CA API Management

CA API Gateway – Enterprise Service Manager User Manual

Version 1.16.0

technologies

TO THE EXTENT PERMITTED BY APPLICABLE LAW OR AS AGREED BY CA IN ITS APPLICABLE LICENSE AGREEMENT, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contents

List of Figures

List of Tables

Chapter One: Getting Started

Welcome to the Enterprise Service Manager

The CA API Gateway - Enterprise Service Manager (ESM) makes it possible to manage many Gateway clusters spread across a wide geographical area, using only a web browser. The rich graphical interface combined with the familiarity of a browser makes ESM simple to learn and use.

Prerequisites:

- Enterprise Service Manager is supported under the latest versions of Internet Explorer or Firefox. Other browsers may work, but are not supported by CA Technologies.
- Java Runtime is required if you intend to launch the Policy Manager from within Enterprise Service Manager.
- Adobe Reader (or equivalent PDF viewer) is required to view the electronic version of the user manual.

The Enterprise Service Manager operates only with Gateways in the appliance or virtual appliance form factors. It does not support software Gateways.

If you are new to Enterprise Service Manager, review these topics first to learn the basics of the interface:

"Starting the Enterprise Service Manager Web Interface" on page 1

"Interface Overview" on page 3

"Using the Enterprise Tree" on page 5

Help date: 4/12/2016

Starting the Enterprise Service Manager Web Interface

To log into the Enterprise Service Manager, you must have a user account and optionally a role.

➤ *To start the Enterprise Service Manager:*

1. Start your web browser and navigate to URL configured during system setup. For more information, see "Setting Up the Enterprise Service Manager" on page 14. This URL will be in the form:

   https://*<host_name>***:***<port>*

   For example: *https://machine.company.com:8182*

2. Enter your **User Name** and **Password**.

3. Click [**Login**]. Your initial start-up page is displayed. You can change this start-up page on the User Settings page, User Interface Preferences section.

Dealing with browser security warnings

You may encounter security warnings from your browser because the Enterprise Service Manager is authenticating itself using a self-signed certificate. If these warnings appear, respond as follows:

- **Internet Explorer:**

  a. Click “**Continue to this website (not recommended)**”.

  b. When Enterprise Service Manager has started, click "**Certificate Error**" next to the address bar.

  c. Click "**View Certificates**" in the Untrusted Certificate box. The Certificates dialog box appears.

  d. Click [**Install Certificate**]. The Certificate Import Wizard begins.

  e. Click [**Next**], then [**Next**] again to accept "Automatically select the certificate store based on the type of certificate".

  f. Click [**Finish**]. The certificate is installed and you will not receive security warnings the next time Enterprise Service Manager is started.

- **Firefox:**

  a. Click [**OK**] to acknowledge the Alert message.

  b. Click “**Or you can add an exception**”.

  c. Click [**Add Exception**...]. The Add Security Exception dialog box appears.

  d. Click [**Get Certificate**], then [**Confirm Security Exception**].

Interface Overview

The Enterprise Service Manager main interface is grouped across five *tabs* that reflect the typical workflow for the product. Within a tab, the functionality is divided across one or more *pages*.

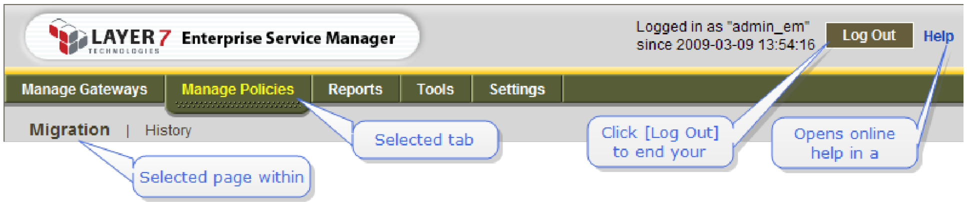


Figure 1: Enterprise Service Manager main interface

The following are the top level tabs:

- **Manage Gateways:** Used to monitor and configure Gateway clusters. This tab is described under "Enterprise Service Manager: Reference Guide" on page 55.
- **Manage Policies:** Used to migrate services and policies from one cluster to another and to manage previous migrations. This tab is described under "[Manage Policies] Tab" on page 63.
- **Reports:** Used to generate reports showing performance and usage statistics. This tab is described under "[Reports] Tab" on page 74.
- **Tools:** Used to view audit and logs generated by the Enterprise Service Manager. This tab is described under "[Tools] Tab" on page 78.
- **Settings:** Used to configure preferences for Enterprise Service Manager and to manage user accounts and assign users to roles. This tab is described under " [Settings] Tab" on page 80.

For a description of interface elements specific to a page, please refer to the topic for that page.

Working with Lists

The following controls are available when lists are used:

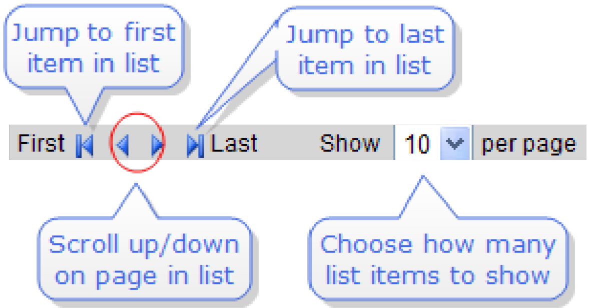

Jump to first item in list
Jump to last item in list
First
Last
Show
10
per page
Scroll up/down on page in list
Choose how many list items to show

Figure 2: List management controls

The following icons indicate that a list can be resized (height only, not width):

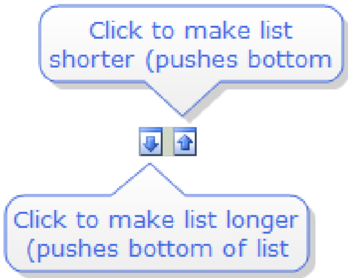

Click to make list shorter (pushes bottom
Click to make list longer (pushes bottom of list

Figure 3: List resize controls

Refreshing a List

When the Refresh icon 🔄 is available, you can click it to update its accompanying list. This helps ensure that you are viewing the most recent information. You can also update a list to see it reflect an action you recently performed.

Tip: Refreshing the browser window produces the same results as refreshing a list, however using the 🔄 icon may update more quickly because only a single list is involved.

Tip: The Monitor page does not need to be manually refreshed—the statistics automatically update themselves.

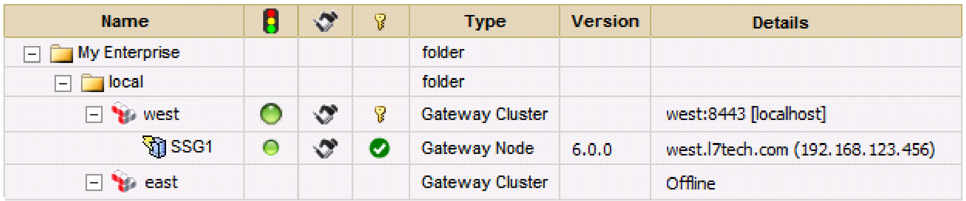
Using the Enterprise Tree

The enterprise tree is the foundation of the system. It lists using a tree view all the Gateway clusters and nodes under the control of the Enterprise Service Manager, plus some important information about cluster and node status. The enterprise tree is used on the following pages:

- "Monitor Page" on page 55
- "Configure Page" on page 61
- "Migration Page" on page 63
- "[Reports] Tab" on page 74

Figure 4 shows the enterprise tree as it appears on the Configure page. A simplified version of the enterprise tree is used on the other pages (for example, the Type, Version, and Details columns may be omitted). This abbreviated version is used to select clusters or nodes to complete an operation (for example, generating a report or migrating a service or policy).

Only users with the Administrator role can modify the enterprise tree. For all other users, information here is for display purposes only.



Name	🚦	🤝	🔑	Type	Version	Details
⊟ My Enterprise				folder		
⊟ local				folder		
⊟ west	●	🤝	🔑	Gateway Cluster		west:8443 [localhost]
SSG1	●	🤝	✓	Gateway Node	6.0.0	west.l7tech.com (192.168.123.456)
⊟ east				Gateway Cluster		Offline

Figure 4: The enterprise tree in the Configure page

The enterprise tree contains three major entities:

- **Folders:** Folders are used to organize your clusters They can be manipulated just like the folders and directories used in your operating system. The enterprise tree initially contains a single root folder named “My Enterprise” that you can rename to your organization’s name. For more information on working with folders, see "Chapter Three: Working with Clusters" on page 19.
- **Clusters:** These are the Gateway clusters being monitored. Clusters can be organized within folders as required. For information on adding clusters, see "Adding a Gateway Cluster to Manage" on page 20.

Offline clusters: These are clusters that cannot be reached by Enterprise Service Manager. They are created in the enterprise tree when you upload a migration archive with an unrecognized source cluster. For information on uploading an archive, see "History Page" on page 72. Note that an "offline cluster" is not the same as a cluster that is currently down (offline).

> **Note:** The cluster name is used only within the Enterprise Service Manager. Its purpose is to help you more easily identify the clusters being monitored. The actual Gateway cluster is not aware of any cluster name settings made through the Enterprise Service Manager.

- **Nodes:** These are the individual Gateway nodes within a cluster and are visible when you have access permission to the parent cluster. The enterprise tree shows the status of each node, but you cannot modify a node from within Enterprise Service Manager (nodes are linked to their clusters). If a node has been enabled for remote management, you can stop and start it from the Configure page. For more information, see "Enabling Remote Management on Nodes" on page 16.

The following table describes the icons used in the enterprise tree.

Table 1: Enterprise tree icons

Icon	Description
🚦 (for a cluster)	The following indicators are used to show the status of a cluster: 🟢 **(Up):** All the Gateway nodes and database are working normally. No attention is required. 🟠 **(Partially up):** Some of the Gateway nodes are working while others are not, or the database is down. Some cluster-based operations may still be available (for example, policy migration). Note that a yellow indicator can never occur if the cluster comprises of a single Gateway. 🔴 **(Down):** The cluster is down; no response or error response. Immediate attention is required. [no icon] **(Offline)**: The cluster is one that is not reachable by Enterprise Service Manager. It is visible in the enterprise tree only after uploading its migration archive. **Note:** The online status of a cluster is displayed only when the user has access permission to the cluster.
🚦 (for a node)	The following indicators are used to show the status of a node: 🟢 **(On):** The node is running normally. ⚫ **(Off):** The node was stopped normally (e.g., by a user). 🔴 **(Down):** The node is down. It stopped abnormally and could not be automatically restarted.

Icon	Description
	● **(Offline):** The status of the node cannot be determined. Node-based operations (such as start/stop or monitor node) are unavailable.
(for a cluster)	Indicates whether trust has been established with the Gateway cluster. (**Trusted**): Trust has been established between the Enterprise Service Manager and the cluster. (**Not trusted**): Trust has not been established with the cluster. Until trust is established, many operations are not available for the cluster and you cannot monitor the performance of the cluster. To establish trust, click and refer to "Adding a Gateway Cluster to Manage" on page 20 for instructions.
(for a node)	Indicates whether a node has been enabled for remote management. (**Enabled**): Remote management has been enabled for the node. (**Disabled**): Remote management has not been enabled for the node. Enterprise Service Manager cannot be used to stop and start the node, nor can it monitor this node. To resolve this, see "Enabling Remote Management on Nodes" on page 16.
(for a cluster)	The following icons are used to show the access status for a cluster: **(Mapped):** The current Enterprise Service Manager user is mapped to a user account on the Gateway cluster. **(Not mapped):** The current Enterprise Service Manager user is not mapped to any user account on the Gateway cluster. Without a mapping, the ESM user's access to the cluster is restricted. To set or change a mapping, click or and then refer to "Mapping an ESM User to a Cluster User Account" on page 23.
(for a node)	The following icons are used to show the user's access privileges for a node: ✓ **(Access):** The user has a role that permits administrative access to the node (i.e., is either an Administrator or has a "Manage *XXXX* Cluster" role for the cluster). ⛔ **(No access):** The user has not been assigned to a role that permits administrative access to the node. Until access is granted, the user cannot start or stop the node. However, node details are visible, as are monitored property values. To grant access, see "Adding a User to a Role" on page 44.
Type	The type of item in the tree: • **folder:** Created by an administrator and used to organize the clusters. • **Gateway Cluster:** A Gateway being managed. • **Gateway Node:** An individual node within the Gateway.

Icon	Description
Version	The version of the Gateway software running on the node.
Details	For a cluster, the following details are displayed: • SSL certificate host name or IP address • Administrative port number • Database host name • Gateway database version • Any other error or status messages For an offline cluster, "Offline" is displayed. For a node, the following details are displayed: • Self host name • IP address • Version • Any other error or status messages **Tip:** You can point at each piece of information in the Details column to see the details in a tool tip.

Understanding the Error Messages

The Details section will display the error messages shown in the table below.

Table 2: Detail Error Messages

Error Message	Issue
ESM Certificate not trusted	The trust relationship between the Enterprise Service Manager and cluster is broken. The ESM certificate in a cluster or node doesn’t match the new certificate in the ESM.
Not licensed	The cluster is not licensed or has an invalid license.
Error accessing node: 'Could not send message' due to 'No route to host'	The node is shut down or unreachable.
Error accessing node: ‘Could not send message’ due to ‘Connection refused'	The node is not running because either the Gateway service on the node has stopped or the ESM interface/port is not configured correctly (network error).
Duplicate node(s) ignored	A cluster with one or more duplicate nodes has been added to the Enterprise Tree. As a result, all duplicates nodes are ignored. To resolve, delete the cluster from the Enterprise Tree (if it is a duplicate of an existing cluster) or remove the duplicated node(s) from the cluster using the Policy Manager.

Error Message	Issue
	Tip: See "Delete a Node" under *Dashboard - Cluster Status* in the Policy Manager documentation for instructions on removing a node.

Viewing Audits and Logs

The Enterprise Service Manager maintains easily accessible logs to help you track down issues or troubleshoot problems.

The logs are accessed from the [Tools] tab. Two types of logs are available: Audits and Logs. These are described below.

Tips: To toggle how the sort order of the log entries, click the “Time” heading. To manage a long list of audits, use the list controls.

Tip for advanced users: You can enable debug logging and control the level of detail in the log files displayed in the [Tools] tab. To learn how to do this, see "Appendix B: Configuring the ESM Logs" on page 91.

Audit Logs

Audit logs are displayed under the **Audit** page of the [Tools] tab. There are two types of messages recorded in the audit log:

- **Administrative:** These audits record the actions that occurred as a result of a user performing a task in Enterprise Service Manager—for example, a Gateway cluster was added and a new role was automatically created to manage this cluster.
- **System:** These audits note the internal messages that are constantly generated in the background by Enterprise Service Manager. These messages typically describe “housekeeping” tasks such as starting/stopping the Enterprise Service Manager, adding/updating the license, etc.

Select a task from the table below.

Table 3: Audit log actions

To...	Do this...
View audits for a specific time frame	1. Click the **Start Date** and **End Date** fields and select the dates from the pop-up calendar 2. Select the **Type** of audit records to view. Choose [Any] to include both Administrative and System audits. 3. Click [**Select**] to display the appropriate audits.

To…	Do this…
Save audits to a file	1. Click [**Download**]. You are prompted for the time frame. 2. Click the **Start Date** and **End Date** fields and select the dates from the pop-up calendar. 3. Click [**OK**]. You are prompted to open or save the file. **Note:** Internet Explorer users may receive a file download warning. Acknowledge this warning to continue the download. You may need to reissue the Download command. 4. Click [**Save**] and then specify a location for the audit file. **Tips:** • The default file name is "audits.zip". You may change this to a more descriptive name prior to saving. • The audits are saved to a standard .ZIP archive. The contents can be viewed in any text editor.
Delete old audit records	1. Click [**Delete**]. You are prompted for the age of the audits to delete. 2. Enter the minimum age, in days. 3. Click [**OK**]. All audit records of this age and older will be deleted. **Tip:** You may want to save the old audit records prior to deleting.

Log Files

Log files are displayed under the Log page of the [Tools] tab. The logs list detailed information about system behaviour.

> **Note:** Internet Explorer users may receive a file download warning when viewing or saving the log. You may need to repeat the view or download action after acknowledging this warning.

➤ *To view a log file:*

1. Select a log file from the list.
2. Click **[View**]. The log details are displayed in the **Log Details** section.

➤ *To download a log file:*

1. Select a log file from the list.
2. Click [**Download**]. You are prompted to open or save the file.
3. Click [**Save**] and then specify a location for the log file.

Enabling/Disabling the Enterprise Service Manager

Enabling or disabling the Enterprise Service Manager requires access (local or remote) to the host Gateway appliance. Once disabled, it will be not possible to connect to the Enterprise Service Manager using a browser.

For more information, see "Configuring the Enterprise Service Manager" in the CA API Gateway Installation and Maintenance Manual.

➤ *To enable or disable the Enterprise Service Manager:*

1. On the Gateway appliance, log in as user **ssgconfig**. The Gateway main menu is displayed. For more information, see "Accessing the Gateway Configuration Interface" in the *CA API Gateway Installation and Maintenance Manual*.
2. Select **7** (Display Enterprise Service Manager configuration menu).
3. Select **2** (Disable|Enable the Enterprise Service Manager).
4. Enter **y** to disable or enable the Enterprise Service Manager immediately or enter **n** to have this take effect only when the appliance is rebooted. **Note:** This prompt appears only when the Enterprise Service Manager is not currently disabled/enabled.
5. Exit to the Gateway main menu.

Chapter Two: Configuring Enterprise Service Manager

Overview of Configuration Process

The following are the steps to set up and configure a new installation of the Enterprise Service Manager:

1. Create the administrative user and configure the ports. This is performed on the appliance on which the Enterprise Service Manager is installed.

   Tip: The user account created here is used to log into the Enterprise Service Manager for the first time. This user is responsible for adding other users and assigning them to roles.

   For more information, see "Setting Up the Enterprise Service Manager" on page 14.

2. Install the Enterprise Service Manager license supplied by CA Technologies. Without a valid license, the Enterprise Service Manager is severely restricted.

   For more information, see "Installing the Enterprise Service Manager License" on page 15.

3. Configure each Gateway node in a cluster to be monitored to allow them to be managed remotely by the Enterprise Service Manager. This is performed on each Gateway node. Though not absolutely required, this step is highly recommended as it will enable node-based operations (start/stop the node, monitor the node).

   For more information, see "Enabling Remote Management on Nodes" on page 16.

