



CHAPTER 8

Administering Cisco ISE

This chapter describes the administrative activities for the Cisco Identity Services Engine (ISE) and how to perform them. The following topics are covered:

- [Logging In, page 8-1](#)
- [System Time and NTP Server Settings, page 8-2](#)
- [Configuring Email Settings, page 8-3](#)
- [Configuring System Alarm Settings, page 8-4](#)
- [Configuring Alarm Syslog Targets, page 8-5](#)
- [Managing Software Patches, page 8-7](#)

Logging In

The Cisco ISE GUI is supported on HTTPS-enabled Mozilla Firefox version 3.x and Microsoft Internet Explorer version 8 (in Internet Explorer 8-only mode).



Note

Cisco ISE GUI is not supported on Internet Explorer version 8 running in Internet Explorer 7 compatibility mode.

After you have installed Cisco ISE as described in the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4](#), you can log into Cisco ISE.

To log into the Cisco ISE GUI, complete the following steps:

-
- Step 1** Enter the ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*).
- The ISE login window appears.
- Step 2** Enter **admin** in the Username field.
- Step 3** Enter **cisco** in the Password field. This value is case-sensitive.



Note

admin and **cisco** are the default values for the username and password that you must use to access the ISE user interface for the first time.

Step 4 Click **Login** or press **Enter**.

If your login is successful, you will be prompted to change your password.

Step 5 Enter your new password and re-enter it for confirmation.

You can now access the menus in the ISE user interface.

**Note**

Any time your login is unsuccessful, click the Problem logging in? link in the Login window and use the default username and password values listed in Steps 2 and 3.

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID enough times, the Cisco ISE user interface “locks you out” of the system, adds a log entry in the **Monitor > Reports > Catalog > Server Instance > Server Administrator Logins** report, and suspends the credentials for that administrator ID until you have an opportunity to reset the password associated with that administrator ID, as described in the “Performing Post-Installation Tasks” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.0.4](#). The number of failed attempts required to disable the administrator account is configurable according to the guidelines described in [Configuring a Password Policy for Administrator Accounts, page 4-56](#).

System Time and NTP Server Settings

Cisco ISE allows you to view the system time setting through the ISE user interface. The Cisco Application Deployment Engine (ADE) operating system, which is the operating system in the Cisco ISE, allows you to configure three Network Time Protocol (NTP) servers. You can use the NTP servers to maintain accurate time and synchronize time across different time zones. This procedure ensures that your logs are always reliable.

**Note**

You must configure the system time and NTP server settings on each ISE node in your deployment individually.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To view system time and configure NTP server settings, complete the following steps:

Step 1 From your primary ISE node, choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **System Time**.

**Note**

If you want to view the system time and configure the NTP server settings on a secondary ISE node, you must log into the user interface of the secondary node and choose **Administration > System > System Time**.

The timezone that you have configured appears in the Time Zone field. You cannot edit this value from the ISE user interface. To configure the time zone, you must enter the following command from the ISE CLI:

clock timezone *timezone*

For more information on the **clock timezone** command, see the [Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4](#).

Step 3 In the NTP Server Configuration area, enter the IP address of your primary, secondary, and tertiary NTP servers.

If you have only one NTP server in your network, enter the IP address in the Primary Server text box. If you have two NTP servers, enter the IP address in the Primary Server and Secondary Server text boxes.

**Note**

If you enter the same IP address for the primary and secondary name servers, when the primary is down, Cisco ISE cannot access any other secondary name server because you have selected the same one as your secondary name server. We recommend that you verify the IP address of the secondary server and ensure that it is different than the primary server.

Step 4 Click **Save** to save the NTP server settings.

Now, when you hover your cursor over to the hostname in the top right corner of the Cisco ISE dashboard window, the current server role and server system time appear in the Server Information quick-view pop-up.

**Note**

We recommend that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Configuring Email Settings


This section shows you how to specify the address of the email server and the name that is displayed for this address. This address is used for sending and receiving log messages.

**Note**

Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. For more information, see [Understanding the Impact of Roles and Admin Groups](#).

