Performing Post-Installation Tasks

This chapter describes several tasks that you must perform after successfully completing the installation and configuration of the Cisco Identity Services Engine (ISE) 3300 Series appliance. This chapter contains information about the following topics:

- Installing a License, page 1-1
- Accessing Cisco ISE Using a Web Browser, page 1-7
- Verifying the Cisco ISE Configuration, page 1-10
- Verifying the Installation of VMware Tools, page 1-12
- Resetting the Administrator Password, page 1-14
- Reimaging a Cisco ISE 3300 Series Appliance, page 1-16
- Configuring the Cisco ISE System, page 1-17
- Enabling System Diagnostic Reports in Cisco ISE, page 1-18
- Installing New Cisco ISE Software, page 1-18
- Configuring Certificates for Inline Posture Nodes, page 1-18

Installing a License

To manage a Cisco ISE system, you must have a valid license. Licensing provides the ability to restrict the use of the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources.

Concurrent endpoints represent the total number of supported users and devices. Endpoints can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices.

Cisco ISE software feature support is split into two functional sets:

- Base Package—Enables basic services of network access, guest, and link encryption
- Advanced Package—Enables more advanced services like Profiler, Posture, and Security Group Access
Chapter 1      Performing Post-Installation Tasks

Installing a License

Each license package supports a specific number of concurrent endpoints that can connect and use the corresponding services. Services for each package type are enabled by installing corresponding licenses. There are two possible license-installation approaches:

- **Base and Advanced Licenses**: Base and Advanced licenses can be installed to enable corresponding feature support, depending on your installation. Each license may be installed separately, and you can also choose to install multiple licenses of the same type to cumulatively increase the number of endpoints for the corresponding package.

- **Wireless License**: The Wireless license enables the same number of endpoints on both the base and advanced package. However, the devices that are supported with this type of license are restricted to wireless devices. It is possible to subsequently remove this restriction by installing a Wireless Upgrade license that enables the base and advanced package feature support for all types of devices.

The following sections provide information about these topics:

- Types of Licenses, page 1-3
- Obtaining a License, page 1-6
- Autoinstallation of the Evaluation License, page 1-7

**Built-In License**

The Cisco ISE system includes an evaluation license that features both Base and Advanced package services, is valid for a 90-day period, and restricts the number of system base and advanced package users to 100. The Cisco ISE system prompts you before the evaluation license expires to download and install a valid production license.

When the evaluation license expires at the end of its 90-day period, the Administration web application will prompt you to install a valid production license for Base, Base and Advanced, or Wireless. (Although the evaluation license allows you to provide support for both wired and wireless users, purchasing and applying a Wireless License option cuts off support for any wired users that you may have been supporting during the evaluation period.) For specific details on using the administrator user interface to add and modify license files, see the “Managing Licenses” chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

**License Management**

When you deploy only one Administration ISE node in your network, licenses are centrally managed by the Administration ISE node and are automatically distributed among all other nodes (except Inline Posture nodes) in the deployment. When you have installed primary and secondary Administration ISE nodes in your network in a distributed deployment, however, each of the Administration ISE nodes in the deployment must have the same license files. In addition, in order to install license files on your Cisco ISE, the node must be in standalone mode or deployed as the primary Administration ISE node for the period of time it takes to install the required licenses.

---

**Note**

Cisco ISE licenses are generated based on the Administration ISE node hardware ID, *not* the MAC address.

**Concurrent Endpoint Counts**

Each Cisco ISE license includes a count value for the Base, Base and Advanced, or Wireless packages that restricts the number of concurrent endpoints that can use Cisco ISE services. The count includes the total number of endpoints across the entire deployment that are concurrently connected to the network and accessing its services. License enforcement within Cisco ISE if the number of endpoints increases beyond the supported license count is a soft one, with the endpoint remaining unblocked from accessing services. For information about the alarms that are generated when endpoints exceed the licensed values,
see License Enforcement, page 1-3.