Once the Enterprise Service Manager is configured, you may begin using it. Some tasks to do first (requires an Administrator):

- Add the clusters to be managed by the Enterprise Service Manager and then establish trust.

  For more information, see "Adding a Gateway Cluster to Manage" on page 20 and "Establishing Trust with a Cluster" on page 21.

- Add users to the Enterprise Service Manager and assign them to the appropriate roles.

For more information, see "Chapter Six: Working with Users" on page 41 and "Adding a User to a Role" on page 44.

- Map the users to the clusters to which they are authorized to access. **This step is important.**

  For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

- Configure the cluster and node properties to be monitored.

  For more information, see "Chapter Four: Configuring Monitoring" on page 27.

Setting Up the Enterprise Service Manager

The following steps describe how to set up the Enterprise Service Manager for the first time. These steps only need to be performed once.

Perform the steps below on the Gateway appliance where the Enterprise Service Manager is installed. Once this setup is complete, you need do the following:

- Configure each node in the cluster to allow it to be managed remotely. For details, see "Enabling Remote Management on Nodes" on page 16. You must have access to each Gateway node to perform this procedure.
- Add the Gateway cluster to Enterprise Service Manager. For details, see "Adding a Gateway Cluster to Manage" on page 20.

➢ *To set up the Enterprise Service Manager:*

1. On the Gateway appliance, log in as user **ssgconfig**. The Gateway Configuration menu appears.
2. Select **7** (Display Enterprise Service Manager configuration menu).
3. Select **1** (Configure the Enterprise Service Manager). This starts the *Configure Enterprise Service Manager* wizard.
4. The first step is to create an administrator account for Enterprise Service Manager. Enter the name of the administrative user and make note of this name (example: “emadmin”). The name can be between 3 and 128 characters and may contain any character except: **# , + " \ < > ;**
5. Enter a password for this administrative user. Retype to confirm. The password may contain letters, numbers, and symbols and be between 6 and 32 characters.
6. Next, you are prompted for the server settings for the Enterprise Service Manager. By default, the factory settings are: monitor all IP addresses over port 8182.

- To accept the factory settings or to configure the settings later, press [**Enter**] to indicate that you are not overriding the defaults.
- To override the factory settings, type **yes** and then press [**Enter**].
  - Enter the IP address for the HTTPS listener or press [**Enter**] to use all available addresses.
  - Enter the port number for the HTTPS listener or press [**Enter**] to use the default port “8182”. **Remember this port number**.

> **Tip:** Ensure that the port number is not currently in use. For more information, see "Appendix A: Ports Used by the ESM" on page 87.

7. The configuration summary is displayed. If any changes are required, type “<” to go to the previous step or press [**Enter**] to apply the configuration.
8. The configuration results should show that the settings were applied successfully. Press [**Enter**] to return to the previous menu, then enter [**x**] to return to the main menu.

Once this setup is complete, do these next:

- Enable the Enterprise Service Manager on the appliance. For more information, see "Enabling/Disabling the Enterprise Service Manager" on page 11.
- Install the license file. For more information, see "Installing the Enterprise Service Manager License" on page 15.

Installing the Enterprise Service Manager License

The Enterprise Service Manager license must be installed before the product can be used. The license only needs to be installed once, by the administrator user.

➤ *To install a license file:*

1. Connect to the Enterprise Service Manager. For more information, see "Starting the Enterprise Service Manager Web Interface" on page 1.

> **Note:** You may encounter security prompts from your browser because the Enterprise Service Manager is using a self-signed certificate. You should acknowledge the prompts and allow the exceptions.

2. You are prompted to install the Enterprise Service Manager license. Click [**Close**] to dismiss the message.

3. The [Settings] tab > **System Settings** page is displayed. Scroll down to the License section and click [**Browse**].
4. Locate the Enterprise Service Manager license file and click [**Open**].
5. Click [**Apply**] in the License section to apply the license. The License Agreement is displayed.
6. Click [**OK**] to confirm that you accept the License Agreement. The Enterprise Service Manager is now licensed.

Once the Enterprise Service Manager is licensed, you can configure each Gateway node to allow it to be remotely managed by Enterprise Service Manager. For more information, see "Enabling Remote Management on Nodes" on page 16.

Enabling Remote Management on Nodes

Perform the following steps on each Gateway node that will be managed remotely by the same Enterprise Service Manager. Enabling remote management allows the Enterprise Service Manager to:

- start/stop the node
- monitor the node

Tip: If remote management has not been enabled for a node, all cluster-based operations (such as migrating a policy or generating a report) will still be available.

Prerequisite: The Enterprise Service Manager must be set up. For more information, see "Setting Up the Enterprise Service Manager" on page 14.

➢ *To enable remote management on a Gateway node:*

1. Log into the node as the user **ssgconfig**. The Gateway Configuration menu is displayed.
2. Select **5** (Display Remote Management configuration menu).
3. Verify that **3** reads: “Remote Node Management Enabled: Yes”. If it doesn’t, select **3** and enter **yes**.
4. Select **4** (New Trusted Certificate).

5. Enter the URL of the Enterprise Service Manager, using a Fully Qualified Domain Name, with the port number from Setting Up Enterprise Service Manager appended (e.g., “https://machine.domain.com:8182”). This downloads the certificate from the Enterprise Service Manager and stores it as a trusted certificate.
6. Examine the certificate details and enter **yes** to accept it.
7. Select **1** (Listener IP Address) and enter the IP address of the Internal Management LAN. This is the “eth0” interface shown in the diagrams under Network Deployment Guide, located in the appendix of the *CA API Gateway Installation and Maintenance Manual*.

   Tip: If the IP of eth0 is not available or if your deployment only has a single network interface, you can enter ‘*’ (asterisk) as the listener IP address.

8. Enter **s** to save changes and exit, then press [**Enter**] to continue.
9. Return to the main menu, enter **R** to reboot the Gateway appliance and then enter **y** to confirm.
10. Repeat these steps on the other nodes in the cluster.

Once all the nodes have been configured to allow remote management, you can add the Gateway clusters to be managed. For more information, see "Adding a Gateway Cluster to Manage" on page 20.

Chapter Three: Working with Clusters

Organizing Clusters and Nodes

You can organize the Gateway clusters on the enterprise tree to make the most sense for you. The following tasks are all performed on the Configure page.

Note: You must have the "Administrator" role in order to perform any of these organizational tasks. For more information, see "User Roles Page" on page 84

Table 4: Organizing clusters and nodes

To...	Do this...
Create a new folder	1. Select the folder under which you are creating the new folder. 2. Click [**New Folder**]. 3. Type the name of the folder and then click [**OK**].
Move a folder to another folder	1. Select the folder to be moved. 2. Click [**Move**]. 3. Select the destination folder and then click [**OK**]. When you move a folder, the content of that folder is moved as well.
Move a cluster to a folder	1. Select the cluster to move. 2. Click [**Move**]. 3. Select the destination folder and then click [**OK**].
Delete a folder	**Note:** A folder must be empty before it can be deleted. 1. Select the folder to delete. 2. Click [**Delete**]. 3. Click [**OK**] to confirm.
Delete a cluster	**Note:** Deleting a cluster only removes it from being monitor in Enterprise Service Manager. The actual cluster is untouched. You can add a deleted cluster back at any time. 1. Select the cluster to delete. 2. Click [**Delete**]. 3. Click [**OK**] to confirm.
Collapse or expand information	- Click the [-] or [+] markers next to a folder or cluster to collapse or expand information.

Adding a Gateway Cluster to Manage

Notes: Only users with the 'Administrator' role can add a Gateway Cluster. For more information about roles, see "User Roles Page" on page 84.

This section assumes that you have completed the initial setup, configuration, and licensing steps:

"Setting Up the Enterprise Service Manager" on page 14

"Enabling Remote Management on Nodes" on page 16

"Installing the Enterprise Service Manager License" on page 15

➢ *To add a Gateway Cluster to manage:*

1. Start the Enterprise Service Manager if it is not already running.
2. Select the [Manage Gateways] tab > **Configure** page. The enterprise tree is displayed, with a single top level folder defined by default. For more information, see "Configure Page" on page 61 and "Using the Enterprise Tree" on page 5.
3. (Optional) Rename the top level folder to your organization's name using the [**Edit**] button.
4. Add a Gateway cluster. A cluster is comprised of one or more nodes, with each node being a single Gateway. To do this:
   a. Select a folder in the enterprise tree (for example, the predefined top level folder).
   b. Click [**Add Cluster**]. The Add Gateway Cluster dialog box appears.

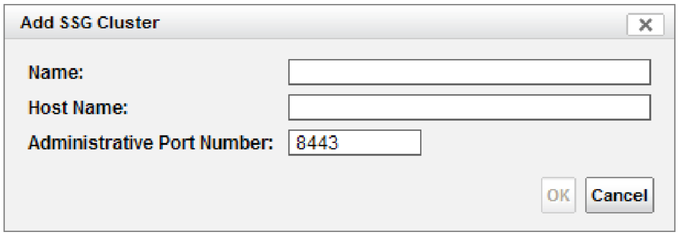


Figure 5: Add Gateway Cluster dialog

   c. Type a **Name** to identify the cluster within the enterprise tree. Any leading or trailing spaces in the name are automatically removed when the name is saved.
   d. Enter a fully qualified domain name of the Gateway cluster for the **Host Name** (do not include "https://" prefix).

e. Enter the **Administrative Port Number** if you are not using the default port '8443'. The administrative port number is defined using the *Manage Listen Ports* task in the Policy Manager. It is the port with the [**Enable Enterprise Manager access**] check box selected.

f. Click [**OK**] to add the cluster.

5. Once the cluster is added, you are prompted to establish trust between the cluster and the Enterprise Service Manager.

   - To establish trust now, click [**OK**] and then follow "Establishing Trust with a Cluster" on page 21
   - To establish trust later, click [**Cancel**]. If you do not establish trust, the Gateway cluster is still added to the enterprise tree, but the individual nodes are not displayed and many operations within Enterprise Service Manager for that cluster will be unavailable. **Tip:** When you are ready to establish trust for this cluster, click the icon next to the cluster name in the enterprise tree and then continue with "Establishing Trust with a Cluster" on page 21.

Establishing Trust with a Cluster

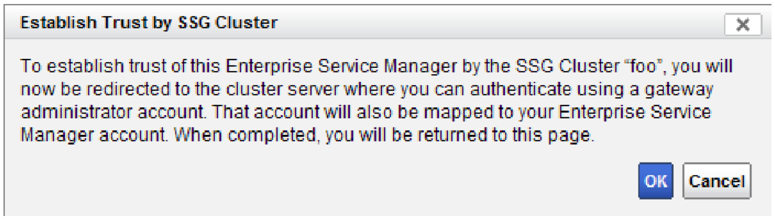
Before a Gateway cluster can be managed by the Enterprise Service Manager, trust must be established between the two. If trust is not established, most operations related to the cluster are not available and the nodes within that cluster are not displayed.

When you add a cluster to the Enterprise Service Manager, you are prompted to establish trust (see Figure 6). If you decline to establish trust, the cluster is still added but will be in an untrusted state. You can resume the trust process at any time by clicking the icon next to the cluster name in the enterprise tree.

Notes: When establishing trust with a cluster, the currently logged-in Enterprise Service Manager user is automatically mapped to the specified Gateway account. If any other Enterprise Service Manager user requires access to the cluster, that user must manually map his or her ESM account to the appropriate account on the Gateway. For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

➢ *To establish trust between the Enterprise Service Manager and a cluster:*

1. If you are adding a cluster, click **[OK**] at the dialog box in Figure 6. If not currently adding a cluster, click the icon to see Figure 6.

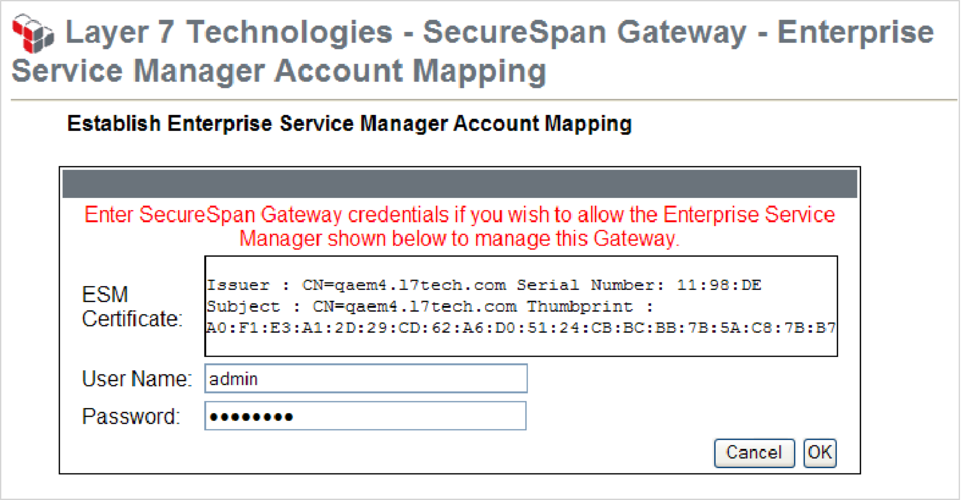


Establish Trust by SSG Cluster

To establish trust of this Enterprise Service Manager by the SSG Cluster "foo", you will now be redirected to the cluster server where you can authenticate using a gateway administrator account. That account will also be mapped to your Enterprise Service Manager account. When completed, you will be returned to this page.

Figure 6: Confirming that you wish to establish trust

2. Choose a client certificate when prompted. Figure 7 is displayed.



Layer 7 Technologies - SecureSpan Gateway - Enterprise Service Manager Account Mapping

Establish Enterprise Service Manager Account Mapping

Enter SecureSpan Gateway credentials if you wish to allow the Enterprise Service Manager shown below to manage this Gateway.

ESM Certificate:

```
Issuer : CN=qaem4.l7tech.com Serial Number: 11:98:DE
Subject : CN=qaem4.l7tech.com Thumbprint :
A0:F1:E3:A1:2D:29:CD:62:A6:D0:51:24:CB:BC:BB:7B:5A:C8:7B:B7
```

User Name: admin

Password: ••••••••

Figure 7: Establishing credentials with the Gateway

3. Examine the **ESM Certificate** details to ensure that everything is in order. This is the certificate that will be used to establish trust. The information is not editable.

4. Enter the **User Name** and **Password** of a Gateway user with an administrator role. **Tip:** You can remap to a different Gateway user later if necessary. For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

5. Click [**OK**] to complete the operation. You return to the "Configure Page" on page 61.

Tip: It may take a moment for the trust status icon to change from "untrusted" to "trusted" on the Configure page. You can click ⟳ to update the display more quickly. Once trust has been established, the Gateway nodes within the cluster are displayed in the enterprise tree, along with information about its current availability, Gateway version, and host information.

Mapping an ESM User to a Cluster User Account

To prove that an Enterprise Service Manager user is permitted to access a Gateway Cluster, it is necessary to map that user to a Gateway user account. This mapping process is very important for without it, there is very little that a user can do within Enterprise Service Manager (even if that user is assigned to an 'Administrator' role).

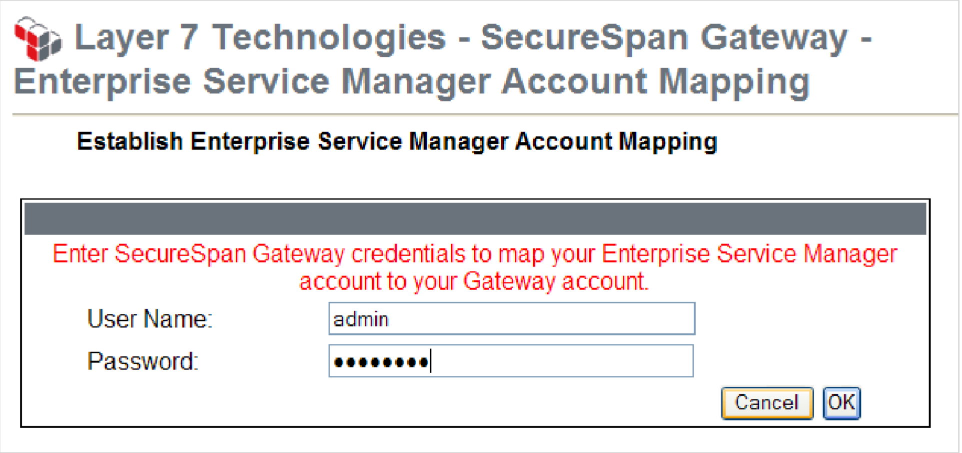
When a cluster is first added to Enterprise Service Manager, the user performing that action is automatically mapped as part of the trust process. All other users who require access to the cluster must be manually mapped.

Note: The role of the mapped Gateway user account determines what the ESM user can do with clusters within Enterprise Service Manager. For example, if the Gateway user has the *Manage Web Services* role, then the ESM user will be able to perform cluster-related tasks such as migrating policies. However if the Gateway user does not have a role that permits write access to the service or policy (for example, *View Service Metrics* or *Operator* roles), then the ESM user will not be permitted to manage the cluster and will be prevented from performing cluster-related tasks.

➢ *To manually map an ESM user to a Gateway cluster:*

1. Click the 🔑 or 🔑 icon next to the cluster name on the enterprise tree. You will see either the Map Access Account or Change Access Account confirmation dialog. **Note:** Trust must already be established before either icon can be clicked.

2. Click [**OK**] to confirm that you wish to map an account. Figure 8 is displayed.



Layer 7 Technologies - SecureSpan Gateway - Enterprise Service Manager Account Mapping

Establish Enterprise Service Manager Account Mapping

Enter SecureSpan Gateway credentials to map your Enterprise Service Manager account to your Gateway account.

User Name: admin

Password: ••••••••

Figure 8: Establishing credentials with the Gateway (mapping only)

3. In **User Name**, enter the user name of the Gateway account to map to.

Note: The error message "Password expired" will be displayed if you attempt to map to a Gateway user account with a pending password change. This will occur if the Gateway user was newly created, with the "Force Password Change" option in effect, and a password change has not yet been made.

4. In **Password**, enter the password of the Gateway user account.
5. Click [**OK**] to complete the operation. You return to the Configure page.

Removing Trust Relationship with a Cluster

When a cluster is added to the Enterprise Service Manager (ESM), a series of processes happen in the background to establish a trust relationship between that cluster and the ESM managing it. If you ever need to remove that trust relationship, you must reverse everything that was done.