To specify email settings for the mail server, complete the following steps:

Step 1 Select **Administration > System > Settings**

- Step 2** In the left-hand Settings panel, expand **Monitoring** and then choose **Email Settings**.
- Step 3** In the Mail Server field, enter the hostname or IPV4 address of the outgoing SMTP mail server. This information is required to send email notifications for alarms.
-  **Note** A hostname requires a format such as mailman.cisco.com. An IPv4 address requires a format such as, 192.168.1.1.
- Step 4** Enter a name or email address (such as admin@somedomain.com) in the Mail From field. This name or email address is what users see when they receive a message from the mail server.
- Step 5** Click **Submit**.
-

Configuring System Alarm Settings

System alarms notify you of critical conditions that are encountered. System alarms are standard and cannot be created or deleted.

This section describes the available system alarms, shows you how to enable and disable the alarms, and how to configure to receive notification. Cisco ISE provides the following system alarms:

- Distributed Management—This alarm is sent during the following operations:
 - Registering a node (Success or Failure)
 - Deleting a node
 - Unregistering a node (Success or Failure)
 - Updating a node (Success or Failure)
- License Enforcement—This alarm is sent when the number of concurrent endpoints or users exceed the total amount allowed for a particular license.
- Software Management—This alarm is sent during the following operations:
 - Patch Installation (Success or Failure) on a node
 - Patch Rollback (Success or Failure) on a node
- Purging Failed—This alarm is sent whenever a purge fails.
- Collector—This alarm is sent whenever collection failures occur.
- Alarm Manager—This alarm is sent when the **Alarm** manager cannot complete monitoring of all thresholds.
- Backup Failed—This alarm is sent whenever there is backup failure.

You can choose to send alarm notifications through email and as syslog messages. To send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. For more information, see [Configuring Alarm Syslog Targets](#).

Enabling and Configuring System Alarms

The following task shows you how to activate and configure notification for system alarms.

To enable and configure a system alarm, complete the following steps:

-
- Step 1** Select **Administration > System > Settings**.
 - Step 2** In the left Settings panel, expand **Monitoring** and then choose **System Alarm Settings**.
 - Step 3** Check the **Notify System Alarms** check box. A green check mark appears to show that the option has been activated.
 - Step 4** Designate the number of hours to suppress duplicate system alarms from being sent to the Email Notification User List.
 - Step 5** To request Email Notification, enter a valid email address in the text field. Then, check the **Email in HTML Format** check box, as desired.
When a system alarm occurs, an email is sent to all the recipients in the Email Notification User List.
 - Step 6** To request Syslog Notification, check the **Send Syslog Message** check box.
 - Step 7** Click **Submit** to apply the settings.
-

For more information:

See the [System Alarm Settings](#) section of [Appendix A, “User Interface Reference.”](#)

Disabling System Alarms

The following task shows you how to deactivate system alarms.

To disable system alarms, complete the following steps:

-
- Step 1** Select **Administration > System > Settings**.
 - Step 2** In the left Settings panel, expand **Monitoring** and then choose **System Alarm Settings**.
 - Step 3** Uncheck the **Notify System Alarms** check box. The green check mark disappears to show that the option has been deactivated.
-

For more information:

See the [System Alarm Settings](#) section of [Appendix A, “User Interface Reference.”](#)

Configuring Alarm Syslog Targets

This section shows you how to create, edit, and delete alarm syslog targets.

If you configure system alarm notifications to be sent as syslog messages, then you need a syslog target to receive the notification. Alarm syslog targets are the destinations to which alarm syslog messages are sent. A system that is configured as a syslog server is also required to receive syslog messages.

Creating and Editing Alarm Syslog Targets

When you create or edit an alarm syslog target, you establish or modify the destination to which syslog messages are sent.

To create and edit an alarm syslog target, complete the following steps:

-
- Step 1** Select **Administration > System > Settings**.
- Step 2** In the left Settings panel, expand **Monitoring** and then choose **Alarm Syslog Targets**.
- Step 3** To create an alarm syslog target, do the following:
- Click **Create**.
 - Enter a unique name in the Name field and a meaningful description in the Description field.
 - Enter a valid IP address in the IP Address field and click **Submit**.
- The newly created alarm syslog target appears in the list.
- Step 4** To edit an alarm syslog target, do the following:
- Click the alarm syslog target Name link from the list.
 - Modify the Name and Description, as necessary.
 - Change the IP Address as needed, and click **Submit**.
- Your changes are applied to the alarm syslog target.
-

For more information:

See the [Alarm Syslog Targets](#) section of [Appendix A, “User Interface Reference.”](#)

Deleting Alarm Syslog Targets

You can delete an alarm syslog target at any time.