**License Enforcement**
Cisco ISE tracks concurrent endpoints on the network and generates alarms when endpoint counts exceed the licensed amounts:

- 80% Info
- 90% Warning
- 100% Critical

**Caution**
Accurate endpoint accounting relies on RADIUS accounting.

**License Expiration**
Alarms will not be sent for license expiration notification. Upon logging into a Cisco ISE node with an expired license, administrators are not able to access the Cisco ISE dashboard or other services, and instead, are redirected to a license page on www.cisco.com.

**Cisco ISE License Application Behavior**

- When you install a Wireless License over the default Evaluation License, the Wireless License overrides the Evaluation License parameters with the specific duration and user count associated with the Wireless License.
- When you install a Base License over the default Evaluation License, the Base License overrides only the “Base” portion of the Evaluation License; thus keeping the Advanced License capabilities available only for the remainder of time allowed by the default Evaluation License duration.
- When you install an Advanced License over the default Evaluation License, the Advanced License overrides only the “Advanced” portion of the Evaluation License; thus keeping the Base License capabilities available only for the remainder of time allowed by the default Evaluation License duration.

**Note**
To avoid expiration issues that are associated with Base or Advanced features in the Cisco ISE, we recommend replacing the default Evaluation License with both a Base and Advanced License at the same time.

**Types of Licenses**

This section describes the four types of licenses that are supported for use with Cisco ISE 3300 Series appliances:

- Evaluation License, page 1-4
- Base License, page 1-5
- Advanced License, page 1-5
- Wireless License, page 1-5

Generally speaking, Base and Advanced licenses are primarily focused on providing Cisco ISE services, and Wireless license options are focused on ensuring that you are able to deploy Cisco ISE more quickly and easily in a purely wireless endpoint environment.

License Guidelines

The following are some license guidelines that you need to observe:

- Licenses are applied on Administration ISE nodes only.
- Deployments cannot have an Advanced license without the Base license.
- Wireless Licenses cannot coexist on an Administration ISE node with Base or Base and Advanced Licenses.
- Administration ISE nodes should ensure that networks cannot add more Advanced endpoint licenses than Base endpoint licenses.
- Inline Posture nodes do not require a separate license.
  - Inline Posture nodes are only supported on Cisco ISE 3300 Series appliances. They are not supported on VMware server systems.
  - Only certain wireless LAN controller (WLC) versions are supported by Inline Posture. (See Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x for details.)

Note: Inline Posture nodes are not supported on VMware server systems.

- When you launch the Cisco ISE before a license has been applied, only a bootstrap configuration that includes a license page appears.
- When the evaluation license approaches expiration, you are prompted to download and install a production license (Base, Base and Advanced, or Wireless) when you attempt web-based access with the Cisco ISE system.
- When a Base license is applied, Cisco ISE user interface screens and tabs are displayed for basic network access and Guest access.
- When an Advanced license is applied, Cisco ISE user interface screens and tabs are displayed for Profiler, Posture, and Security Group Access.

Evaluation License

The evaluation license consists of both the Base and Advanced license packages. An evaluation license is limited to support only 100 endpoints, and it expires in 90 days. This duration is not based on a real-time clock, but on the Cisco ISE system clock. The evaluation license comes preinstalled, and it does not require a separate installation.

As the evaluation license approaches the end of its 90-day period, the Cisco ISE system prompts the user to download and install a valid product license (Base or Advanced) by generating an alarm to upgrade the license. Upon installing a regular license, the services are continued as per the chosen package.
**Base License**

Base licenses are installed by using the Cisco ISE administrative interface on the device. Like the evaluation license, the Base license usage is also recorded on the device. The Base licenses are perpetual licenses. The Base package includes Authentication, Authorization, Guest, and Sponsor services, and this license package never expires.

**Advanced License**

Advanced licenses can be installed only on top of the Base license. You cannot upgrade the evaluation license to an Advanced license without first installing the Base license. In addition to the features that are available in the Base license package, the Advanced license activates the Profiler, Posture, and Security Group Access services of the Cisco ISE.