Removing trust with a cluster is not a common procedure, but you may need to do it if:

- Establishing trust relationship failed for whatever reason and you want to start again with everything in its original state.
- A trusted cluster needs to be added back to the Enterprise Service Manager for whatever reason.
- The Enterprise Service Manager is to stop managing a cluster and you need to remove all traces of the trust relationship.

Note: Removing trust relationship requires access to all of these systems: Enterprise Service Manager, Policy Manager, and the Gateway cluster. This procedure should be performed by someone with administrator rights to all the systems.

➤ *To remove the trust relationship with a cluster:*

1. Do the following in the Enterprise Service Manager:
   a. Open the Configure page.
   b. From the enterprise tree, select the cluster to remove and then click [**Delete**]. Confirm the deletion.
2. Do the following on a Gateway node belonging to the cluster you are removing:
   a. Log in as user '**ssgconfig**'. This displays the Gateway main menu.

      Reference: "Accessing the Gateway Configuration Interface" in the *CA API Gateway Installation and Maintenance Manual (Appliance Edition)*

b. On the Gateway main menu, select **5** (Display Remote Management configuration menu).

c. On the Remote Management configuration menu, select **5** (Delete Trusted Certificate CN=*cluster.company.com*). Enter **yes** to confirm. Exit the configuration menu.

Reference: "Configuring the Gateway for Remote Access" in the *CA API Gateway Installation and Maintenance Manual (Appliance Edition)*

3. Do the following in the Policy Manager:

a. Start the *Manage ESM User Mappings* task.

Reference: Managing ESM User Mappings in the *CA API Gateway - Policy Manager User Manual*

b. Select the ESM system under **Trusted Enterprise Service Managers** and then click [**Remove Registration**]. Click [**OK**] to confirm. Close the form.

c. Start the *Manage Certificates* task.

Reference: Managing Certificates in the CA API Gateway - Policy Manager User Manual

d. Select the ESM certificate used to establish trust with the Enterprise Service Manager. To confirm that you've selected the right one, click [**Properties**] and carefully examine the certificate's properties.

e. If everything is in order, dismiss the properties, then click [**Remove**]. Confirm this action by clicking [**Remove**] on the confirmation dialog. Close the form.

Trust between the Enterprise Service Manager and the Gateway cluster is now completely removed and the two entities have no relationship to each other.

Chapter Four: Configuring Monitoring

Configuring Monitored Properties

The Monitor page can display a large number of statistics about the clusters and nodes currently managed by Enterprise Service Manager. By default, no property is monitored when a cluster is added and no statistics will appear in the Monitored Properties grid. You can choose which properties to monitor and then configure them accordingly.

> **Note:** Only users with the 'Administrator' role can configure monitored properties. It is not necessary to be mapped to each Gateway cluster in order to configure monitoring.

➤ *To configure a property to monitor:*

1. From the [Manage Gateways] tab, open the Monitor page.
2. In the Monitored Properties grid in the Enterprise Gateways section, move the mouse pointer over the cell containing the property you wish to configure. This cell can be either unconfigured (Figure 9) or currently configured to display statistics (Figure 10).

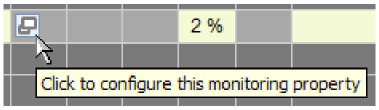


Figure 9: Configuring a property not yet set up

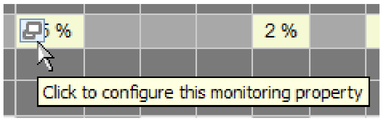
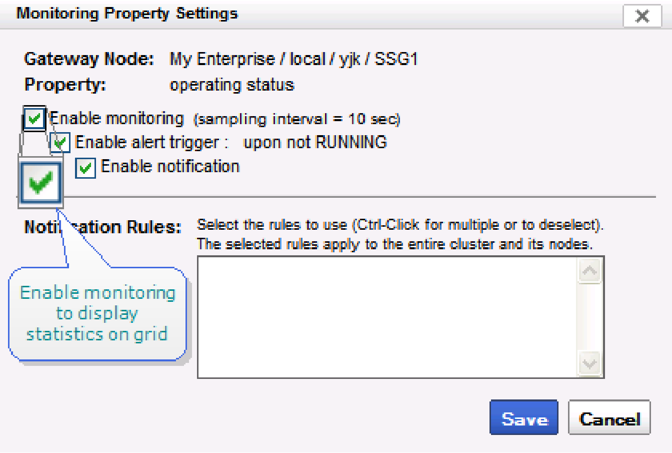


Figure 10: Configuring a property currently being monitored

3. Click the 🗗 icon to view the Monitoring Property Settings dialog box (Figure 11).



Monitoring Property Settings

Gateway Node: My Enterprise / local / yjk / SSG1

Property: operating status

☑ Enable monitoring (sampling interval = 10 sec)

☑ Enable alert trigger : upon not RUNNING

☑ Enable notification

Noti ation Rules: Select the rules to use (Ctrl-Click for multiple or to deselect). The selected rules apply to the entire cluster and its nodes.

Figure 11: Monitoring Property Settings dialog box

4. Configure the settings for the property.

Table 5: Monitoring Property Settings

Element	Description
Gateway Node	Displays the full path of the node selected for monitoring in the format: *[root folder] / [subfolder(s)] / [cluster] / [node]*
Property	The type of property being configured.
Enable monitoring	Select this check box to enable monitoring and display statistics in the grid. Clear this check box to disable monitoring and suppress the statistics. The sampling interval indicates how often the statistic is refreshed. The value shown is from the "Monitoring Setup" section of the Monitor page. **Note:** By default, monitoring is not enabled for any property when a cluster is first added to the Enterprise Service Manager. You must manually enable the properties you wish to monitor.
Enable alert trigger	Select this check box to have the following occur when a property exceeds the trigger threshold: • The property exceeding the trigger is highlighted in red text with a yellow background on the grid. Clear this check box to not use a trigger threshold: • No property is highlighted in the grid, regardless of the values recorded • No notifications are sent out, regardless of the [Disable all notifications] check box in the "Notifications and Audits" settings.
trigger threshold	Enter the threshold value at which an alert is triggered. Either use the default value shown from the "Monitoring Setup" section of the Monitor page, or enter another value specific to this property. The threshold value must be an integer. The ⚠ icon warns you if the value is invalid.

Element	Description
	The trigger threshold value applies only if **[Enable alert trigger**] is selected.
Use Default	Click this to restore the trigger threshold to the default value set in the "Monitoring Setup" section of the Monitor page.
Enable notifications	Select this check box to be notified when an alert is triggered. Clear this check box to suppress notifications for this property. Any rules selected will be ignored. Notifications are possible only when the [**Enable alert trigger**] check box is selected. **Note:** The [**Enable notifications**] check box is overridden if notifications are disabled globally using the [**Disable all notifications**] check box in the "Monitoring Setup" section of the Monitor page.
Notification rules	Select one or more rule to use if [**Enable notifications**] is set. These notification rules are defined in the "Monitoring Setup" section of the Monitor page. You can select multiple rules to send out multiple notifications. At least one rule should be selected if notifications are enabled. **Note:** The selected rules apply to the entire cluster and all of its nodes (in other words, you cannot select one rule for a node and a different rule for another node).If no rule is selected, then no notifications are sent out. .

5. Click [**Save**]. The dialog box closes and the new settings take effect immediately.

Creating Notification Rules for Monitoring

You can configure the Enterprise Service Manager to notify you when a monitored property exceeds a predefined threshold. For these notifications to occur, ensure the following has been done:

- One or more notification rules have been defined in the "Monitoring Setup" section of the Monitor page
- Monitoring has been enabled for the relevant properties and notification rules have been chosen. For more information, see "Chapter Four: Configuring Monitoring" on page 27.
- Notifications have *not* been disabled globally (see "Notification Rules" on the Monitor page).

You can create the following types of notifications:

- **E-mail**

A pre-configured email message will be sent when an alert is triggered. This works similar to the *Send Email Alert Assertion* in the Policy Manager.

- **SNMP Trap**

  A Simple Network Management Protocol (SNMP) trap will be broadcast to a predefined network address when an alert is triggered. This works similar to the *Send SNMP Trap Assertion* in the Policy Manager.

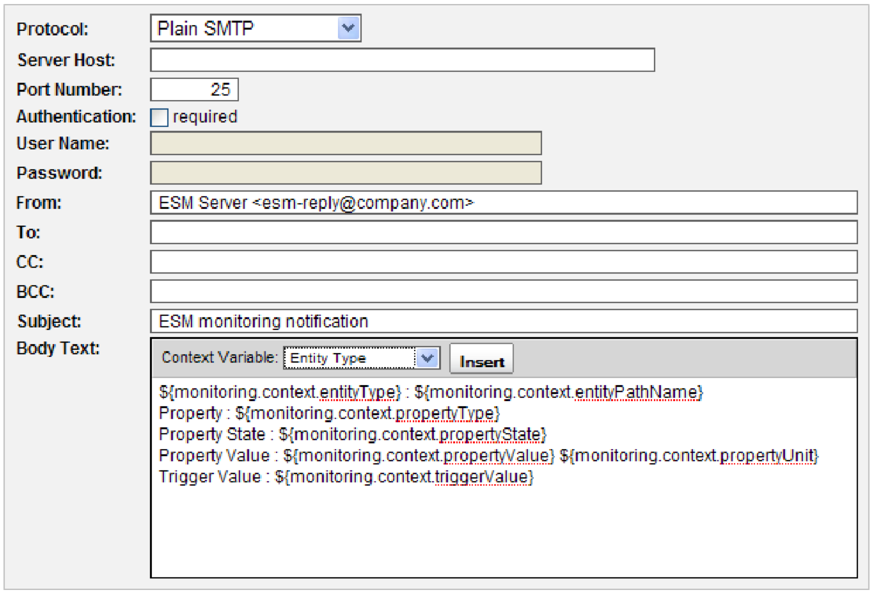
- **HTTP Request**

  An HTTP request will be sent to a predefined URL when an alert is triggered. The HTTP method can be GET or POST.

➢ *To create a notification rule:*

1. Open the Monitor page and expand the Monitoring Setup section.
2. Under "Notification Rules", click [**New**]. The New Notification Rule dialog box appears.
3. Enter a **Name** for the rule. Type a descriptive name that explains the purpose of the rule. Keep in mind that the rule can be used for any monitored property.
4. Select the rule **Type** from the drop-down list.
5. Complete the remaining fields for the type of rule chosen:

E-mail



Protocol:	Plain SMTP
Server Host:	
Port Number:	25
Authentication:	□ required
User Name:	
Password:	
From:	ESM Server <esm-reply@company.com>
To:	
CC:	
BCC:	
Subject:	ESM monitoring notification
Body Text:	Context Variable: Entity Type [Insert]

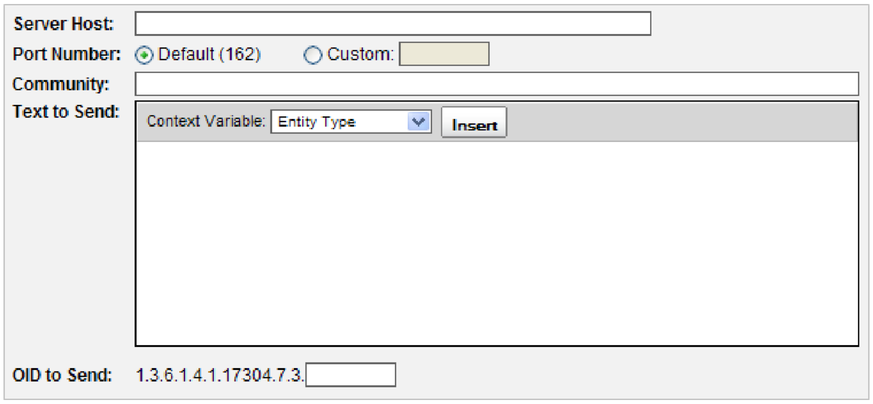
```
${monitoring.context.entityType} : ${monitoring.context.entityPathName}
Property : ${monitoring.context.propertyType}
Property State : ${monitoring.context.propertyState}
Property Value : ${monitoring.context.propertyValue} ${monitoring.context.propertyUnit}
Trigger Value : ${monitoring.context.triggerValue}
```

Figure 12: E-mail notifications

Table 6: Fields for E-mail notifications

Field	Description
Protocol	Select the email protocol to use: **Plain SMTP** (default), **SMTP over SSL**, or **SMTP with STARTTLS**. The default setting should work in most instances. Consult your system administrator if you are unsure of the protocol.
Server Host	Enter the hostname of the outgoing mail server to use.
Port Number	The port used by the default mail server is displayed. Modify if necessary.
Authentication	Select this check box if a user name and password is required to log onto the email server.
User Name / Password	If authentication is required, enter the **Use Name** and **Password**.
From	Enter a response email address. The dummy address "esm-reply@company.com" is inserted by default. **Tip:** Be sure that the email address entered here is not blocked by your corporate junk mail filter.
To	Optionally enter the email addresses of the recipients who will receive the alert. Separate multiple addresses with a comma. **Tip:** You can exclude the "To" recipients if you intend to add everyone as "BCC" recipients.
CC	Optionally enter email addresses for CC (carbon copy) recipients. Separate multiple addresses with a comma.
BCC	Optionally enter email addresses for BCC (blind carbon copy) recipients. Separate multiple addresses with a comma. Recipients in the 'To' and 'CC' lists will not see the recipients in the 'BCC' list.
Subject	Enter a subject line describing the alert email. The default subject "ESM monitoring notification" is offered.
Body Text	Create the body of the e-mail by adding text and context variables. To add a variable, select it from the drop-down list and then click [**Insert**]. These variables will be replaced with the appropriate values at the time of emailing. A sample email body text has been provided. For more information about the variables, see "Context Variables for Notifications" below.

SNMP Trap



Server Host:

Port Number: ● Default (162) ○ Custom:

Community:

Text to Send: Context Variable: Entity Type

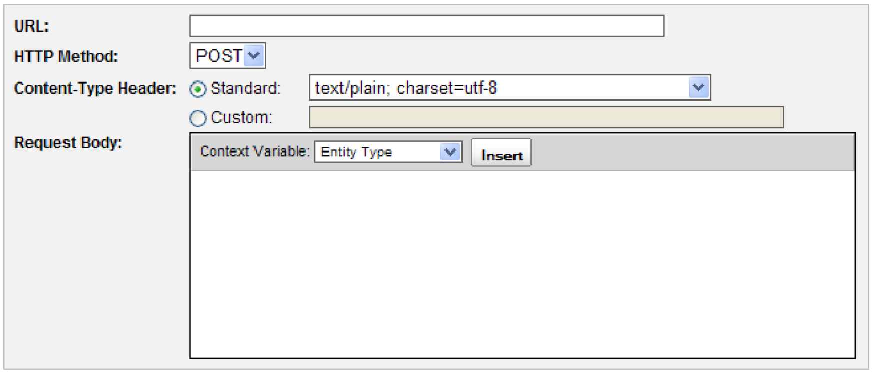
OID to Send: 1.3.6.1.4.1.17304.7.3.

Figure 13: SNMP Trap notifications

Table 7: Fields for SNMP Trap notifications

Field	Description
Server Host	Enter the network address that will be receiving the SNMP alert.
Port Number	The default SNMP trap destination port is set to "162". This is the IANA (Internet Assigned Numbers Authority) standard SNMP trap port. To configure a different port, select [**Custom**] and enter an alternate port number.
Community	Enter the SNMP community that should be used by the SNMP trap.
Text to Send	Create the body of the SNMP broadcast by adding text and context variables. To add a variable, select it from the drop-down list and then click [**Insert**]. These variables will be replaced with the appropriate values at the time of broadcast. For more information about the variables, see "Context Variables for Notifications" below.
OID to Send	Complete the OID (Object Identifier) of the SNMP trap. Must be greater than 0. The OID is used for identification purposes on a network.

HTTP Request



URL:

HTTP Method: POST

Content-Type Header: ● Standard: text/plain; charset=utf-8
○ Custom:

Request Body: Context Variable: Entity Type

Figure 14: HTTP Request notifications

Table 8: Fields for HTTP Request notifications

Field	Description
URL	Enter the URL that will be receiving the HTTP request.
HTTP Method	Select the HTTP method to use: GET or POST.
Content-Type Header	Specify the content-type header to use. Choose either a **Standard** header from drop-down list or enter a **Custom** header. **Note:** The Content-Type is only used for the 'POST' HTTP method.
Request Body	Create the body of the HTTP request by adding text and context variables. To add a variable, select it from the drop-down list and then click [**Insert**]. These variables will be replaced with the appropriate values at the time of sending request. For more information about the variables, see "Context Variables for Notifications" below.

6. Click [**Save**] to save the notification rule. This rule will appear under "Notification Rules" in the Monitoring Setup section and in the Monitor Property Settings dialog box.

Context Variables for Notifications

For notification alerts to be useful, you should add context variables to the body of the notification. These variables will be replaced with the actual values at run time. The following variables are available:

Table 9: Context Variables for notifications

Variable	Description
Entity Type	Identifies whether the alert pertains to "NODE", "HOST', or "CLUSTER". **Syntax:** *${monitoring.context.entityType}*
Entity Path & Name	Lists the identifier of the entity. **Syntax:** *${monitoring.context.entityPathName}*
Property Type	Identifies the monitored property. The list of property types is shown in the "Monitoring Setup" section of the Monitor page. **Syntax:** *${monitoring.context.propertyType}*
Property Value	The value of the property when it triggered the notification (for example, "52" for CPU temperature or "BAD" for RAID status). **Syntax:** *${monitoring.context.propertyValue}*
Property Unit	The measurement unit (for example, "deg C" for CPU temperature,

Variable	Description
	blank for RAID status). **Syntax:** *${monitoring.context.propertyUnit}*
Property State	Identifies whether the property is in a "normal" or "alert" state. **Syntax:** *${monitoring.context.propertyState}*
Trigger Value	The trigger threshold value set for the property. The default thresholds are defined in the Monitoring Setup" section of the Monitor page, but may be overridden in the monitoring settings of the property. **Syntax:** *${monitoring.context.triggerValue}*

Chapter Five: Migrating Services and Policies

Migrating a Service or Policy

Enterprise Service Manager allows you to copy (migrate) policies from one Gateway cluster to another, assuming you are managing more than one cluster. Migrating is a quick and convenient way to copy a policy and all its dependencies to a different Gateway, so that the policy is ready to run on the target system.

For more information about migrating, see "Migration Page" on page 63.