To delete an alarm syslog target, complete the following steps:

-
- Step 1** Select **Administration > System > Settings**.
- Step 2** In the left Settings panel, expand **Monitoring** and then choose **Alarm Syslog Targets**.
- Step 3** Check the check box next to the alarm syslog target that you want to delete. A green check mark appears to show that it is selected.
- Step 4** Click **Delete**, and then click **Yes** in the dialog prompt to confirm the deletion.
-

For more information:

See the [Alarm Syslog Targets](#) section of [Appendix A, “User Interface Reference.”](#)

Managing Software Patches

You can install patches on ISE servers in your deployment from the primary administration node. ISE patches are usually cumulative, however, any restrictions on the patch installation will be described in the *README* file that will be included with the patch. Cisco ISE allows you to perform patch installation and rollback from either the command-line interface (CLI) or GUI.

When you install or roll back a patch from a standalone or primary administration node, ISE restarts the application. You might have to wait for a few minutes before you can log back in.

**Note**

When you install or roll back a patch from the primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary and all the secondary nodes in the deployment. If the patch installation is successful on the primary node, Cisco ISE then proceeds to the secondary nodes. If it fails on the primary node, the installation is aborted. However, if the installation fails on any of the secondary nodes for any reason, it still continues with the next secondary node in your deployment.

To roll back a patch from ISE nodes in a deployment, you must roll back the change from the primary node and if successful, the patch is rolled back from the secondary nodes. If it fails on the primary node, the rollback process is aborted. However, if it fails on any of the secondary nodes, it still continues to roll back the patch from the next secondary node in your deployment.

**Note**

You cannot install a patch whose version is lower than the patch that is currently installed on ISE. Similarly, you cannot roll back changes of a lower version patch if a higher version is currently installed on Cisco ISE. For example, if patch 3 is installed on your ISE servers, you cannot install patch 1 or 2, or roll back patch 1 or 2.

To install and roll back patches from the CLI, refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4](#).

This section contains:

- [Installing a Software Patch, page 8-7](#)
- [Rolling Back Software Patches, page 8-10](#)
- [Viewing Patch Install and Rollback Changes in the Audit Report, page 8-12](#)

Installing a Software Patch

To install a patch from the GUI, you must download the patch from the following location to the system that runs your client browser:

**Note**

Cisco ISE allows you to install a patch on an Inline Posture node only through the CLI.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To install a patch on Cisco ISE nodes in a deployment, complete the following steps:

Step 1 Choose **Administration > System > Operations > Patch Management**.

The Patch Management page appears, which lists the patches that are installed on your ISE node.

Step 2 Click **Install**.

The Install Patch Bundle page appears.

Step 3 Click **Browse** to choose the patch that you downloaded earlier.

Step 4 Click **Install** to install the patch.

Ensure that you install patches that are applicable for the Cisco ISE version that is deployed in your network. Cisco ISE reports any mismatch in versions and also any errors in the patch file.

After the patch is installed on the primary administration node, Cisco ISE logs you out and you have to wait for a few minutes before you can log back in.



