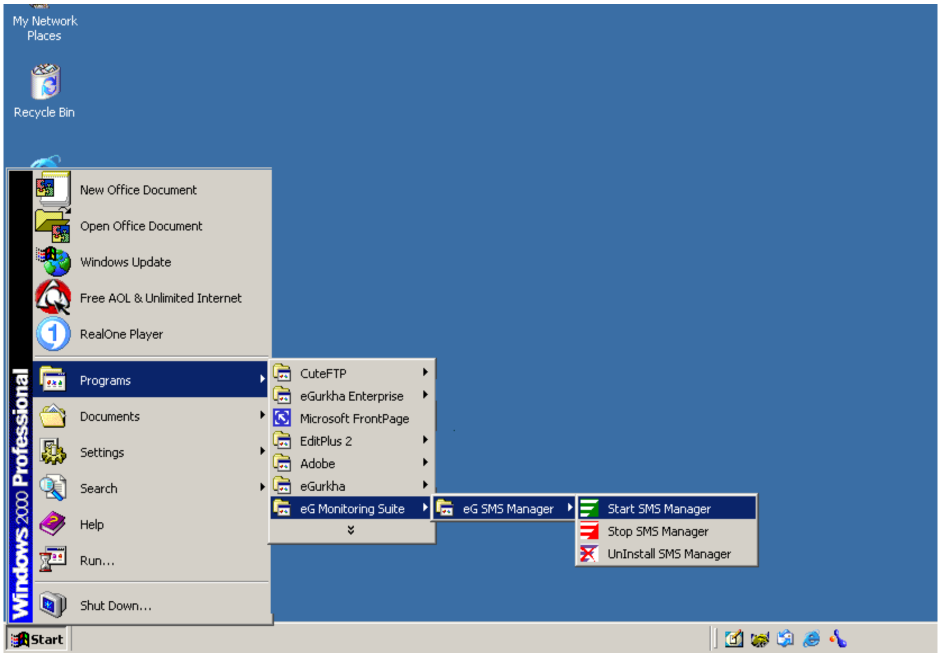
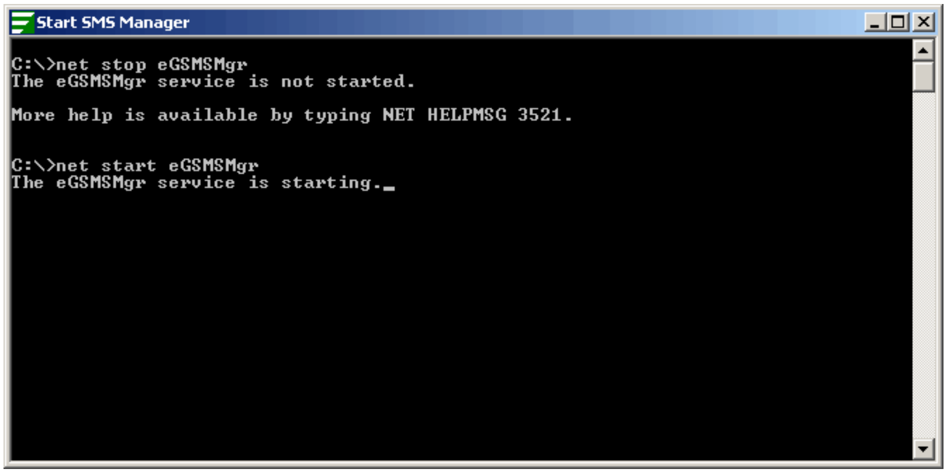


Figure 7.10: Starting the eG SMS Manager

If the manager successfully starts, then the following screen will then appear:



```
C:\>net stop eGSMSMgr
The eGSMSMgr service is not started.

More help is available by typing NET HELPMSG 3521.


C:\>net start eGSMSMgr
The eGSMSMgr service is starting._
```

Figure 7.11: A screen indicating that the eG SMS manager has successfully started

Now, whenever the eG manager generates alarms to a monitor user who has been configured to receive SMS alerts, then the eG manager will forward the alarms to the monitor user's mobile phone using SMS. For more details about configuring a monitor user, refer to the *eG User Manual*.

7.3.5 Uninstalling the eG SMS Manager

To uninstall the eG SMS manager, do the following:

1. Stop the eG SMS manager by following the menu sequence: Start -> Programs -> eG Monitoring Suite -> eG SMS Manager -> Stop SMS Manager (see Figure 7.12)

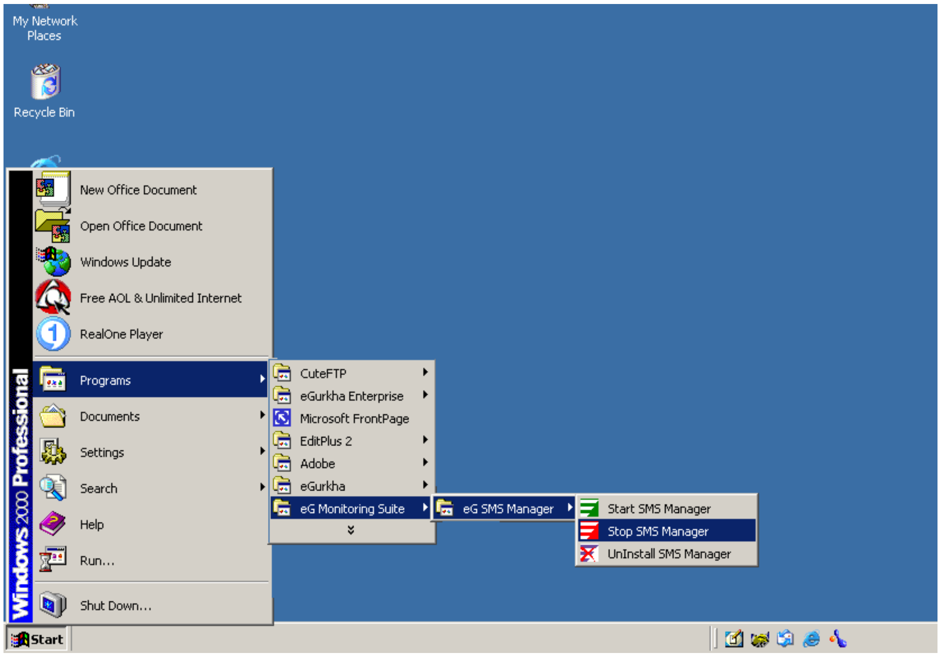


Figure 7.12: Stopping the SMS manager

2. Then, begin uninstalling the SMS manager, by following the menu sequence: Start -> Programs -> eG Monitoring Suite -> eG SMS Manager -> Uninstall SMS Manager (see Figure 7.13).