Notes: (1) If the target cluster is rebooted while migration is in process, the Migration page may be temporarily disabled. If this happens, simply refresh the browser window to restore normal operation. (2) When migrating a policy containing encapsulated assertions, ensure that the encapsulated assertions are first imported into the target Gateway. For more information, see "Managing Encapsulated Assertions" in the *CA API Gateway - Policy Manager User Manual*.

IMPORTANT: Migration is not compatible with services and policies that have been previously migrated outside of the ESM, such as via export/import using the Policy Manager or via the Gateway Management Service.

➤ *To migrate a policy:*

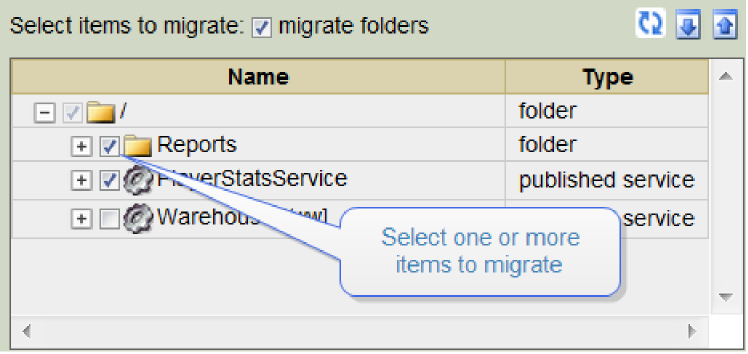
1. Open the Migration page.
2. If there are settings from a previous migration that you want to use, select it from the drop-down list and then click [**Reload Migration**]. *Reference:*"Reload Migration" on page 67

   Offline Note: If you wish to migrate from an offline cluster, ensure that an archive from that cluster has been uploaded, then select that archive from the drop-down list. For information on downloading and uploading an archive, see "History Page" on page 72. It is possible to map dependencies for an offline cluster after it has been uploaded.

3. In the Source panel, select the source Gateway cluster from the enterprise tree. *Reference:*"Source/Destination Clusters" on page 68
4. To preserve the folder structure in the source cluster after migration, select the [**migrate folders**] check box. If you leave this check box unselected, everything will be "flattened" after migration (i.e., no folders and all entities will be at the same

level).

5. Select the items to migrate using the check boxes. *Reference:* "Items to Migrate/Destination Folder" on page 68



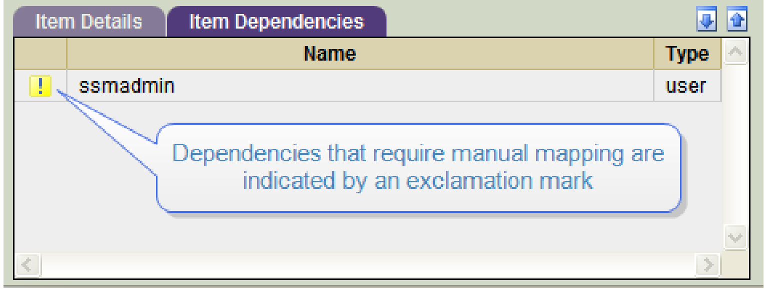
Select items to migrate: ☑ migrate folders

Name	Type
⊟ ☑ /	folder
⊞ ☑ Reports	folder
⊞ ☑ F...erStatsService	published service
⊞ □ Warehou...	...service

Select one or more items to migrate

Figure 15: Selecting the items to migrate

6. Optionally click a child item to view more information under the [Item Details] tab or its dependencies under the [Item Dependencies] tab. *Reference:* "Understanding Dependencies" on page 65 and "Item Details/Item Dependencies" on page 70



	Name	Type
!	ssmadmin	user

Dependencies that require manual mapping are indicated by an exclamation mark

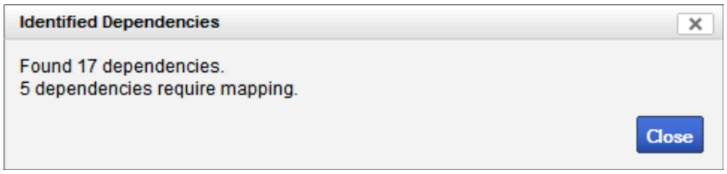
Figure 16: Viewing item dependencies

7. In the Destination panel, select the Gateway cluster and folder which will receive the entities. Make sure the destination cluster is different from the source cluster. *Reference:*"Source/Destination Clusters" on page 68

Offline Note: The Destination panel does not display offline clusters. If you need to migrate to an offline cluster, select the [**offline destination**] check box. This hides the destination clusters and folder tree in the panel and replaces them with "Offline destination". Note that you cannot map dependencies when migrating to an offline destination.

8. Set the [**enable new services**] and [**overwrite existing items**] check boxes required. *Reference:*"Items to Migrate/Destination Folder" on page 68

9. Once a source and destination are selected, click ! to see if any dependencies require manual intervention. You will see a summary similar to the following:



Found 17 dependencies.
5 dependencies require mapping.

Figure 17: Identified Dependencies

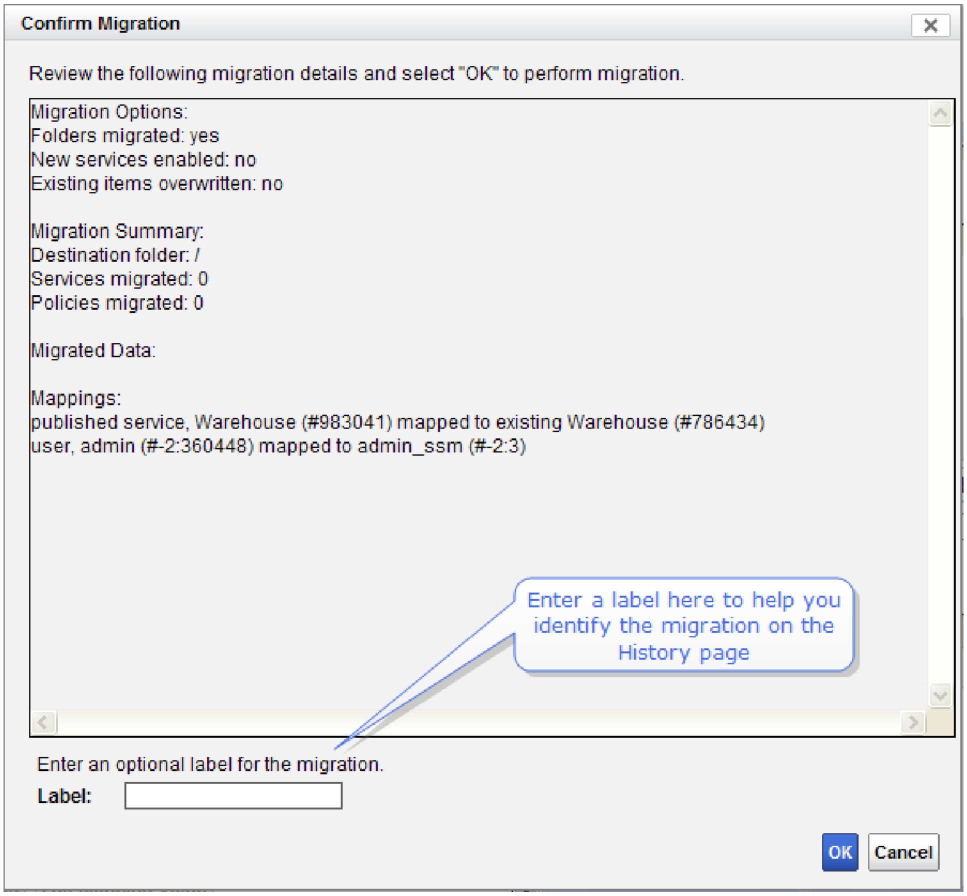
10. If dependencies that require mapping were identified, map them now. *Reference:*"Dependencies Mapping" on page 71

    If dependencies were found, but none which require mapping, optionally review the dependency list and decide whether any of these dependencies should still be mapped. *Reference:*"Dependencies Mapping" on page 71

    If no dependencies were found, you may begin the migration now.

11. Click ➡ to begin the migration. A migration confirmation dialog is displayed. Note that migration has NOT yet occurred at this point.

Tip: If the ➡ button is not enabled, it may be caused by either of the following: (1) no destination folder has been selected, or (2) the destination is the same as the source.



Review the following migration details and select "OK" to perform migration.

```
Migration Options:
Folders migrated: yes
New services enabled: no
Existing items overwritten: no

Migration Summary:
Destination folder: /
Services migrated: 0
Policies migrated: 0

Migrated Data:

Mappings:
published service, Warehouse (#983041) mapped to existing Warehouse (#786434)
user, admin (#-2:360448) mapped to admin_ssm (#-2:3)
```

Enter a label here to help you identify the migration on the History page

Enter an optional label for the migration.

Label:

Figure 18: Confirm Migration dialog box

12. Examine the confirmation carefully. If the results are satisfactory:

    a. (Optional) Enter a label that describes the migration. This label makes it easier to identify the migration on the History page. It also makes this migration available under "Reload Migration" on page 67. **Tip:** If you do not enter a label now, you can still add or change the label later on the History page.

    b. Click [**OK**] to proceed with the migration.

Offline Note: If migrating to an offline destination, no migration is actually performed. Instead, the migration archive is available for download for use on another Enterprise Service Manager. For information on downloading an archive, see "History Page" on page 72.

Migration Summary

To see a summary of all the policy migrations and mappings, open the History page under the [Manage Policies] tab.

Viewing Migration History

To see a summary of all the service/policy migrations, open the History page under the [Manage Policies] tab.

➢ *To view a migration record:*

1. In the Migration Selection section, specify a date range to filter the list of migrations. Click the **Start Date** and **End Date** fields and choose from the calendar control.
2. Click [**Select**] to display all the migrations that were performed during that date range.
3. From the list of migrations, select the migration to view. The details are displayed in the Migration Summary section.

➢ *To delete a migration record:*

If you do not need to retain details for a migration, you can delete the record from the list.

Tip: The migration record details can be copied and pasted to another application.

1. Follow the steps under "To view a migration record" to locate the record to remove.
2. Click [**Delete**]. The record is deleted.

➢ *To rename a migration record:*

When a migration is performed, it is identified only by date and source/destination cluster. You can add a name to help identify a particular record.

1. Follow the steps under "To view a migration record" to locate the record to rename.
2. Click [**Rename**].
3. Type a name and then click [**OK**]. The list is updated with the new name.

Chapter Six: Working with Users

Creating a New User Account

Note: Only users with the 'Administrator' role can create a user account.

➢ *To add a new user to the Enterprise Service Manager:*

1. From the [Settings] tab, open the User Accounts page.
2. Click [**New**]. The Create User section is displayed.
3. Enter the following required user information:
   - **User Name:** The user name can be 3-128 characters and cannot contain these characters: # , + " \ < > ;

     The User Name cannot be changed once entered.
   - **Password:** The password must be between 6-32 characters and may include letters, numbers, or symbols.
   - **Confirm Password:** Retype the password to confirm
4. Optionally enter these user details; you can add these later by modifying the account:
   - **Email:** The user's email address, up to 128 characters.
   - **Surname:** The user's last name, up to 32 characters.
   - **Given Name:** The user's first name, up to 32 characters.
   - **Description:** A description or note about the user, up to 255 characters.
5. Click [**Apply**]. The new account is available immediately.

After a new user account is created, the following should be done:

- The new user should log in and then map himself or herself to a Gateway cluster. This step is very important, because it is the privileges of the mapped Gateway account that define what the ESM user can do with the cluster. (For example, a mapping to a Gateway *Administrator* allows unrestricted access to the cluster; however, a mapping to a Gateway *Operator* restricts the ESM user from performing cluster-related tasks such as migrating a service or policy.)

For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

- The ESM Administrator can optionally assign the new user to a role. A role determines whether a user can perform node-based operations on a specific cluster (such as start/stop a node, or monitor a node). Without a role, a user can still log into the Enterprise Service Manager and perform cluster-based tasks, provided the user has mapped an account from the cluster.

  For more information, see "Managing User Roles" on page 43

Editing a User Account

Note: Only users with the 'Administrator' role can edit a user account.

➤ *To modify an existing user in the Enterprise Service Manager:*

1. From the [Settings] tab, open the User Accounts page.
2. From the list of users, select the user to modify. The optional user details are displayed.
3. Enter or edit the user details as necessary. For a description of each field, see "User Accounts Page" on page 83.
4. Click [**Apply**] to save the changes.

Deleting a User Account

Note: Only users with a role of 'Administrator' can delete a user account.

➤ *To delete an existing user in the Enterprise Service Manager:*

1. From the [Settings] tab, open the User Accounts page.
2. From the list of users, select the user to remove.
3. Click [**Delete**]. The user is removed from the list. If the user is currently logged in, that user will be denied access as soon as he performs an action that requires communication with the Enterprise Service Manager server.

Managing User Roles

You add and remove users from roles using the User Roles page.

The *Administrator* role is predefined with a single user. The *Manage Gateway Cluster Nodes* roles are automatically created when a Gateway cluster is added to the enterprise tree, but no one is assigned to these roles by default. It is the responsibility of Administrators to add users to the appropriate roles.

Note: Adding users to roles is optional. Of greater importance is ensuring that every user maps himself or herself to the appropriate user account on the Gateway cluster. It is this mapping that determines most of a user's access privileges within the Enterprise Service Manager. For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

Table 10: Working with roles

To...	Do this...
Add a user to a role	1. Select a role from the list. The Role Management section is displayed. Users currently belonging to that role are listed under "Assigned Users". 2. Under "Unassigned Users", locate the user to add. 3. Click [**Assign**]. The user's name is added to the "Assigned Users" list.
Remove a user from a role	1. Select a role from the list. The Role Management section is displayed. Users currently belonging to that role are listed under "Assigned Users". 2. Under "Assigned Users", select the user to remove. 3. Click [**Unassign**]. The user's name is moved back to the "Unassigned Users" list.
Quickly locate a user in a list	To quickly locate a user when the list is long, you can try either of the following: • Click the "User Name" column heading to sort the list in ascending/descending alphabetical order. • Search by user name: • "**contains**" will locate the text anywhere in the name—for example, searching for "smit" will locate "JSmith" and "ASmithe". • "**starts with**" will match only the beginning characters of the user name—for example, "js" will locate "JSmith" and "JSimpson".

Adding a User to a Role

Note: Only users with the 'Administrator' role can add another user to a role.

Adding users to a role is optional. You will do this if you wish to grant Administrator privileges to another user, or if you want to allow a user to be able to start or stop a node within a cluster.

For more information about roles, see "User Roles Page" on page 84

Tip: Users without a role can still perform cluster-specific tasks such as migrating policies if they have been mapped to a Gateway user with sufficient privileges. For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

➢ *To add a user to a role:*

1. Under the [Settings] tab, open the User Roles page.
2. In the **Select a Role** list, select the role to which you are adding the user. The **Role Description** is displayed, as well as existing assigned users under **Role Management**.
3. In the **Unassigned Users** list, select the user to add.
   - If the list of users is not long, simply browse the list to locate the user.
   - If the list is lengthy, enter some search criteria to narrow down the list. You can search based on the first few characters of the user name ("**starts with**") or any part of the user name ("**contains**"). Searching is case insensitive. **Note:** Only the User Name is searched, not the Surname or Given Name. Clearing the search field returns all users.
4. Click [**Assign**]. The user name is moved from the "Unassigned Users" list to the "Assigned Users" list. The new privileges take effect the next time the user logs into the system. If the user is currently logged in, the privileges are available as soon as the user performs an action that connects to the database (for example, switches pages or tabs, refreshes a list).

Removing a User from a Role

You will remove a user from a role if you wish to rescind access to a specific cluster or if you need to rescind 'Administrator' privileges.

Note: Even after removing a user from all roles, that user will still be able to log in. To prevent a user from logging into the Enterprise Service Manager, see "Deleting a User Account" on page 42

For more information on roles, see "User Roles Page" on page 84

➢ *To remove a user from a role:*

1. Under the [Settings] tab, open the User Roles page.
2. In the **Select a Role** list, select the role from which you are removing the user.
3. In the **Assigned Users** list, select the user to remove.
   - If the list of users is not long, simply browse the list to locate the user.
   - If the list is lengthy, enter some search criteria to narrow down the list. You can search based on the first few characters of the user name ("**starts with**") or any part of the user name ("**contains**"). Searching is case insensitive. **Note:** Only the User Name is searched, not the Surname or Given Name. Clearing the search field returns all users.
4. Click [**Unassign**]. The user name is moved from the "Assigned Users" list to the "Unassigned Users" list. The privileges will be removed the next time the user logs into the system. If the user is currently logged in, the privileges are removed as soon as the user performs an action that connects to the database (for example, switches pages or tabs, refreshes a list).

Resetting a Password

An Administrator can reset the password for a user if that user has forgotten it.

Note: Only users with a role of 'Administrator' can reset a password.

➢ *To reset a user password:*

1. From the Settings tab, open the User Accounts page.
2. From the list of users, select the user whose password is to be reset.

3. In the Reset Password section, enter a new password and then retype to confirm.
4. Click [**Reset**] to reset the password. The new password is effective immediately.

Chapter Seven: Generating Reports

Reports are created from the [Reports] tab and can be saved in either PDF or HTML formats.

For information on viewing or saving a generated report, see "Managing Reports" on page 51. For information on the report columns, see "Explanation of Report Columns" on page 52.

Note: The reporting mechanism within Enterprise Service Manager operates on hourly and daily metric. This means that all service activity that occurred within the hour will not appear on any reports until the next hour. *Example:* A service is requested 100 times between 1:00 and 1:30. A report run at 1:45 will not show these 100 requests, but a report run after 2:00 will include them.

➢*To create a new report:*

Tip: You can save time by loading previously saved settings. For details on this and all the reporting fields, see "[Reports] Tab" on page 74.

1. From the **Report Type** drop-down list, select the type of report to generate: **Performance Statistics** or **Usage Report**.
2. For **Entity Selection**, select either **Published Service** or **Operation** to report at the service or operation level.
3. In the **Gateway Clusters** list, select the cluster to be reported on. The list of published services or operations appears in the **Content** list to the right.

   Note: A separate report will be generated for each cluster you select.
4. Select the check box next to each service or operation you wish to include in the report. You must make at least one selection. **Tip:** Selecting a folder automatically selects or deselects all items within it.
5. Click [**Add Checked Published Services**] or **[Add Checked Operations**] to select the entities to report on. The selected services or operations are added to the list below. **Tip:** To remove an entity from the list, click ☒ next to the cluster name.

