



CHAPTER 9

Setting Up Cisco ISE in a Distributed Environment

The Cisco Identity Services Engine (Cisco ISE) provides distributed deployment of runtime services with centralized configuration and management. Multiple nodes can be deployed together in a distributed fashion to support failover.

This chapter describes the type of nodes, personas, roles, and services that constitute Cisco ISE, and how to configure Cisco ISE nodes and create a Cisco ISE distributed environment.

For information about the Cisco ISE deployment scenarios, refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

This chapter contains the following topics:

- [Understanding Node Types, Personas, Roles, and Services, page 9-2](#)
- [Understanding Distributed Deployment, page 9-5](#)
- [Guidelines for Setting Up a Distributed Deployment, page 9-7](#)
- [Configuring an ISE Node, page 9-7](#)
- [Registering and Configuring a Secondary Node, page 9-13](#)
- [Configuring Administration Cisco ISE Nodes for High Availability, page 9-15](#)
- [Viewing Nodes in a Deployment, page 9-17](#)
- [Managing Node Groups, page 9-19](#)
- [Changing Node Personas and Services, page 9-23](#)
- [Configuring Monitoring ISE Nodes for Automatic Failover, page 9-24](#)
- [Removing a Node from Deployment, page 9-26](#)
- [Changing the IP Address of the Monitoring Node, page 9-27](#)
- [Replacing the ISE Appliance Hardware, page 9-28](#)



Note

See [Chapter 10, “Setting Up Inline Posture”](#) for information on setting up an Inline Posture node on your network.

Understanding Node Types, Personas, Roles, and Services

Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. In a distributed environment, you configure one primary Administration ISE node to manage the secondary ISE nodes that are deployed onto the network. This section contains the following topics:

- [Cisco ISE Deployment Terminology, page 9-2](#)
- [Types of Nodes, page 9-2](#)
- [ISE Nodes and Available Menu Options, page 9-4](#)

Cisco ISE Deployment Terminology

This section describes some of the common terms used in Cisco ISE deployment scenarios. [Table 9-1](#) lists these terms and their descriptions.

Table 9-1 *Cisco ISE Deployment Terminology*

| Term | Description |
|-----------|---|
| Service | A service is a specific feature that a persona provides such as network access, profiler, posture, security group access, monitoring and troubleshooting, and so on. |
| Node | A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a software that can be run on VMware. Each instance (appliance or VMware) that runs the Cisco ISE software is called a node. |
| Node Type | A node can be of two types: ISE node and Inline Posture node. The node type and persona determine the type of functionality provided by that node. |
| Persona | The persona or personas of a node determine the services provided by a node. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring. The menu options that are available through the administrative user interface are dependent on the role and personas that an ISE node assumes. See ISE Nodes and Available Menu Options for more information. |
| Role | Determines if a node is a standalone, primary, or secondary node. Applies only to administration and Monitoring ISE nodes. |

Types of Nodes

In a Cisco ISE distributed deployment, there are two types of nodes. These include the following:

- ISE node—A Cisco ISE node could assume any of the following personas:
 - Administration—Allows you to perform all administrative operations on Cisco ISE. It handles all system-related configuration and configurations that are related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have only one or a maximum of two nodes running the administration persona. The administration

persona can take on any one of the following roles: Standalone, Primary, or Secondary. If the primary Administration ISE node goes down, you have to manually promote the secondary Administration ISE node. There is no automatic failover for the Administration persona.



Note At least one node in your distributed setup should assume the Administration persona.

- Policy Service—Provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assume this persona. Typically, there would be more than one Policy Service ISE node in a distributed deployment. All Policy Service ISE nodes that reside behind a load balancer share a common multicast address and can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset any pending sessions.



Note To promote device status replication and network profiling efficiency among Policy Service ISE nodes, Cisco recommends installing multiple Policy Service ISE nodes within local area network segments tangent to the Administrative ISE node, and avoid relying on wide-area network connections between Policy Service ISE nodes as much as possible.



Note At least one node in your distributed setup should assume the Policy Service persona.

- Monitoring—Enables Cisco ISE to function as the log collector and store log messages from all the administration and Policy Service ISE nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources. A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports. Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring ISE nodes collect log messages. In case the primary Monitoring ISE node goes down, the secondary Monitoring ISE node automatically becomes the primary Monitoring ISE node.



Note At least one node in your distributed setup should assume the Monitoring persona. We recommend that you not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. We recommend that the node be dedicated solely to monitoring for optimum performance.

- Inline Posture node—A gatekeeping node that is positioned behind network access devices such as wireless LAN controllers (WLC) and Virtual Private Network (VPN) concentrators on the network. Inline Posture enforces access policies after a user has been authenticated and granted access, and handles change of authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows you to have two Inline Posture nodes that can take on primary or secondary roles for high availability. For more information, see [Chapter 10, “Setting Up Inline Posture”](#)

**Note**

An Inline Posture node is dedicated solely to that service, and cannot operate concurrently with other Cisco ISE services. Likewise, due to the specialized nature of its service, an Inline Posture node cannot assume any persona. For example, it cannot act as an Administration ISE node (that offers administration service), or a Policy Service ISE node (that offers network access, posture, profile, and guest services), or a Monitoring ISE node (that offers monitoring and troubleshooting services) for a Cisco ISE network.

Each node in a deployment, with the exception of the Inline Posture node, can assume the Administration, Policy Service, and Monitoring personas. The Inline Posture node must be a dedicated node.

In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration ISE nodes for high availability
- A pair of Monitoring ISE nodes for automatic failover
- One or more Policy Service ISE nodes for session failover
- A pair of Inline Posture nodes for high availability

ISE Nodes and Available Menu Options

The menu options that are available for Cisco ISE nodes that are part of a distributed deployment depend on the personas that are enabled on them. All administration and monitoring activities should be performed through the administrative user interface of the primary Administration ISE node. Some of the operations, though, need to be performed on the secondary nodes. Therefore the administrative user interface of the secondary nodes provides limited menu options based on the personas that have been enabled on them. [Table 9-2](#) lists the nodes and the menu options that are available through the administrative user interface. If a node assumes more than one persona, for example, the Policy Service persona, and a Monitoring persona with an Active role, then the menu options listed for Policy Service ISE nodes and Active Monitoring ISE node will be available on that node.