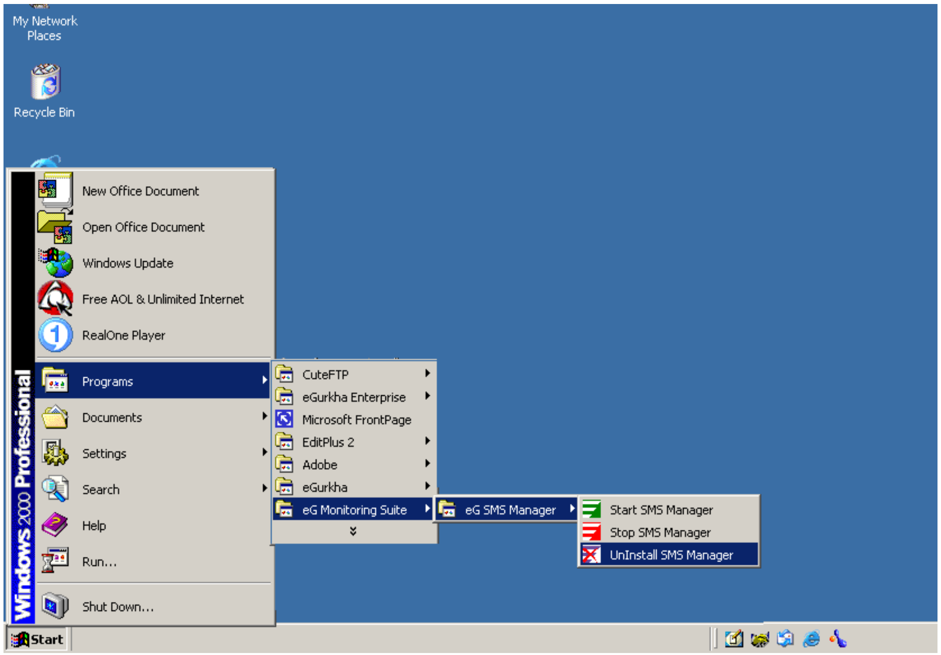
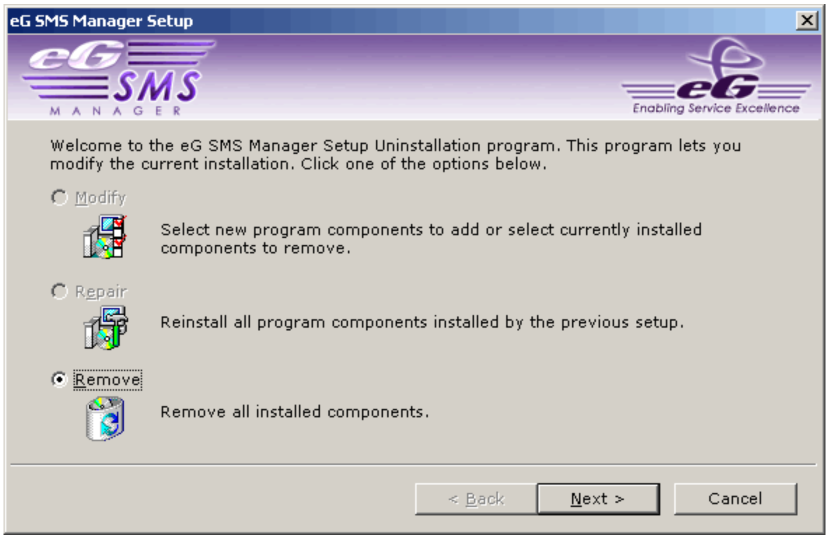


Figure 7.13: Uninstalling the eG SMS Manager

3. Now, select **Remove** from Figure 7.14 and click the **Next >** button to proceed with the uninstallation.



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

○ Modify

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

○ Repair

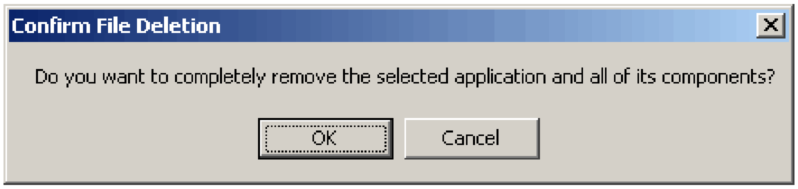
Reinstall all program components installed by the previous setup.

● Remove

Remove all installed components.

Figure 7.14: Selecting the Remove option

4. Next, click on the **OK** button in Figure 7.15 to confirm deletion of the entire eG SMS manager application.



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

Figure 7.15: Confirming the complete removal of the eG SMS manager

7.4 Integrating the eG Manager with Air2Web

Air2Web's Mobile Internet Platform (MIP) allows customers to build, implement, and run data solutions that enable wireless access to their major back office software solutions. Content Gateway is Air2Web's core platform that delivers messages—SMS, MMS and WAP Push—through all major US and international carriers.

In environments that either have the gateway in-house or subscribe to Air2Web's Content Gateway services, users have the option of configuring the eG manager to send SMS alerts to mobile phones via Air2Web's service offering, instead of the eG SMS manager. The key advantages of this approach are:

- The eG SMS manager need not be procured, installed, and configured
- No modems would be required
- Users need not subscribe to any service provider's SMS service

The only requirements of this approach therefore, are:

- A valid subscription to Air2Web's services
- An eG manager installation, with the license enabled ror **SMS Alerts**

To integrate this eG manager with Air2Web, do the following:

1. Edit the **eg_services.ini** file in the **<EG_INSTALL_DIR>\manager\config** directory.
2. You will find the following entries in the **[SMS_SETTINGS]** section of the file:

```
[SMS_SETTINGS]
SmsServer=
SmsPort=
SmsService=
#Air2WebUrl=
```

The **SmsServer**, **SmsPort**, and **SmsService** parameters in this section are of relevance only if the eG SMS manager is being used for sending SMS alerts. Similarly, the **Air2WebUrl** specification gains significance only if the eG manager integrates with Air2Web.

If the **Air2WebUrl** parameter holds no value, it indicates that the eG manager does not integrate with Air2Web. To ensure that the eG manager automatically attempts to transmit SMS alerts via Air2Web, you need to ensure that this parameter is first uncommented and then set to a valid URL; if this is done, then the **Air2WebUrl** specification automatically supercedes any **SmsServer**, **SmsPort**, or **SmsService** that you might have previously configured in the **eg_services.ini** file.

The **Air2WebUrl** specification should be of the following format:

http://<IP_Address_of_Air2web_Service>/failsafe/HttpPublishLink?pcode=<Pass_code_provided_by_Air2web>?acode=<Application_code_provided_by_Air2web>&mnumber=&message=&pin=<Identification_code_provided_by_Air2web>

For instance, say, the details of your Air2Web subscription are as follows:

IP Address of Air2web service: 192.168.10.112

Pass code provided by Air2web: egaweb112

Application code provided by Air2web: egapp112

Identification code provided by Air2web: eginv112

In this case, your **Air2WebURL**specification would be:

*http://**192.168.10.112**/failsafe/HttpPublishLink?pcode=**egaweb112**?acode=**egapp112**&mnumber=&message=&pin=**eginv112***

3. Then, save the **eg_services.ini** file.
4. Once this is done, then every time an SMS alert is to be sent to a user, the following occur automatically:
5. The eG manager reads the mobile number configured for that user from the user profile
6. This mobile number is then automatically inserted against the **mnumber** parameter in the **Air2WebUrl** specification.
7. Likewise, the eG manager also inserts the contents of the SMS alert against the **message** parameter in the **Air2WebUrl** specification.
8. Once the entire URL is complete, the eG manager connects to the URL and sends the SMS alert.

7.5 Integrating the eG Manager with PageGate

PageGate software allows for network paging or network wide alphanumeric paging and text messaging from any combination of the following modules: web, email, commandline/ascii, serial, TAP-in and (GUI) windows workstations. Alphanumeric or text messages can be sent to alphanumeric pagers, numeric pagers, cell phones, PIMs, billboards or pcmcia pager cards. PageGate is a flexible powerful way to take control of corporate communications.

The eG manager can be integrated with PageGate, so that the alarms generated by the eG manager are sent as SMS' to pagers via PageGate. To submit messages to PageGate, the eG manager uses a Commandline/ASCII interface.

Given below are the pre-requisites for this integration:

- PageGate with the required number of pagers licenses.
- Commandline /ASCII Interface
- The eG Manager with a valid license for SMS Alerting capability
- A Dial-up modem

7.5.1 Configuring the PageGate Software to Transmit Alarms Sent by the eG Manager

To achieve this, follow the steps given below:

1. Please make sure that a dial-up modem is connected to the eG manager host.
2. Install the PageGate software on the eG manager host and start the PageGate server as shown below:

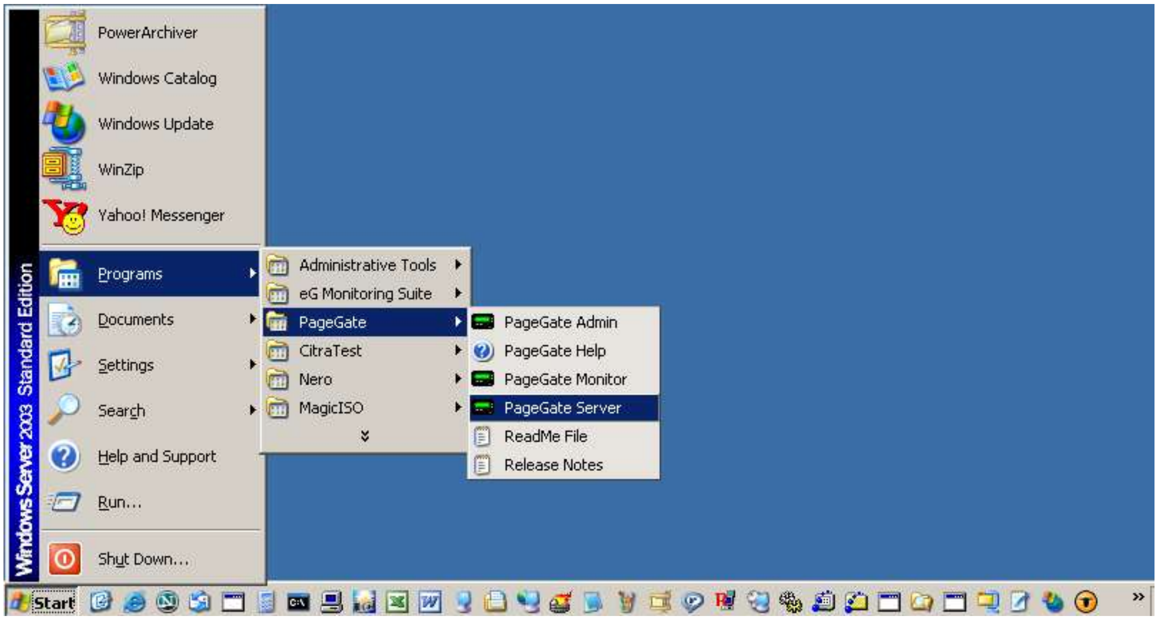


Figure 7.16: Starting the PageGate server

3. Once the PageGate server is started, a PageGate icon will appear in the SystemTray. By clicking on this icon, a pop-up menu depicted by Figure 7.16 appears:

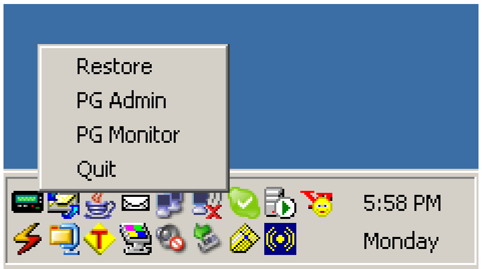


Figure 7.17: Clicking on the PageGate icon to view a pop-up menu

4. From the menu, click on **PG Admin** to lauch the PageGate Admin console. Alternatively, you can start PageGate admin by following menu sequence depicted by Figure 7.17.

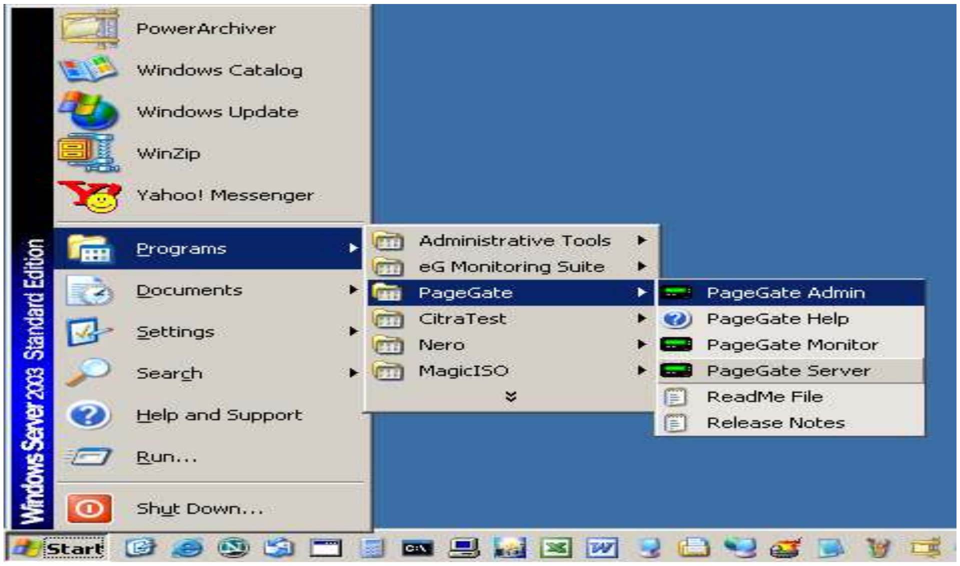
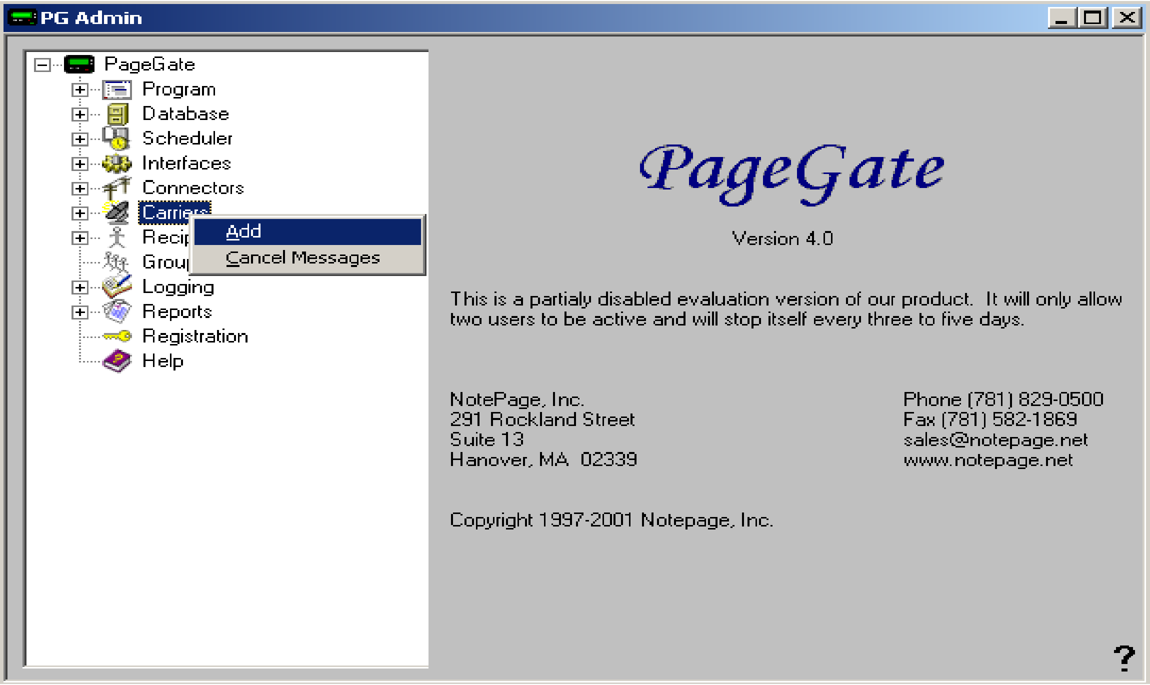


Figure 7.18: Launching the PG Admin console

5. The **PG Admin** console that then appears displays a tree-structure in the left pane. Expand the global **PageGate** node in the tree to view its sub-nodes. Now, proceed to add a new carrier by right-clicking on the **Carriers** sub-node and selecting the **Add** option from the shortcut menu that appears. The carrier represents the paging service provider using whose services PageGate will be transmitting SMS messages to configured recipients.



This is a partialy disabled evaluation version of our product. It will only allow two users to be active and will stop itself every three to five days.

