



Administer ISE-PIC

- [Manage ISE-PIC Nodes, on page 1](#)
- [Manage the ISE-PIC Installation, on page 6](#)
- [Manage Settings in ISE-PIC, on page 25](#)

Manage ISE-PIC Nodes

Add or remove the secondary node, synchronize data between nodes, promote the secondary node to be the primary node, and more.

Cisco ISE-PIC Deployment Setup

After you install Cisco ISE-PIC on all your nodes, as described in the *Cisco Identity Services Engine Hardware Installation Guide*, the nodes come up in a standalone state. You must then define one node as your Primary Administration Node (PAN) and register the secondary node to the PAN.

All Cisco ISE-PIC system and functionality-related configurations should be done only on the PAN. The configuration changes that you perform on the PAN are replicated to the secondary node in your deployment. From the secondary node, the only action you can perform is to promote that secondary node to become the PAN.

After you have registered the secondary node to the PAN, while logging in to the Admin portal of that secondary node, you must use the login credentials of the PAN.

Data Replication from Primary to Secondary ISE-PIC Nodes

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

A full replication typically occurs when you first register an ISE-PIC node as a secondary node. 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 PAN are reflected in the secondary nodes. The process of replication ensures that the Cisco ISE-PIC nodes in a deployment are in sync. You can view the status of replication in the Node Status column from the deployment pages of the Cisco ISE-PIC admin portal. When you register a

Cisco ISE-PIC node as a secondary node or perform a manual synchronization with the PAN, the node status shows an orange icon indicating that the requested action is in progress. Once it is complete, the node status turns green indicating that the secondary node is synchronized with the PAN.

Effects of Modifying Nodes in Cisco ISE-PIC

When you make any of the following changes to a node in a Cisco ISE-PIC, that node restarts, which causes a delay:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Change a primary node to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Promote an node (Secondary to Primary)
- Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes



Note When you promote the secondary Administration node to the primary PAN position, the primary node will assume a secondary role. This causes both the primary and secondary nodes to restart, causing a delay.

Guidelines for Setting Up Two Nodes in a Deployment

Read the following statements carefully before you set up Cisco ISE-PIC with two nodes.

- Choose the same Network Time Protocol (NTP) server for both the nodes. To avoid timezone issues among the nodes, you must provide the same NTP server name during the setup of each node. This setting ensures that the reports and logs from the various nodes in your deployment are always synchronized with timestamps.
- Configure the Cisco ISE-PIC Admin password when you install Cisco ISE-PIC. The previous Cisco ISE-PIC Admin default login credentials (admin/cisco) are no longer valid. Use the username and password that was created during the initial setup or the current password if it was changed later.
- Configure the Domain Name System (DNS) server. Enter the IP addresses and fully qualified domain names (FQDNs) of both the Cisco ISE-PIC nodes that are part of your deployment in the DNS server. Otherwise, node registration will fail.
- Configure the forward and reverse DNS lookup for both Cisco ISE-PIC nodes in your high-availability deployment from the DNS server. Otherwise, you may run into deployment related issues when registering and restarting Cisco ISE-PIC nodes. Performance might be degraded if reverse DNS lookup is not configured for both of the nodes.
- (Optional) Deregister a secondary Cisco ISE-PIC node from the PAN to uninstall Cisco ISE-PIC from it.
- Ensure that the PAN and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE-PIC.

View Nodes in a Deployment

In the **Deployment Nodes** window, you can view the ISE-PIC nodes, primary and secondary, that are a part of your deployment.

-
- Step 1** Log in to the primary Cisco ISE-PIC Admin portal.
- Step 2** Choose **Administration** > **Deployment**.
- All the Cisco ISE nodes that are part of your deployment are listed.
-

Register a Secondary Cisco ISE-PIC Node

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, you can view all the configuration changes that you make from the Deployment page of the PAN. However, expect a delay of 5 minutes for your changes to take effect and appear on the Deployment page.

-
- Step 1** Log in to the PAN.
- Step 2** Choose **Administration** > **Deployment**.
If no secondary node is registered in the deployment then the **Add Secondary Node** section appears at the bottom of the page.
- Step 3** From the **Add Secondary Node** section, enter the DNS-resolvable hostname of the secondary Cisco ISE node.
If you are using the hostname while registering the Cisco ISE-PIC node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com*, must be DNS-resolvable from the PAN. Otherwise, node registration fails. You must have previously defined the IP address and the FQDN of the secondary node in the DNS server.
- Step 4** Enter a UI-based administrator credential for the standalone node in the Username and Password fields.
- Step 5** Click **Save**.
Cisco ISE-PIC contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it.
-

When the secondary node is registered to the deployment, the node is restarted, which may take up to 5 minutes before the secondary node information is displayed from the Deployment page.

Once the secondary node is registered successfully, the Deployment page displays the details for that node in the **Secondary Node** section.

After a secondary node is registered successfully, you will receive an alarm on your PAN that confirms a successful node registration. If the secondary node fails to register with the PAN, the alarm is not generated. When a node is registered, the application server on that node is restarted. After successful registration and database synchronization, enter the credentials of the primary administrative node to log in to the user interface of the secondary node.



Note In addition to the existing Primary node in the deployment, when you successfully register a new node, no alarm corresponding to the newly registered node is displayed. The Configuration Changed alarms reflect information corresponding to the newly registered nodes. You can use this information to ascertain the successful registration of the new node.

Synchronize Primary and Secondary Cisco ISE-PIC Nodes

You can make configuration changes to Cisco ISE-PIC only through the primary PAN. The configuration changes get replicated to all the secondary nodes. If, for some reason, this replication does not occur properly, you can manually synchronize the secondary PAN with the primary PAN.

-
- Step 1** Log in to the primary PAN.
 - Step 2** Choose **Administration > Deployment**.
 - Step 3** Check the check box next to the node that you want to synchronize with the primary PAN, and click **Syncup** to force a full database replication.
-

Manually Promote Secondary PAN to Primary

If the Primary PAN fails you must manually promote the Secondary PAN to become the new Primary PAN.

Before you begin

Ensure that you have a second Cisco ISE-PIC node configured to promote as your Primary PAN.

-
- Step 1** Log in to the Secondary PAN GUI.
 - Step 2** Choose **Administration > Deployment**.
 - Step 3** Click **Promote to Primary**.

If the node that was originally the Primary PAN, comes back up, it will be demoted automatically and become the Secondary PAN. You must perform a manual synchronization on this node (that was originally the Primary PAN) to bring it back into the deployment.

- Step 4** Click **Save**.
-

Remove a Node from Deployment

To remove a node from a deployment, you must deregister it. The deregistered node becomes a standalone Cisco ISE-PIC node.