**Note**

After you have registered your secondary nodes to your primary Administration ISE node, while logging into the administrative user interface of any of the secondary nodes, you must use the login credentials of the primary Administration ISE node.

Table 9-2 Cisco ISE Nodes and Available Menu Options

| Node and Persona | Menu Options |
|-----------------------------------|--|
| All Nodes | Options to: <ul style="list-style-type: none"> • View and configure system time and NTP server settings. • Install server certificate, manage certificate signing request. <p>Note The server certificate operations must be performed directly on each individual node. The private keys are not stored in the local database and are not copied from the relevant node; the private keys are stored in the local file system.</p> |
| Primary Administration ISE Node | All options. |
| Active Monitoring ISE Node | Access to Home and Operations menus. Provides redundant access to monitoring data that can be accessed from both the Primary and the Active Monitoring ISE nodes. |
| Policy Service ISE Nodes | Option to join, leave, and test Active Directory connection. <p>Note Each Policy Service ISE node must be separately joined to the Active Directory domain. You must first define the domain information and join the primary Administration ISE node to the Active Directory domain. Then, join the other Policy Service ISE nodes to the Active Directory domain individually.</p> |
| Secondary Administration ISE Node | Option to promote the secondary Administration ISE node to become the primary Administration ISE node. |

Understanding Distributed Deployment

A Cisco ISE distributed deployment consists of one primary Administration ISE node and multiple secondary nodes. Each ISE node in a deployment can assume any of the following personas: Administration, Policy Service, and Monitoring.



Note

The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node. For more information, see [Chapter 10, “Setting Up Inline Posture”](#)

After you install Cisco ISE on all your nodes, as described in the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x](#), the nodes come up in a standalone state. You must then define one node as your primary Administration ISE node. While defining your primary Administration

ISE node, you must enable the Administration and Monitoring personas on that node. You can optionally enable the Policy Service persona on the primary Administration ISE node. After you complete the task of defining personas on the primary Administration ISE node, you can then register other secondary nodes to the primary Administration ISE node and define personas for the secondary nodes.

**Note**

There must be at least one Monitoring ISE node in a distributed deployment. At the time of configuring your primary Administration ISE node, you must enable the Monitoring persona. After you have registered a secondary Monitoring ISE node in your deployment, you can edit the primary Administration ISE node and disable the Monitoring persona, if required.

When you register an ISE node as a secondary node, Cisco ISE immediately creates a database link from the primary to the secondary node and begins the process of replication. Replication is the process of sharing ISE configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data present in all the ISE nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE node as a secondary node. An incremental replication occurs after a full replication, and ensures that any new changes such as additions, modifications, or deletions to the configuration data in the primary Administration ISE node are reflected in the secondary nodes. The process of replication ensures that all ISE nodes in a deployment are in sync. You can view the status of replication from the deployment pages of the Cisco ISE administrative user interface.

The Policy Service ISE nodes that reside in a single location behind a load balancer and share a common multicast address can be grouped together. In such scenarios, you can define node groups and assign the nodes to the particular group. See the [“Managing Node Groups” section on page 9-19](#) for information on how to manage node groups.

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the primary Administration ISE node, the status of the deregistered node changes to standalone and the connection between the primary and the secondary node will be lost. Replication updates are no longer sent to the deregistered standby node.

**Note**

You cannot deregister a primary Administration ISE node.

See [Chapter 10, “Setting Up Inline Posture”](#) for information on how to deregister Inline Posture nodes.

The application server in an ISE node restarts when you make any of the following changes:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Primary node is changed to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Administration ISE node is promoted (Secondary to Primary)
- Change the personas (when you assign or remove the Policy Service or Monitoring persona from a node)
- Modify the services in the Policy Service ISE node (enable or disable the session and profiler services)
- Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes

**Note**

When you make any of the above changes, the application services are restarted. You must expect a delay while these services restart.

Guidelines for Setting Up a Distributed Deployment

Read the following statements carefully before you set up Cisco ISE in a distributed environment:

- There are two types of nodes in a Cisco ISE distributed deployment: the ISE node and the Inline Posture node. An ISE node can assume the Administration, Policy Service, and Monitoring personas at the same time. An ISE node can be a primary, secondary, or standalone node.
- The Administration, Policy Service, and Monitoring personas will be enabled by default in a standalone ISE node.
- You must first configure a primary Administration ISE node and then register secondary nodes to set up a distributed deployment.
- There can be only one primary ISE node in a distributed deployment and it must assume the Administration persona. You can have a maximum of two ISE nodes that assume the Administration persona, one being your primary and the other a secondary node.
- All Cisco ISE system-related configuration and configuration related to functionality should be done only on the primary Administration ISE node. The configuration changes that you perform on the primary Administration ISE node is replicated to all the secondary nodes in your deployment.
- In order to avoid timezone issues among the nodes, you must provide the same NTP server name during the setup mode of each node.
- When the primary Administration ISE node goes down, you must log into the user interface of the secondary Administration ISE node and make it the primary node.
- The Inline Posture node requires a dedicated node. No other persona or service can run on a node that is designated as an Inline Posture node.
- A properly configured Domain Name System (DNS) server is required for a distributed deployment to work correctly. You must enter the IP addresses and fully qualified domain names (FQDNs) of the ISE nodes that are part of your distributed deployment in the DNS server.
- If you want to uninstall Cisco ISE from a secondary node, you must first deregister it from the primary Administration ISE node. You can then reimage the standalone node and reregister it with the primary Administration ISE node.

Configuring an ISE Node

After you install an ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas will run on it. This node will be in a standalone state. You must log into the administrative user interface of the ISE node to configure it. You cannot edit the personas or services of a standalone ISE node. You can, however, edit the personas and services of ISE nodes that are part of a distributed setup.

**Note**

If you are logging into the node for the first time, you must change the default administrator password and install a valid license. For more information on these tasks, .

**Note**

If you are logging into the secondary Administration ISE node to promote it as your primary Administration ISE node, see [“Configuring Administration Cisco ISE Nodes for High Availability” section on page 9-15](#).

**Note**

It is recommended not to change the host name and the domain name on Cisco ISE that have been configured or in production. If it is required, then reimage the appliance, make changes, and configure the details during the initial deployment.