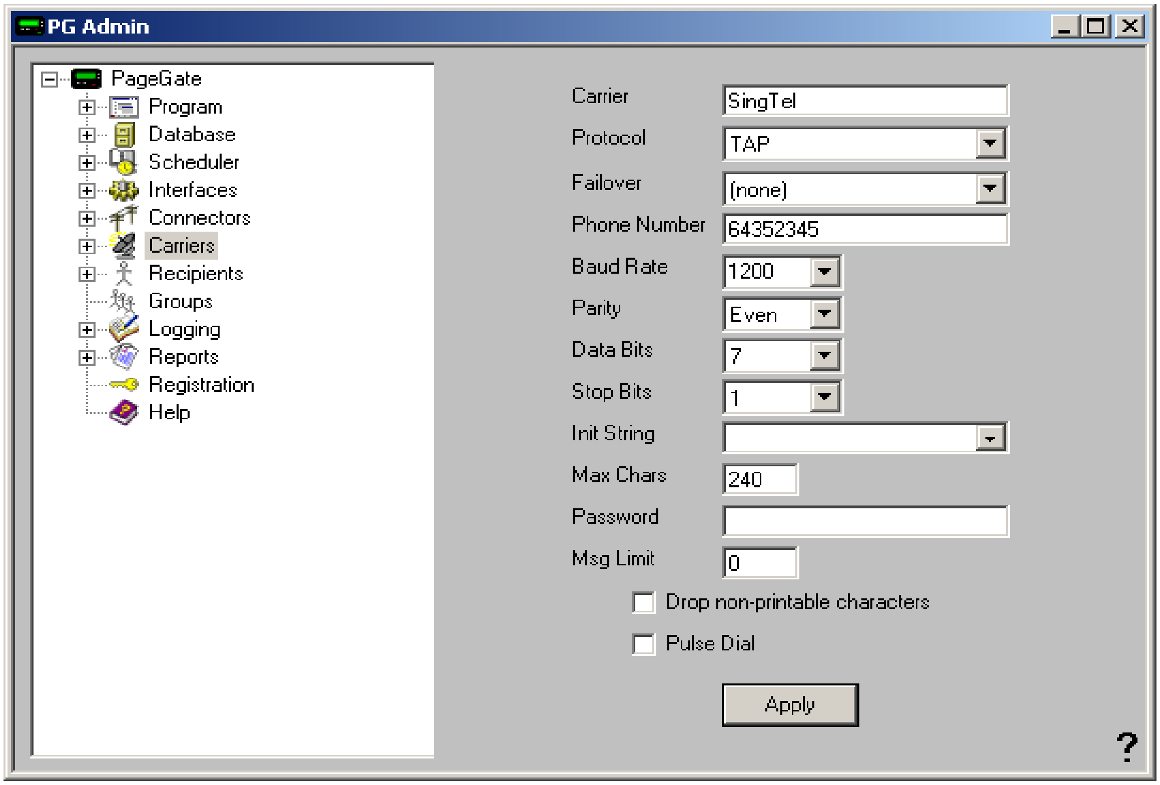
NotePage, Inc.
291 Rockland Street
Suite 13
Hanover, MA 02339

Phone (781) 829-0500
Fax (781) 582-1869
sales@notepage.net
www.notepage.net

Copyright 1997-2001 Notepage, Inc.

Figure 7.19: Adding a carrier

6. Upon selecting the **Add** option, the right-pane will change to display an interface using which the new carrier's details can be provided.



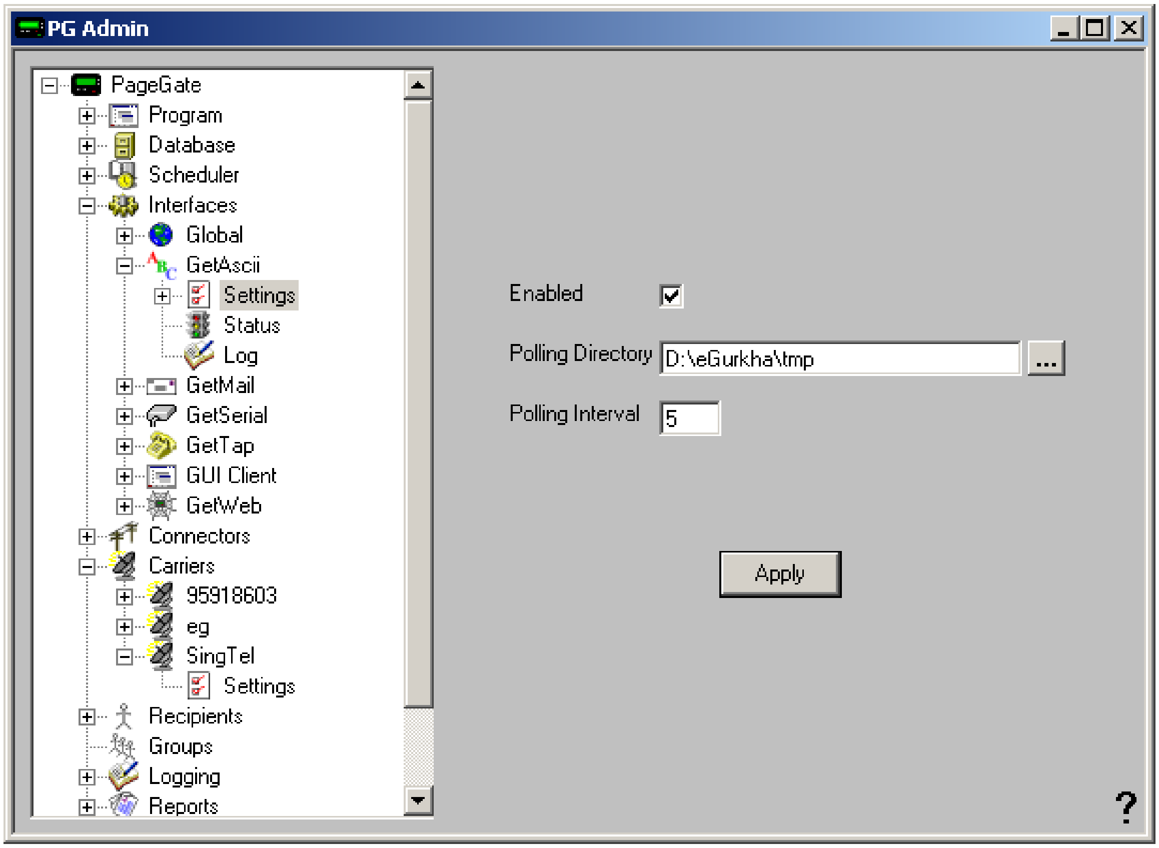
Carrier: SingTel
Protocol: TAP
Failover: (none)
Phone Number: 64352345
Baud Rate: 1200
Parity: Even
Data Bits: 7
Stop Bits: 1
Init String:
Max Chars: 240
Password:
Msg Limit: 0
□ Drop non-printable characters
□ Pulse Dial

Figure 7.20: Specifying the details of the new carrier

7. In Figure 7.19, enter the carrier name and phone number, and retain the default values for all other fields.

8. Finally, click on the **Apply** button to create the carrier.

9. Next, to enable the PageGate server to get SMS messages using a command-line/ASCII interface, expand the **Interfaces** node in the tree, expand its **GetAscii** sub-node, and select **Settings** (see Figure 7.20).