When a node is deregistered, the endpoint data is lost. If you want the node to retain the endpoint data after it becomes a standalone node, you can obtain a backup from the primary PAN and restore this data backup on it.

You can view these changes in the **Deployment** window of the primary PAN. However, expect a delay of five minutes for the changes to take effect and appear in the **Deployment** window.

Before you begin

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the PAN, 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 standalone node.

Before you remove a secondary node from a deployment, perform a backup of Cisco ISE-PIC configuration, which you can then restore later, if needed.

-
- Step 1** Choose **Administration** > **Deployment**.
 - Step 2** Click **Deregister**, located next to the secondary node details.
 - Step 3** Click **OK**.
 - Step 4** Verify the receipt of an alarm on your primary PAN to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the primary PAN, it means the alarm is not generated.
-

Change the Hostname or IP Address of a Cisco ISE-PIC Node

You can change the hostname, IP address, or domain name of standalone Cisco ISE-PIC nodes. However, you cannot use **localhost** as the hostname for a node.

Before you begin

If a Cisco ISE-PIC node is a part of a two-node deployment, you must first remove it from the deployment and ensure that it is a standalone node.

-
- Step 1** Change the hostname or IP address of the Cisco ISE-PIC node using the **hostname**, **ip address**, or **ip domain-name** command from the Cisco ISE CLI.
 - Step 2** Reset the Cisco ISE-PIC application configuration using the **application stop ise** command from the Cisco ISE CLI to restart all the services.
 - Step 3** Register the Cisco ISE-PIC node to the primary PAN if it is a part of a two-node deployment.
 - Note** If you are using the hostname while registering the Cisco ISE-PIC node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com*, must be DNS-resolvable from the primary PAN. Otherwise, node registration fails. You must enter the IP addresses and FQDNs of the Cisco ISE-PIC nodes that are a part of your deployment in the DNS server.

After you register the Cisco ISE-PIC node as a secondary node, the primary PAN replicates the change in the IP address, hostname, or domain name to the other Cisco ISE-PIC nodes in your deployment.

Replace the Cisco ISE-PIC Appliance Hardware

You should replace the Cisco ISE-PIC 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-PIC software.

-
- Step 1** Re-image or re-install the Cisco ISE-PIC software on the new nodes.
 - Step 2** Obtain a license with the UDI for the Primary and Secondary PANs and install it on the Primary PAN.
 - Step 3** Restore the backup on the replaced Primary PAN.
The restore script will try to sync the data on the Secondary PAN, but the Secondary PAN is now a standalone node and the sync will fail. Data is set to the time the backup was taken on the Primary PAN.
 - Step 4** Register the new node as a secondary server with the Primary PAN.
-

Manage the ISE-PIC Installation

Install patches, run backups or implement a system restoration.

Install a Software Patch


-
- Step 1** Choose **Administration > Maintenance > Patch Management** and click **Install**.
 - Step 2** Click **Browse** and choose the patch that you downloaded from Cisco.com.
 - Step 3** Click **Install** to install the patch.
After the patch is installed on the PAN, Cisco ISE-PIC logs you out and you have to wait for a few minutes before you can log in again.
Note When patch installation is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.
 - Step 4** Choose **Administration > Maintenance > Patch Management** to return to the Patch Installation page.
 - Step 5** Click the radio button next to the patch that you have installed and click **Show Node Status** to verify whether installation is complete.
-

Cisco ISE-PIC Software Patches

Cisco ISE-PIC software patches are always cumulative. Cisco ISE-PIC allows you to perform patch installation and rollback from CLI or GUI.

You can install patches on Cisco ISE-PIC servers in your deployment from the Primary PAN. To install a patch from the Primary PAN, you must download the patch from Cisco.com to the system that runs your client browser.

If you are installing the patch from the GUI, the patch is automatically installed on the Primary PAN first. The system then installs the patch on the other nodes in the deployment in the order listed in the GUI. You

cannot control the order in which the nodes are updated. You can also manually install, roll back, and view patch version. In the Cisco ISE GUI, click the **Menu** icon () and choose **Administrator > System > Maintenance > Patch management**.

If you are installing the patch from the CLI, you can control the order in which the nodes are updated. However, we recommend that you install the patch on the Primary PAN first. The order of installation on the rest of the nodes is irrelevant. You can install the patch on multiple nodes simultaneously, to speed up the process.

If you want to validate the patch on some of the nodes before upgrading the entire deployment, you can use the CLI to install the patch on selected nodes. Use the following CLI command to install the patch:

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

For more information, see the "install Patch" section in the "Cisco ISE CLI Commands in EXEC Mode" chapter in [Cisco Identity Services Engine CLI Reference Guide](#).

You can install the required patch version directly. For example, if you are currently using Cisco ISE 2.x and would like to install Cisco ISE 2.x patch 5, you can directly install Cisco ISE 2.x patch 5, without installing the previous patches (in this example, Cisco ISE 2.x patches 1 – 4). To view the patch version in the CLI, use the following CLI command:

```
show version
```

Software Patch Installation Guidelines

When you install a patch on an ISE node, the node is rebooted after the installation is complete. You might have to wait for a few minutes before you can log in again. You can schedule patch installations during a maintenance window to avoid temporary outage.

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




Note Cisco ISE patches can be installed on ISE-PIC as well.

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

When you install a patch from the Primary PAN that is part of a two-node deployment, Cisco ISE-PIC installs the patch on the primary node and then on the secondary node. If the patch installation is successful on the Primary PAN, Cisco ISE-PIC then continues patch installation on the secondary node. If it fails on the Primary PAN, the installation does not proceed to the secondary node.

Roll Back Software Patches

When you roll back a patch from the PAN that is part of a deployment with multiple nodes, Cisco ISE-PIC rolls back the patch on the primary node and then the secondary node in the deployment.

-
- Step 1** In the ISE-PIC GUI, click the **Menu** icon () and choose **Administration > Maintenance > Patch Management**.
- Step 2** Click the radio button for the patch version whose changes you want to roll back and click **Rollback**.

Note When a patch rollback is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

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

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

Step 4 To view the progress of the patch rollback, choose the patch in the Patch Management page and click **Show Node Status**.

Step 5 Click the radio button for the patch and click **Show Node Status** on a secondary node to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process to roll back the changes from the remaining nodes. Cisco ISE-PIC only rolls back the patch from the nodes that still have this version of the patch installed.

Software Patch Rollback Guidelines

To roll back a patch from Cisco ISE-PIC nodes in a deployment, you must first roll back the change from the PAN. If this is successful, the patch is then rolled back from the secondary node. If the rollback process fails on the PAN, the patches are not rolled back from the secondary node.