Prerequisites:

Before you perform this task, you should do the following:

- Have a basic understanding of how distributed deployments are set up in Cisco ISE. See the [“Understanding Distributed Deployment” section on page 9-5](#) for more information.
- Read the [“Guidelines for Setting Up a Distributed Deployment” section on page 9-7](#).
- Every Cisco 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.

**Note**

For a standalone Cisco ISE deployment, no specific node configuration is required. All the default personas and services are running on a newly installed Cisco ISE node.

To configure a Cisco ISE node, complete the following steps:

- Step 1** From the Cisco ISE administrative user interface, choose **Administration > System > Deployment**.
- Step 2** From the Deployment navigation pane on the left, click **Deployment**.
The Deployment List page appears.
- Step 3** Check the check box next to the ISE node, and click **Edit**.
The Node Edit page appears with a list of fields as described in [Table 9-3](#).
- Step 4** To set up Cisco ISE in a distributed environment, you must complete the following tasks:
 - a. [Configuring a Primary Administration Cisco ISE Node, page 9-11](#)
 - b. [Registering and Configuring a Secondary Node, page 9-13](#)

Troubleshooting Topics:

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)

Description of the Fields in the Cisco ISE Node Edit Page

[Table 9-3](#) describes the fields in the Cisco ISE Node Edit page.

Table 9-3 Cisco ISE Node Edit Page

| Field | Description |
|-----------------|---|
| Hostname | (Display only) Hostname of the ISE node. |
| FQDN | (Display only) The fully qualified domain name of the ISE node. For example, ise1.cisco.com. |
| IP Address | (Display only) IP address of the ISE node. |
| Node Type | (Display only) Could be any one of the following: <ul style="list-style-type: none"> Identity Services Engine (ISE) Inline Posture Node |
| Personas | |
| Administration | <p>Check this check box if you want this ISE node to assume the Administration persona.</p> <p>Note You can enable the Administration persona only on nodes that are licensed to provide the administrative services. For more information, see Chapter 12, “Managing Licenses”</p> <ul style="list-style-type: none"> Role—(Display only) The role that the Administration persona has assumed in the deployment. Could take on any one of the following values: <ul style="list-style-type: none"> Standalone Primary Secondary Make Primary—Click this button to make this node your primary ISE node. You can have only one primary ISE node in a deployment. The other options on this page will become active only after you make this node primary. <ul style="list-style-type: none"> You can have only two Administration ISE nodes in a deployment. If the node has a Standalone role, a Make Primary button appears next to it. If the node has a Secondary role, a Promote to Primary button appears next to it. If the node has a Primary role and there are no other nodes registered with it, a Make Standalone button appears next to it. You can click this button to make your primary node a standalone node. |

Table 9-3 Cisco ISE Node Edit Page (continued)

| Field | Description |
|------------|--|
| Monitoring | <p>Note To configure a Cisco ISE node on a VMware platform as your log collector, use the following guidelines to determine the minimum amount of disk space that you need:</p> <ul style="list-style-type: none"> – 180 KB per endpoint in your network per day – 2.5 MB per Cisco ISE node in your network per day <p>You can calculate the maximum disk space that you need based on how many months of data you want to have in your Monitoring ISE node.</p> <p>Check this check box if you want this ISE node to assume the Monitoring persona and function as your log collector.</p> <p>Note There must be at least one Monitoring ISE node in a distributed deployment. At the time of configuring your primary Administration ISE node, you must enable the Monitoring persona. After you have registered a secondary Monitoring ISE node in your deployment, you can edit the primary Administration ISE node and disable the Monitoring persona, if required.</p> <p>When you have only one Monitoring ISE node in your deployment, it will assume the standalone role. When you have two Monitoring ISE nodes in your deployment, Cisco ISE displays the name of the other monitoring and troubleshooting node for you to configure the Primary-Secondary roles.</p> <p>To configure these roles, from the Role drop-down list, you can choose one of the following:</p> <ul style="list-style-type: none"> • Primary—For the current node to be the primary Monitoring ISE node. • Secondary—For the current node to be the secondary Monitoring ISE node. • None—If you do not want the Monitoring ISE nodes to assume the primary-secondary roles. <p>Note You can access the Monitoring menu from the primary Administration ISE node and the primary Monitoring ISE node in your deployment.</p> <p>Both the primary and secondary Monitoring ISE nodes receive Administration and Policy Service logs.</p> <p>You can have only two Monitoring ISE nodes in a deployment. If you configure one of your Monitoring ISE nodes as primary or secondary, the other Monitoring ISE node automatically becomes the secondary or primary node, respectively.</p> <p>If you change the role for one Monitoring ISE node to None, the role of the other Monitoring ISE node also becomes None, thereby cancelling the high availability pair.</p> <p>After you designate a node as a Monitoring ISE node, you will find this node listed as a syslog target in the following page:</p> <p>Administration > System > Logging > Remote Logging Targets</p> <p>All the other Administration and Policy Service ISE nodes will send their logs to this log collector. If you have two Monitoring ISE nodes defined, then you will find both of them listed as your log collectors.</p> |

Table 9-3 Cisco ISE Node Edit Page (continued)

| Field | Description |
|----------------|--|
| Policy Service | <p>When you check this check box, you must enable any one or all of the following services:</p> <ul style="list-style-type: none"> Check the Enable Session Services check box to enable network access, posture, guest, and client provisioning services. <ul style="list-style-type: none"> Click the Include Node in Node Group drop-down list to choose the group to which this Policy Service ISE node belongs. Choose <none> if you do not want this Policy Service ISE node to be part of any group. See Managing Node Groups for more information on node groups. <p>Note All nodes within a node group should be Layer 2 adjacent (should be on the same subnet) and there should be multicast connectivity between the nodes.</p> <ul style="list-style-type: none"> Check the Enable Profiling Service check box to enable the Profiler service. If you enable the Profiling service, you must click the Profiling Configuration tab and enter the details as required. For more information, see Chapter 18, “Configuring the Probes” <p>Note When you enable or disable any of the services that run on the Policy Service ISE node or make any changes to this node, you will be restarting the application server processes on which these services run. You must expect a delay while these services restart. You can determine when the application server has restarted on a node by using the show application status ise command from the CLI.</p> |

Configuring a Primary Administration Cisco ISE Node

To set up a distributed deployment, you must first configure an ISE node as your primary Administration ISE node.