Enabled ☑

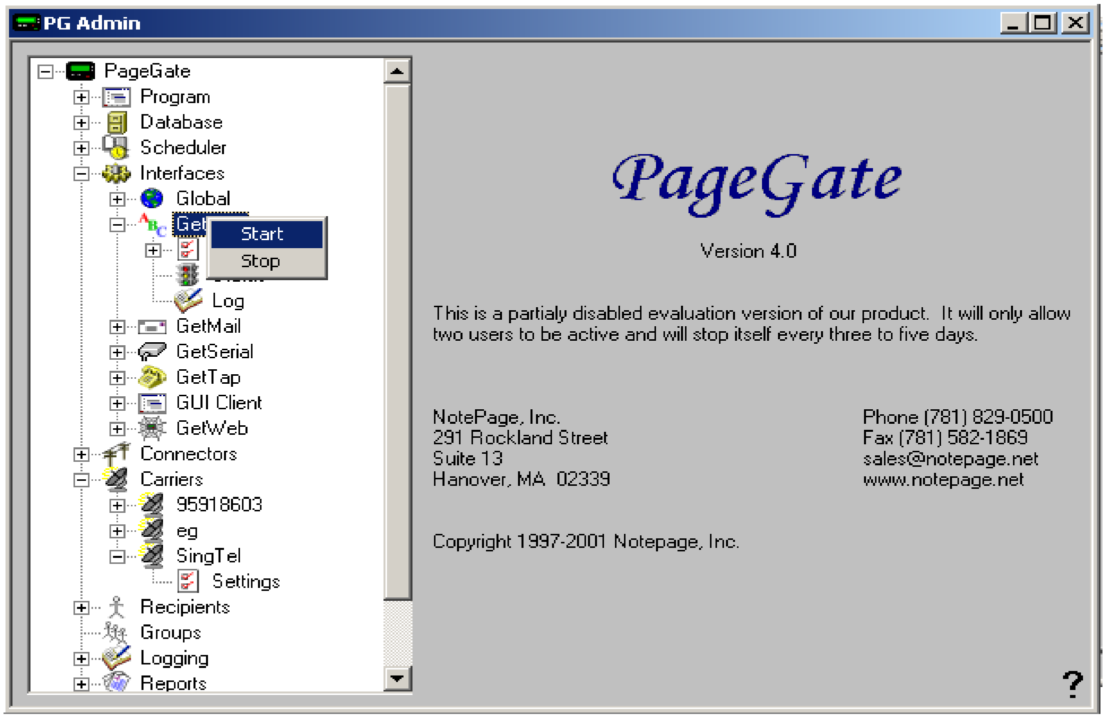
Polling Directory D:\eGurkha\tmp

Polling Interval 5

Figure 7.21: Configuring ASCII settings

10. When Figure 7.20 appears, select the **Enabled** check box to enable the **GetAscii** interface, and then proceed to provide a **Polling Directory** and a **Polling Interval.** At a configured **Polling Interval**, the **GetAscii** interface polls the **Polling Directory** for any messages to be sent out via pager. To ensure that the **GetAscii** interface polls the **tmp** directory of the eG manager for SMS messages to be paged, set **<EG_MANAGER_INSTALL_DIR>\tmp** as the **Polling Directory**. Finally, click the **Apply** button.

11. Then, proceed to start the **GetAscii** interface. For that, right-click the **GetAscii** sub-node of the **Interfaces** node in the tree structure, and pick the **Start** option from the shortcut menu that appears.



Version 4.0

This is a partialy disabled evaluation version of our product. It will only allow two users to be active and will stop itself every three to five days.

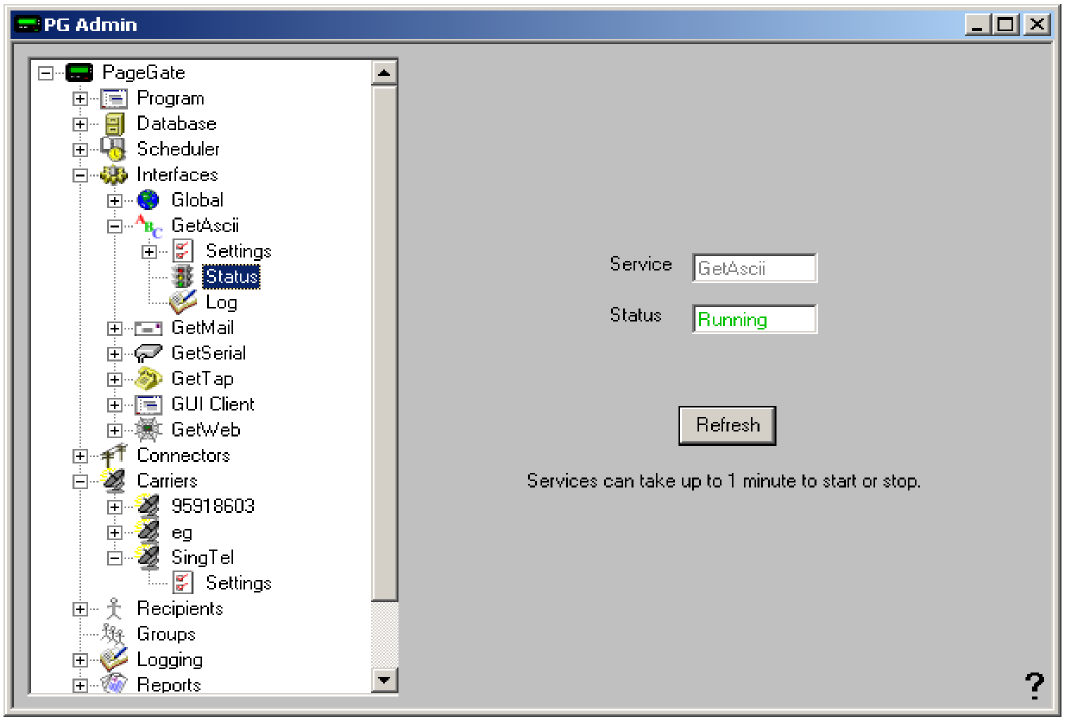
NotePage, Inc.
291 Rockland Street
Suite 13
Hanover, MA 02339

Phone (781) 829-0500
Fax (781) 582-1869
sales@notepage.net
www.notepage.net

Copyright 1997-2001 Notepage, Inc.

Figure 7.22 : Starting the GetAscii interface

12. You can confirm whether the interface actually started or not by selecting the **Status** sub-node under the **GetAscii** node in the tree structure (see Figure 7.22). The **Status** field in the right panel will then indicade whether the **GetAscii** interface is currently running or not.



Service: GetAscii

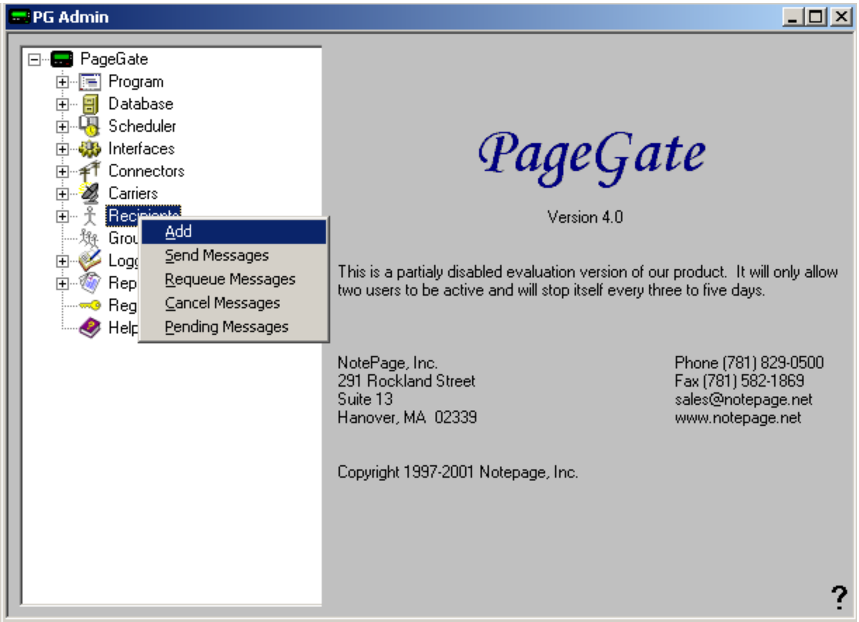
Status: Running

Services can take up to 1 minute to start or stop.

Figure 7.23: Confirming the status of the GetAscii service

13. Next, proceed to configure the recipients to whom the SMS messages have to be paged. For that, righ-click on

the **Recipients** sub-node under the **PageGate** node and pick the **Add** option from the menu that pops out.



PageGate

Version 4.0

This is a partialy disabled evaluation version of our product. It will only allow two users to be active and will stop itself every three to five days.