While Cisco ISE-PIC rolls back the patch from the secondary node, you can continue to perform other tasks from the PAN GUI. The secondary node will be restarted after the rollback.

Backup and Restore Data



Note Cisco ISE-PIC functions in many cases identically to the Cisco ISE backup and restore procedures, and therefore, the term Cisco ISE may occasionally be used interchangeably to indicate operations and features relevant for Cisco ISE-PIC.

Cisco ISE-PIC allows you to back up data from the primary or standalone node. Backup can be done from the CLI or user interface.

Cisco ISE-PIC allows you to back up the following type of data:

- Configuration data—Contains both application-specific and Cisco ADE operating system configuration data.
- Operational Data—Contains monitoring and troubleshooting data.

Backup and Restore Repositories

Cisco ISE-PIC allows you to create and delete repositories. You can create the following types of repositories:

- DISK
- FTP
- SFTP

- NFS
- CD-ROM
- HTTP
- HTTPS

You can create the repository type as CD-ROM for the virtual CD-ROM created using the KVM.



Note Repositories are local to each device.



Note We recommend that you have a repository size of 10 GB for small deployments (100 endpoints or less), 100 GB for medium deployments, and 200 GB for large deployments.

Create Repositories

You can use the CLI and GUI to create repositories. We recommend that you use the GUI due to the following reasons:

- Repositories that are created through the CLI are saved locally and do not get replicated to the other deployment nodes. These repositories do not get listed in the GUI's repository page.
- Repositories that are created on the primary PAN get replicated to the other deployment nodes.

The keys are generated only at the primary PAN on GUI, and so during upgrade you need to generate the keys again at GUI of new primary admin and export it to the SFTP server. If you remove the nodes from your deployment, you need to generate the keys on GUI of non-admin nodes and export it to the SFTP server.

You can configure an SFTP repository in Cisco ISE-PIC with RSA public key authentication. Instead of using an administrator-created password to encrypt the database and logs, you can choose the RSA public key authentication that uses secure keys. In case of SFTP repository created with RSA public key, the repositories created through the GUI do not get replicated in the CLI and the repositories created through the CLI do not get replicated in the GUI. To configure same repository on the CLI and GUI, generate RSA public keys on both CLI and GUI and export both the keys to the SFTP server.



Note Cisco ISE initiates outbound SSH or SFTP connections in FIPS mode even if FIPS mode is not enabled on ISE. Ensure that the remote SSH or SFTP servers that communicate with ISE allow FIPS 140 approved cryptographic algorithms.

Cisco ISE uses embedded FIPS 140 validated cryptographic modules. For details of the FIPS compliance claims, see the [FIPS Compliance Letter](#).

Before you begin

- If you want to create an SFTP repository with RSA public key authentication, perform the following steps:

- Enable RSA public key authentication in the SFTP repository.
- You must log in as the Admin CLI user. Enter the host key of the SFTP server from the Cisco ISE CLI using the **crypto host_key add** command. The host key string should match the hostname that you enter in the **Path** field of the repository configuration page.
- Generate the key pairs and export the public key to your local system from the GUI. From the Cisco ISE CLI, generate the key pairs using the **crypto key generate rsa passphrase test123** command, where, passphrase must be greater than 13 letters, and export the keys to any repository (local disk or any other configured repository).
- Copy the exported RSA public key to the PKI-enabled SFTP server and add it to the "authorized_keys" file.



Note When primary PAN and primary MnT are separate nodes, you can use the **Generate Key Pairs** option in the **Repository List** window to generate RSA keys for both primary PAN and primary MnT nodes. You can use the **Export Public Key** option in the **Repository List** window to export the generated RSA keys from both primary PAN and primary MnT nodes.

- Step 1** Choose **Administration > Maintenance > Repository**.
- Step 2** Click **Add** to add a new repository.
- Step 3** Enter the values as required to set up new repository. See [Repository Settings, on page 11](#) for a description of the fields.
- Step 4** Click **Submit** to create the repository.
- Step 5** Verify that the repository is created successfully by clicking **Repository** from the **Operations** navigation pane on the left or click the **Repository List** link at the top of **Repository** window to go to the repository listing page.

What to do next

- Ensure that the repository that you have created is valid. You can do so from the **Repository Listing** window. Select the corresponding repository and click **Validate**. Alternatively, you can execute the following command from the Cisco ISE command-line interface:

```
show repository repository_name
```

where *repository_name* is the name of the repository that you have created.



Note If the path that you provided while creating the repository does not exist, then you will get the following error:

```
%Invalid Directory
```

- Run an on-demand backup or schedule a backup.

Repository Settings


The following table describes the fields on the **Repository List** window, which you can use to create repositories to store your backup files. To view this window, click the **Menu** icon () and choose **Administration > Maintenance > Repository**.

Table 1: Repository Settings

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Host	(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IP address (IPv4 or IPv6) of the server where you want to create the repository. Note Ensure that the ISE eth0 interface of is configured with an IPv6 address if you are adding a repository with an IPv6 address.
Path	Enter the path to your repository. The path must be valid and must exist at the time you create the repository. Note that some of the special characters like !, ?, ~ (that are not included in the list above) are allowed for the FTP and SFTP password configuration via GUI. However, these special characters are not allowed for configuration via CLI or Open API.

Related Topics

[Backup and Restore Repositories](#)
[Create Repositories](#), on page 9

Enable RSA Public Key Authentication in SFTP Repository

In the SFTP server, each node must have two RSA public keys, one each for CLI and for GUI. To enable RSA public key authentication in SFTP repository, perform the following steps:



Note After you enable RSA public key authentication in SFTP repository, you will not be able to log in using SFTP credentials. You can either use PKI-based authentication or credential-based authentication. If you want to use credential-based authentication again, you must remove the public key pair from the SFTP server.

Step 1 Log in to SFTP server with an account that has permission to edit the `/etc/ssh/sshd_config` file.

Note The location of the `sshd_config` file might vary based on the operating system installation.

Step 2 Enter the `vi /etc/ssh/sshd_config` command.
The contents of the `sshd_config` file is listed.

Step 3 Remove the `"#"` symbol from the following lines to enable RSA public key authentication:

- RSAAuthentication yes
 - PubkeyAuthentication yes
- Note** If Public Auth Key is no, change it to yes.
- AuthorizedKeysFile ~/.ssh/authorized_keys

On-Demand and Scheduled Backups

You can configure on-demand backups of the primary PAN. Perform an on-demand backup when you want to back up data immediately.

You can schedule system-level backups to run once, daily, weekly, or monthly. Because backup operations can be lengthy, you can schedule them so they are not a disruption. You can schedule a backup from the Admin portal.