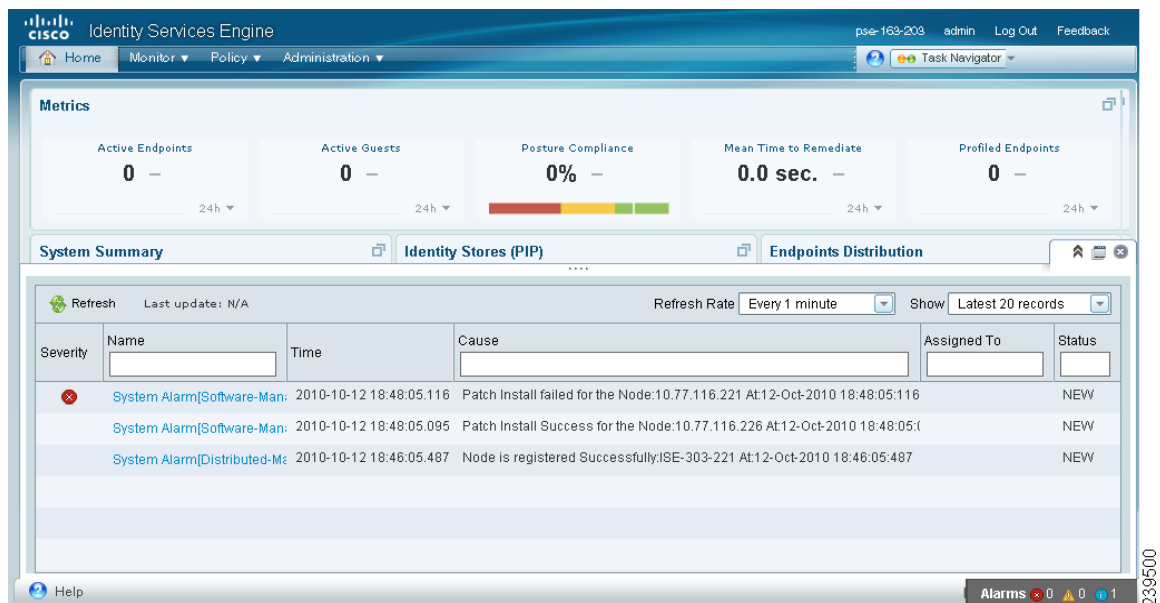
Note When patch installation is in progress, Show Node Status is the only option that is enabled in the Patch Management page.

Step 5 After you log back in, from the dashboard, click the **Alarms** link at the bottom of your screen as shown in [Figure 8-1](#).



Note The alarms are generated only for patch install or rollback operations performed from the GUI. To view the status of patch installation from the CLI, you must check the *ade.log* file, which you can access by [Downloading Support Bundles](#).

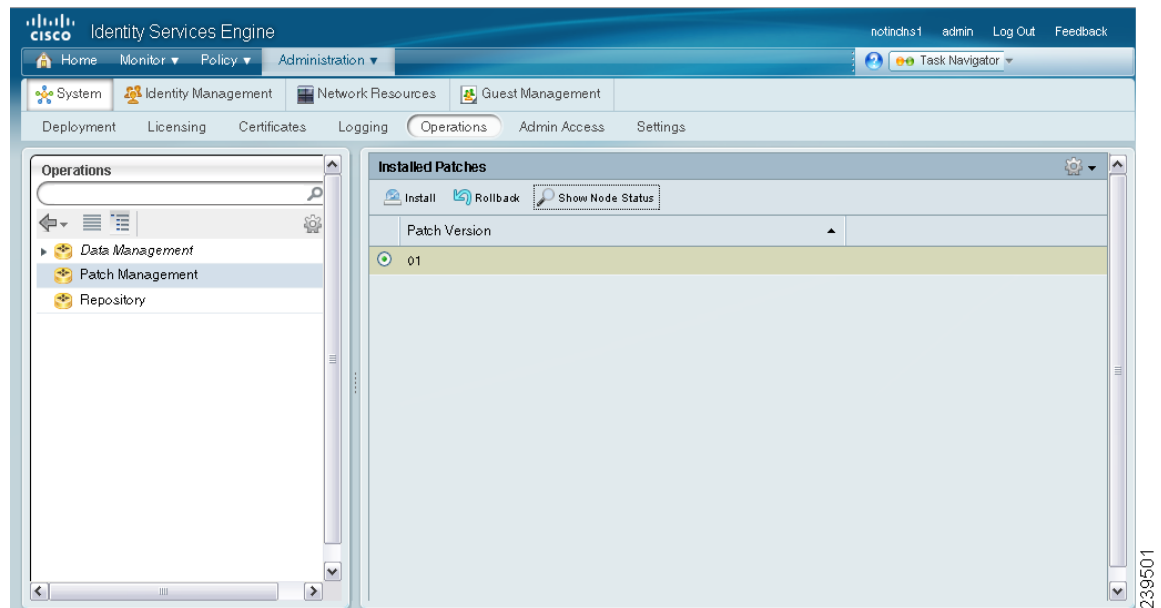
Figure 8-1 Patch Installation Status in the Dashboard



Step 6 You can go back to the Patch Installation page (choose **Administration > System > Operations > Patch Management**).

Step 7 The Installed Patches page appears as shown in [Figure 8-2](#).