Prerequisite:

Every Cisco 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 configure a primary Administration ISE node, complete the following steps:

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Click **Deployment** from the navigation pane on the left to launch the Deployment Nodes list page. All the operations related to deployment can be performed from this page.

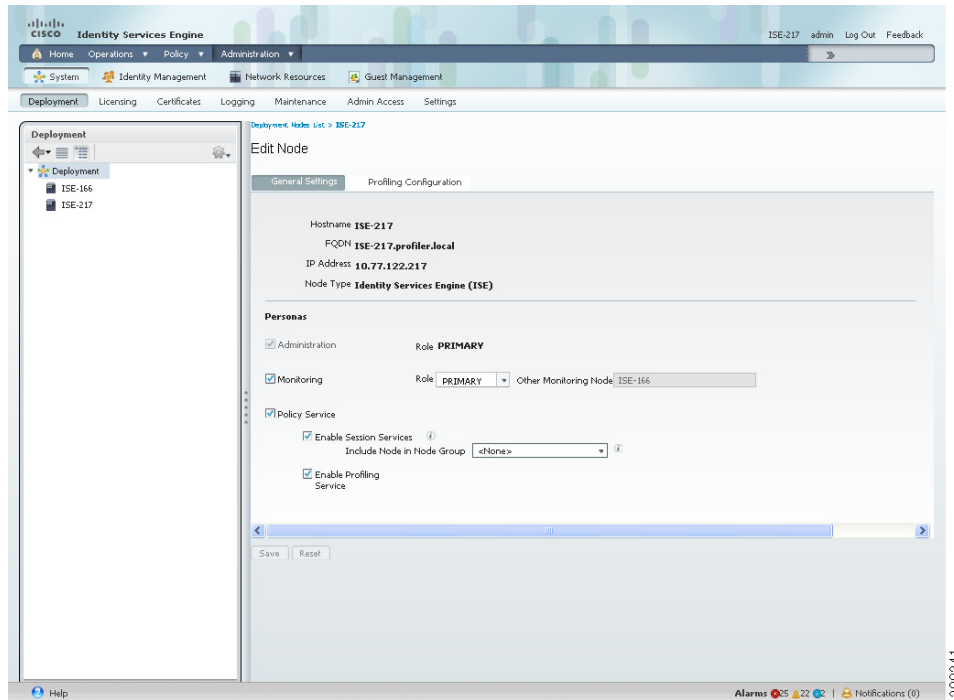


Note The Register button will be disabled initially. To enable this button, you must configure a primary Administration ISE node.

- Step 3** Check the check box next to the current node, and click **Edit**.

Step 4 The Edit Node page appears as shown in [Figure 9-1](#).

Figure 9-1 Edit Node Page



- Step 5** The Administration persona is enabled by default. Click **Make Primary** to configure your primary Administration ISE node.
- Step 6** Enter data on the General Settings tab as described in [Table 9-3](#).
- Step 7** Click the **Profiling Configuration** tab if you have enabled the Profiler service, and configure the probes as described in the “[Configuring the Probes](#)” section on page 18-13.
- Step 8** Click **Save** to save the node configuration.
- Step 9** Click the **Deployment Node List** link at the top of this page or the Deployment link from the left navigation pane to go to the list page.

Next Step

To add secondary nodes to your deployment, you must successfully complete the task described in the “[Registering and Configuring a Secondary Node](#)” section on page 9-13.

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation](#), page D-7

Registering and Configuring a Secondary Node

**Note**

If you register a secondary Monitoring ISE node, we recommend that you first back up the primary Monitoring ISE node, and then restore the data to the new secondary Monitoring ISE node. This ensures that the history of the primary Monitoring ISE node is in sync with the new secondary node as new changes are replicated. For more information, see [Performing On-Demand Backups, page 24-55](#) and [Restoring the Monitoring Database, page 24-56](#).

Prerequisites:

- The fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *ise1.cisco.com* must be DNS-resolvable from the primary Administration ISE node. Otherwise, node registration will fail. You must enter the IP addresses and FQDNs of the ISE nodes that are part of your distributed deployment in the DNS server.
- The primary Administration ISE node and the standalone node that you are about to register as a secondary node should be running the same version of Cisco ISE.
- You must configure the Cisco ISE Admin password at the time you install the Cisco ISE. The previous Cisco ISE Admin default login credentials (admin/cisco) are no longer valid.
- Use the username/password that was created during the initial Setup or the current password, if it was changed later.
- The DB passwords of the primary and secondary nodes should be the same. If these passwords are set to be different during node installation, you can modify them using the following commands:
 - `application reset-passwd ise internal-database-admin`
 - `application reset-passwd ise internal-database-user`

Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x](#) for more details on how to use the CLI commands.

- You can alternatively create an administrator account on the node that is to be registered and use those credentials for registering that node. Every Cisco ISE administrator account is assigned one or more administrative roles. To register and configure a secondary node, you must have either the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.
- If you plan to register a secondary Administration ISE node for high availability, we recommend that you register the secondary Administration ISE node with the primary first before you register other Cisco ISE nodes. If Cisco ISE nodes are registered in this sequence, you do not have to restart the secondary ISE nodes after you promote the secondary Administration ISE node as your primary.
- If you plan to register multiple Policy Service ISE nodes running Session services and you require mutual failover among those nodes, you must place the Policy Service ISE nodes in a node group. You must create the node group first before you register the nodes because you must select the node group to be used on the registration page. See [“Creating, Editing, and Deleting Node Groups” section on page 9-21](#) for more information.
- Ensure that the Certificate Trust List (CTL) of the primary node is populated with the appropriate Certificate Authority (CA) certificates that can be used to validate the HTTPS certificate of the standalone node (that you are going to register as the secondary node). See the [“Creating Certificate Trust Lists in the Primary ISE Node” section on page 13-23](#) for more information.

- After registering your secondary node to the primary node, if you change the HTTPS certificate on the registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node's HTTPS certificate and import it to the CTL of the primary node. See [“Creating Certificate Trust Lists in the Primary ISE Node” section on page 13-23](#) for more information.

**Note**

We recommend that you set all Cisco ISE nodes to the same 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.