Note If you are using the internal CA, you should use the CLI to export certificates and keys. Backup using in the administration portal does not back up the CA chain.

For more information, see the "Export Cisco ISE CA Certificates and Keys" section in the "Basic Setup" chapter *Cisco Identity Services Engine Administrator Guide* .

Configurational and operational backups on Cisco ISE can overload your system for a short time. This expected behaviour of temporary system overload will depend on the configuration and monitoring database size of your system.

Perform an On-Demand Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE-PIC to the configuration state that existed at the time of obtaining the backup.



Important When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you have to choose from one of these options to avoid errors:

• **Option 1:**

Export the CA certificates from the source ISE-PIC node through the CLI and import them in to the target system through the CLI.

Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

• **Option 2:**

After the restore process, generate all new certificates for the internal CA.

Pros: This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system continues to be trusted.

Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Before you begin

- Before you perform an on-demand backup, you should have a basic understanding of the backup data types in Cisco ISE-PIC.
- Ensure that you have created repositories for storing the backup files.
- Do not back up using a local repository.

-
- Step 1** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose **Administration > Maintenance > Backup and Restore**.
 - Step 2** Choose the type of backup: Configuration or Operational.
 - Step 3** Click **Backup Now**.
 - Step 4** Enter the values as required to perform a backup.
 - Step 5** Click **Backup**.
 - Step 6** Verify that the backup completed successfully.

Cisco ISE-PIC appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE-PIC adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository.

Do not promote a node when the backup is running. This will shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node changes.

Note High CPU usage might be observed and High Load Average alarm might be seen when the backup is running. CPU usage will be back to normal when the backup is complete.

Schedule a Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE-PIC to the configuration state that existed at the time of obtaining the backup.



Important When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**

Export the CA certificates from the source ISE-PIC node through the CLI and import them in to the target system through the CLI.

Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

After the restore process, generate all new certificates for the internal CA.

Pros: This option is the recommended and clean method, where the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.

Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Before you begin

- Before you schedule a backup, you should have a basic understanding of the backup data types in Cisco ISE-PIC.
- Ensure that you have configured repositories.
- Do not back up using a local repository.



Note For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

Backup Using the CLI

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI. However, you can perform operational backup on the secondary monitoring node only from the CLI.

Backup History

Backup history provides basic information about scheduled and on-demand backups. It lists the name of the backup, backup file size, repository where the backup is stored, and time stamp that indicates when the backup was obtained. This information is available in the Operations Audit report and on the Backup and Restore page in the History table.

For failed backups, Cisco ISE-PIC triggers an alarm. The backup history page provides the failure reason. The failure reason is also cited in the Operations Audit report. If the failure reason is missing or is not clear, you can run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

While the backup operation is in progress, you can use the **show backup status** CLI command to check the progress of the backup operation.

Backup history is stored along with the Cisco ADE operating system configuration data. It remains there even after an application upgrade and are only removed when you reimage the PAN.

Backup Failures

If backup fails, check the following:

- Check if there is any NTP sync or service failure issue. When the NTP service on Cisco ISE is not working, Cisco ISE raises the NTP Service Failure alarm. When Cisco ISE cannot sync with all the configured NTP servers, Cisco ISE raises the NTP Sync Failure alarm. Cisco ISE backup might fail if the NTP services are down or if there is any sync issue. Check the Alarms dashlet and fix the NTP sync or service issue before you retry the backup operation.
- Make sure that no other backup is running at the same time.
- Check the available disk space for the configured repository.
 - Monitoring (operational) backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your node is allocated 600 GB, and the monitoring data takes up more than 450 GB of storage, then monitoring backup fails.
 - If the database disk usage is greater than 90%, a purge occurs to bring the database size to less than or equal to 75% of its allocated size.
- Verify if a purge is in progress. Backup and restore operations will not work while a purge is in progress.
- Verify if the repository is configured correctly.

Cisco ISE Restore Operation

You can restore configuration data on a primary or standalone node. After you restore data on the Primary PAN, you must manually synchronize the secondary nodes with the Primary PAN.



Note The new backup/restore user interface in Cisco ISE-PIC makes use of meta-data in the backup filename. Therefore, after a backup completes, you should not modify the backup filename manually. If you manually modify the backup filename, the Cisco ISE-PIC backup/restore user interface will not be able to recognize the backup file. If you have to modify the backup filename, you should use the Cisco ISE CLI to restore the backup.

Guidelines for Data Restoration



Note

- From Cisco ISE Release 3.2 and above, Root CA regeneration happens automatically in the restore flow. Thus, Root CA regeneration post config-backup is not required.

Following are guidelines to follow when you restore Cisco ISE-PIC backup data.

- Cisco ISE allows you to obtain a backup from an ISE node (A) and restore it on another ISE node (B), both having the same host names (but different IP addresses). However, after you restore the backup on node B, do not change the hostname of node B because it might cause issues with certificates and portal group tags.
- If you obtain a backup from the Primary PAN in one timezone and try to restore it on another Cisco ISE-PIC node in another timezone, the restore process might fail. This failure happens if the timestamp in the backup file is later than the system time on the Cisco ISE-PIC node on which the backup is restored. If you restore the same backup a day after it was obtained, then the timestamp in the backup file is in the past and the restore process succeeds.
- When you restore a backup on the Primary PAN with a different hostname than the one from which the backup was obtained, the Primary PAN becomes a standalone node. The deployment is broken and the secondary nodes become nonfunctional. You must make the standalone node the primary node, reset the configuration on the secondary nodes, and reregister them with the primary node. To reset the configuration on Cisco ISE-PIC nodes, enter the following command from the Cisco ISE CLI:
 - **application reset-config ise**
- We recommend that you do not change the system timezone after the initial Cisco ISE-PIC installation and setup.
- If you changed the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data from the standalone Cisco ISE-PIC node or Primary PAN. Otherwise, if you try to restore data using an older backup, the communication between the nodes might fail.
- After you restore the configuration backup on the Primary PAN, you can import the Cisco ISE CA certificates and keys that you exported earlier.



Note If you did not export the Cisco ISE CA certificates and keys, then after you restore the configuration backup on the Primary PAN, generate the root CA and subordinate CAs on the Primary PAN.

- If you are trying to restore a platinum database without using the correct FQDN (FQDN of a platinum database), you need to regenerate the CA certificates. (To view this window, click the **Menu** icon (☰) and choose **Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain**). However, If you restore the platinum database with the correct FQDN, note that the CA certificates regenerated automatically.
- You need a data repository, which is the location where Cisco ISE-PIC saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.
- If you have a standalone node that fails, you must run the configuration backup to restore it. If the Primary PAN fails, you can promote your Secondary Administration Node to become the primary. You can then restore data on the Primary PAN after it comes up.