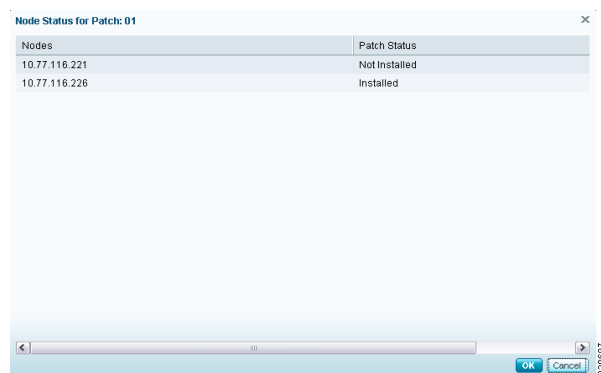
Figure 8-2 Patch Listing Page



This page lists all the patches that you have installed so far.

Step 8 Click the radio button next to the patch whose status you want to view and click **Show Node Status**. A pop-up appears that shows the status of this patch (Installed, Not Installed, or Node is Down) on the various nodes in your deployment as shown in [Figure 8-3](#).

Figure 8-3 Node Status Pop-Up



Step 9 After the patch is installed on the primary node, ISE will install it on your secondary nodes consecutively.

While installing a patch on the secondary nodes, the primary administration node is not restarted and you can continue to perform your tasks on the primary administration node. During this time, the secondary ISE nodes are restarted consecutively after the patch is installed on those nodes. At any point during the installation process, you can click the **Show Node Status** button to see the status of patch installation.

If for some reason, the patch installation fails on the primary administration node, the installation does not proceed to the secondary nodes.

- Step 10** To check if the installation is complete, click the radio button next to the patch that you have installed and click **Show Node Status**.



Note The Node Status pop-up only provides information about patch installation on ISE nodes. Patch installation and rollback on Inline Posture nodes can only be done through the Cisco ISE CLI and this status will not be displayed in the Node Status pop-up.

A pop-up similar to the one shown in [Figure 8-4](#) appears.

Figure 8-4 Node Status Pop Up: Installation Complete



Patch installation is now complete on all the ISE nodes.

If for some reason the patch is not installed on one or more secondary nodes, ensure that the node is up and repeat the process from [Step 2](#) to install it on the remaining nodes. Cisco ISE installs the patch on those nodes that do not have this version of the patch.

Related Topics:

- [Managing Software Patches, page 8-7](#)
- [Rolling Back Software Patches, page 8-10](#)
- [Viewing Patch Install and Rollback Changes in the Audit Report, page 8-12](#)

Rolling Back Software Patches

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To roll back a patch from Cisco ISE nodes in your deployment, complete the following steps:

Step 1 Choose **Administration > System > Operations > Patch Management**.

The Installed Patches page appears.

Step 2 Click the radio button for the patch version whose changes you want to roll back, then click **Rollback**.



Note When patch rollback is in progress, Show Node Status is the only option that is enabled in the Patch Management page.

After the patch has been rolled back on the primary administration node, Cisco ISE will roll back the patch from the secondary nodes. If for some reason the patch rollback fails on the primary node, the patches are not rolled back from the secondary nodes.

After the patch is rolled back from the primary administration node, Cisco ISE logs you out and you have to wait for a few minutes before you can log back in.

Step 3 After you log in, click the **Alarms** link at the bottom of the dashboard screen to view the status of the rollback operation.



Note The alarms are generated only for patch install or rollback operations performed from the GUI. To view the status of patch installation from the CLI, you must check the *ade.log* file, which you can access by [Downloading Support Bundles](#).

Step 4 Go back to the Installed Patches page (choose **Administration > System > Operations > Patch Management**) to check the status of this rollback on the other nodes in your deployment.

Step 5 If the patch rollback is in progress, this status will be visible in the Installed Patches page. To view the status of the patch rollback, you can choose the patch and click **Show Node Status**.

A pop-up appears that shows the status of the patch on the various ISE nodes in your deployment.

While Cisco ISE rolls back the patch from the secondary nodes, you can continue to perform other tasks from your primary administration node GUI. The secondary nodes will be restarted after the rollback.

Step 6 Click the radio button for the patch and click **Show Node Status** to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process from [Step 2](#) to roll back the changes from the remaining nodes. Cisco ISE rolls back the patch only from those nodes that still have this version of the patch installed.