To register a secondary node, complete the following steps:

-
- Step 1** Log into the primary Administration ISE node.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Click **Deployment** from the navigation pane on the left.
The Deployment list page appears.
- Step 4** After you have configured your primary Administration ISE node, do one of the following:
- Choose **Register > Register an ISE Node** to register a secondary ISE node. See the [“Configuring an ISE Node” section on page 9-7](#) for information on how to configure your primary Administration ISE node.
 - Choose **Register > Register an Inline Posture Node** to register a secondary Inline Posture node. For more information on deploying an Inline Posture node, see [Chapter 10, “Setting Up Inline Posture.”](#)

**Note**

We recommend that you decide on the type of node at the time of registration. If you want to change the node type later, you have to deregister the node from the deployment, restart Cisco ISE on the standalone node, and then reregister it.

Cisco ISE prompts you to enter the following information:

- Node hostname or IP address.
- User Name
- Password

- Step 5** Enter a DNS-resolvable hostname or IP address of the secondary Cisco ISE node.

**Note**

You must have defined the IP address and the FQDN of the secondary node in the DNS server.

- Step 6** Enter a UI-based administrator credential for the standalone node in the Username and Password fields.
Before you register, the secondary node should be in the standalone state. After you register it to the primary, it begins to receive database updates from the primary. To view the status of the replication, you can go to the Deployment list page (**Administration > System > Deployment**) and look at the Replication Status information provided there.
- Step 7** Click **Next** to go to the edit configuration page. Cisco ISE contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it in this page.

If you have chosen to register a secondary ISE node, you can edit the configuration of the secondary node. See [Next Step](#) for information on the Administration, Monitoring, and Policy Service options.

If you have chosen to register a secondary Inline Posture node, no additional configuration needs to be performed at this point.

Step 8 Click **Save** to save the configuration.

After you register the secondary node, the configuration of the secondary node is added to the database of the primary node and the application server on the secondary node is restarted. After the restart is complete, the secondary node will be running the personas and services that you have enabled on it.

Result

After a secondary node is registered successfully, an alarm is generated on your primary Administration ISE node that confirms a successful node registration. If the secondary node fails to register with the primary Administration ISE node, the alarm is not generated. When a node is registered, the application server on that node is restarted. After successful registration and database synchronization, you must enter the credentials of the primary administrative node to log into the administrative user interface of the secondary node and perform any of the operations listed in [ISE Nodes and Available Menu Options](#).

Next Steps

- For time-sensitive tasks such as time profiles, guest user access and authorization, logging, and so on, ensure that the system time on your nodes are synchronized. See the [“System Time and NTP Server Settings” section on page 8-18](#) for information on how to synchronize the system time.
- To configure for high availability, you must complete the tasks described in the following sections:
 - [Configuring Administration Cisco ISE Nodes for High Availability, page 9-15](#)
 - [Configuring Monitoring ISE Nodes for Automatic Failover, page 9-24](#)
- To add an inline PEP node to your deployment, follow the instructions as described in the [“Setting Up Inline Posture” section on page 10-1](#).

Configuring Administration Cisco ISE Nodes for High Availability

Cisco ISE allows you to have a maximum of two Administration ISE nodes in your deployment, for high availability. To create a high availability pair, you configure one Administration ISE node as primary active, and the other Administration ISE node a secondary standby.

High Availability

In a high availability configuration, the primary Administration ISE node is in the active state to which all configuration changes are made. The secondary Administration ISE node is in the standby state, and will receive all configuration updates from the primary Administration ISE node. Therefore, it will always have a complete copy of the configuration from the primary Administration ISE node.

When the primary Administration ISE node becomes unavailable, you must log into the secondary Administration ISE node and promote it to become the primary Administration ISE node. There is no automatic failover for the Administration ISE node.

**Note**

When the primary Administration ISE node is down, Sponsor administrators cannot create new guest user accounts. During this time, the guest and sponsor portals will provide read-only access to already created guest and sponsor users, respectively. Also, a sponsor administrator who has never logged into the sponsor portal before the primary Administration ISE node went offline, will not be able to log into the sponsor portal until a secondary Administration ISE node is promoted or the primary Administration ISE node becomes available.

Prerequisites:

- Ensure that you have a second ISE node configured with the Administration persona before you can promote it to become your primary Administration ISE node.
- Before you configure the Administration ISE nodes for high availability, we recommend that you obtain a backup of the Cisco ISE configuration from the standalone node that you are going to register as a secondary Administration ISE node.
- 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 promote the secondary Administration ISE node to become the primary, complete the following steps:

Step 1 Log into the user interface of the secondary Administration ISE node.

Step 2 Choose **Administration > System > Deployment**.

The Edit Node page appears.

Step 3 In the Edit Node page, click **Promote to Primary**.

**Note**

You can only promote a secondary Administration ISE node to become a primary Administration ISE node. Cisco ISE nodes that assume only the Policy Service or Monitoring persona or both cannot be promoted to a primary Administration ISE node.

Step 4 Click **Save** to promote the secondary Administration ISE node to become the primary Administration ISE node.

Step 5 Restart the secondary Cisco ISE nodes (Policy Service and Monitoring nodes) that were registered with the primary Administration ISE node before the secondary Administration ISE node was registered.

For example, after you configure your primary Administration ISE node, you register a few Policy Service nodes, and then the secondary Administration ISE node followed by a few Policy Service nodes. In this case, if your primary Administration ISE node fails and you promote the secondary Administration ISE node to become your primary, then you must restart the Policy Service nodes that were registered before the secondary Administration ISE node was registered.

If the node that was originally the primary Administration ISE node comes back up again, it will become a secondary Administration ISE node.

From the Edit Node page of a secondary node, you cannot modify any persona or service. These options will be disabled. You have to log into the user interface of the primary Administration ISE node, choose the secondary node whose personas or services you want to change, and then click **Edit** to make these changes.

**Note**

After you promote your secondary Administration ISE node to become the primary Administration ISE node, you must reconfigure your scheduled ISE backups in the newly promoted primary Administration ISE node because scheduled backups are not replicated from the primary to secondary Administration ISE nodes. See [“Scheduled Backups” section on page 15-6](#) for more information.

Viewing Nodes in a Deployment

From the Deployment Nodes page, you can view all the Cisco ISE nodes that are part of your deployment (both the primary and secondary nodes).

Prerequisite:

Every Cisco 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 all the nodes, complete the following steps:

- Step 1** Log into the primary or secondary ISE administrative user interface.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Click **Deployment** from the navigation pane on the left.

The Deployment Nodes page appears with a list of nodes as shown in [Figure 9-2](#).