At any time, the total number of endpoints supported by the Advanced package cannot be higher than the Base license count (it can be equal to or less than Base license count).

*Note*

The Advanced Licenses are subscription-based and there are two valid subscription terms: three-year or five-year.

**Wireless License**

Wireless Licenses are designed to provide a flexible option to exclusively wireless service providers that not only offers the essential Base License functions like basic network access (authentication and authorization), Guest services, and link encryption, but also all Advanced License services, including Profiler, Posture, and Security Group Access services. The Cisco ISE ensures that only exclusively wireless customers are able to take advantage of the Wireless License options by only allowing RADIUS Wireless authentication requests that come from a wireless LAN controller (WLC) (Other authentication request methods are dropped.) In addition, the LiveLogs entries also indicate reasons for the dropped requests by indicating, “Request from a non-wireless device was dropped due to installed Wireless license.”

*Note*

Like Advanced License packages, Wireless Licenses are subscription-based.

If you currently subscribe to a Wireless License model for your deployment and then decide you want to offer Cisco ISE support for non-wireless endpoints on your network, rather than revert to a Base and Advanced License scheme as described earlier, you can move to a Wireless Upgrade License. These licenses are designed to provide the full range of Cisco ISE functions and policy management capabilities for all wireless and non-wireless client access methods, including wired and VPN concentrator access.

*Note*

You can only install a Wireless Upgrade license option on top of an existing Wireless license with the same allowable endpoint count. You cannot install a Wireless Upgrade on top of a Base plus Advanced license package.
Obtaining a License

To continue to use Cisco ISE services after the 90-day evaluation license expires, and to support more than 100 concurrent endpoints on the network, you must obtain and install your own Base or Base and Advanced license packages in the Cisco ISE. License files are based on a combination of the Cisco ISE hardware ID and Product Authorization Key (PAK). At the time you purchase your Cisco ISE, or before the 90-day license expires, you can access Cisco.com and order your Base or Base and Advanced licenses.

Within an hour of ordering your license files from Cisco.com, you should receive an email with the Cisco Supplemental End-User License Agreement and a Claim Certificate containing a PAK for each license that you order. After receiving the Claim Certificate, you can log in and access the Cisco Product License Registration site at http://www.cisco.com/go/license and provide the appropriate hardware ID information and PAK to generate your license.

You must supply the following specific information to generate your license file:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)
- Product Authorization Key (PAK)

Remember, if you are installing primary and secondary Administration ISE nodes in your network in a distributed deployment, each of the Administration ISE nodes in the deployment must have the same license files. In addition, in order to install license files on your Cisco ISE, the node must be in standalone mode or deployed as the primary Administration ISE node for the period of time it takes to install the required licenses. The day after you submit your license information in the Cisco Product License Registration site, you will receive an email with your license file as an attachment. Save the license file to a known location on your local machine and use the instructions in Managing Licenses in see the “Managing Licenses” chapter of the Cisco Identity Services Engine User Guide, Release 1.1.x to add and update your product licenses in the Cisco ISE.

To determine your primary Administration ISE node hardware ID, complete the following:

**Step 1** Access the direct-console CLI and enter the `show inventory` command. The output includes a line that is similar to the following:

```
PID: NAC3315, VID: V01, SN: ABCDEFG
```

**Step 2** (Optional) If the license has not expired, you can view the primary Administration ISE node hardware ID by completing the following steps:

a. Choose Administration > System > Licensing.

   The License Operations navigation pane and Current Licenses page appears.

b. In the License Operations navigation pane, click Current Licenses.

   The Current Licenses page appears.

c. Select the button corresponding to the Cisco ISE node that you want to check for the primary Administration ISE node hardware ID, and click Administration Node.

   The product identifier, version identifier, and serial number appear.
Note  Cisco ISE licenses are generated based on the primary Administration ISE node hardware ID, not the MAC address.