Note Cisco ISE-PIC also provides the **backup-logs** CLI command that you can use to collect log and configuration files for troubleshooting purposes.

Restoration of Configuration or Monitoring (Operational) Backup from the CLI

To restore configuration data through the Cisco ISE CLI, use the **restore** command in the EXEC mode. Use the following command to restore data from a configuration or operational backup:

restore *filename* **repository** *repository-name* **encryption-key** **hash|plain** *encryption-key name* **include-adeos**

Syntax Description

restore	Type this command to restore data from a configuration or operational backup.
<i>filename</i>	Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. Note You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository	Specifies the repository that contains the backup.
<i>repository-name</i>	Name of the repository you want to restore the backup from.
encryption-key	(Optional) Specifies user-defined encryption key to restore backup.
hash	Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.
<i>encryption-key name</i>	Enter the encryption key.
include-adeos	(Optional, applicable only for configuration backup) Enter this command operator parameter if you want to restore ADE-OS configuration from a configuration backup. When you restore a configuration backup, if you do not include this parameter, Cisco ISE restores only the Cisco ISE application configuration data.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you use restore commands in Cisco ISE-PIC, the Cisco ISE-PIC server restarts automatically.

The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the **restore** command without the encryption key.

Examples

```

ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore. Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#

```

Related Commands

	Description
backup	Performs a backup (Cisco ISE-PIC and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.
show backup status	Displays the status of the backup operation.
show restore status	Displays the status of the restore operation.

If the sync status and replication status after application restore for any secondary node is *Out of Sync*, you have to reimport the certificate of that secondary node to the Primary PAN and perform a manual synchronization.

Restore Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal.

-
- Step 1** Choose **Administration** > **Maintenance** > **Backup and Restore**.
 - Step 2** Select the name of the backup from the list of Configurational backup and click **Restore**.
 - Step 3** Enter the Encryption Key used during the backup.
 - Step 4** Click **Restore**.
-

What to do next

If you are using the Cisco ISE CA service, you must:

1. Regenerate the entire Cisco ISE CA root chain.
2. Obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. This ensures that the secondary PAN can function as the root CA or subordinate CA of an external PKI in case of a Primary PAN failure and you promote the secondary PAN to be the primary PAN.

Restore History

You can obtain information about all restore operations, log events, and statuses from the **Operations Audit Report** window.



Note However, the **Operations Audit Report** window does not provide information about the start times corresponding to the previous restore operations.

For troubleshooting information, you have to run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log file.

While the restore operation is in progress, all Cisco ISE-PIC services are stopped. You can use the **show restore status** CLI command to check the progress of the restore operation.

Synchronize Primary and Secondary Nodes

the Cisco ISE-PIC database in the primary and secondary nodes are not synchronized automatically after restoring a backup file on the PAN. If this happens, you can manually force a full replication from the PAN to the secondary ISE-PIC nodes. You can force a synchronization only from the PAN to the secondary nodes. During the sync-up operation, you cannot make any configuration changes. Cisco ISE-PIC allows you to navigate to other Cisco ISE-PIC Admin portal pages and make any configuration changes only after the synchronization is complete.

-
- Step 1** Choose **Administration > Deployment**.
- Step 2** Check the check box next to the secondary node if it has an Out of Sync replication status.
- Step 3** Click **Syncup** and wait until the nodes are synchronized with the PAN. You will have to wait until this process is complete before you can access the Cisco ISE-PIC Admin portal again.
-

Recovery of Lost Nodes in Standalone and Two-Node Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and two-node deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data.

Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Two-Node Deployment

Scenario

In a two-node deployment, a natural disaster leads to a loss of all the nodes. After recovery, you want to use the existing IP addresses and hostnames.

For example, you have two nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Administration Node or Secondary PAN.) A backup of the N1 node, which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster.

Assumption

All Cisco ISE-PIC nodes in the deployment were destroyed. The new hardware was imaged using the same hostnames and IP addresses.

Resolution Steps

1. You have to replace both the N1 and N2 nodes. N1 and N2 nodes will now have a standalone configuration.
2. Obtain a license with the UDI of the N1 and N2 nodes and install it on the N1 node.
3. You must then restore the backup on the replaced N1 node. The restore script will try to sync the data on N2, but N2 is now a standalone node and the synchronization fails. Data on N1 will be reset to time T1.
4. You must log in to the N1 Admin portal to delete and reregister the N2 node. Both the N1 and N2 nodes will have data reset to time T1.

Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Two-Node Deployment

Scenario

In a two-node deployment, a natural disaster leads to loss of all the nodes. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

For example, you have two ISE-PIC nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Node.) A backup of the N1 node which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster. The Cisco ISE-PIC nodes are replaced at a new location and the new hostnames are N1A (primary PAN) and N2A (secondary Node). N1A and N2A are standalone nodes at this point in time.

Assumptions

All Cisco ISE-PIC nodes in the deployment were destroyed. The new hardware was imaged at a different location using different hostnames and IP addresses.

Resolution Steps

1. Obtain the N1 backup and restore it on N1A. The restore script will identify the hostname change and domain name change, and will update the hostname and domain name in the deployment configuration based on the current hostname.
2. You must generate a new self-signed certificate.
3. Delete the old N2 node.
Register the new N2A node as a secondary node. Data from the N1A node will be replicated to the N2A node.

Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database was taken at time T1. The N1 node goes down because of a physical failure and must be reimaged or a new hardware is required. The N1 node must be brought back up with the same IP address and hostname.

Assumptions

This deployment is a standalone deployment and the new or reimaged hardware has the same IP address and hostname.

Resolution Steps

Once the N1 node is up after a reimage or you have introduced a new Cisco ISE-PIC node with the same IP address and hostname, you must restore the backup taken from the old N1 node. You do not have to make any role changes.

Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database taken at time T1 is available. The N1 node is down because of a physical failure and will be replaced by a new hardware at a different location with a different IP address and hostname.

Assumptions

This is a standalone deployment and the replaced hardware has a different IP address and hostname.

Resolution Steps

1. Replace the N1 node with a new hardware. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. No role changes are required.

Configuration Rollback

Problem

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. In this case, you can revert to the original configuration by restoring a backup that was taken before you made the changes.

Possible Causes

There are two nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Policy Administration Node or secondary PAN) and a backup of the N1 node is available. You made some incorrect configuration changes on N1 and want to remove the changes.

Solution

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. The restore script will synchronize the data from N1 to N2.

Recovery of Primary Node in Case of Failure in a Two-Node Deployment

Scenario


In a multinode deployment, the PAN fails.