Figure 9-2 Distributed Deployment Listing Page

| Host Name | Node Type | Roles | Services | Replication Status | Sync Status |
|-----------|-----------|--|----------------|--------------------|----------------|
| ISE-166 | ISE | Administration, Monitoring, Policy Service | PIR(A), PIR(M) | All | Not Applicable |
| ISE-217 | ISE | Administration, Monitoring, Policy Service | SEC(A), SEC(M) | All | Sync Complete |

This page provides the following information:

- Hostname—Hostname of the node.
- Node Type—The node type can be one of the following:
 - ISE
 - Inline Posture node.
- Personas—(Only appears if the node type is ISE) Lists the personas that an ISE node has assumed. For example, Administration, Policy Service.
- Role—Indicates the role (primary, secondary, or standalone) that the Administration and Monitoring personas have assumed, if these personas are enabled on this node. The role can be any one or more of the following:
 - PRI(A)—Refers to a primary Administration ISE node
 - SEC(A)—Refers to a secondary Administration ISE node
 - PRI(M)—Refers to a primary Monitoring ISE node
 - SEC(M)—Refers to a secondary Monitoring ISE node
- Services—(Only appears if the Policy Service persona is enabled) Lists the services that run on this ISE node. Services can include any one of the following:
 - Session
 - Profiling
 - All
- Replication Status—(Only appears for secondary ISE nodes) Indicates whether incremental replication from the primary Administration ISE node to the secondary node is complete or not. You will see one of the following states:
 - Failed—Incremental database replication has failed.
 - In-Progress—Incremental database replication is currently in progress.
 - Complete—Incremental database replication is complete.
 - Not Applicable—Displayed if the ISE node is a standalone or primary node.
 - Replication Disabled—Displayed if the certificate on that node gets expired or if the node is not reachable for more than 6 hours.
- Sync Status—(Only appears for secondary ISE nodes) Indicates whether full database replication from the primary Administration ISE node to the secondary node is complete or not. A full database replication happens when a node is registered as secondary or when you click Syncup to force a full database replication. You will see one of the following states:
 - Sync Completed—Full database replication is complete.
 - Sync in Progress—Database replication is currently in progress.
 - Out of Sync—Database was down when the secondary node was registered with the primary ISE node.
 - Not Applicable—Displayed if the ISE node is a standalone node.
 - Replication Disabled—Displayed if the certificate on that node gets expired or if the node is not reachable for more than 6 hours. In such a case, a manual sync needs to be done on the node.

Step 4 If the sync status for any secondary node is out of sync, check the check box next to that node, and click **Syncup** to force a full database replication.

**Note**

You must use the Syncup option to force a full replication if the Sync Status is *Out of Sync* or the Replication Status is *Failed* or *Disabled*.

From this page, you can do the following:

- Edit a node. This option is enabled only when you choose a single node. After you choose a node, click the Edit button to edit the personas and roles of that node.
- Register a secondary node. This option is enabled only after you configure a primary Administration ISE node. Click the Register button to register an ISE or Inline Posture node.
- Initiate a full database replication from the primary to the selected secondary nodes.
- Deregister one or more secondary nodes.

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)

Managing Node Groups

In distributed deployments, you might have multiple Policy Service ISE nodes located behind a load balancer to distribute the requests evenly. The load balancer distributes load to the functional nodes behind it. All the nodes in a node group share the same multicast address and use it to communicate their health status.

In a deployment, configuration data (user, resource, distribution, mappings, and so on) is replicated to all Policy Service ISE nodes, whereas the session information is not replicated across all Policy Service ISE nodes.

To detect node failure and to reset sessions in pending state on the failed node, two or more Policy Service ISE nodes can be placed in the same node group. When a node that belongs to a node group goes down, another node in the same node group issues a CoA for pending sessions on the failed node.

**Note**

A session is said to be in the pending state if it has been authorized, but posture assessment is not yet complete. It is possible to set up a distributed deployment without node groups, but sessions in pending state on a failed Policy Service ISE node will not be automatically reset.

Session Failover in Policy Service ISE Nodes

The heartbeat functionality in Cisco ISE handles session failover in Policy Service ISE nodes. When a Policy Service ISE node that has a few active sessions goes down, the endpoints are stuck in an intermediate state. Even if the posture agent detects that the Policy Service ISE node that it has been communicating with has gone down, it cannot re-initiate authorization. If the Policy Service ISE nodes are part of a node group, the nodes within a node group exchange heartbeats to detect node failures. If a node fails, one of its peers from the node group learns about the active sessions on the failed node and issues a CoA to disconnect those sessions. As a result, restarts and the sessions are handled by another Policy Service ISE node that is available using RADIUS load balancing. The session failover does not automatically move the sessions over from a Policy Service ISE node that has gone down to one that is available, but issues a CoA to achieve that.

**Note**

The PDP nodes in a distributed deployment do not share their Machine Access Restriction (MAR) cache with each other. For example, If a client machine is authenticated by one of the Policy Service ISE nodes, PDP1 and PDP1 goes down, then another Policy Service ISE node in the deployment, PDP2 handles the user authentication. The user authentication in this case fails because PDP2 does not have the host authentication information in its MAR cache.

All the nodes in a node group must be configured on the network access device (NAD) as RADIUS clients to issue a CoA. Typically, these nodes would also be configured as RADIUS servers. See the [“Enable RADIUS Change of Authorization \(CoA\)” section on page C-4](#) for CoA-related configuration on the switch.

While a single NAD can be configured with many ISE nodes (as RADIUS servers and dynamic-author clients), it is not necessary that all these nodes are in the same node group.

All the nodes within the same node group should be configured on the NAD as RADIUS servers and clients, because any one of them can issue a CoA request for the sessions that are established through that NAD to any node in the node group. The nodes in a node group should be the same as, or a subset of, the RADIUS servers and clients configured on the NAD.

For information about session failover in Policy Service ISE nodes, you can view the Server Operations Audit report (Operations > Reports > Catalog > Server Instance > Server Operations Audit).

Number of Nodes in a Node Group

The number of nodes that you can have in a node group depends on your deployment requirements. Node groups ensure that node failures are detected and that a peer issues a CoA for sessions that are authorized, but not yet postured. The size of the node group does not have to be very large.

If you want to minimize the number of node groups and thereby reduce the number of multicast addresses that must be managed, then you can group all the RADIUS servers and clients that are configured on the NADs as one node group.