Related Topics:

- [Managing Software Patches, page 8-7](#)
- [Installing a Software Patch, page 8-7](#)
- [Viewing Patch Install and Rollback Changes in the Audit Report, page 8-12](#)

Viewing Patch Install and Rollback Changes in the Audit Report

The monitoring and troubleshooting component of Cisco ISE provides information on the patch installation and rollback operations that are performed on your ISE nodes.

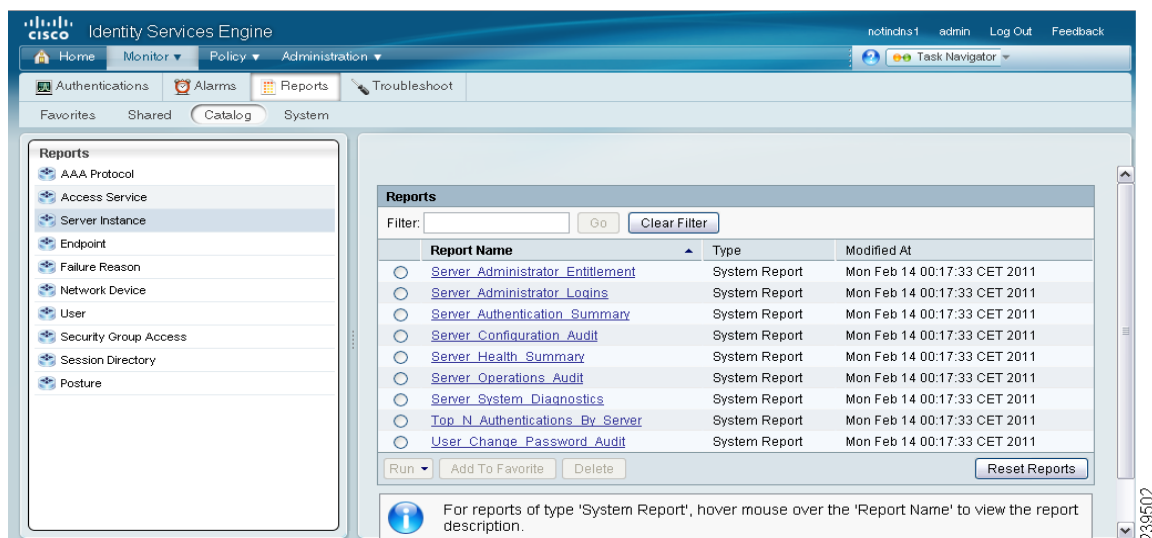
Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Monitoring Admin or Helpdesk Admin. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To view these reports, complete the following steps:

- Step 1** Choose **Monitor > Reports > Catalog**.
- Step 2** From the Reports navigation pane on the left, click **Server Instance**.
A page similar to the one shown in [Figure 8-5](#) appears.