For detailed information and license part numbers that are available for Cisco ISE, including licensing options for new installations as well as migration from an existing Cisco security product like Cisco Secure Access Control System, see the Cisco Identity Services Engine Ordering Guidelines at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/guide_c07-656177.html.

Autoinstallation of the Evaluation License

If you are using a virtual machine for Cisco ISE with disk space between 60 and 600 GB, the Cisco ISE automatically installs the evaluation license. All Cisco ISE 3300 Series appliances ship with an evaluation license that is limited to 90 days and 100 endpoints.

After you have installed the Cisco ISE software and initially configured the appliance as the primary Administration ISE node, you must obtain and apply a license for your Cisco ISE as described in Obtaining a License, page 1-6. You apply all licenses to the Cisco ISE primary Administration ISE node by using the primary Administration ISE node hardware ID. The primary Administration ISE node then centrally manages all the licenses that are installed for your deployment.

Cisco ISE licenses are generated based on the primary Administration ISE node hardware ID, not the MAC address. The process of managing the licenses is the same for dual Administration ISE nodes as it is for a single Administration ISE node.

Next Steps:
To manage your licenses by using the Cisco ISE user interface, see the “Managing Licenses” chapter of the Cisco Identity Services Engine User Guide, Release 1.1.x and complete the following tasks:
- Adding and upgrading a license
- Editing a license

Accessing Cisco ISE Using a Web Browser

The Cisco ISE 3300 Series appliances support a web interface using the following HTTPS-enabled browsers:
- Mozilla Firefox version 3.6
- Mozilla Firefox version 9
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9 (in Internet Explorer 8 compatibility mode)

Note  The Cisco ISE user interface does not support using the Microsoft IE8 browser in its IE7 compatibility mode (the Microsoft IE8 is supported in its IE8-only mode).
This section provides information about the following topics:

- Logging In, page 1-8
- Logging Out, page 1-9

### Logging In

When you login to the Cisco ISE web-based interface for the first time, you will be using the preinstalled Evaluation license. You must use only the supported HTTPS-enabled browsers listed in the previous section. After you have installed Cisco ISE as described in this guide, you can log into the Cisco ISE web-based interface.

**To log into Cisco ISE using the web-based interface, complete the following steps:**

**Step 1**
After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

**Step 2**
In the Address field, enter the IP address (or hostname) of the Cisco ISE appliance by using the following format, and press **Enter**.

http://<IP address or host name>/admin/

For example, entering **http://10.10.10.10/admin/** displays the Cisco ISE Login page.

**Step 3**
In the Cisco ISE Login page, enter the username and password that you defined during setup.

**Step 4**
Click **Login**, and the Cisco ISE dashboard appears.
To recover or reset the Cisco ISE CLI-admin username or password, see the Resetting the Administrator Password, page 1-14.

If you forget your CLI-admin username or password, use the Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.1.xxx) DVD, and choose Password Recovery. This option allows you to reset the CLI-admin username and password.

The minimum required screen resolution to view the Cisco ISE GUI and for better user experience is 1280*800 pixels.

CLI-based and web-based username and password values are not the same when logging into the Cisco ISE. For more information about the differences between the Cisco ISE CLI-admin user and the Cisco ISE web-based admin user, see Admin Rights Differences: CLI-Admin and Web-Based Admin Users, page 1-2.

The license page appears only the first time that you log into Cisco ISE after the evaluation license has expired.

We recommend that you use the Cisco ISE user interface to periodically reset your administrator login password after you successfully log into the Cisco ISE system. To reset your administrator password, see “Configuring Cisco ISE Administrators” in the Cisco Identity Services Engine User Guide, Release 1.1.x for details.

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 Password Negated Due to Administrator Lockout, page 1-15. The number of failed attempts required to disable the administrator account is configurable according to the guidelines that are described in the “Managing Identities” chapter of the Cisco Identity Services Engine User Guide, Release 1.1.x. After an administrator user account gets locked out, an email is sent to the associated admin user.

