



## Managing Backup and Restore Operations

This chapter describes the Cisco Identity Services Engine (ISE) database backup and restore operations, which include Cisco ISE application configuration, Cisco Application Deployment Engine operating system (ADE operating system) configuration and Cisco ISE Monitoring and Troubleshooting database.



### Note

Backup and restore is not available for Inline Posture nodes in Cisco ISE, Release 1.2. For more information on other known issues, see [Release Notes for the Cisco Identity Services Engine, Release 1.2](#).

This chapter contains the following sections:

- [Backup Data Type, page 12-1](#)
- [Backup and Restore Repositories, page 12-2](#)
- [On-Demand and Scheduled Backups, page 12-3](#)
- [Cisco ISE Restore Operation, page 12-7](#)
- [Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 12-12](#)
- [Recovery of Lost Nodes in Standalone and Distributed Deployments, page 12-13](#)

## Backup Data Type

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

Cisco ISE 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.

Restore operation, can be performed with the backup files of previous versions of Cisco ISE and restored on a later version, for example, if you have a backup from an ISE node from Cisco ISE, Release 1.1, you can restore it on Cisco ISE, Release 1.2.

# Backup and Restore Repositories

Cisco ISE allows you to create and delete repositories through the Admin portal. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

For the SNS 3415 and SNS 3495 Appliances, there is no physical CD-ROM available. 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.

**Related Topics**

- [Creating Repositories, page 12-2](#)
- [On-Demand and Scheduled Backups, page 12-3](#)

## Creating Repositories

You can use the CLI and GUI to create repositories, but for Cisco ISE, Release 1.2, it is recommended to 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 administration node get replicated to the other deployment nodes.

**Before You Begin**

To perform the following task, you must be a Super Admin or System Admin.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Choose <b>Administration &gt; System &gt; Maintenance &gt; Repository</b> |
| <b>Step 2</b> | Click <b>Add</b> to add a new repository.                                 |
| <b>Step 3</b> | Enter the values as required to set up new repository.                    |
| <b>Step 4</b> | Click <b>Submit</b> to create the repository.                             |

- Step 5** Verify that the repository is created successfully by clicking **Repository** in the Operations navigation pane on the left or click the **Repository List** link at the top of this page to go to the repository listing page.
- 

#### Related Topics

- [Repository Settings, page A-15](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

#### What to Do Next

- Ensure that the repository that you created is working by executing 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. For more information, see the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).



**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. See [Performing an On-Demand Backup](#) and [Scheduling a Backup](#) for more information.

## On-Demand and Scheduled Backups

Cisco ISE provides on-demand backups of the primary administration node and the primary monitoring node. Perform an on-demand backup when you want to backup data immediately.

Cisco ISE also allows you to schedule system-level backups that can be scheduled 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 Cisco ISE CLI or through the Cisco ISE Admin portal.



**Note** If you upgrade to Cisco ISE, Release 1.2, the scheduled backup jobs need to be recreated.

---

#### Related Topics

- [Scheduling a Backup, page 12-5](#)
- [Performing an On-Demand Backup, page 12-4](#)
- [Performing a Backup from the CLI, page 12-6](#)
- [Backup History, page 12-6](#)
- [Backup Failures, page 12-6](#)
- [Cisco ISE Restore Operation, page 12-7](#)

## Performing an On-Demand Backup

You can perform an On-demand backup to instantly backup the configuration data or monitoring data.

### Before You Begin

- Before you perform this task, you should have a basic understanding of the [Backup Data Type](#) in Cisco ISE.
- Ensure that you have completed [Creating Repositories](#).
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.



#### 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.

---

**Step 1** Choose **Administration > System > Backup and Restore**.

**Step 2** Click **Backup Now**.

**Step 3** Enter the values as required to perform a backup.

**Step 4** Click **OK**.

**Step 5** Verify that the backup completed successfully.

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

---

In a distributed deployment, do not change the role of a node or promote a node when the backup is running. Changing node roles 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 role changes.

### Related Topics

- [On-Demand Backup Settings, page A-16](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Backup and Restore Repositories, page 12-2](#)
- [Scheduling a Backup, page 12-5](#)
- [Performing a Backup from the CLI, page 12-6](#)
- [Backup History, page 12-6](#)
- [Backup Failures, page 12-6](#)

## Scheduling a Backup

You can use this page to schedule configuration or monitoring backups.

### Before You Begin

- Before you perform this task, you should have a basic understanding of the [Backup Data Type](#) and [On-Demand and Scheduled Backups](#) operations in Cisco ISE.
- Ensure that you have configured repositories.
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.
- If you have upgraded to Cisco ISE 1.2 from Cisco ISE 1.1 or earlier releases, you should reconfigure your scheduled backups. See the Known Upgrade Issues section in the *Cisco Identity Services Engine Upgrade Guide, Release 1.2*.