6. Select a **Time Zone** for the report from the drop-down list, if the default time zone shown is not applicable to the cluster you are reporting against.

7. Specify the **Time Period** for the report:

   - *Relevant time period:* Select the **Last**... option to specify a relative time period. Enter the time period and then select the time unit (for example, 3 hours/days/weeks/months).
   - *Absolute time period:* Select the **From**... option to include data between a specified date and time. For the date, click inside the field and choose the date from the popup calendar. For the time, select the time from the drop-down list.

8. Specify the **Time Interval** for the report. By default, a Summary Report is created (no time intervals). To create an interval report, select **Interval** and then specify an interval.

9. *This step is optional for Performance Statistics reports but required for Usage Reports.* You can group by report keys, which can also be filtered by adding a key value filter. For more information, see "Grouping by Message Context Key" on page 49.

   Note: For groupings to work in your report, the published services being reported on must contain one or more *Capture Identity of Requestor Assertions* that have been configured to collect the message context keys that you specify here. Only keys that exist on the cluster are shown. For more information, see *Capture Identity of Requestor Assertion* in the *CA API Gateway - Policy Manager Authoring Manual*.

10. A summary chart is included by default at the start of each report. To exclude this chart, clear the **Include Summary Chart** check box.

11. Enter a **Report Name** to briefly describe the purpose of the report. You must enter a report name before you can generate the report.

12. Click **Generate Report** to submit the report. If this button is unavailable, verify that all the parameters have been set correctly, including entering a Report Name and adding the selected entities for reporting (see step 5).

13. When the report is submitted, click [**OK**] to dismiss the confirmation dialog.

    Tip: Once a report has been submitted, processing continues in the background. You do not need to wait or remain logged in for the report to complete. Once it has finished, it will appear in the list in the Generated Reports section when you click 🔄 next to “Generated Reports”. If the report is not finished yet, its state will be "Submitted" . For more information, see the "Generated Reports" section on the "[Reports] Tab" on page 74.

Grouping by Message Context Key

A report can be grouped by message context keys. Adding a grouping by some message content (for example, IP address or authenticated user) will organize report data by those key values (IP address, authenticated user, etc). Furthermore, you can specify a key value filter to further constrain the output.

Grouping by message context key is optional when creating a Performance Statistics Report, but required for Usage Reports.

The following is an example of grouping by message context key:

- A service policy contains one or more *Capture Identity of Requestor Assertions*.
- This assertion captures identifying information about a requestor (for example, a customer). By default, the requestor's IP address and authenticated user are recorded, but custom mappings can also be created.
- When generating a report in Enterprise Service Manager, you decide to group by the AUTH_USER (authenticated user) Message Context Key, but do not specify a Key Value Filter. This will result in a separate breakdown for each authenticated user. For example, if the service was requested by Bob, Mary, and Clara, there will be three grouping sections in the report, one each for Bob, Mary, and Clara.
- If you only wish to see statistics for user 'Clara', you do this by entering her name in the Key Value Filter field. The resulting report will only include Clara's statistics and exclude those from Bob and Mary.

Note: For groupings to work in your report, the published services being reported on must contain one or more *Capture Identity of Requestor Assertions* that have been configured to collect the message context keys that you specify here. For more information, see *Capture Identity of Requestor Assertions in the CA API Gateway - Policy Manager Authoring Manual*.

➢ *To create a grouping by message context key:*

1. Follow the steps under "Chapter Seven: Generating Reports" on page 47 to create a new report.
2. In the Grouping step, click [**Add Grouping by Message Context Key**]. A row is added to the table.
3. In the **Gateway Cluster** column, select the cluster to use.
4. In the **Message Context Key** column, select the context key to use. You can choose from either of the two predefined system context keys plus any custom mapping keys that may have been defined:

- AUTH_USER: A grouping will be created for each authenticated user ID. If a Key Value Filter is specified in the next step, then only the groupings that match the filter will be included in the report.
- IP_ADDRESS: A grouping will be created for each requestor's IP address. If a Key Value Filter is specified in the next step, then only the groupings that match the filter will be included in the report.

Tip: If you have defined a custom mapping key but it is not visible in this list, the service containing the *Capture Identity of Requestor Assertion* may not have been consumed yet. After consumption, it may take a minute or more for the service metrics to become available (assuming metrics have not been disabled using the *serviceMetrics.enabled* cluster property on a Gateway).

Note: The drop-down list shows all the keys in the Gateway cluster—this list is not filtered by the selected services/operations. Be aware that the presence of a key: (1) does not imply that the selected services or operations have the required *Capture Identity of Requestor Assertion*, or (2) if the assertion is present, there is no guarantee that it includes the keys listed in the drop-down list. If you select a Message Context Key for which no values were collected, the report will display *"There were no service metrics for the criteria chosen."*.

5. To include only a specific group or groups, enter a **Key Value Filter**. The value must match the value in the database exactly and is case sensitive. For greater flexibility, you can use the '*' wildcard character. Leave the Key Value Filter field blank to create a grouping for every message context value received.

Note: For the AUTH_USER context key, if you want to filter the exact match for a key value, specify the authenticated user in the format 'username [Identity Provider Name]' (space after username; square brackets required) or enter the user name with a wildcard (for example, 'user1*').

Tip: The same key can be added multiple times, each with a different key value constraint. This allows more than one filter value to be entered for a key. When a key is added more than once, the filter values use AND logic. For example, an authenticated user is added with value 'admin*' and an IP address is added with '192.168.1.*'. This will only retrieve data for users with names beginning with 'admin' (admin, administrator, etc.) from IP addresses beginning with 192.168.1.*.

Examples:

- Message Context Key = AUTH_USER, no Key Value Filter added: This will create a grouping for every user ID who submitted a request during the time period specified in the report parameters.

- Message Context Key = AUTH_USER, Key Value Filter = JSMITH: This will create a grouping showing the performance statistics or usage data for user 'JSMITH' for the specified time period.
- Message Context Key = IP_ADDRESS, Key Value Filter = 192.168*: This will create a grouping for every IP address that begins with "192.168" for the specified time period.

Note: *Capture Identity of Requestor Assertions* with values that evaluate to either empty strings or spaces at runtime will result in a single 'blank' category in report output. A context key can have an empty string as its value under the following conditions: (1) either nothing or spaces is entered, or (2) a nonexistent context variable is used, or (3) a context variable that evaluates to an empty string or spaces.

Managing Reports

The Generated Reports section on the [Reports] tab shows the reports that have been submitted and their current status:

- SUBMITTED: The report has been submitted for processing and is either awaiting processing or currently being processed.
- COMPLETED: The report is finished and can be viewed or downloaded.
- FAILED: The report could not be completed. The Status Detail column explains the error.

Choose an action from the table below.

Tip: If you do not see your report, click 🔄 next to the "Generated Reports" heading to refresh the list.

Table 11: Generated Report actions

To...	Do this...
View a generated report	1. Select the report to view. 2. Click [**View**]. The report is displayed in your browser. For information about the column headings in a report, see "Explanation of Report Columns" on page 52.
Download a generated report	1. Select the output format: **PDF** or **HTML**. 2. Select one or more reports to save. **Tips:** (1) Only completed reports can be saved. (2) Several reports can be saved together in one archive. 3. Click [**Download**]. Depending on your browser, the report is either saved immediately to your default download directory, or

To...	Do this...
	you may be given the choice to either open or save the file. • When downloading a single report, you can specify a name for the saved report. • When downloading multiple reports, they will be stored in a ZIP archive. You can specify a name for the ZIP archive and the reports within the archive will be named in this format: *<date>*_*<time>*_*<ID>*_*<name>* Where: *<date>* is when the report completed *<time>* is report completion time, in 24-hour notation *<ID>* is a unique identifier *<name>* is the name of the report **Tip:** If your browser's security blocks the report download, acknowledge the security warning and then repeat the download.
Delete a generated report	1. Select one or more reports to delete. 2. Click [**Delete**]. The reports are deleted immediately. **Tip:** Deleted reports cannot be recovered. You may wish to save the report first for archival purposes before deleting.

Explanation of Report Columns

The following table provides more details about the columns that may appear in a report.

Table 12: Report columns

Column	Details
Throughput	The number of successful requests to a service for the given time period.
Policy Violations	The number of requests which result in a policy violation.
Routing Failures	The number of requests that result in a routing failure.
Front end response time	Front end response time is the length of time between a Gateway node receiving a request from a client and that same node sending a response back to the client. **Tip:** The front end times always include the back end times.
Front end response time – Min	The minimum front end response time, in milliseconds.
Front end response time – Max	The maximum front end response time, in milliseconds.

Column	Details
Front end response time – Average	The average front end response time, in milliseconds, for intervals/time periods that have a value.
Back end response time	Back end response time is the length of time between a Gateway node routing a request to a web service and that same node receiving a response from the web service. **Tip:** Back end response times are included in the front end response time values.
Back end response time – Max	The minimum back end response time, in milliseconds.
Back end response time – Max	The maximum back end response time, in milliseconds.
Back end response time – Average	The average back end response time, in milliseconds, for intervals/time periods that have a value.
% Service Availability	How often the service was available, expressed as a percentage. For more information on how this value is determined, see "How Availability Percentage is Calculated" below.
Totals	The column totals are as follows: • **Throughput:** A sum of all the throughput values. • **Policy Violations:** A sum of all the violation values. • **Routing Failures:** A sum of all the routing failures. • **Front end response min:** The minimum front end response for the time period. • **Front end response max:** The maximum front end response for the time period. • **Front end response average:** A total average calculated based on the underlying data. This total is not an average of the 'Average' values. • **Back end totals:** As per front end values. • **% Service Availability:** The total availability is calculated based on the underlying data. This total is not an average of the "% Service Availability" values.

How Availability Percentage is Calculated

The "% Service Availability" (AP) shown in Performance Statistic reports is the percentage of the total number of requests to a service, that were completed successfully by the back end service. This can be expressed as:

AP = (1.0 – (Routing Failures / All Requests)) * 100

Where “All Requests” = all requests regardless of outcome. This can be further expanded as follows:

AP = (1.0 – (Routing Failures / (Throughput + Policy Violations + Routing Failures))) * 100

For example, if there were 100 requests of which 80 completed and 10 failed for policy authorization and 10 failed due to routing failure, then the service availability is:

AP = (1 – (10 / (80+10+10))) * 100 = 90%

Enterprise Service Manager: Reference Guide

[Manage Gateways] Tab

The [Manage Gateways] tab is used to organize and monitor the Gateways under the control of the Enterprise Service Manager.

The [Manage Gateways] tab contains the following pages:

- "Monitor Page" on page 55
- "Configure Page" on page 61

Monitor Page

The Monitor page under the [Manage Gateways] tab displays comprehensive information about the monitored Gateway nodes in real time.

This page contains two sections:

- Monitoring Setup**:** Used to customize when and how you should be notified when a property exceeds preset limits.
- Enterprise Gateways**:** Displays the monitored properties for the clusters and nodes.

Note: By default, no monitoring occurs after a cluster is added to the Enterprise Service Manager. You must manually enable the properties to monitor. For more information, see "Chapter Four: Configuring Monitoring" on page 27.

Tip: To ensure uninterrupted monitoring, the session timeout feature is temporarily disabled when you have the Monitor page open. For information on setting the timeout value, see the "System Settings Page" on page 81.

Monitoring Setup Section

The Monitoring Setup section is where you set the frequency and trigger thresholds for each of the monitored properties. Customizing this information is optional, as the factory presets work well in most instances.

Note: Only users with the 'Administrator' role can set up monitoring.

Table 13 summarizes the properties that can be monitored along with the factory default settings.

Table 13: Monitored properties

Property Type	Description	Sampling interval	Default Alert Trigger
audit size	Number of audit events in the Gateway database	30 sec	100000 audit events
replication delay	How long it takes for database replication to occur across the Gateway cluster **Note:** 'Error' displays if there is an error preventing the actual delay from being calculated.	30 sec	over 60 seconds
operating status	The current operating status: UNKNOWN, STARTING, WONT_START, RUNNING, CRASHED, STOPPING, STOPPED	10 sec	Any status other than RUNNING
log file size	This is the total size of all the Gateway log files	20 sec	100 MB
disk usage (root partition)	How much of the hard disk is in use in the root partition	30 sec	80% usage
disk free (root partition)	How much free disk space in the root partition	30 sec	less than 1 GB
RAID status	The current status of the RAID array: OK, REBUILDING, NOT_RAID, BAD	10 sec	upon BAD
CPU temperature	The highest temperature among all the CPUs	10 sec	55 C
CPU usage	The load on the CPU, aggregated across all CPUs and cores	15 sec	98%
swap space used	How much of the swap file is currently in use	15 sec	250 MB
NTP status	The current status of the NTP server: OK, UNSYNCHRONIZED, UNKNOWN	15 sec	Any status other than OK

Notifications and Audits

During the course of monitoring, the Monitor page can generate *notifications* and *audits*:

- *Notifications* occur when the Enterprise Service Manager detects a potential problem. It will use the notification rules that you define to communicate with you. You can choose to receive or suppress notifications:
  - **Disable all notifications:** Select this check box to stop receiving notifications. When this check box is selected, this will override the selection in the individual settings of each monitored property. *Example:* A problem node causes you to receive a flurry of notifications. Since you know about the problem, you wish to cease the notifications until the problem is corrected.
- *Audits* can record certain events that happen on the Monitor page. Use the Audits page to view the events.
  - **When a notification is sent:** Record an audit event each time a notification is sent out (note that notifications can occur only if "Notification Rules" are defined and selected in the property's settings). This is enabled by default.

Saving and Reverting

To apply new monitoring parameters, click [**Save**]. To revert the displayed parameter values to what are currently in effect, click [**Revert**].

> **Note:** 'Revert' is not the same as undo. It will only retrieve saved settings. It does not reverse typed entries.

Notification Rules

The Notification Rules define how the Enterprise Service Manager will attempt to notify you when an alert is triggered. There are three types of notifications:

- **E-mail:** An email is sent to predefined recipients (similar to the *Send Email Alert Assertion* in the Policy Manager)
- **SNMP Trap:** An SNMP (Simple Network Management Protocol) trap is broadcast to a predefined network address
- **HTTP Request:** An HTTP request (using either the GET or POST methods) is sent to a predefined URL

Notifications will be suppressed if either of the following applies:

- The [**Disable all notifications**] check box is selected
- No notification rule has been defined

For detailed information on creating each type of notification rule, see "Creating Notification Rules for Monitoring" on page 29.

Enterprise Gateways Section

The Enterprise Gateways section displays statistics for clusters and nodes in the enterprise tree. This section has been designed to show a large amount of information at a glance.

Prerequisites

The following must be done before statistics will appear for the monitored properties:

- Ensure that the Gateway clusters to be monitored have been added, trusted, and the nodes have been configured for remote management. For more information, see:

  "Adding a Gateway Cluster to Manage" on page 20

  "Establishing Trust with a Cluster" on page 21

  "Enabling Remote Management on Nodes" on page 16

- Ensure that the properties you wish to monitor have been configured. For more information, see "Chapter Four: Configuring Monitoring" on page 27

Setting up monitoring limits is optional, if you wish to override any of the system defaults. See "Monitoring Setup Section".

Monitored Properties Grid

Tips: (1) The Monitored Properties grid displays information in real time, with values refreshed according to the property's sampling interval (see Table 13). You do not need to manually refresh the page. (2) Anyone with a user account can see statistics for the monitored properties, regardless of role.

The Monitored Properties grid provides the following interface features:

Collapsible column headings

- To fit a large number of columns into a limited screen space, the column headings are abbreviated by default:

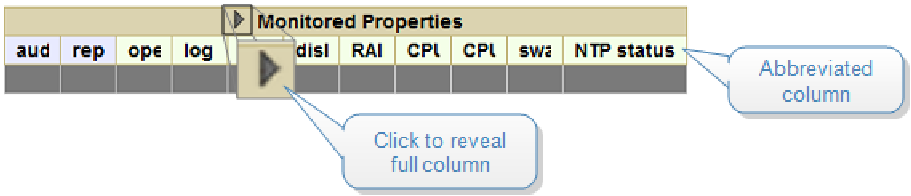


Figure 19: Monitored Properties, collapsed view

- To see the full column headings, click ▶ next to "Monitored Properties":

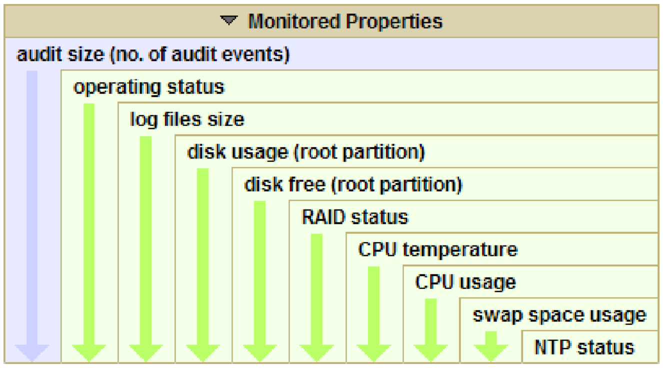
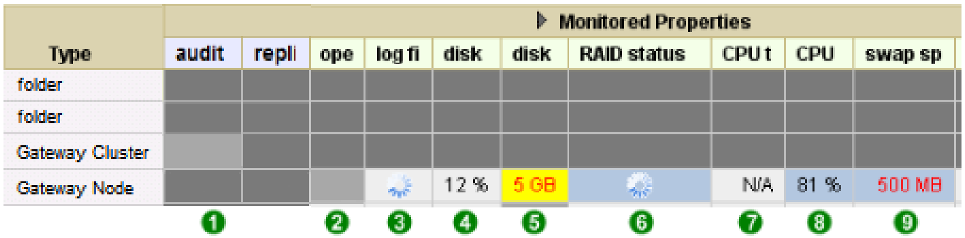


Figure 20: Monitored Properties, expanded view

Display states of property values

Each property can have various states. Figure 21 illustrates the indicators for all the possible states.