For example, you have two Cisco ISE-PIC nodes, N1 (PAN) and N2 (Secondary Administration Node). N1 fails because of hardware issues.

Assumptions

Only the primary node in a two-node deployment has failed.

Resolution Steps

1. Log in to the N2 administrator portal. In the Cisco ISE GUI, click the **Menu** icon () and choose **and** configure N2 as your primary node.

The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 administrator portal, register the new N1 node as a secondary node.

Now, the N2 node becomes your primary node and the N1 node becomes your secondary node.

If you wish to make the N1 node the primary node again, log in to the N1 administrator portal and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

Recovery of Secondary Node in Case of Failure in a Two-Node Deployment

Scenario

In a multinode deployment, a single secondary node has failed. No restore is required.

Resolution Steps

1. Reimage the secondary node to the default standalone state.
2. Log in to the Admin portal from the primary node and delete the secondary node.
3. Reregister the secondary node.

Data is replicated from the primary to the secondary node. No restore is required.

Database Purge

The purging process allows you to manage the size of the database by specifying the number of months to retain the data during a purge. The default is three months. This value is utilized when the disk space usage threshold for purging (80 percentage of the total disk space) is met. For this option, each month consists of 30 days. A default of three months equals 90 days.

Guidelines for Purging the Database

Follow these guidelines for optimal Monitoring database disk usage:

- If the database disk usage is greater than 80 percent of the threshold setting, that is 60 percent of total disk space, a critical alarm is generated, indicating that the database size is about to exceed the maximum amount of allocated disk size. If the disk usage is greater than 90 percent of the threshold setting, that is 70 percent of total disk space, another alarm is generated, indicating that the database size has exceeded the maximum amount of allocated disk size.
- Purging is also based on the percentage of consumed disk space for the database. When the consumed disk space for the database is equal to or exceeds the threshold (the default is 80 percentage of the total disk space), the purge process starts. This process deletes only the oldest seven days' monitoring data, irrespective of what is configured in the Admin portal. It continues this process in a loop until the disk space is below 80 percent. Purging always checks the database disk space limit before proceeding.

Operational Data Purging

Cisco ISE Monitoring Operational database contains information that is generated as Cisco ISE reports. Recent Cisco ISE (Cisco ISE Release 2.4 and above) releases have options to purge the monitoring operational data and reset the monitoring database when the **application configure ise** command is run.

The purge option is used to clean up the data and prompts you to enter the number of days for which to retain the data. The reset option is used to reset the database to the factory default, so that all the data that is backed up is permanently deleted. Specify the database if the files are consuming too much file system space.



Note The reset option causes Cisco ISE services to be temporarily unavailable.

Related Topics

[Purge Older Operational Data](#), on page 24

Purge Older Operational Data

The operational data is collected in the server over a period of time. It can be purged either instantly or periodically.

Step 1 Choose **Administration > Maintenance > Operational Data Purging**.

Step 2 Do one of the following:

- In the **Data Retention Period** area:
 - a. Specify the time period, in days, for which RADIUS and TACACS data should be retained. All the data prior to the specified time period is exported to a repository. While ISE-PIC does not offer RADIUS or TACACS functionality, some of the infrastructure is shared with Cisco ISE and therefore, it may be necessary to purge such information from the database periodically.
 - b. In the **Repository** area, check the **Enable Export Repository** check box to choose the repository to save data.
 - c. In the **Encryption Key** field, enter the required password.
 - d. Click **Save**.

Note If the configured retention period is less than the existing retention thresholds corresponding to the diagnostics data, the configured value overrides the existing threshold values. For example, if you configure the retention period as three days and this value is less than the existing thresholds in the diagnostics tables (for example, a default of five days), the data is purged according to the value that you configure (three days) in this window.

- In the **Purge Data Now** area:
 - a. Choose to purge all the data or to purge the data that is older than the specified number of days. Data is not saved in any repository.
 - b. Click **Purge**.

Upgrading ISE-PIC to a Full ISE Installation

Cisco ISE-PIC is displayed in a simple user-intuitive GUI, based on the full Cisco ISE GUI. As a result, the installation of ISE-PIC enables you to easily upgrade to ISE quickly and efficiently. When upgrading from ISE-PIC to the Essential license for ISE, ISE continues to offer all features that were available to you in ISE-PIC prior to upgrade and you will not need to reconfigure any settings that you had already configured if you use the upgraded ISE-PIC node as your primary PAN.



Note If you do not use the existing upgraded ISE-PIC node as your primary PAN, then the data on that node will be erased when you upgrade and you will be able to access the data from your existing full ISE deployment from the newly added node.

For more information about the benefits of upgrading to ISE, see [Comparing ISE-PIC with Cisco ISE and Cisco Context Directory Agent](#).

Upgrade to ISE by Registering Licenses

Before you begin

An ISE-PIC node can be upgraded to a Cisco ISE node by enabling the Essential license. Before enabling the Essential license, you must purchase and enable both ISE-PIC and ISE-PIC Upgrade licenses on the ISE-PIC node. The Essential license is displayed in the Licenses table after you register the license in CSSM. The application services are restarted during the upgrade.

For more information about the licensing model, see [ISE-PIC Smart Licensing](#)

-
- Step 1** If you have a secondary node installed, from your Cisco ISE-PIC primary node installation, choose **Administration > Deployment** and Deregister the secondary node. Both nodes then become primary nodes and either of them can be upgraded.
- Step 2** Choose **Administration > Licensing**.
- Step 3** Click **Import License**.
- Step 4** Click **Choose File**, browse for the Upgrade license file, and click **OK**.
- Step 5** **Note** If you are adding this ISE-PIC node to an existing ISE deployment, you have completed the upgrade once you have completed this step and now can add the node by registering it from the primary node in that deployment. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).
- From the **Import New License File** screen, click **Import**.
- Step 6** To make this upgraded node the primary node in a full ISE deployment import a Essential license now. Click **Import License** again.
- Step 7** Click **Choose File**, browse for the license that you received from your Cisco representative, and click **OK**.
- Step 8** From the **Import New License File** screen, click **Import**.
- Step 9** Click **OK**.
The upgrade to being a primary node of ISE begins and the following message appears: *This node is now being upgraded to ISE in the background. Please wait several minutes and then log in to ISE.*
- Step 10** Click **OK**.
The log in screen appears after several minutes. Log back in and access all menus offered by the Essential license installation.
- You have now upgraded your primary ISE-PIC node to be the primary node in a full ISE installation and the former secondary node is now the primary and only node in the ISE-PIC standalone installation. You can now separately upgrade the last ISE-PIC node in the same manner.
-

Manage Settings in ISE-PIC

Role-Based Access Control

Cisco ISE-PIC allows you to define role-based access control (RBAC) policies that allow or deny certain system-operation permissions to an administrator. These RBAC policies are defined based on the identity of individual administrators or the admin group to which they belong.