### 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.

- 
- Step 1** Choose **Administration > System > Backup and Restore**.
  - Step 2** Click **Create** to schedule a Configuration or an Operational backup.
  - Step 3** Enter the values as required to schedule a backup.
  - Step 4** Click **Save** to schedule the backup.
  - Step 5** Click the **Refresh** link at the top of this page to see the scheduled backup list.
- 

You can create only one schedule at a time for a Configuration or Operational backup. You can enable or disable a scheduled backup, but you cannot delete it.

To schedule a backup from the CLI, you must use the **kron** CLI command. Although you can schedule backups from the CLI as well as the GUI, it is recommended to use the GUI for better options.

### Related Topics

- [Scheduled Backup Settings, page A-16](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Performing an On-Demand Backup, page 12-4](#)
- [Performing a Backup from the CLI, page 12-6](#)
- [Backup History, page 12-6](#)
- [Backup Failures, page 12-6](#)
- [Backup and Restore Repositories](#)
- Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#) for more information on the **kron** command.

## Performing a Backup from the CLI

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI for better options. But, you can perform Operational backup on the secondary monitoring node only from the CLI.

For information on how to perform a backup from the CLI, see the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

## 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 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 primary administration node.

## Backup Failures

If backup fails, check the following:

- Make sure that no other backup is running at the same time.
- Check the available disk space for the configured repository.
  - Monitoring backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your Monitoring 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 administration node. After you restore data on the primary administration node, you must manually synchronize the secondary nodes with the primary administration node.

The process for restoring the operational data is different depending on the type of deployment.

**Note**

The new backup/restore user interface in Cisco ISE, Release 1.2 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 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.

**Related Topics**

- [Restoration of Configuration or Monitoring Backup from the CLI, page 12-8](#)
- [Restoring Configuration Backups from the GUI, page 12-10](#)
- [Restoration of Monitoring Database, page 12-10](#)
- [Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 12-12](#)

## Data Restoration Guidelines

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

- If you obtain a backup from your primary Administration node in one timezone and try to restore it on another Cisco ISE 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 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 a primary Cisco ISE node with a different hostname than the one from which the backup was obtained, the primary Cisco ISE node 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 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 installation and setup.
- If you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data after you obtain a backup from the standalone Cisco ISE node or primary Administration node. Otherwise, if you try to restore data using the older backup, the communication between the nodes might fail.
- If you want to retain the existing certificate configuration on a Cisco ISE node after restore, then before you begin restore the data, ensure that you export the certificate along with the private key to the system running your client browser. Then, after you restore the data, import the certificate along with the private key in to the Cisco ISE node.

- You need a data repository, which is the location where Cisco ISE saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.
- If you have a standalone administration node that fails, you must run the configuration backup to restore it. If your primary Administration node fails, you can use the distributed setup to promote your secondary Administration node to become the primary. You can then restore data on your primary Administration node after it comes up.

**Note**

Cisco ISE also provides the **backup-logs** CLI command that you can use to collect log and configuration files for troubleshooting purposes. For more information, refer to [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

## Restoration of Configuration or Monitoring 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**

<b>restore</b>	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.  <b>Note</b> You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
<b>repository</b>	Specifies the repository that contains the backup.
<i>repository-name</i>	Name of the repository you want to restore the backup from.
<b>encryption-key</b>	(Optional) Specifies user-defined encryption key to restore backup.
<b>hash</b>	Hashed encryption key for restoring backup. Specifies an <i>encrypted</i> (hashed) encryption key that follows. Supports up to 40 characters.
<b>plain</b>	Plaintext encryption key for restoring backup. Specifies an <i>unencrypted</i> plaintext encryption key that follows. Supports up to 15 characters.
<i>encryption-key name</i>	Enter the encryption key.
<b>include-adeos</b>	(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, the Cisco ISE 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**

Command	Description
backup	Performs a backup (Cisco ISE 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.

For more information, refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

For information on checking the status of a restore operation, see the “Restore History” section on [page 12-12](#).

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 administration node and perform a manual synchronization. See [Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 12-12](#) for the procedure to perform manual synchronization.

**Related Topic**

[Restoring Configuration Backups from the GUI, page 12-10](#)

## Restoring Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal. The GUI lists only the backups that are taken from Cisco ISE, Release 1.2. To restore backups that are prior to this release, use the restore command from the CLI.

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Administration &gt; System &gt; Backup and Restore</b> .                               |
| <b>Step 2</b> | Select the name of the backup from the list of Configurational backup and click <b>Restore</b> . |
| <b>Step 3</b> | Enter the Encryption Key used during the backup.   |
| <b>Step 4</b> | Click <b>Restore</b> .   |
- 

### Related Topics

[Restoration of Configuration or Monitoring Backup from the CLI, page 12-8](#)

## Restoration of Monitoring Database

The process for restoring the Monitoring database is different depending on the type of deployment. The following sections explain how to restore the Monitoring database in standalone and distributed deployments.