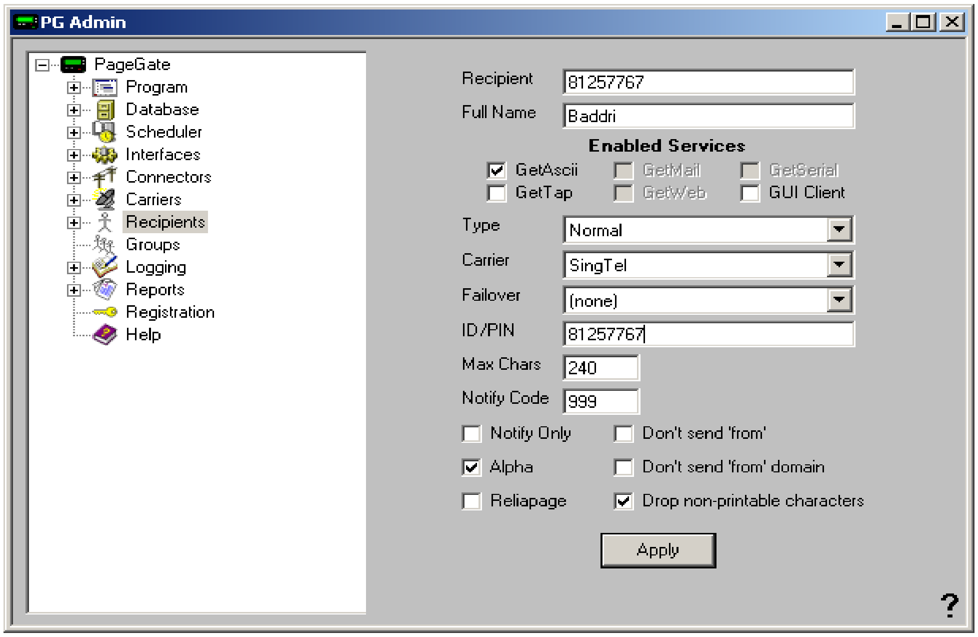
NotePage, Inc.
291 Rockland Street
Suite 13
Hanover, MA 02339

Phone (781) 829-0500
Fax (781) 582-1869
sales@notepage.net
www.notepage.net

Copyright 1997-2001 Notepage, Inc.

Figure 7.24: Adding a new recipient

14. In the right panel, provide the details of the new recipient, as depicted by Figure 7.23 below.



Recipient: 81257767

Full Name: Baddri

Enabled Services

☑ GetAscii ☐ GetMail ☐ GetSerial
☐ GetTap ☐ GetWeb ☐ GUI Client

Type: Normal

Carrier: SingTel

Failover: (none)

ID/PIN: 81257767

Max Chars: 240

Notify Code: 999

☐ Notify Only ☐ Don't send 'from'
☑ Alpha ☐ Don't send 'from' domain
☐ Reliapage ☑ Drop non-printable characters

Figure 7.25: Providing the recipeint's details

15. While furnishing recipient information, make sure that you provide the same value in the **Recipient** and in the **ID/PIN** text boxes. In other words, provide the **ID** or **PIN** of the new recipient in the **Recipient** text box as well.

Also, make sure that the **GetAscii** check box is selected in the **Enabled Services** section, choose the appropriate carrier, and also select the **Alpha** checkbox (necessary for sending alphanumeric pages).

16. Finally, click on the **Apply** button to create the recipient.
17. Next, either copy the **sendpage32.exe** from the **PageGate install directory** to the **<EG_INSTALL_DIR>\lib** folder, or include the **PageGate install directory** in the eG manager's **PATH** variable. The second approach will need a manager restart for the changes to take affect.

7.6 Integrating the eG Manager with a Web-based Interface

Some environments may support a web-based interface that receives alarm information from a third-party source via HTTP/HTTPS, converts this information into SMS, and transmits the SMS alerts to configured recipients. To enable the eG manager to integrate with such an interface so that eG alerts are converted into SMS for transmission to configured mobile numbers, do the following:

1. Edit the **eg_services.ini** file (in the **<EG_INSTALL_DIR>\manager\config** directory).
2. Set the **SendSMSAlertsOverHTTP** flag in the **[HTTP_SMS_ALERTS]** section of the file to **true**.
3. Next, configure the URL to which the eG alerts need to be sent, against the **HTTPSMSURL** parameter.
4. Save the file.
5. Once this is done, then the next time the eG manager generates alerts on a component, the same will be routed to the **HTTPSMSURL** that has been configured, in the following format:

   In case of a single alert:

   Mobile number#eG- Alarm: Component name # Component type # Priority- Test name: Measure name# Problem description#Site name# Last measurement value# Problem time

   Where multiple alerts are clubbed into one:

   Mobile number#eG- Alarm: Component name # Component type # Priority- Test name1: Measure name1# Problem description1#Site name1# Last measurement value1, Priority- Test name2: Measure name2# Problem description2#Site name2# Last measurement value2 #Problem time

If multiple alerts are clubbed in a single alert, then **note that the 'Problem Time' will appear only once for all the alerts**.

7.7 Logging of SMS Alerts

By default, all the eG alarms forwarded to an HTTP/HTTPS address will be logged in the **<EG_INSTALL_DIR>\manager\logs\HTTPSMS.log** file. The details and status of all other SMS alerts are logged in the **<EG_INSTALL_DIR>\manager\logs\egsmsaudit_log** file.

Both these files are governed by the following parameters in the **[HTTP_SMS_ALERTS]** section of the **eg_services.ini** file.

```
Max_log_files=10
Log_file_size=1
```

If say, the **HTTPSMS.log** file grows to the size of 1 MB (by default), another **HTTPSMS.log** file is automatically created to which the contents of the original file are copied. The details of the subsequent alerts will then be logged to the original file. This way, a maximum of 10 **HTTPSMSl.log** files can be created (by default). The same default settings apply to the **egsmsaudit.log** file as well. These default log settings can however be overridden using the above-mentioned parameters.

To increase the maximum size (in MB) upto which a log file (**HTTPSMS.log** and/or the **egsmsaudit.log**) can grow before a new log file is created, increase the value of the **Log_file_size** parameter. Likewise, to increase the maximum number of log files that can be created, change the value of the **Max_log_files** parameter. Then, save the file to register the changes.

8

Troubleshooting

This chapter in deals with the queries that may arise while installing and configuring eG.

8.1 Installing the eG Manager

- **The eG manager installation does not even start. What could be wrong?**

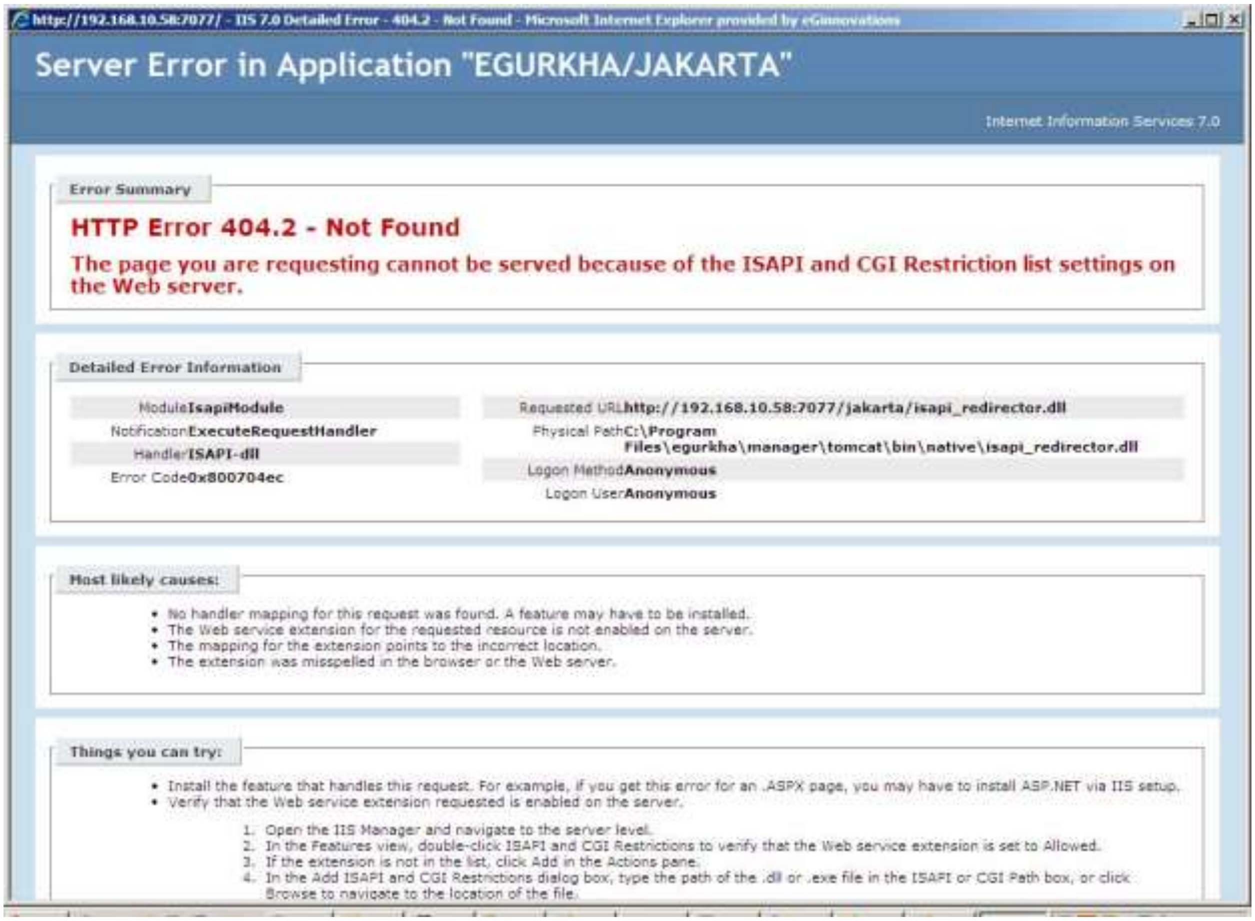
  Please check for the following:

  - Did you accept the license agreement?
  - Check if you possess the administrative privileges on Windows.
  - Do you have the pre-requisites for
    - JDK (with the appropriate version)
    - An operating system version that eG supports
    - The right service pack and option pack (for Windows environments)

- **The eG manager installation failed. What could be wrong?**

  1. 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. Please refer to the *eG User Manual* for details.
  2. 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)
  3. Check that the tablespaces specified when creating a new user are valid. Please refer to *the eG User Manual* for a method of determining the tablespaces available for a database server.
  4. Ensure that the tablespaces specified have enough space to host the eG database tables.
  5. Verify that if the eG manager and agent are being installed on the same system, the same user owns the eG directories.
  6. Finally, make sure that the operating system locale setting is English.

- **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

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	Requested URL	http://192.168.10.58:7077/jakarta/isapi_redirector.dll
Notification	ExecuteRequestHandler	Physical Path	C:\Program Files\egurkha\manager\tomcat\bin\native\isapi_redirector.dll
Handler	ISAPI-dll	Logon Method	Anonymous
Error Code	0x800704ec	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 8.1: The error message that appeared when the 'egurkha' web site listing in the IIS 2008 manager console was clicked

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 8.2).

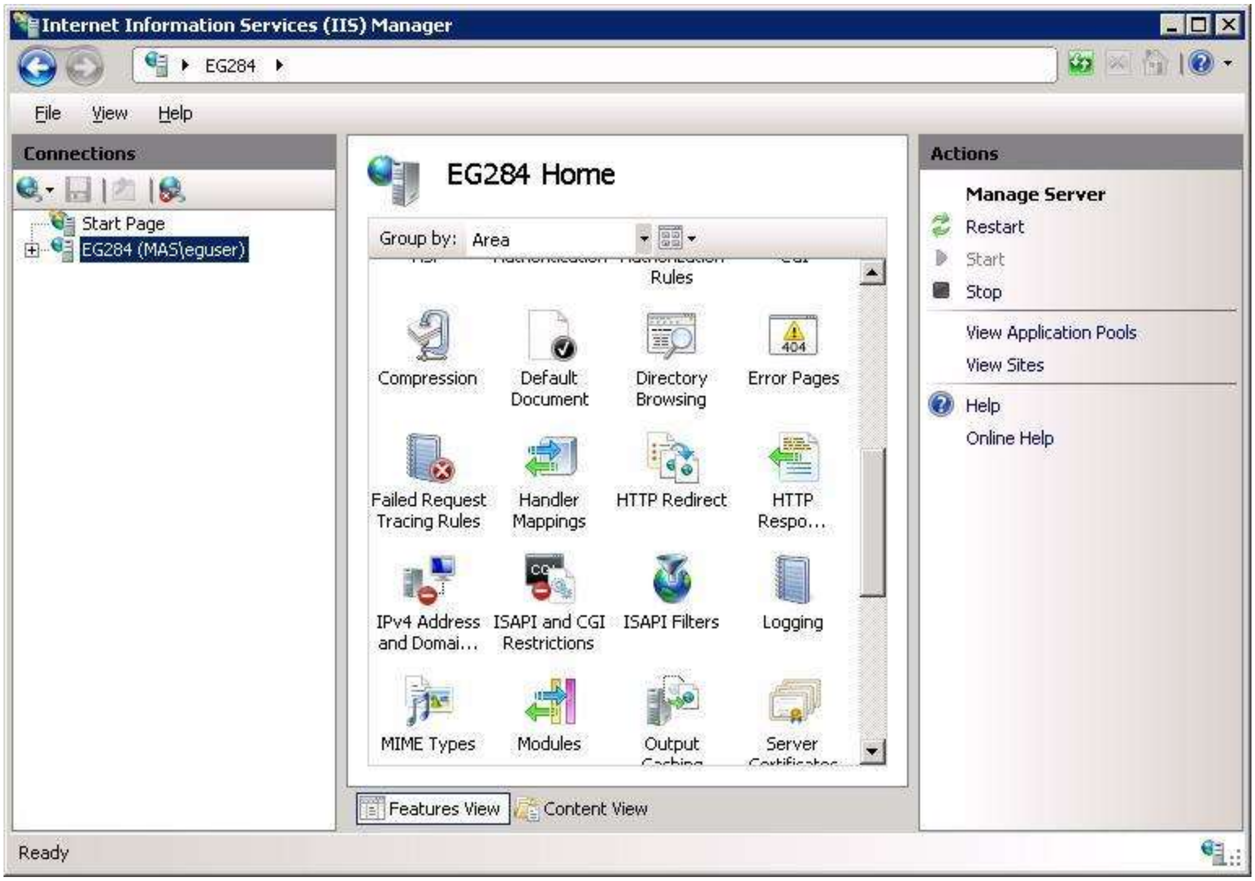
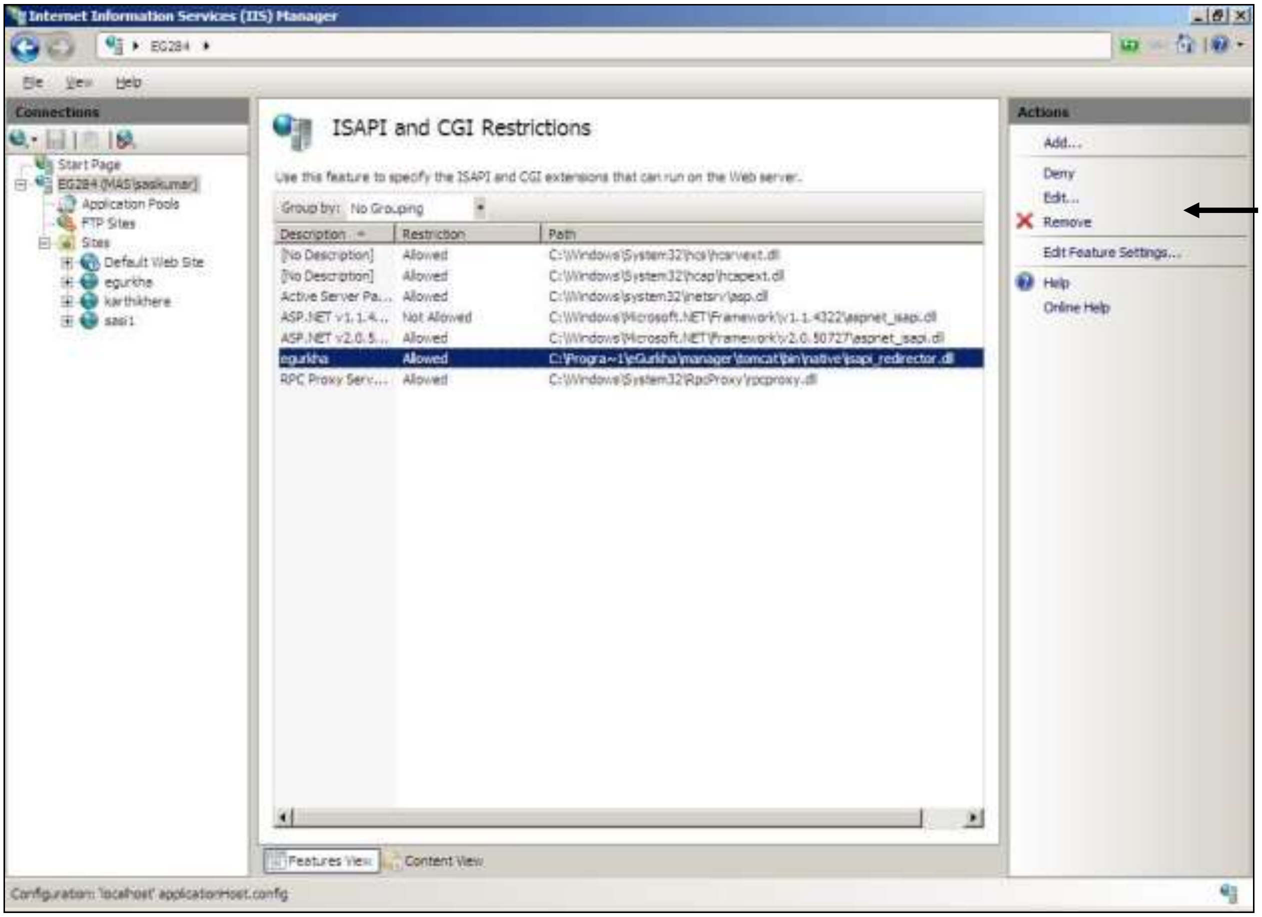