Type	audit	repli	ope	log fi	disk	disk	RAID status	CPU t	CPU	swap sp
folder										
folder										
Gateway Cluster										
Gateway Node					12 %	5 GB		N/A	81 %	500 MB

Figure 21: Display states of property values

The following is an explanation of each state:

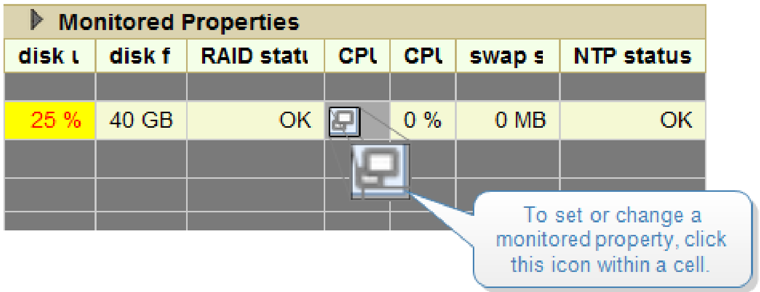
1	The monitored property type is not applicable to the entity type (for example, 'audit size' does not apply to 'Gateway Node').
2	The monitored property type applies to the entity type, but either monitoring of this property is not enabled or the node has not been configured to be remotely managed by the ESM.
3	Monitoring has been enabled but no value yet.
4	An up-to-date value.
5	An up-to-date value that is in an alert state (exceeds the trigger threshold defined for the property).
6	No value yet (stale).
7	A property that cannot be monitored on the current hardware configuration. For example, CPU temperature cannot be monitored when the Gateway is running on a virtual appliance.

8	Value displayed is from a previous refresh (stale).
9	Alert value displayed is from a previous refresh (stale).

"Stale" values as shown in 6, 8, and 9 mean that the monitored property has not changed value during the current refresh cycle. The value displayed is from a previous sampling interval (see "Monitoring Setup Section").

Enabling or changing monitoring

To enable or change monitoring for a property, position the mouse pointer over its cell and then click the icon when it appears (see Figure 22).



Monitored Properties

disk ι	disk f	RAID statı	CPL	CPL	swap s	NTP status
25 %	40 GB	OK		0 %	0 MB	OK

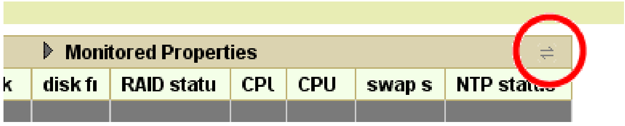
To set or change a monitored property, click this icon within a cell.

Figure 22: Enabling or changing a monitored property

For information on enabling or changing a monitored property, see "Chapter Four: Configuring Monitoring" on page 27.

Refreshing of monitored values

The following indicator provides visual confirmation that monitoring values are being retrieved from the Enterprise Service Manager server:



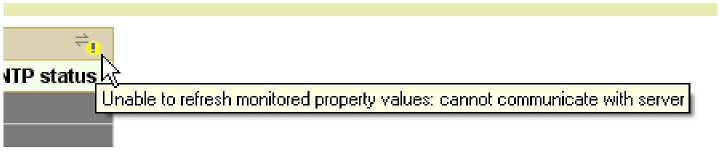
Monitored Properties

k	disk fı	RAID statu	CPL	CPU	swap s	NTP status

Figure 23: Indicator showing monitored property values being refreshed

This indicator flashes briefly at each refresh and is useful when values are steady (in other words, you see the indicator flash but the value does not change).

If connection to the Enterprise Service Manager server is severed or if the server goes down, the indicator changes to this:

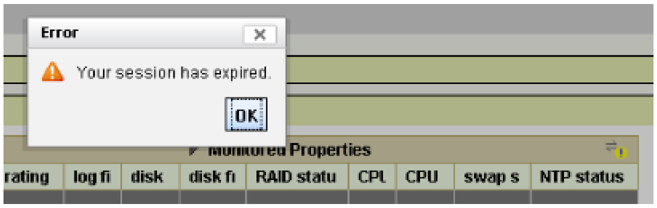


Unable to refresh monitored property values: cannot communicate with server

Figure 24: Unable to refresh monitored properties

When the Enterprise Service Manager restarts, your session automatically ends and you will be prompted to log back in.

Tip: If the ! icon is simply due to networking problems (i.e., not due to the ESM server going down), when networking is restored, the ! icon will simply disappear and a refresh will resume the connection without needing to log back in.



Your session has expired.

Figure 25: Expired session warning

Configure Page

The Configure page under the [Manage Gateways] tab is used to add and organize clusters, stop and start nodes, and launch the browser version of the Policy Manager. Users with the 'Administrator' role can use all the controls on this page. Users with a 'Manage Cluster Nodes' role can only start or stop a node.

Note: "Offline clusters" are created automatically for use with policy migration when a migration archive for an offline destination is uploaded and the source cluster is not recognized.

The Configure page displays the enterprise tree and a series of action buttons across the top. The enterprise tree is described in detail in "Using the Enterprise Tree" on page 5. The action buttons are described in Table 14. **Tip:** You can also right-click on any row to see a context menu displaying the applicable actions.

Table 14: Action buttons on the Configure page

Action	Description
New Folder	Creates a new folder in the enterprise tree. Folders are useful in organizing Gateway clusters. Enter the name of the folder and then click [**OK**]. The new folder is created as a subfolder of the selected folder.

Action	Description
	Tips: (1) Leading and trailing spaces in a folder name are automatically removed when the name is saved. (2) Use the [**Move**] button to reposition the newly created folder. *Availability:* When a folder is selected.
Add Cluster	Adds a Gateway cluster to the enterprise tree. For details, see "Adding a Gateway Cluster to Manage" on page 20. **Note:** If you are adding a cluster after a previous failed attempt to add that same cluster, you must perform some cleanup steps before attempting to add again. For details, see "Removing Trust Relationship with a Cluster" on page 24. **Tip:** Use the [**Move**] button if you need to move the cluster into a different folder. *Availability:* When a folder is selected.
Edit	Modify details for a folder or cluster. • *If editing a folder:* Type a new folder name and then click [**OK**]. The name can be between 1 and 128 characters, and may contain letters, numbers, and symbols (excluding the "/" character). • *If editing a cluster:* Modify the following details as appropriate: • Enter a **New Name** for the cluster. This name is used for display purposes within the Enterprise Service Manager only—the actual cluster itself is not renamed. • Enter a **New Host Name**. This may be required if the cluster has changed host names. • Enter a **New Administrative Port Number**. This may be required if the previous port number becomes unavailable on the host machine. **Tip:** Leading and trailing spaces in a folder or cluster name are automatically removed when the name is saved. *Availability:* When a folder or cluster is selected.
Move	Moves the selected cluster or folder to another folder. Select the destination folder and then click **[OK]**. **Note:** You cannot move the root folder nor to a destination where a cluster or folder with the same name already exists. *Availability:* When a cluster or folder is selected.
Delete	Removes the cluster or folder from the enterprise tree, including related information such as migration history and dependency mappings. If a folder is selected, it must be empty before it can be deleted. **Tip:** The [**Delete**] button only removes the clusters from being managed by the Enterprise Service Manager. It does not delete the

Action	Description
	actual cluster nor does it remove the trust relationship. A deleted cluster can be added back at any time. For more information, see "Removing Trust Relationship with a Cluster" on page 24. *Availability:* When a folder or cluster is selected. Not available when the root folder is selected.
● Start	Starts the selected Gateway node. Node must be enabled for remote management. *Availability:* When a stopped node is selected.
● Stop	Stops the selected Gateway node. Node must be enabled for remote management. *Availability:* When a node that is running is selected.
Launch Policy Manager	Starts the Policy Manager browser client and connects to the selected Gateway cluster. Requires Java Runtime. For more information on using the browser client, see *Policy Manager Browser Client* in the *CA API Gateway - Policy Manager User Manual*. *Availability:* When a non-offline cluster is selected.
🔄	Refreshes the enterprise tree with the most recent information from all Gateway clusters.

[Manage Policies] Tab

The [Manage Policies] tab is used to organize service policies across different Gateway clusters. You typically use this tab after adding the clusters through the [Manage Gateways] Tab.

The [Manage Policies] tab contains the following pages:

- "Migration Page" on page 63
- "History Page" on page 72

Migration Page

If you have multiple Gateway clusters, you can use the Migration Page to copy entities such as service policies or policy fragments from one cluster to another. When an entity is copied to another cluster, its dependencies are transferred (either automatically or manually mapped) so that the migrated entity is ready to run on the destination cluster.

Note: In order to perform a migration, your ESM user account must be mapped to a Gateway cluster account with sufficient permissions. Migration may not be possible, even if your role in Enterprise Service Manager is 'Administrator', if your mapped equivalent's role does not allow it. (Conversely, migration is possible if you are mapped to a Gateway administrator but hold no role in Enterprise Service Manager.) For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

The following are some examples of when migration is useful:

- Migrating a policy from one related cluster to another—for example, from a "Dev" cluster to a "Staging" cluster.
- Migrating from an unrelated cluster to another—for example, migrating a service from an east coast cluster to a west coast cluster to act as a standby.

Tip: This topic provides background information on the migration process. For a step-by-step description on how to use the Migration page, see "Chapter Five: Migrating Services and Policies" on page 35

Items that can be migrated on the enterprise tree:

- folders
- policy fragments – the imported policy fragments become the active policy version on the target system
- published services – the imported policies become the active policy version on the target system.

Note that global policies and internal use policies are not migrated. For more information about these types of policies, refer to the following topics in the *CA API Gateway - Policy Manager User Manual:*

Working with Global Policies
Working with Internal Use Policies

Prerequisites

- The Enterprise Service Manager is managing more than one cluster
- The source and destination clusters are running the same version of the Gateway software, with the same product features enabled (see *Features by Product in the CA API Gateway - Policy Manager User Manual*)

Understanding Dependencies

Every service or policy has a whole host of dependencies; these are the supporting entities that make up the cluster—for example: users, groups, certificates, cluster properties, etc. It is important to understand how dependencies are treated during the migration process.

The Enterprise Service Manager groups all dependencies into these three categories:

- **Always copy:** These dependencies cannot be mapped and will always be copied from the source to the destination cluster:

  Folders
  User certificates
  Service properties (name, routing URI, etc.)
  Service documents (service WSDL, if any)
  Service policy

- **Always map:** These dependencies cannot be copied as-is and require that you specify a mapped equivalent on the destination cluster:

  Users
  Groups
  Cluster properties
  Identity providers
  JMS Queues
  Trusted certificates
  Global Schema
  SSL Certificates (trusted certificates, private keys from non-default keystores)
  Private keys from non-default keystores

- **Optionally map:** These dependencies can be copied over as-is or you can specify a mapped equivalent on the destination cluster. These are all the dependencies not listed under the "Always copy" or "Always map" categories

Migration can proceed once you have resolved all the dependencies are required to be mapped.

Other Migration Ramifications

Below are other ramifications of migrating items from one cluster to another.

Aliases

When an alias is selected for migration, both the alias and the original entity are migrated. In the destination cluster, the alias and original are placed in the same folder path as on the source cluster.

> **Note:** If folders are not being migrated then aliases are not migrated. This is because it is meaningless to have both the original and the alias in the same flat folder structure.

For more information about aliases, please refer to *Working with Aliases* in the *CA API Gateway - Policy Manager Authoring Manual*.

Roles and Permissions

The roles and permissions associated with the entities in the source Gateway cluster are not migrated directly. Rather, they will be recreated on the destination cluster as required.

For example, consider the following scenario:

- there is source cluster A and destination cluster B
- cluster A has a "Warehouse" service; this service does not exist on cluster B
- cluster A has the role *Manage Warehouse Service*; this role does not exist in cluster B
- Bob, Fred, and Sue hold the *Manage Warehouse Service* role in cluster A

When the "Warehouse" service is migrated from cluster A to B, the *Manage Warehouse Service* role is created on cluster B. This role will be empty initially—a cluster B administrator will need to assign the appropriate users to the role. The original holders of this role in cluster A (Bob, Fred, and Sue) do not play a factor, because they may not be part of the migration. Even if they were, they will be mapped to new users in cluster B.

If the "Warehouse" service exists in both cluster A and B and the *Manage Warehouse Service* role exists on cluster B, then the migration is seamless and no role needs to be created.

For more information, see *Managing Roles* and *Predefined Roles and Permissions* in the *CA API Gateway - Policy Manager User Manual*.

Limitations

The following are limitations of the migration process:

- Custom assertions are not migrated. If such assertions exist in the source cluster, they must be manually reinstalled on the destination cluster.
- Version history is not migrated. Only the current version of a policy is migrated. This means that the version numbers between the source and destination are independent.
- Sample messages for the service are not migrated.

Causes of Migration Failure

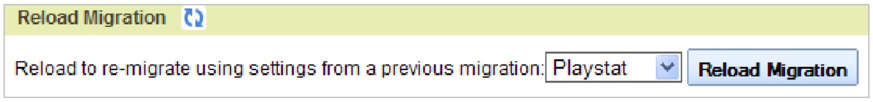
The following conditions will prevent a successful migration:

- **Entity conflict:** The migration will create or update an entity in the target cluster that causes an entity constraint violation (for example, duplicate names, database keys, etc).
- **Service resolution conflict:** The migrated service will cause a service resolution conflict.
- **Source or destination cluster rebooted:** Migration will fail and must be manually restarted if either the source or destination cluster is rebooted while migration is in progress. **Tip:** The Migration page may be temporarily disabled if a reboot occurs. If this happens, refresh the browser window to restore normal operation.

Migration Page Interface

The following is a summary of each interface element on the Migration page.

Reload Migration



Reload to re-migrate using settings from a previous migration: Playstat

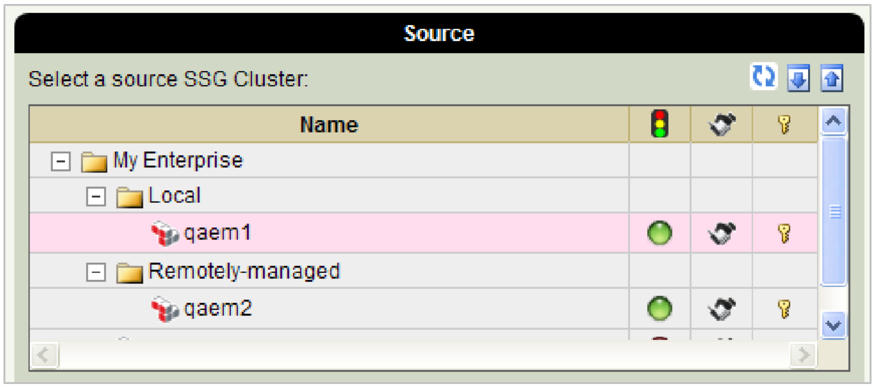
Figure 26: Reload Migrations

To use settings from a previous migration, select it from the drop-down list and then click [**Reload Migration**]. Reloading a previous migration can save you time, especially for migrations performed on a regular basis.

Tips:

- Only migrations that have a label will appear in the drop-down list.
- A label can be entered on the migration confirmation screen or on the History page.
- Reloading a previous migration discards current settings on the Migration page

Source/Destination Clusters



Source

Select a source SSG Cluster:

Name			
⊟ My Enterprise			
⊟ Local			
qaem1	●		
⊟ Remotely-managed			
qaem2	●		

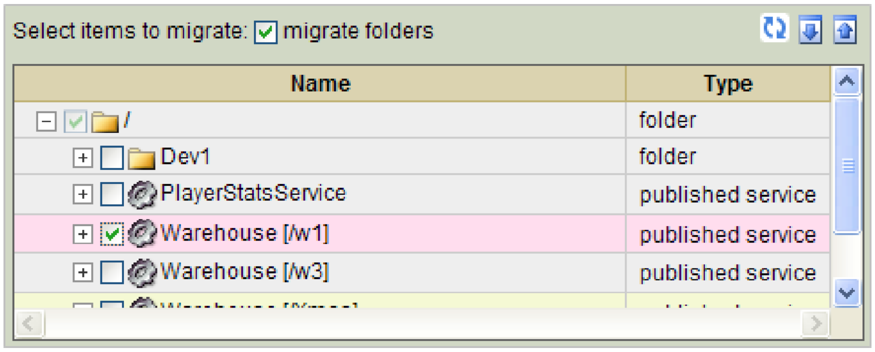
Figure 27: Source/Destination Clusters

In the enterprise tree, select a source or destination cluster. These clusters must be different. For information on the icons displayed, see "Using the Enterprise Tree" on page 5.

Tips:

- Only clusters that are both up and trusted can be selected.
- Only clusters can be selected, not folders.

Items to Migrate/Destination Folder



Select items to migrate: ☑ migrate folders

Name	Type
⊟ ☑ /	folder
⊞ □ Dev1	folder
⊞ □ PlayerStatsService	published service
⊞ ☑ Warehouse [/w1]	published service
⊞ □ Warehouse [/w3]	published service

Figure 28: Items to Migrate/Destination Folder

On the **Source** side: Select the check box next to the items to be migrated. Note that selecting a folder automatically selects all child items, but you can unselect child items as necessary.

- [**migrate folders**]: Select this check box to maintain the folder structure in Services and Policies list in the source cluster after migration. If you do not migrate folders, then all entities will be "flattened" after migration (i.e., all entities will be at the same level, with no folders).

On the **Destination** side: Select the radio button for the destination folder. Optionally select one of the following:

- [**enable new services**]: This option depends on whether the service already exists on the destination cluster:
  - For services new to the destination cluster, select the [**enable new services**] check box to enable the service after migration. Clear this check box to leave the service in a disabled state on the destination cluster after migration.
  - For services that already exist on the destination cluster, the service will maintain its current status on the target system—the [**enable new services**] check box will have no effect.
- [**overwrite existing items**]: Select this check box to overwrite items on the destination cluster. For example, if the service “Warehouse” exists on both the source and target clusters, selecting this check box will overwrite the destination “Warehouse” with contents from the source “Warehouse”.

  Clear this check box to prevent any overwriting. For example, if the service “Warehouse” exists on both the source and destination clusters, the two services will be mapped but the target "Warehouse" is not overwritten.

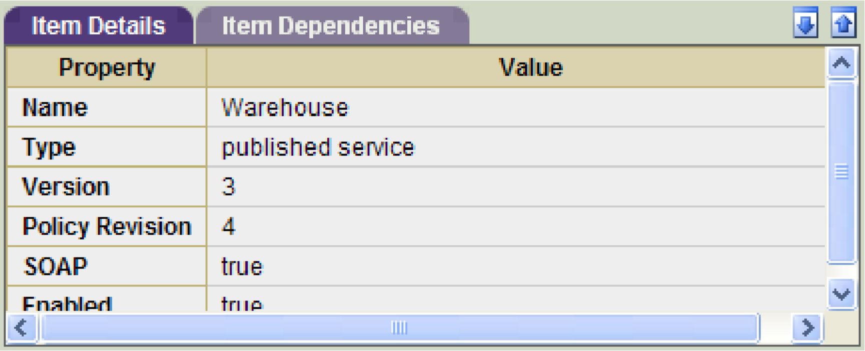
  Note: If both source and destination services use the same URI, URN, and SOAPAction, then the migration will fail with a "duplicate resolution parameters" error.