Logging Out

To log out of the Cisco ISE web-based web interface, click Log Out in the Cisco ISE main window toolbar. This act ends your administrative session and logs you out.

For security reasons, we recommend that you log out of the Cisco ISE when you complete your administrative session. If you do not log out, the Cisco ISE web-based web interface logs you out after 30 minutes of inactivity, and does not save any unsubmitted configuration data.
For more information on using the Cisco ISE web-based web interface, see the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

**Verifying the Cisco ISE Configuration**

This section provides two methods that each use a different set of username and password credentials for logging into and verifying your Cisco ISE configuration:

- Verifying the Configuration Using a Web Browser, page 1-10
- Verifying the Configuration Using the CLI, page 1-11

**Note**

For first time web-based access to the Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup. For CLI-based access to the Cisco ISE system, the administrator username by default is **admin** and the administrator password (which is user-defined because there is no default) represents the values that you configured during setup.

To better understand the rights differences between the CLI-admin user and the web-based admin user, see Admin Rights Differences: CLI-Admin and Web-Based Admin Users, page 1-2.

**Verifying the Configuration Using a Web Browser**

To verify that you successfully configured your Cisco ISE 3300 Series appliance, complete the following steps using a web browser:

**Step 1**

After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

**Step 2**

In the **Address**: field, enter the IP address (or host name) of the Cisco ISE appliance using the following format, and press **Enter**.

http://<IP address or host name>/admin/

For example, entering http://10.10.10.10/admin/ displays the Cisco ISE Login page.
Chapter 1    Performing Post-Installation Tasks

Verifying the Cisco ISE Configuration

Step 3  In the Cisco ISE Login page, enter the username and password that you have defined during setup, and click Login.

The Cisco ISE dashboard appears.

Note  We recommend that you use the Cisco ISE user interface to periodically reset your administrator login password after you have successfully logged into the Cisco ISE system. To reset your administrator password, see “Configuring Cisco ISE Administrators” in the Cisco Identity Services Engine User Guide, Release 1.1.x for details.

Verifying the Configuration Using the CLI

To verify that you successfully configured your Cisco ISE 3300 Series appliance, use the Cisco CLI and complete the following steps:

Step 1  After the Cisco ISE appliance reboot has completed, launch a supported product for establishing a Secure Shell (SSH) connection to the ISE appliance (for example, by using PuTTY, an open source Telnet/SSH client).

Step 2  In the Host Name (or IP Address) field, type in the hostname (or the IP address of the Cisco ISE appliance by using dotted decimal formation), and click Open to display the system prompt for the Cisco ISE appliance.

Step 3  At the login prompt, enter the CLI-admin username (admin is the default) that you configured during Setup, and press Enter.

Step 4  At the password prompt, enter the CLI-admin password that you configured during Setup (this is user-defined and there is no default), and press Enter.

Step 5  To verify that the application has been installed properly, at the system prompt enter show application version ise and press Enter.
Verifying the Installation of VMware Tools

You can verify the installation of the VMware tools in the following two ways:

- Using Summary Tab in the vSphere Client
- Using the CLI

Using Summary Tab in the vSphere Client

Go to the Summary tab of the vSphere Client. The value for VMware Tools should be “OK”. The red arrow in Figure 1-1 indicates that the VMware tools are installed since the value is “OK”. 

Note

The build number reflects the currently installed version of the Cisco ISE software.

Step 6

To check the status of the Cisco ISE processes, at the system prompt enter `show application status ise` and press Enter.

The console displays the following screen.

```
ise-4/admin# show application status ise
Cisco Identity Services Engine
-------------------------------------------
Version : 1.0.2.303
Build Date : Mon Oct 4 04:44:16 2010
Install Date : Mon Oct 4 22:51:55 2010
```

Note

To get the latest Cisco ISE patches and to keep your Cisco ISE up-to-date, visit the following web site: http://software.cisco.com/download/navigator.html

Step 7

To check the Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS) version, at the system prompt, enter `show version` and press Enter.