Figure 8.2: Clicking on the node representing the IIS web server in the left pane of the console

- 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 8.3 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 8.3.



ISAPI and CGI Restrictions

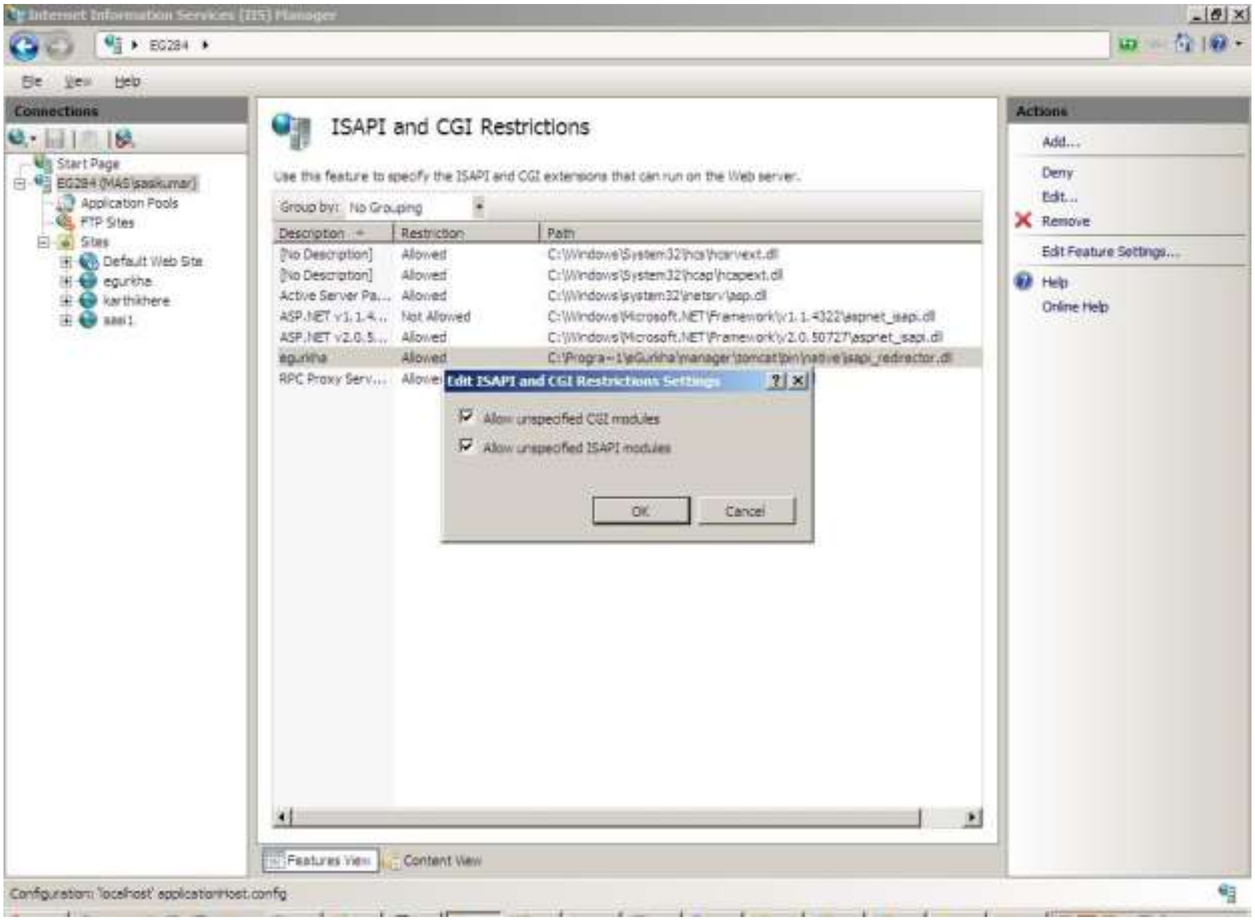
Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping

Description	Restriction	Path
[No Description]	Allowed	C:\Windows\System32\hcs\hcarvext.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

Figure 8.3: 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 8.4: Lifting the ISAPI and CGI restrictions from the egurkha extension

8.2 Configuring the eG Manager

- **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.

- **How do I configure eG on a Linux default Apache?**

  Linux includes a default apache server (actually a daemon) that starts running as soon as the server is booted up. This server listens on port 80. The server startup file is in **/etc/rc.d/init.d/** and is called "httpd". The server configuration file is picked from the directory **/etc/httpd/conf**.

  To stop this server, use the command **/etc/rc.d/init.d/httpd stop.**

  To start this server, use the command **/etc/rc.d/init.d/httpd start**.

  The eG agent installation script expects the apache start up file to be called **"apachectl"**. Moreover, this script expects the **apachectl** file to be in the **apacheServerRoot/bin** directory.

  To configure the default httpd to work with eG, follow the following steps:

  - Create the directory in **/etc/httpd/bin**
  - **cd /etc/httpd/bin**
  - **ln –s /etc/rc.d/init.d/httpd apachectl**
  - **ln -s /usr/sbin/httpd httpd**
  - Run **/opt/egurkha/bin/setup_webadapter**
  - Provide **/etc/httpd** as the web server's root directory (admin of the web server is root)
  - **mv /etc/rc.d/init.d/httpd /etc/rc.d/init.d/httpd.save**
  - **ln -s/etc/httpd/bin/apachectl /etc/rc.d/init.d/httpd**
  - Start the Apache server using the command **/etc/httpd/bin/apachectl start**

- **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.

8.3 Configuring the eG Database

- **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, If 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.

8.4 Starting the eG Manager

- **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.

- **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.
  - This problem can also occur if you have uninstalled the Java environment that you had specified when installing the eG manager. 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_manager** script on Unix to restart the manager. On Windows, reinstall Java in the same location.
  - 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**.

8.5 Installing the eG Agent

- **The eG agent failed to install properly. What could be wrong?**

  Please check for the following:

  - Did you accept the license agreement?
  - Do you have the pre-requisites
    - An operating system version that eG supports
    - The right service pack and option pack (for Windows environments)

8.6 Configuring the eG Agent

- **While configuring a web server to be monitored by eG, I specified "yes" when the Setup enquired if this web server has SSL support. I get an error message. Why?**

  The error message appears if the web server is not configured for SSL support.

8.7 Starting the eG Agent

The eG agent was installed successfully, but it does not seem to be reporting any measures. What could be wrong?

- Make sure that the IP address or the hostname of the manager specified during the agent install is correct.
- Please check to see if the eGAgent 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.
- 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.

- **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.

- **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.

8.8 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.

9

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.

Index