Tips:

- Folders are always updated, regardless of the [**overwrite existing items**] check box.
- If you do not migrate folders, then aliases are not migrated. See "Aliases" above.
- The folders referenced here are *not* the folders created in the Configure page to organize your clusters. Rather, they are the folders created in the Policy Manager to organize the published services and policies. For more information, see *Services and Policies* in the *CA API Gateway - Policy Manager User Manual* .

- In the Destination list, you can select a published service or policy fragment even though you cannot use these as migration destinations. Reason: This is so that you can view details and dependencies for the item.

Item Details/Item Dependencies



Property	Value
Name	Warehouse
Type	published service
Version	3
Policy Revision	4
SOAP	true
Enabled	true

Figure 29: Item Details/Item Dependencies

Displays details and dependency information for a service or policy selected from the list above.

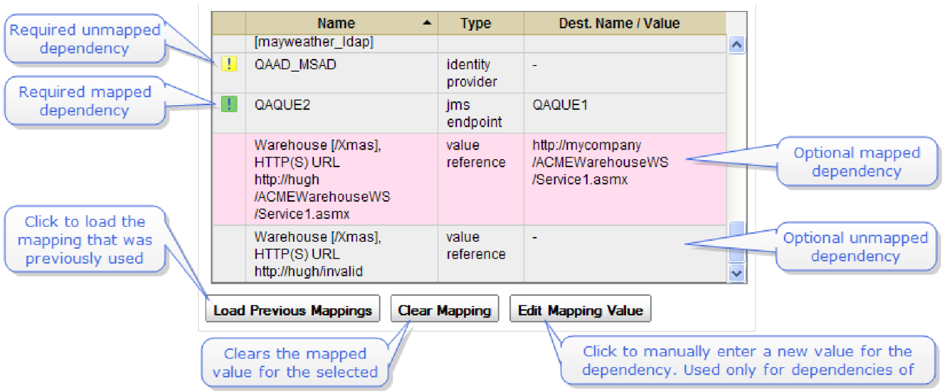
Select a published service or policy fragment from the Items to Migrate/Destination Folder to view its details or dependencies.

Tips:

- It may take a moment for the dependency list to update after selecting an item to view.
- To resolve the dependencies identified in the [Item Dependencies] tab, use the Dependencies Mapping section.
- The "Policy Revision" shown in the [Item Details] tab is the version number of the policy involved in the migration. This revision number is from the Policy Manager and it is incremented with each change to the service policy. For more information, see *Policy Revisions* in the *CA API Gateway - Policy Manager User Manual*.
- The "Version" shown in the [Item Details] tab is an internal counter that increments each time a service is changed or each time a previous revision is made the active version. It has no relation to the version numbers shown in *Policy Revisions*.

Dependencies Mapping

The Dependencies Mapping section is used to map the dependencies identified in the [Item Dependencies] tab. The dependencies flagged "Always map" (!) must be resolved before migration can proceed. For more background information, see "Understanding Dependencies" above.



	Name	Type	Dest. Name / Value
	[mayweather_ldap]		
!	QAAD_MSAD	identity provider	-
!	QAQUE2	jms endpoint	QAQUE1
	Warehouse [/Xmas], HTTP(S) URL http://hugh /ACMEWarehouseWS /Service1.asmx	value reference	http://mycompany /ACMEWarehouseWS /Service1.asmx
	Warehouse [/Xmas], HTTP(S) URL http://hugh/invalid	value reference	-

Required unmapped dependency

Required mapped dependency

Optional mapped dependency

Optional unmapped dependency

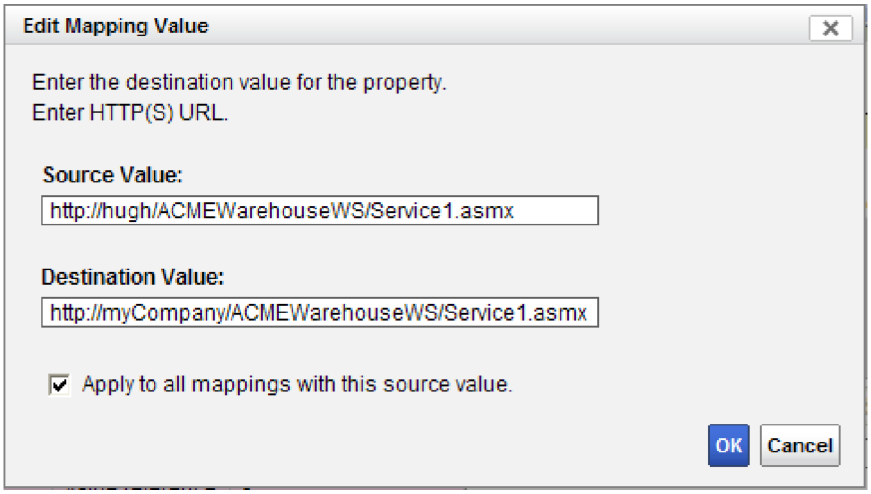
Click to load the mapping that was previously used

Clears the mapped value for the selected

Click to manually enter a new value for the dependency. Used only for dependencies of

Figure 30: Dependencies Mapping

- To map dependencies of type 'value reference', click [**Edit Mapping Value**] and complete the Edit Mapping Value dialog box:



Edit Mapping Value

Enter the destination value for the property.
Enter HTTP(S) URL.

Source Value:
http://hugh/ACMEWarehouseWS/Service1.asmx

Destination Value:
http://myCompany/ACMEWarehouseWS/Service1.asmx

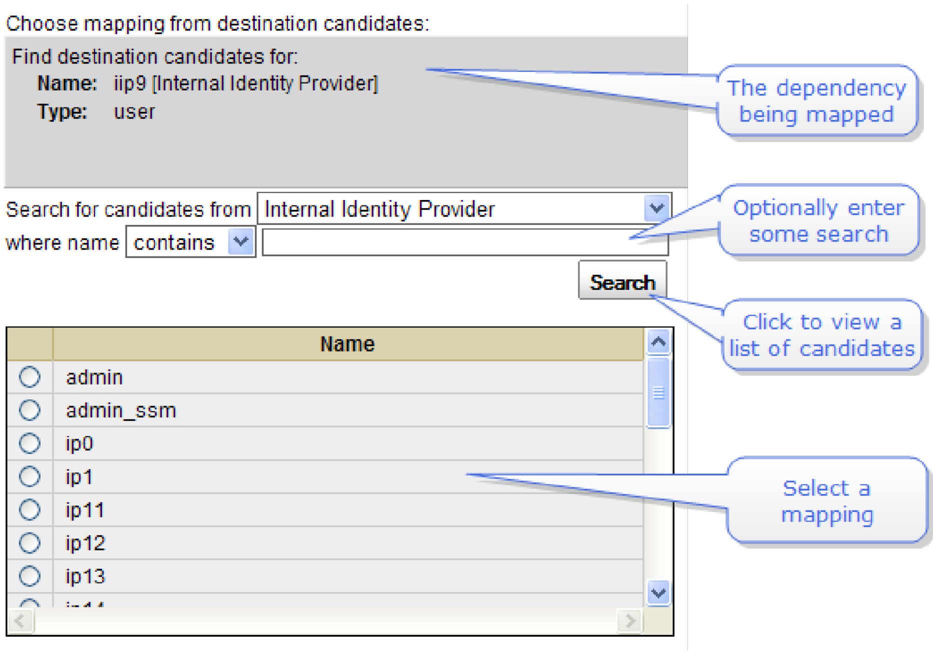
☑ Apply to all mappings with this source value.

Figure 31: Edit Mapping Value

- **Source Value:** The original value to be mapped. This is display only and cannot be changed.
- **Destination Value:** Enter the value as it should appear in the target system.

- **Apply to all mappings with this source value:** Have the migration process automatically apply the destination value to all sources with the same value. Selecting this option can reduce the amount of mapping required. Not selecting this option lets you enter a different destination value each time.

- To map dependencies of all other types, locate a destination candidate:



Choose mapping from destination candidates:

Find destination candidates for:

Name: iip9 [Internal Identity Provider]

Type: user

Search for candidates from: Internal Identity Provider

where name: contains

	Name
○	admin
○	admin_ssm
○	ip0
○	ip1
○	ip11
○	ip12
○	ip13

The dependency being mapped

Optionally enter some search

Click to view a list of candidates

Select a mapping

Figure 32: Searching for mapping candidates

- For candidates that have more than one category (for example, multiple identity providers), you can refine the search by selecting a category.
- Optionally further refine the search with "contains" or "starts with":
  - "**contains**" will locate the text anywhere in the name—for example, searching for "smith" will locate "JSmith"
  - "**starts with**" will match only the beginning characters of the user name—for example, "js" will locate "JSmith" and "JSimpson"
- You must click [**Search**] to continue. Searching with no search text is the same as displaying all values.

History Page

The History page is used to view and manage the migration archives. This page lists every migration performed and is searchable by date. Users with the 'Administrator' role can see all migrations. All other users can only see their own migrations.

For more information, see "Migration Page" on page 63.

Table 15: History page

Control	Description
Start/End Date	Display migrations performed within this date range. Use the pop-up calendar control to select the date. **Note:** For offline archives, the date range must include the date when the offline archive was created in order for that archive to appear on the page.
Select	Click to update the migration list based on the specified dates.
Label	An optional label to help identify the migration. Migrations with labels can be reused in the future via the "Reload Migration" section of the Migration page.
Date	The date and time when the migration was performed, based on the Enterprise Service Manager host machine.
From (Source Cluster)	The source cluster used in the migration.
To (Destination Cluster)	The destination cluster used in the migration.
Archive Size	The disk space occupied by the archive, including the migrated entries. Note that the space may vary, depending on the entities involved in the migration and the number of dependencies. The archive is compressed to save space.
Change Label	Used to add or change the label for an archive.
Download Archive	Save the archive to a local drive. You can optionally protect the archive by selecting the [**Encrypt migration archive**] check box, then entering a password. Unencrypted archives are saved as standard .ZIP files. Encrypted archives are saved as .PGP files.
Remove Archive	Remove the migrated entities from the selected archive, but retain the mappings. This allows the archive to be reloaded for future migrations. **Note:** When the archive is removed, you can no longer download it.
Delete	Deletes the selected migration record from the list. This migration record can no longer be downloaded or reused for mapping. **Tip:** Download and save the archive before deleting it. If you need to use it again in the future, simply upload it back.
Upload Archive	Uploads a saved migration archive back into the Enterprise Service Manager. This is useful is situation where you want to restore a deleted archive using a saved local copy. To upload an archive: 1. Optionally enter a **Label** for the uploaded migration. 2. Click [**Browse**] and locate the appropriate archive file. 3. Enter a **Password** if the archive is encrypted. 4. Click [**OK**]. The uploaded archive appears in the list. **Tip:** To see details about the uploaded archive, go to the Configure page.

Control	Description
Migration Summary	A summary of the selected migration.

[Reports] Tab

The [Reports] tab provides a powerful reporting tool to analyze the service metrics data collected in the Gateway clusters. You can generate two types of reports:

- **Performance Statistics:** Provides performance statistics information for protected services at the service or operation level. The statistics include: throughput, policy violations, routing failures, min, max and average front and back end response times and availability percentage.
- **Usage Statistics:** Provides service usage information at the service or operation level, for a specific set of requestors of a service. Usage is equivalent to throughput from a performance statistics report. Usage reports allow this information to be viewed together for a set of users of a service.

  Users of a service are defined by the keys added to the *Capture Identity of Requestor Assertion* of a service policy and the values which can be assigned to the keys at run time.

Tip: For step-by-step directions on creating a report, see "Chapter Seven: Generating Reports" on page 47.

There are two sections in the [Reports] tab:

- **Generate New Report:** This section is used to generate a new report.
- **Generated Reports:** This section lists the reports that have been submitted. You can view, download, or delete generated reports.

Generate New Report

The following table describes the controls in this section.

Table 16: Controls for generating a report

Control	Description
Saved Settings	Select a previously saved report settings from the drop-down list. This list is empty if no report settings have been saved. **Tip:** Saved report settings are private to a user. They are not accessible to other users.

Control	Description
Load	Loads the selected report settings. **Note:** When the settings are loaded, the names of the services or operations are as they were when the settings were saved. If service/operation names have been changed when a report is run, the information section at the top of the report will contain the old names, while the tabulated data in the report body shows the up-to-date service/operation names.
Delete	Remove the selected report settings from the list.
Save Current Settings	Saves the current report settings to a name that you specify. It is not necessary to generate a report in order to save its settings. **Note:** Once report settings have been saved, any changes to the services or operations will not be reflected when the settings are loaded.
Report Type	Select the type of report to generate: **Performance Statistics** or **Usage Statistics**.
Entity Selection	Choose **Published Service** to be able to select specific published services for reporting. The report output will be at the service level, which encompasses all operations defined in the WSDL document. Choose **Operation** to be able to select specific operations within a service for reporting.
Gateway Clusters	In the enterprise tree, locate the Gateway cluster to report on.
Content	Depending on the Entity Selection, either select the published services to report on, or select the specific operations within a service to include. The operations available are given in the WSDL document.
Add Checked Published Service(s)	Click this button to include the selected services in the report. Note that you cannot generate a report if published services have not been added.
<entity list>	The services/operations that you added are shown in the list below. Verify that these are what you intended. To remove an entity from the list, click ☒ next to the appropriate row. Alternatively, you can go back and choose another **Gateway Cluster** or **Content**. **Tip:** If the entity list shows *"Please add at least one entity",* it means you did not select from the **Content** list or you failed to click [**Add Checked Published Service(s)**].
Time Zone	The time zone on which the report is based. This allows the report's time period to be calculated relative to a specific time zone. This is useful if a cluster is in a different time zone than the Enterprise Service Manager. The default time zone shown is from the [Settings] tab. If no time zone has been set on that tab, then it is the time zone of the server machine.
Last *xxx* hours /	For specifying a relative time period. See Table 17 below for a detailed

Control	Description
days / weeks / months	explanation of the scope of each time period.
From <*start*> to <*end*>	For specifying an absolute time period. For the date, click inside the field and choose the date from the popup calendar. For the time, select the time from the drop-down list. **Tip:** All start times are inclusive, while all end times are exclusive.
Time Interval	The interval to break the report time period down by. Report data will be grouped by the chosen interval. "None" will produce a summary report.
Grouping	Groups the report by message context key. These groupings are required when creating a Usage Report, but optional for Performance Statistics Reports. For details on using this feature, see Grouping by Message Context Key.
Charting	Include or exclude a summary chart at the start of the report.
Formatting	Select the check box to add page breaks to the generated report. Report output is sized initially for US Letter size pages in landscape mode. When page breaks are included, then both PDF and HTML output will contain page breaks at the width of a US Letter size piece of paper. Clear the check box to format the report as one continuous page. This makes reports easier to use when viewing on screen. **Notes:** (1) Reports with many columns of data may grow in width, making it difficult to print if they grow too wide. (2) If page breaks are not used, the PDF output may consist entirely of blank pages. This is a known issue and is caused by the page size growing too large. If this occurs, use the HTML output instead or regenerate the report with page breaks.
Report Name	Name of the report. Used to identify the report in the list of generated reports and is used in the file name when the report is saved. The Report Name is required.
Generate Report	Submits the report for processing. The time it takes for the report to complete depends on several factors: the time period covered by the report, the interval chosen, the number of groupings involved, and the load on the target cluster. For example, a report covering 30 days with 1 hour intervals and 10 groupings will take a long time to complete and will be extremely lengthy. **Tip:** Once the report is submitted, you can exit the [Reports] tab or log out of the Enterprise Service Manager. Report processing will continue in the background.

The following table describes in greater detail how the Enterprise Service Manager responds for each *Last...* time period setting.

Table 17: Scope of relevant time periods

Period	Description
Hours	The last full hour, not including the current partial hour. *Example:* The current time is 18:30 and 1 Hour is entered. The time period of the report will be 17:00 to 18:00.
Days	The last full day, not including the current partial day. *Example:* The current day is Thursday 13:00 and 1 Day is entered. The time period of the report will be Wednesday, from 00:00 to Thursday 00:00 (up to the last millisecond of Wednesday, not including the first millisecond from Thursday).
Weeks	The last 7 full days, not including the current partial day. *Example:* It is Monday 13:00 and 1 Week is entered. The time period of the report will be Monday (week previous) 00:00 to Monday 00:00 (up to the last millisecond of Sunday, not including the first millisecond from Monday).
Months	The last calendar month, not including the current partial month. *Example:* It is March 14th and 1 Month is entered. The time period of the report will be the month of February.

Generated Reports

The Generated Reports section lists all the reports that have been submitted or generated. If a report could not be completed, it is listed here along with an explanation if one is available. Administrator users can access reports generated by all users. Non-administrator users can access only reports generated by themselves.

Tip: To ensure that this section is up to date, click the 🔄 icon to refresh the list.

Table 18: Generated Reports section

Control	Description
Download	Downloads the selected report(s) in the chosen format, to a location that you specify. The default name is: *yyyymmdd_hhmmss_ <reportname>_ <clustername>*. Only completed reports can be saved. **Tip:** The time stamp in the file name indicates when the report was completed, not when it was downloaded.
Format	Select whether the [**Download**] button downloads the reports in **PDF** or **HTML** format.
Delete	Deletes the selected report(s). Deletion occurs immediately and cannot be undone.

Control	Description
Name	The name of the report, as entered in the "Report Name" field.
Date	The date and time when the report reached the state currently showing on this page.
Cluster	The Gateway cluster being reported on.
Status	Indicates the current status of the report. **Tip:** Refresh the list for the most recent status. • SUBMITTED: The report has been submitted for processing and is either awaiting processing or currently being processed. • COMPLETED: The report is finished and can be viewed or downloaded. • FAILED: The report could not be completed. The Status Detail column explains the error.
Status Detail	If the report failed to generate, more information is listed here, if available.
View	Displays the selected report in HTML format in a new browser window or tab. Only completed reports can be viewed.

[Tools] Tab

The [Tools] tab is used to view audit and log information generated by the Enterprise Service Manager. It contains the following pages:

- "Audits Page" on page 78
- "Logs Page" on page 79

Audits Page

The Audits page displays audit information recorded by the Enterprise Service Manager. On this page, you can view, download, or delete audit messages that are past a certain age.