The console displays the following output:

```
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.2.083
ADE-OS System Architecture: i386
```
Chapter 1  Performing Post-Installation Tasks

Verifying the Installation of VMware Tools

Using the CLI

You can also verify if the VMware tools are installed with the use of the `show inventory` CLI command. This command lists the NIC driver information. On a virtual machine with VMware tools installed, the driver information will be listed as “VMware Virtual Ethernet driver.” Refer to the following example:

```
vm36/admin# show inv
NAME: "ISE-VM-K9          chassis", DESCR: "ISE-VM-K9          chassis"
PID: ISE-VM-K9         , VID: V01 , SN: 8JDC6LIDL3A
Total RAM Memory: 4016564 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU           E5504  @ 2.00GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:BA:C7:82
NIC 0: Driver Descr: VMware Virtual Ethernet driver

(*) Hard Disk Count may be Logical.
vm36/admin#
```

Upgrading VMware Tools

Cisco ISE software contains the supported VMware tools. Although you can upgrade VMware tools through the VMware client user interface, that action does not update the tools on Cisco ISE. The VMware tools are only updated upon installing a new Cisco ISE software version via an ISO installation package, applying an upgrade bundle, or applying a patch. (Patches only have updates for VMware tools if there is a critical need.)
Resetting the Administrator Password

There are two ways to reset the administrator password in Cisco ISE. Depending on the nature of your particular password loss, use one of the following sets of instructions:

- **Lost, Forgotten, or Compromised Password, page 1-14**—Use this procedure if no one is able to log into the Cisco ISE system because the administrator password has been lost, forgotten, or compromised.

- **Password Negated Due to Administrator Lockout, page 1-15**—Use this procedure if your password has been rendered unusable because login failed the specified number of times in a row for the administrator ID.

Lost, Forgotten, or Compromised Password

If no one is able to log into the Cisco ISE system because the administrator password has been lost, forgotten, or compromised, you can use the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD to reset the administrator password.

**Prerequisites:**

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD to start up a Cisco ISE appliance:

- An error may occur if you attempt to start up a Cisco ISE appliance by using the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD under the following conditions:
  - You have a terminal server associated with the serial console connection to the Cisco ISE appliance that includes the `exec` line setting (you are not using the `no exec` line setting).
  - You have a keyboard and video monitor (KVM) connection to the Cisco ISE appliance (this can be either a remote KVM or a VMware vSphere client console connection).

  and

  - You have a serial console connection to the Cisco ISE appliance.

**Note**

You can prevent these connection-related problems when using the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD to start up a Cisco ISE appliance by setting the terminal server setting for the serial console line to use the “no exec” setting. This allows you to use both a KVM connection and a serial console connection.

Resetting the Administrator Password for a Cisco ISE Appliance

To reset the administrator password, complete the following steps:

**Step 1** Ensure that the Cisco ISE appliance is powered up.

**Step 2** Insert the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD in the appliance CD/DVD drive.

**Step 3** Reboot the Cisco ISE appliance to boot from the DVD.
The console displays the following message (this example shows a Cisco ISE 3355):

Welcome to Cisco Identity Services Engine - ISE 3355
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Keyboard/Monitor)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)

<Enter> Boot from hard disk
Please enter boot option and press <Enter>.

boot:

**Step 4**  To reset the administrator password, at the system prompt, enter 3 if you use a keyboard and video monitor connection to the appliance, or enter 4 if you use a local serial console port connection.

The console displays a set of parameters.