If management of multiple multicast addresses is not a problem, but there is a need for minimizing multicast traffic, then you can have fewer nodes in a node group.

**Note**

We recommend that you have two, three, or a maximum of four nodes in a node group.

If the size of the node group increases, the number of messages and heartbeats that are exchanged between nodes increases significantly. As a result, multicast traffic also increases. Having fewer nodes in a node group helps reduce the multicast traffic and at the same time provides sufficient redundancy to detect Policy Service ISE node failures.

You can create, edit, and delete node groups. You can perform these operations from the Deployment pages of the Cisco ISE administrative user interface.

This section contains the following topic:

- [Creating, Editing, and Deleting Node Groups, page 9-21](#)

Creating, Editing, and Deleting Node Groups

You can create and edit node groups in Cisco ISE.

Prerequisites:

- All nodes within a node group should be Layer 2 adjacent (should be on the same subnet). Layer 2 adjacent means that the nodes are connected to the same switch and are in the same VLAN.
- You must enable IP multicast between nodes that are part of the same node group. Typically, all the nodes in a node group will be connected to the same switch and be in the same VLAN.
- Two node groups cannot have the same multicast address.
- The multicast address that you assign to a node group should not be reserved for use by other network protocols in the deployment. Cisco ISE checks if the multicast address that you enter is a valid and allowed multicast address. It does not allow 224.0.0.0 to be used as a multicast address, but does not check for the reserved list of multicast addresses. For a list of reserved multicast addresses that you should not use, see <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml>.
- Every Cisco 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 create a node group, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Choose Administration > System > Deployment . |
| Step 2 | Click Deployment from the navigation pane. |
| Step 3 | Click the action icon, and click Create Node Group . The Create Node Group page appears. |
| Step 4 | Enter a unique name for your node group. |
| Step 5 | You can also enter an optional description. |

- Step 6** Enter a unique multicast address. The multicast address must be between 224.0.0.1 and 239.255.255.255.



Note The multicast address that you assign to a node group should not be reserved for use by other network protocols in the deployment. For a list of reserved multicast addresses, see <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml>.

The multicast address is used to communicate between nodes in a group to monitor the health of the nodes and for session cleanup.

- Step 7** Click **Submit** to save the node group.

Results

After you save the node group, it should appear in the navigation pane on the left. If you do not see the node group in the left pane, it may be hidden. Click the Expand button on the navigation pane to view the hidden objects.

Optional Steps:

- To add a node to a node group, you must edit the node and choose the node group from the Member of Node Group drop-down list.
- To remove a node from a node group, you must edit the node and choose <none> from the Member of Node Group drop-down list.

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)

To edit a node group, complete the following steps:

- Step 1** Choose **Administration > System > Deployment**.
- Step 2** From the Deployment navigation pane on the left, click the node group that you want to edit.



Note If you do not see the node group in the left pane, it may be hidden. Click the Expand button on the navigation pane to view the hidden objects.

The Edit Node Group page appears. You can only edit the description and multicast address.

- Step 3** (Optional) Enter the new description.
- Step 4** Enter the new multicast address. The multicast address should be unique.
- Step 5** Click **Submit** to save the changes.

Optional Steps:

- To add a node to a node group, you must edit the node and choose the node group from the Member of Node Group drop-down list.
- To remove a node from a node group, you must edit the node and choose <none> from the Member of Node Group drop-down list.

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)

To delete a node group, complete the following steps:

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** From the Deployment navigation pane on the left, click the node group that you want to delete.
The Edit Node Group page appears.
- Step 3** Click the action icon from the navigation pane on the left, and click **Delete Node Group**.
The following message appears:
Are you sure you want to delete?
- Step 4** Click **OK** to delete the node group.
A confirmation message appears in the page after the node group is deleted. Deleting a node group does not delete any of the nodes that belong to it. The nodes are simply dissociated from the group.
-

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)

Changing Node Personas and Services

You can edit the Cisco ISE node configuration to change the personas and services that run on the node. For example, on a node that profiles your devices, you can disable the services and enable them. However, you cannot add any services or roles to a node that is designated as an Inline Posture node.

Prerequisites:

- If you want to reuse an Inline Posture node, first deregister the node and reset the configuration of the node using the **application reset-config ise** command. Then, reregister the node as a new node.
When an Inline Posture node is deregistered, it defaults to the Administration, Policy Service, and Monitoring personas that are in effect in a standalone state, and then restarts. When the node comes back up, it is returned to an Inline Posture node configuration.
- Every Cisco 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.

**Note**

When you enable or disable any of the services that run on a Policy Service ISE node or make any changes to a Policy Service ISE node, you will be restarting the application server processes on which these services run. You must expect a delay while these services restart.

To change the roles and services of an ISE node, complete the following steps:

-
- Step 1** Log into the primary Administration ISE node.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Click **Deployment** from the navigation pane on the left.
The Deployment Nodes List page appears.
- Step 4** Check the check box next to the node whose personas or services you want to change, then click **Edit**.
- Step 5** Edit the node personas and services. See [Table 9-3](#) for a description of the fields in the ISE Edit Node page.
- Step 6** Click **Save** to save the changes.

After the persona or service change is saved successfully, an alarm is generated on your primary Administration ISE node that confirms the persona or service change. If the persona or service change is not saved successfully, the alarm is not generated.

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)
- [Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node, page D-10](#)

Configuring Monitoring ISE Nodes for Automatic Failover

The term automatic failover is used because high availability is not supported on Monitoring ISE nodes in the true sense. For Monitoring ISE nodes, operation audit data is duplicated by the Policy Service ISE node(s), which then sends copies to both the primary and secondary Monitoring ISE nodes.



Note

Monitoring is served from the primary (active) Monitoring ISE node. Monitoring data is only served from the secondary (standby) Monitoring ISE node when the active node is down. The secondary Monitoring ISE node is read-only. For this reason, you are not allowed to make any configuration changes to a secondary Monitoring ISE node.

Automatic Failover Process

When a primary Monitoring ISE node goes down, the secondary Monitoring ISE node takes over all monitoring and troubleshooting information. The secondary node provides read-only capabilities, which means you cannot make configuration changes to that node.