Only users with the 'Administrator' role can access the Audits page.

For more information, see "Viewing Audits and Logs" on page 9.

Table 19: Audits page

Control	Description
Download	Saves audit information for a specified time period to a standard .ZIP file that can be extracted and viewed in any text editor.

Control	Description
	Note: You can specify the time period to save—the system does not automatically assume the time period currently displayed. If your browser's security blocks the download, acknowledge the warning and try the download again.
Delete	Deletes all audit entries older than *x* days, where *'x'* is a value that you specify. The minimum value is **7**.
Start Date	Display audit records starting from this date. Use the pop-up calendar control to select the date.
End Date	Display audit records ending on this date. Use the pop-up calendar control to select the date.
Type	The type of audit records to show: • **Administrative:** These audits record the actions that occurred as a result of a user performing a task in Enterprise Service Manager—for example, a Gateway cluster was added and a new role was automatically created to manage this cluster. • **System:** These audits note the internal messages that are constantly generated in the background by Enterprise Service Manager. These messages typically describe "housekeeping" tasks such as starting/stopping the Enterprise Service Manager, adding/updating the license, etc.
Select	Click to update the audit list based on the specified dates and type.
Time	When the audit event occurred.
Severity	The severity of the audit event: SEVERE WARNING INFO FINE Any 'Severe' events should be investigated immediately.
Message	The audit event message.

Logs Page

The Logs page displays the low level system events that occur continually in the background. Use this page to help you diagnose system-related issues. Unlike the Audits page, the Logs page does not contain information relevant to business events.

Only users with the role 'Administrator' can access the Logs page. Log files are rotated automatically once the file size reaches 1MB. A maximum of 10 log files are retained.

For more information, see "Viewing Audits and Logs" on page 9.

Table 20: Logs page

Control	Description
View	Displays the select log file. This button is active only when a log file is selected.
Download	Saves the selected log file to a standard .ZIP file that can be extracted and viewed in any text editor. **Note:** If your browser's security blocks the download, acknowledge the warning and try the download again.
Name	The name of the log file. The names run from *ssem.0.log* to *ssem.9.log*. Rollover occurs once the log file reaches 1MB.
Date	When the log file was created.
Size	The size of the log file.
Log Details	Details about each log event.

[Settings] Tab

The [Settings] tab is used to access system and user-specific settings. Enterprise Service Manager contains many configuration settings that you can customize for how you work and how the application should respond. The settings are grouped across the following pages:

- "User Settings Page" on page 80
- "System Settings Page" on page 81
- "User Accounts Page" on page 83 (Administrators only)
- "User Roles Page" on page 84 (Administrators only)

User Settings Page

The User Settings page is used to change the password and specify some basic user interface preferences. The settings here apply to the user currently logged in. Click [**Apply**] in the appropriate section when complete.

Table 21: User Settings page

Setting	Description
Change Password	
Old Password	To change the password, first enter the old password. **Tip:** If the user has forgotten the old password, an administrator can reset the password instead using the [User Accounts] tab.
New Password	Type a new password that conforms to the following: • minimum 6 characters

Setting	Description
	• maximum 32 characters • letters, numbers, and symbols are acceptable A password never expires.
Retype New Password	Type the password again for confirmation.
User Interface Preferences	
Time Zone	Select your time zone from the Time Zone drop-down list.
Date Format	Choose your preferred date format from the Date Format drop-down list: • YYYY-MM-DD (all numeric) • MMM DD, YYYY The date format affects the interface and reports.
Time Format	Choose your preferred time format from the Time Format drop-down list: • 24-hour clock • 12-hour clock The time format affects the interface and reports.
Start Up View	Select which tab should be displayed initially once the user has logged into Enterprise Service Manager or upon clicking the ESM product logo on the upper left corner of every page.

System Settings Page

The System Settings page displays system-specific settings and is intended for advanced users and system administrators. It contains information useful for troubleshooting. The settings on this page affect all users of Enterprise Service Manager.

Product Information Section

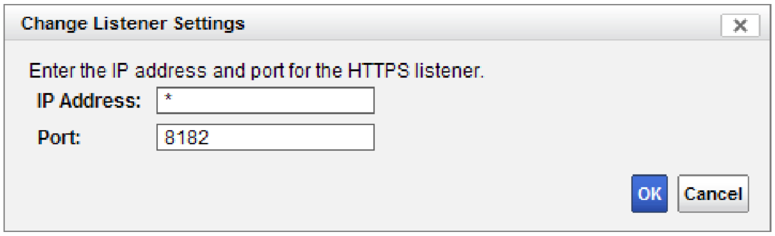
This section displays the product name and version information.

System Information Section

This section displays information about the machine running the Enterprise Service Manager. You can change the HTTPS Listener or SSL Certificate in this section.

➢ *To change the HTTPS Listener:*

1. Click [**Change**]. The Change Listener Settings dialog box is displayed.



Enter the IP address and port for the HTTPS listener.

IP Address: *

Port: 8182

Figure 33: Change Listener Settings

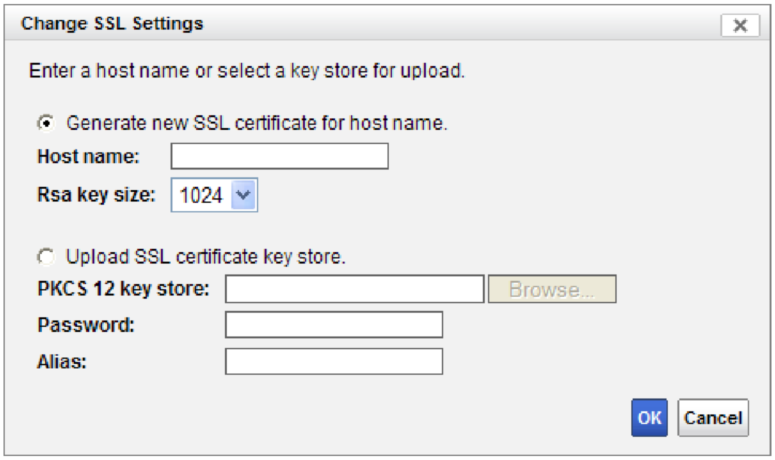
2. Enter the **IP Address** on which to monitor. The asterisk '*' represents all IP addresses.

3. Enter the **Port** number used to communicate with the Enterprise Service Manager. For more information, see "Setting Up the Enterprise Service Manager" on page 14.

4. Click [**OK**]. The new listener settings take effect immediately.

➤ *To change the SSL Settings:*

1. Click [**Change**]. The Change SSL Settings dialog box is displayed.



Enter a host name or select a key store for upload.

● Generate new SSL certificate for host name.

Host name:

Rsa key size: 1024

○ Upload SSL certificate key store.

PKCS 12 key store:

Password:

Alias:

Figure 34: Change SSL Settings

2. Select the action you wish to perform:

   - **Generate a new SSL certificate:** Enter the **Host name** and optionally select an **RSA key size**.

     > **Note:** After generating a new SSL certificate, you must remove the user mappings between the Gateway and the Enterprise Service Manager. For more information, see *Managing ESM User Mappings* in the *CA API Gateway - Policy Manager User Manual* (use the "Remove Registration" option).

- **Upload a SSL certificate key store:** Click [**Browse**] to locate the key store file (for example, a *.p12 SSL key file), then enter the **Password** and **Alias**.

Tip: The Alias is required if the key store contains multiple key. It specifies the key to be used. This Alias value must be the one used to create the key store in the Policy Manager, using the same password.

3. Click [**OK**]. The new SSL settings take effect immediately.

License Section

This section displays information about the Enterprise Service Manager license.

- To delete the existing license file, click [**Delete**] and then confirm the deletion.
- To install a new license file, use [**Browse**] to locate the file, then click [**Apply**].

Global Settings Section

This section is used to configure settings that apply to all users.

- **Session Inactivity Timeout:** Enter the timeout period, in minutes. The Enterprise Service Manager will automatically log the user out after this period of inactivity. Click [**Apply**] to set a new value. Changes in timeout will take effect the next time a user logs into Enterprise Service Manager. The minimum timeout is 1 minute; the maximum is 1440 minutes (one day). The default is 30 minutes.

Tip: The session timeout is disabled when the Monitor page is open.

User Accounts Page

Note: Only users with a role of 'Administrator' can access the User Accounts page.

The User Accounts page under the [Settings] tab is used to manage the user accounts for Enterprise Service Manager.

Table 22: User Accounts page

Control	Description
New	Creates a new user. For more information, see "Chapter Six: Working with Users" on page 41.
Delete	Deletes the selected user. For more information, see "Deleting a User Account" on page 42.
User Name	The user name can be 3-128 characters and can include letters,

Control	Description
	numbers, and symbols except for these characters: # , + " \ < > ; The user name cannot be changed once entered.
Password	The password can be between 6-32 characters and may include letters, numbers, and symbols.
Email	The email address can be 128 characters maximum.
Surname	The user's surname, 32 characters maximum.
Given Name	The user's given name(s), 32 characters maximum.
Description	This field can be used to record additional information about the user, 255 characters maximum.

User Roles Page

Note: Only users with the 'Administrator' role can access the User Roles page.

The User Roles page under the [Settings] tab is used to manage the user roles for Enterprise Service Manager. A role dictates the permissions granted to a user within the Enterprise Service Manager, for example permission to manage nodes in a cluster.

Currently there are two types of roles in the system:

- **Administrator:** Users with this role have full access to the entire Enterprise Service Manager, including the ability to manage the nodes of every Gateway cluster. Administrators can also see pages that are otherwise "off limits" to other users.
- **Manage** <*clusterName*> **Gateway Cluster Nodes:** Users in these roles can perform node-specific operations such as stop/start individual nodes in the cluster. Pages that are for "Administrator use only" are not visible to "Manage clusters" users. **Note:** Only administrators can add clusters and it is the responsibility of the administrators to assign the appropriate users to these roles.

Tip: Users without a role can still perform cluster-specific tasks such as migrating policies if they have been mapped to a Gateway user with sufficient privileges. For more information, see "Mapping an ESM User to a Cluster User Account" on page 23.

Table 23: User Roles page

Label/Control	Description
Select a Role	The roles defined in Enterprise Service Manager. By default there is the 'Administrator' role with the administrator user, added when the Enterprise Service Manager was configured. The 'Manage Gateway

Label/Control	Description
	Cluster Node' role is automatically created when someone adds a Gateway cluster. The numbers shown after the role name are cluster OIDs used to uniquely identify a cluster.
Role Description	A brief description about the role, automatically created by the system.
Search by User Name	When searching the list of users, specify whether the search text should be treated as "**contains**" (anywhere within the name) or "**starts with**" (name begins with the search string).
Search box	To quickly locate a user in the "Assigned Users" and "Unassigned Users" lists, type the name or part of the name to search here. How the name is matched depends on the "Search by User Name" setting.
Go	Click to display the matching users in the list beneath.
List of users	In the "Assigned Users" list, this list shows all users who are in this role. In the "Unassigned Users" list, this list shows all users who are *not* in this role. Note that the 'Manage Gateway Cluster Nodes' roles are initially created with nobody assigned to that role. (The implied members are the Administrators, who have access to everything.) It is up to an Administrator to assign the appropriate non-administrative users to a 'Manage Gateway Cluster Nodes' role.
Unassign	Removes the selected assigned user from the role. The user's access permissions will be updated at the next login.
Assign	Adds the selected unassigned user to the role. The user's access permissions will be updated at the next login.

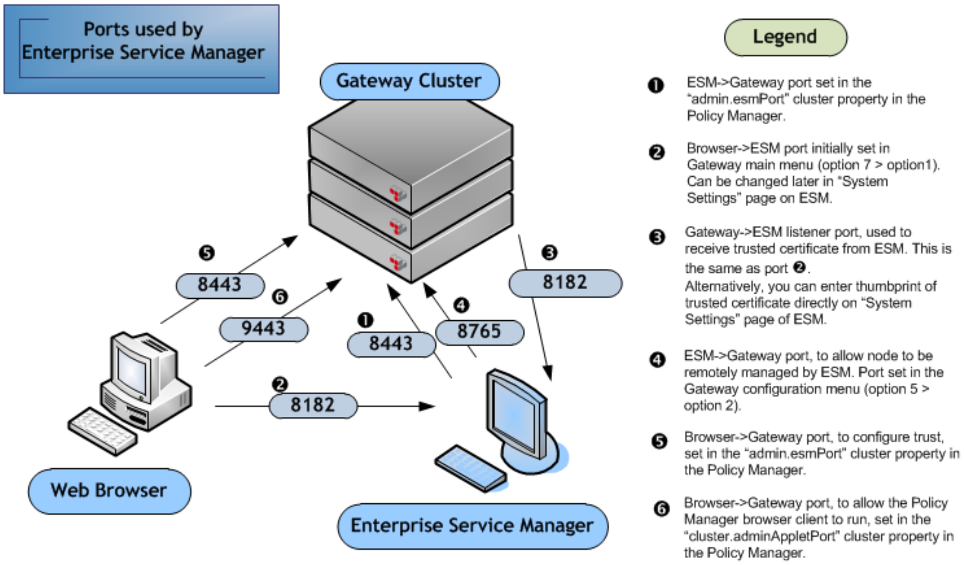
Appendix A: Ports Used by the ESM

The Enterprise Service Manager uses the following ports to communicate with the Gateway clusters and with the web clients requesting access. Figure 35 provides a visual representation of the relationships.

Table 24: Ports used by the Enterprise Service Manager

Source	Target	Default Port	Required for	Description
Enterprise Service Manager	Gateway cluster	8443	Configuration and Runtime	❶ This port is used by the ESM to communicate with the Gateway cluster via HTTPS. The port number is defined in the *admin.esmPort* cluster property in the Policy Manager. For more information, see the following topics in the *CA API Gateway - Policy Manager User Manual*: *Managing Listen Ports* *Listen Port Properties* *Gateway (Cluster) Properties*
Browser	Enterprise Service Manager	8182	Configuration and Runtime	❷ The port is the HTTPS listener for the ESM. Any port number between 1025 and 65535 may be used. This port is configured initially on the Gateway main menu using option **7** (Display ESM configuration menu) > option **1** (Configure the ESM). It can be changed on the "System Settings Page" on page 81.
Gateway cluster	Enterprise Service Manager	8182	Configuration	❸ This port is used to configure the certificate trusted for remote management on the Gateway. By default, it is the same as the "Browser->ESM" port described above. Alternatively, you can establish trust directly on the Gateway cluster by entering the thumbprint of the trusted certificate on the "System Settings Page" on page 81.

Source	Target	Default Port	Required for	Description
Enterprise Service Manager	Gateway Cluster	8765	Configuration and Runtime	❹ The port allows a Gateway node to be remotely managed by the ESM. Used for monitoring and Gateway control (start/stop). This port is configured on the Gateway main menu using option **5** (Display Remote Management configuration menu) > option **2** (Listener port). For more information, see "Configuring the Gateway for Remote Access" in the *CA API Gateway Installation and Maintenance Manual (Appliance Edition)*.
Browser	Gateway Cluster	8443	Configuration	❺ This port is used to configure Gateway cluster trust of the ESM. The port number is defined in the *admin.esmPort* cluster property in the Policy Manager.
Browser	Gateway Cluster	9443	Runtime	❻ This port allows the Policy Manager browser client to connect to the Gateway cluster. The port number is defined in the *cluster.adminAppletPort* cluster property in the Policy Manager. For more information, see *Policy Manager Browser Client* in the *CA API Gateway - Policy Manager User Manual*.



❶ ESM->Gateway port set in the "admin.esmPort" cluster property in the Policy Manager.

❷ Browser->ESM port initially set in Gateway main menu (option 7 > option1). Can be changed later in "System Settings" page on ESM.

❸ Gateway->ESM listener port, used to receive trusted certificate from ESM. This is the same as port ❷.
Alternatively, you can enter thumbprint of trusted certificate directly on "System Settings" page of ESM.

❹ ESM->Gateway port, to allow node to be remotely managed by ESM. Port set in the Gateway configuration menu (option 5 > option 2).

❺ Browser->Gateway port, to configure trust, set in the "admin.esmPort" cluster property in the Policy Manager.

❻ Browser->Gateway port, to allow the Policy Manager browser client to run, set in the "cluster.adminAppletPort" cluster property in the Policy Manager.

Figure 35: Ports used by Enterprise Service Manager

Appendix B:
Configuring the ESM Logs

The Enterprise Service Manager maintains system logs which occur automatically in the background (these can be viewed on the "Viewing Audits and Logs" on page 9 page). By default, debug logging is not enabled due to the impact it will have on performance. Follow the steps below if you wish to enable debug logging or if you need to control the level of detail contained in the log files displayed in the "[Tools] Tab" on page 78.

Note: Debug logging is *not* recommended in production environments, due to the performance impact. Please consult with CA Technical Support before altering the debug logging levels.

➢ *To configure logging on the Enterprise Service Manager:*

1. On the Gateway appliance, log in as user **ssgconfig**. The Gateway Configuration menu appears.
2. Select **3** (Use a privileged shell [root]). This opens a command prompt with root privileges.
3. Edit the *logging.properties* file as per Table 25:

   /opt/SecureSpan/EnterpriseManager/etc/logging.properties

   Changes to *logging.properties* take effect immediately.

The *logging.properties* file is used to configure the details recorded in the Enterprise Service Manager logs. Refer to the following table for configuration details.

Table 25: Configuring ESM logging

To:	Add this line to ***logging.properties***:
Enable debug logging	**com.l7tech.logging.debug = true** Enabling debug logging will add stack traces to the log, to assist in troubleshooting. **Note:** Debug logging is not recommended in production environments due to the performance impact.
Modify the logging levels	**com.l7tech.level = <*level*>** Where <*level*> is a valid Java logging level. For more information about the levels, see "Logging Levels" in the *CA API Gateway Installation and Maintenance Manual*. The default logging level if *the com.l7tech.level* property is not defined is 'CONFIG'.

➢ *To view the Enterprise Service Manager logs:*

- These logs can be viewed inside or outside of the Enterprise Service Manager:
  - **Inside ESM:** In the [Tools] tab. For more information, see "Viewing Audits and Logs" on page 9 and "[Tools] Tab" on page 78.
  - **Outside ESM:** In the following directory on the Gateway machine being monitored:

    /opt/SecureSpan/EnterpriseManager/var/logs

Index