**Step 5**  Enter the parameters by using the descriptions that are listed in Table 1-1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin username</td>
<td>Enter the number of the corresponding administrator whose password you want to reset.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the new password for the designated administrator.</td>
</tr>
<tr>
<td>Verify password</td>
<td>Enter the password again.</td>
</tr>
<tr>
<td>Save change and reboot</td>
<td>Enter Y to save.</td>
</tr>
</tbody>
</table>

The console displays:

Admin username:
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
Enter number of admin for password recovery:2
Password:
Verify password:
Save change and reboot? [Y/N]:

See the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*, for commands to reset DB passwords and other CLI commands.

### Password Negated Due to Administrator Lockout

You might enter an incorrect password for your administrator user ID enough times to disable the administrator password. The minimum and default number is five. The Cisco ISE user interface “locks you out” of the system and suspends the credentials for that administrator ID until you have an opportunity to reset the password that is associated with that administrator ID.
Chapter 1      Performing Post-Installation Tasks

Changing the IP Address of a Cisco ISE 3300 Series Appliance

To change the IP address of a Cisco ISE 3300 series appliance, complete the following steps:

Step 1  Log into the Cisco ISE CLI.
Step 2  Enter the following:
        configure terminal
        interface GigabitEthernet 0
        ip address <new_ip_address> <new_subnet_mask>
        exit

Note  Do not use the no ip address command when you change the Cisco ISE appliance IP address.

Note  All the Cisco ISE services have to be restarted after changing the Cisco ISE appliance IP address.

Reimaging a Cisco ISE 3300 Series Appliance

You might need to reimage a Cisco ISE 3300 Series appliance, or you might want to reimage an appliance that was previously used for a Cisco Secure ACS Release 5.1 installation. For example, you plan to migrate Cisco Secure ACS data to Cisco ISE and want to re-use the appliance.
To reimage a Cisco ISE 3300 Series appliance, complete the following steps:

**Step 1** If the Cisco Secure ACS appliance is turned on, turn off the appliance.

**Step 2** Turn on the Cisco Secure ACS appliance.

**Step 3** Press **F1** to enter the BIOS setup mode.

**Step 4** Use the arrow key to navigate to **Date and Time** and press **Enter**.

**Step 5** Set the time for your appliance to the UTC/GMT time zone.

---

**Note** We recommend that you set all Cisco ISE nodes to the UTC time zone. This time zone setting ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

**Step 6** Press **Esc** to exit to main BIOS menu.

**Step 7** Press **Esc** to exit from the BIOS Setup mode.

**Step 8** Perform the instructions described in Before Configuring a Cisco ISE Series Appliance, page 1-1.

**Step 9** Perform the instructions described in Understanding the Setup Program Parameters, page 1-3.

**Step 10** Insert the *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD in the appliance CD/DVD drive.

The console displays (this example shows a Cisco ISE 3315):

```
Welcome to Cisco Identity Services Engine - ISE 3315
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Keyboard/Monitor)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
```

**Step 11** At the console prompt, enter **1** if you use a keyboard and video monitor, or enter **2** if you use a serial console port, and press **Enter**.

The reimage process uninstalls the existing Cisco ADE-OS and software versions, and installs the latest Cisco ADE-OS and Cisco ISE software versions.

For details about the installation and configuration process, see Before Configuring a Cisco ISE Series Appliance, page 1-1 and Understanding the Setup Program Parameters, page 1-3.

For details about migrating Cisco Secure ACS Release 5.1/5.2 data to a Cisco ISE Release 1.0 appliance, see the *Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x*.

---

**Configuring the Cisco ISE System**

By using the Cisco ISE web-based user interface menus and options, you can configure the Cisco ISE system to suit your needs. For details on configuring authentication policies, authorization, policies, and using all the features, menus, and options, see the *Cisco Identity Services Engine User Guide, Release 1.1.x*.
Enabling System Diagnostic Reports in Cisco ISE

After installing Cisco ISE the first time or reimaging an appliance, you can choose to enable the system-level diagnostic reports using the Cisco ISE CLI (the logging function that reports on system diagnostics is not enabled in Cisco ISE by default).