To make configuration changes on the secondary node, the administrator must first manually promote the secondary node to a primary role. If the primary node comes back up after the secondary node has been promoted, it assumes the secondary role. If the secondary node was not promoted, the primary Monitoring ISE node will resume its role after it comes back up.



Warning

When the primary node comes back up after a failover, a manual backup and restore is required to update the primary node so it can reclaim the data that was lost.

Configuring Primary and Secondary Monitoring ISE Nodes

You can specify two Monitoring ISE nodes on an ISE network and create an active-standby pair. Once the active-standby pair is defined, the following rules apply:

- All configuration changes must be made on the primary Monitoring ISE node. The secondary node is read-only.
- Configuration changes made to the primary node are automatically replicated on the secondary node.
- Both the primary and secondary nodes are listed as log collectors to which all other nodes send logs.
- The Cisco ISE dashboard is the main entry point for monitoring and troubleshooting. Monitoring information is displayed on the dashboard from the primary Monitoring ISE node. If the primary node goes down, the information is served from the secondary node.
- Backing up and purging monitoring data is not part of a standard Cisco ISE node backup process. You must configure repositories for backup and data purging on both the primary and secondary Monitoring ISE nodes, using the same repositories for each.



Note

When you register a secondary Monitoring ISE node, we recommend that you back up the primary Monitoring ISE node and then restore the data to the new secondary Monitoring ISE node. This ensures that the history of the primary Monitoring ISE node is in sync with the new secondary node as new changes are replicated. For more information, see [Performing On-Demand Backups, page 24-55](#) and [Restoring the Monitoring Database, page 24-56](#).

Prerequisites:

- Before you can configure two Monitoring ISE nodes for automatic failover, they must first be registered as Cisco ISE nodes, as described in [Guidelines for Setting Up a Distributed Deployment, page 9-7](#) and [Configuring an ISE Node, page 9-7](#).
- Specify monitoring roles and services on both nodes and name them for their primary and secondary roles, as appropriate.
- You must configure repositories for backup and data purging on both the primary and secondary Monitoring ISE nodes, using the same repositories for each. This is important for the backup and purging features to work properly. Purging takes place on both the primary and secondary nodes of a redundant pair. For example, if the primary Monitoring ISE node uses two repositories for backup and purging, you must specify the same repositories for the secondary node.



You can configure a data repository for a Monitoring ISE node using the **repository** command in the system command line interface (CLI). For more information, see [Backing Up and Restoring the Monitoring Database, page 24-49](#) and the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*.



Warning

For scheduled backup and purge to work properly on the nodes of a Monitoring redundant pair, you must configure the same repository, or repositories, on both the primary and secondary nodes using the CLI. The repositories are not automatically synced between the two nodes.

To configure Monitoring ISE nodes for automatic failover, complete the following steps:

-
- Step 1** From the Cisco ISE dashboard, verify that the Monitoring ISE nodes are ready.
- The System Summary dashlet shows the Monitoring ISE nodes with a green check mark to the left when their services are ready.
-  **Note** Deployment changes may require the start of services. It can take a minute for the services to come up.
-
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** In the Deployment navigation pane, click **Deployment**.
- Step 4** In the Deployment Nodes page, check the check box next to the Monitoring ISE node that you want to specify as active.
- Step 5** Click **Edit**.
- Step 6** Click the General Settings tab and choose **Primary** from the Role drop-down list..
-  **Note** When you choose a Monitoring ISE node as primary, the other Monitoring ISE node automatically becomes secondary. In the case of a standalone deployment, primary and secondary role configuration is disabled.
-
- Step 7** Click **Save**. The active and standby nodes restart.
-


Removing a Node from Deployment

To remove a node from the deployment, you must deregister it.

Prerequisite:

Every Cisco 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 remove a node from deployment, complete the following steps:

-  **Note** Before you remove any secondary node from the deployment, we recommend that you run a backup of Cisco ISE configuration, which you can then restore later on, if needed.
-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Click **Deployment** in the Deployment navigation pane.
- Step 3** Check the check box next to the secondary node that you want to remove, then click **Deregister**.
- The system prompts you with the following message:

Are you sure you want to deregister the selected items?

Step 4 Click **OK** to remove the node from the deployment.

The deregistered node now becomes a standalone ISE node. It retains the last configuration that it received from the primary Administration ISE node and assumes the default personas of a standalone node (Administration, Policy Service (session and profiling services), and Monitoring).

If you deregister a Monitoring ISE node, this node will not be listed as a syslog target: Administration > System > Logging > Logging Targets.

After a secondary node is deregistered successfully, an alarm is generated on your primary Administration ISE node that confirms a successful node deregistration. If the secondary node fails to deregister from the primary Administration ISE node, the alarm is not generated.

Troubleshooting Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page D-7](#)

Changing the IP Address of the Monitoring Node

You must follow the procedure described in this section to change the IP address of the Monitoring node.

Prerequisite

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any 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 change the IP Address of the Monitoring node, complete the following tasks:

-
- Step 1** Remove the Monitoring node from the deployment. See the [“Removing a Node from Deployment” section on page 9-26](#) for more information.
- Step 2** Change the IP address of the Monitoring node.
- Step 3** Register the Monitoring node as a secondary server with the primary Administration ISE node. See the [“Registering and Configuring a Secondary Node” section on page 9-13](#) for more information.



Note

If you are using the hostname while registering the Monitoring node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *ise1.cisco.com* must be DNS-resolvable from the primary Administration ISE node. Otherwise, node registration will fail. You must enter the IP addresses and FQDNs of the ISE nodes that are part of your distributed deployment in the DNS server.

The primary Administration node replicates the change in the Monitoring node's IP address to the other ISE nodes in your deployment.

Replacing the ISE Appliance Hardware

You should choose to replace the Cisco ISE appliance hardware only if there is an issue with the hardware. For any software issues, you can reimage the appliance and reinstall the Cisco ISE software.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any 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 replace a Cisco ISE appliance hardware in your distributed deployment, complete the following tasks:

-
- | | |
|---------------|---|
| Step 1 | Remove the node from the deployment. See the “Removing a Node from Deployment” section on page 9-26 for more information. |
| Step 2 | Register the new node as a secondary server with the primary Administration ISE node. See the “Registering and Configuring a Secondary Node” section on page 9-13 for more information. |
| Step 3 | Configure the same personas and services that were running on the node that was removed. See the “Changing Node Personas and Services” section on page 9-23 for more information. |
-