To further enhance security and control who has access to the Admin portal, you can:

- Configure administrative access settings based on the IP address of remote clients.
- Define strong password policies for administrative accounts.
- Configure session timeouts for administrative GUI sessions.

Cisco ISE-PIC Administrators

Administrators can use the admin portal to:

- Manage deployments node monitoring and troubleshooting.
- Manage Cisco ISE-PIC servicesadministrator accounts, and system configuration and operations.
- Change administrator and user passwords.

A CLI administrator can start and stop the Cisco ISE application, apply software patches and upgrades, reload or shut down the Cisco ISE appliance, and view all the system and application logs. Because of the special privileges that are granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments.

The username and password that you configure during setup is intended only for administrative access to the CLI. This role is considered to be the CLI admin user, also known as CLI administrator. By default, the username for a CLI admin user is admin, and the password is defined during setup. There is no default password. This CLI admin user is the default admin user, and this user account cannot be deleted. However, other administrators can edit it, including options to enable, disable, or change password for the corresponding account.

You can either create an administrator, or promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges.

Administrators are users who have local privileges to configure and operate the Cisco ISE-PIC system.

Administrators are assigned to one or more admin groups. These admin groups are predefined in the system for your convenience, as described in the following section.



Note From Cisco ISE Release 2.7, use alphanumeric values while creating user accounts in Cisco ISE.

Related Topics

[Cisco ISE-PIC Administrator Groups](#), on page 26

Cisco ISE-PIC Administrator Groups

Administrator groups are role-based access control (RBAC) groups in Cisco ISE-PIC. All the administrators who belong to the same group share a common identity and have the same privileges. An administrator's identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

Cisco ISE supports multiple external identity stores for enhanced user access management by admins.

An administrator account with any level of access can be used to modify or delete the objects for which it has permission, on any window it has access to.

The following table lists the admin groups that are predefined in Cisco ISE-PIC, and the tasks that members from these groups can perform. Only these pre-defined groups are available for defining administrator users in the system.

Table 2: Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Admin Group Role	Access Level	Permissions	Restrictions
Super Admin	All Cisco ISE-PIC administrative functions. The default administrator account belongs to this group.	Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE-PIC resources.	
External RESTful Services (ERS) Admin	Full access to all ERS API requests such as GET, POST, DELETE, PUT	<ul style="list-style-type: none"> Create, Read, Update, and Delete ERS API requests 	The role is meant only for ERS authorization supporting Internal Users, Identity Groups, and Endpoints

Privileges of a CLI Administrator Versus a Web-Based Administrator

A CLI administrator can start and stop the Cisco ISE-PIC application, apply software patches and upgrades, reload or shut down the Cisco ISE-PIC appliance, and view all the system and application logs. Because of the special privileges granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE-PIC deployments.

Create a New Administrator

Cisco ISE-PIC administrators need accounts with specific roles assigned to them in order to perform specific administrative tasks. You can create multiple administrator accounts and assign one or more roles to these admins based on the administrative tasks that these admins have to perform.

Use the **Admin Users** window to view, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE-PIC administrators.



Note We recommend that you configure Active Directory access in the CLI before you join it in the GUI if the admin user's domain is the same in both the CLI and the GUI. Else, you must rejoin the domain from the GUI to avoid authentication failures to that domain.

Step 1 Choose **Administration > Admin Access > Admin Users > Add > Create an Admin User**.

Step 2 Enter values in the fields. The characters supported for the **Name** field are # \$ ' () * + - . / @ _ .

The admin user name must be unique. If you have entered an existing user name, an error pop-up window displays the following message:

User can't be created. A User with that name already exists.

Step 3 Click **Submit** to create a new administrator in the Cisco ISE-PIC internal database.

Related Topics

[Read-Only Admin Policy](#)

[Customize Menu Access for the Read-Only Administrator](#)

Administrative Access to Cisco ISE-PIC

Cisco ISE-PIC administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical. Grant administrative access only to users who are authorized to administer Cisco ISE-PIC in your network.



Note When a Cisco ISE server is added to a network, it is marked to be in Running state after its web interface comes up. However, it might take some more time for all the services to be fully operational because some advanced services, such as posture services, might take longer to be available.

Administrative Access Methods

You can connect to the Cisco ISE servers in several ways. The policy administration node (PAN) runs the Administrators portal. An admin password is required to log in. Other ISE persona servers are accessible through SSH or the console, from where you run the CLI. This section describes the process and password options available for each connection type:

- **Admin password:** The Cisco ISE Admin user that you created during installation, times out in 45 days by default. You can prevent that by turning off **Password Lifetime** from **Administration > System > Admin Settings**. Click the **Password Policy** tab, and uncheck the **Administrative passwords expire** check box under **Password Lifetime**.

If you do not do this, and the password expires, you can reset the admin password in the CLI by running the **application reset-passwd** command. You can reset the admin password by connecting to the console to access the CLI, or by rebooting the ISE image file to access the boot options menu.

- **CLI password:** You must enter a CLI password during installation. If you have a problem logging in to the CLI because of an invalid password, you can reset the CLI password. Connect to the console and run the **password** CLI command to reset the password. See the [Cisco Identity Services Engine CLI Reference Guide](#) for more information.

•

Administrator Access Settings

Cisco ISE-PIC allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define in the Administrator Account Settings in Cisco ISE-PIC applies to all administrator accounts.

Cisco ISE-PIC supports administrator passwords with UTF-8 characters.

Configure Maximum Number of Concurrent Administrative Sessions and Login Banners

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners

are disabled. However, you cannot configure the maximum number of concurrent sessions for individual administrator accounts.

Step 1 Choose **Administration > Admin Access > Access Settings > Session**.

Step 2 Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.

Step 3 If you want Cisco ISE-PIC to display a message before an administrator logs in, check the **Pre-login banner** check box and enter your message in the text box.

Step 4 If you want Cisco ISE-PIC to display a message after an administrator logs in, check the **Post-login banner** check box and enter your message in the text box.

Step 5 Click **Save**.

Note The character limit is set at 1500 for the Pre-login banner and 3000 for the Post-login banner. All characters except % and < are supported. For login banner installation through CLI, the maximum length of the file name used is 256 characters.

Allow Administrative Access to Cisco ISE-PIC from Select IP Addresses

Cisco ISE-PIC allows you to configure a list of IP addresses from which administrators can access the Cisco ISE-PIC management interfaces.

Step 1 Choose **Administration > Admin Access > Access Settings > IP Access**.