To enable system diagnostic reports, do the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log into the Cisco ISE CLI console using your default administrator user ID and password.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the following commands:</td>
</tr>
<tr>
<td></td>
<td>admin# configure terminal</td>
</tr>
<tr>
<td></td>
<td>admin# logging 127.0.0.1:20514</td>
</tr>
<tr>
<td></td>
<td>admin# end</td>
</tr>
<tr>
<td></td>
<td>admin# write memory</td>
</tr>
</tbody>
</table>

You can configure system diagnostic settings through the Cisco ISE UI (Administration > System > Logging > Logging Categories > System Diagnostics).

Installing New Cisco ISE Software

Each Cisco ISE 3300 Series appliance comes preinstalled with Cisco ISE software. We recommend that should it be necessary to upgrade the preinstalled Cisco ISE ADE-OS and Cisco ISE software with a new version, that you make sure to preserve your existing system configuration information. Performing a new installation of Cisco ISE software on your appliance can take from between 10 minutes to 60 or more minutes (per deployed Cisco ISE node) depending on how much configuration data needs to be restored.

Note

After the new software installation is complete, clear the cache of any active browsers that have been used to access Cisco ISE before this installation process.

For more information

For details on installing the Cisco 3300 Series appliances with new Cisco ISE Release 1.0 software, see “Installing Cisco ISE Software” in the Release Notes for Cisco Identity Service Engine, Release 1.1.x.

Configuring Certificates for Inline Posture Nodes

After you have installed the IPN 1.1.4 ISO image on any of the supported appliance platforms and run the setup program, you must configure certificates for Inline Posture nodes before you can add them to the deployment.
Before You Begin

- Your Inline Posture node must be certified from the same CA that has certified your primary Administration ISE node.
- You can configure Inline Posture node certificates only from the command-line interface (CLI).
- If you wish to deploy an active-standby pair of Inline Posture nodes, you must configure the certificates on both the active and standby Inline Posture nodes.

Step 1 Log in to the Inline Posture node through the CLI.

Step 2 Enter the following command:

```
pep certificate server generatecsr
```

Step 3 Enter `n` to use an existing private key file to use with the certificate signing request or enter `y` to generate a new one.

Step 4 Enter your desired key size.

Step 5 Enter the type of digest that you want to sign the certificate with.

Step 6 Enter your country code name (2 letter code).

Step 7 Enter values for your state, city, organization, organizational unit.

Step 8 Enter the Common Name. The Common Name is the same as your hostname. You must enter the fully qualified domain name (FQDN). For example, if your hostname is `IPEP1` and your DNS domain name is `cisco.com`, you must enter `IPEP1.cisco.com` as your Common Name.

Step 9 Enter your e-mail address.

Step 10 Copy the entire block of text including the blank line after the END CERTIFICATE REQUEST tag (to include the carriage return).

Step 11 Send this CSR to the Certificate Authority that signed your primary Administration ISE node’s certificate.

If you are using the Microsoft CA, choose Web Server as the Certificate Template while sending the signing request.

**Note** Only server authentication is supported in the 1.1.4 release. If you use other CAs to sign your certificate, ensure that the extended key usage specifies server authentication alone.

Step 12 Download your signed certificate in the DER or base64 format, and copy it to an ftp server.

Step 13 Enter the following command from the Inline Posture node CLI:

```
copy ftp://a.b.c.d/ipep1.cer disk:
```

where `a.b.c.d` is the ip address of the ftp server and `ipep1.cer` is the CA-signed certificate that you are adding to the Inline Posture node.

Step 14 Enter the username and password for the ftp server.

Step 15 Enter the following command from the Inline Posture node CLI:

```
pep certificate server add
```

Step 16 Enter `y` for the application to restart.

Step 17 Enter `y` to bind the certificate to the last certificate signing request.
**Step 18** Enter the name of the CA-signed certificate. The Inline Posture application restarts. You can now register this Inline Posture node with your primary Administration ISE node. Refer to the *Cisco Identity Services Engine User Guide, Release 1.1.x* for more information.