Figure 8-5 Server Instance Reports Page

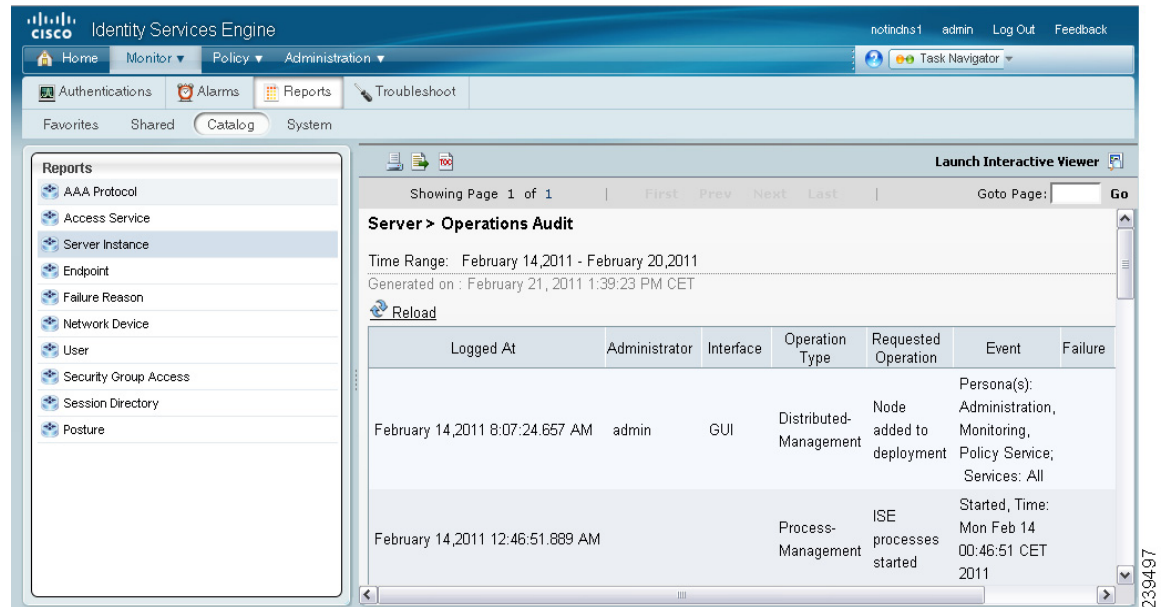


- Step 3** Click the **Server Operations Audit** radio button, then click **Run** and choose the time period for which you want to generate the report.

Step 4 A report similar to the one shown in [Figure 8-6](#) appears.

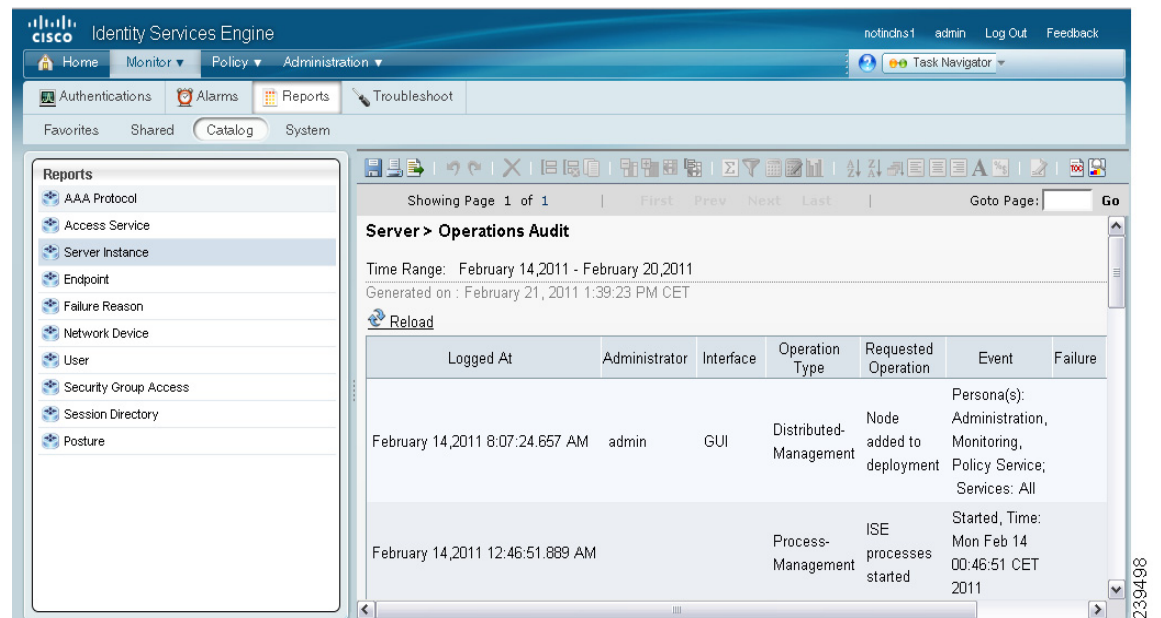
This report provides information on the patch installation and rollback operations that were performed within the time period that you have chosen.

Figure 8-6 ISE Operations Audit Report



Step 5 Click the Launch Interactive Viewer link in the right upper corner of this screen to view, sort, and filter the data in this report. A screen similar to the one shown in [Figure 8-7](#) will appear.

Figure 8-7 ISE Operations Report: Interactive View



For information on how to use the interactive viewer features, see the [“Working with the Interactive Viewer Toolbar”](#) section on page 23-12.

Related Topics:

- [Managing Software Patches](#)
- [Installing a Software Patch](#)
- [Rolling Back Software Patches](#)