Step 2 Choose the service for which you want to configure access restriction by clicking the corresponding service tab. You can configure access restriction for the following services:

- **Admin GUI and CLI**
- **Admin Services** (ERS API, OpenAPI)
- **User Services** (Guest, BYOD, and Posture)

Step 3 Click the **Allow only Listed IP addresses to Connect** radio button.

Note Connection on Port 161 (SNMP) is used for administrative access. However, when IP access restrictions are configured, the **snmpwalk** fails if the node from which it was performed is not configured for administrative access.

Step 4 In the **Configure IP List for Access Restriction** area, click **Add**.

Step 5 In the **Add IP CIDR** dialog box, enter the IP addresses in the classless interdomain routing (CIDR) format in the **IP Address** field.

Note This IP address can be an IPv4 or an IPv6 address. You can configure multiple IPv6 addresses for a Cisco ISE node.

Step 6 Enter the subnet mask in the **Netmask in CIDR format** field.

Step 7 Click **OK**.

Repeat steps 4 to 7 to add more IP address ranges to this list.

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

Step 9 Click **Reset** to refresh the **IP Access** window.

Configure a Password Policy for Administrator Accounts

Cisco ISE-PIC also allows you to create a password policy for administrator accounts to enhance security. The password policy that you define here is applied to all the administrator accounts in Cisco ISE-PIC.



Note

- Email notifications for internal admin users are sent to root@host. You cannot configure the email address, and many SMTP servers reject this email.
Follow open defect CSCui5583, which is an enhancement to allow you to change the email address.
- Cisco ISE-PIC supports administrator passwords with UTF-8 characters.

Step 1 Choose **Administration > Admin Access > Authentication**.

Step 2 Click the **Password Policy** tab and enter the required values to configure the Cisco ISE GUI and CLI password requirements.

Step 3 Click **Save** to save the administrator password policy.

Note If you use an external identity store to authenticate administrators at login, note that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator's username and password.

Configure Account Disable Policy for Administrator Accounts

Cisco ISE-PIC allows you to disable an administrator account if the administrator account is not authenticated for the configured consecutive number of days.

Step 1 Choose **Administration > Admin Access > Authentication > Account Disable Policy**.

Step 2 Check the **Disable account after n days of inactivity** check box, and enter the number of days in the corresponding field.

This option allows you to disable the administrator account if the administrator account was inactive for the specified number of days.

When an administrator account is disabled and enabled later, it does not remain active for more than 24 hours. If you want an administrator account to remain active even when disabled, keep the **Disable account after n days of inactivity** checkbox unchecked.

Attention Cisco ISE does not support the **Disable account after n days of inactivity** option even if it is enabled, for administrator accounts that have **Collection Filters (Work Centers > Network Access > Settings > Collection Filters > Filter All)** configured.

Step 3 Click **Save** to configure the global account disable policy for administrators.

Configure Session Timeout for Administrators

Cisco ISE-PIC allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE-PIC logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE-PIC Admin portal.

Step 1 Choose **Administration** > **Admin Access** > **Session Settings** > **Session Timeout**.

Step 2 Enter the time in minutes that you want Cisco ISE-PIC to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

Step 3 Click **Save**.

Terminate an Active Administrative Session

Cisco ISE-PIC displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

Step 1 Choose **Administration** > **Admin Access** > **Session Settings** > **Session Info**.

Step 2 Check the check box next to the session ID that you want to terminate and click **Invalidate**.

Ports Used by the Administration Portal

The administration portal uses HTTP port 80 and HTTPS port 443 and you cannot change these settings. You cannot configure any of the end user portals to use these ports, to reduce the risk to the administration portal.

Configure SMTP Server to Support Notifications

Configure a Simple Mail Transfer Protocol (SMTP) server to send email notifications for alarms.

Which ISE Nodes Send Email

The following list shows which node in a distributed ISE environment sends email.

Email Purpose	Node That Sends the Email
guest expiration	Primary PAN
alarms	Active MnT
sponsor and guest notifications from guest and sponsor portals	PSN

Email Purpose	Node That Sends the Email
password expirations	Primary PAN

-
- Step 1** Choose **Settings > SMTP Server**.
- Step 2** Enter the hostname of the outbound SMTP server in the **SMTP server** field. This SMTP host server must be accessible from the Cisco ISE-PIC server. The maximum length for this field is 60 characters.
- Step 3** Click **Save**.
-

The recipient of alarm notifications can be any internal admin users with the **Include system alarms in emails** option enabled. The sender's email address for sending alarm notifications is hardcoded as `ise@<hostname>`.

Enabling External RESTful Services APIs from the GUI—ERS Settings

Before you begin

You must enable the Cisco ISE REST API in order for applications developed for a Cisco ISE REST API to be able to access Cisco ISE. The Cisco REST APIs uses HTTPS port 9060, which is closed by default. If the Cisco ISE REST APIs are not enabled on the Cisco ISE admin server, the client application will receive a time-out error from the server for any Guest REST API request.

External RESTful Service requests of all types are valid only for the primary ISE node. Secondary nodes have read-access (GET requests).

-
- Step 1** Choose **Settings > ERS Settings**.
- Step 2** Choose **Enable ERS for Read/Write** and click **Save**.
-

What to do next

See the [ISE API reference guide](#) for more information and details about API calls and ISE-PIC.

Configure Security Settings

To configure the security settings:

-
- Step 1** Choose **Settings > Security Settings**.
- Step 2** In the **Security Settings** window, choose the required options:
- a. **Allow TLS 1.0:** Allows TLS 1.0 for communication with legacy peers for the following workflows:
 - Cisco ISE is configured as an EAP server
 - Cisco ISE downloads CRL from HTTPS or a secure LDAP server

- Cisco ISE is configured as a secure TCP syslog client
- Cisco ISE is configured as a secure LDAP client
- Cisco ISE is configured as an ERS server

Also allows TLS 1.0 for communication with the following ISE components:

- All portals
- Certificate Authority
- MDM Client
- pxGrid
- PassiveID Agent

Note It is recommended that clients and servers negotiate to use a higher version of TLS for enhanced security.

b. Allow TLS 1.1: Allows TLS 1.1 for communication with legacy peers for the following workflows:

- Cisco ISE is configured as an EAP server
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure TCP syslog client
- Cisco ISE is configured as a secure LDAP client
- Cisco ISE is configured as an ERS server

Also allows TLS 1.1 for communication with the following ISE components:

- Admin UI
- All portals
- Certificate Authority
- External RESTful Services (ERS)
- MDM Client
- pxGrid

Note It is recommended that clients and servers negotiate to use a higher version of TLS for enhanced security.

Step 3 Click **Save**.