You must use the CLI to restore an on-demand Monitoring database backup from Cisco ISE, Release 1.0, 1.0.4, or 1.1, to Cisco ISE, Release 1.2. Restoring a scheduled backup across Cisco ISE releases is NOT supported.



### Note

If you attempt to restore data to a node other than the one from which the data was taken, you must configure the logging target settings to point to the new node. This ensures that the monitoring syslogs are sent to the correct node. For more information, see [Configuring Remote Syslog Collection Locations, page 11-4](#).

### Related Topics

- [Restoring a Monitoring Backup in a Standalone Environment or with a Monitoring Persona, page 12-10](#)
- [Restoring a Monitoring Backup with Administration and Monitor Personas, page 12-11](#)

## Restoring a Monitoring Backup in a Standalone Environment or with a Monitoring Persona

The GUI lists only the backups that are taken from Cisco ISE, Release 1.2. To restore backups that are prior to this release, use the restore command from the CLI.

**Before You Begin**

You should have successfully performed the following procedures:

- [Scheduling a Backup, page 12-5](#) or
- [Performing an On-Demand Backup, page 12-4.](#)

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Choose <b>Administration &gt; System &gt; Backup and Restore</b> .                           |
| <b>Step 2</b> | Select the name of the backup from the list of Operational backup and click <b>Restore</b> . |
| <b>Step 3</b> | Enter the Encryption Key used during the backup.   |
| <b>Step 4</b> | Click <b>Restore</b> .   |
- 

**Related Topics**

- [Restoration of Configuration or Monitoring Backup from the CLI, page 12-8](#)
- [Restoring a Monitoring Backup with Administration and Monitor Personas, page 12-11](#)

## Restoring a Monitoring Backup with Administration and Monitor Personas

You can restore a Monitoring backup in a distributed environment with Administration and Monitor personas.

**Before You Begin**

You should have successfully performed the following procedures:

- [Scheduling a Backup, page 12-5](#) or
- [Performing an On-Demand Backup, page 12-4.](#)

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Prepare to promote another Cisco ISE node as the primary Administration node, by syncing the node with the existing primary node you want to backup. For more information, see <a href="#">Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 12-12</a> .<br><br>This ensures that the configuration of the Cisco ISE node you are going to promote is up to date. |
| <b>Step 2</b> | Promote the newly synced Administration node to primary status. For more information, see <a href="#">Configuring a Primary Administration Node, page 3-12</a> .   |
| <b>Step 3</b> | Prepare to deregister the node to be backed up by assigning the Monitoring persona to another node in the deployment. For more information, see <a href="#">Changing Node Personas and Services, page 3-17</a> .<br><br>A deployment must have at least one functioning Monitoring node.   |
| <b>Step 4</b> | Deregister the node to be backed up. For more information, see <a href="#">Removing a Node from Deployment, page 3-19</a> .  |
| <b>Step 5</b> | Restore the Monitoring backup to the newly deregistered node, as described in <a href="#">Restoring a Monitoring Backup in a Standalone Environment or with a Monitoring Persona, page 12-10</a> .   |
| <b>Step 6</b> | Register the newly restored node with the current Administration node. For more information, see <a href="#">Registering a Secondary Cisco ISE Node, page 3-12</a> .   |

- Step 7** Promote the newly restored and registered node as the primary Administration node. For more information, see [Configuring a Primary Administration Node, page 3-12](#).
- 

#### Related Topics

- [Restoring a Monitoring Backup in a Standalone Environment or with a Monitoring Persona, page 12-10](#)

## Restore History

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



#### Note

However, the Operations Audit report 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 services are stopped. You can use the **show restore status** CLI command to check the progress of the restore operation.

#### Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

## Synchronizing Primary and Secondary Nodes in a Distributed Environment

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

#### Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

---

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

**Related Topics**

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

## Recovery of Lost Nodes in Standalone and Distributed Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and distributed 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 Distributed Deployment, page 12-13](#)
- [Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment, page 12-14](#)
- [Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment, page 12-15](#)
- [Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment, page 12-15](#)
- [Configuration Rollback, page 12-16](#)
- [Recovery of Primary Node in Case of Failure in a Distributed Deployment, page 12-16](#)
- [Recovery of Secondary Node in Case of Failure in a Distributed Deployment, page 12-16](#)

## Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment

**Scenario**

In a distributed 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 Administration node) and N2 (secondary Administration 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.

**Assumption**

All Cisco ISE 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. See [“Replacing the Cisco ISE Appliance Hardware” section on page 3-20](#) for more information. 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. See [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information. The restore script will try to sync the data on N2, but N2 is now a standalone node and the sync will fail. 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. See the following for more information:
  - [“Removing a Node from Deployment” section on page 3-19](#)
  - [“Registering a Secondary Cisco ISE Node” section on page 3-12](#)

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 Distributed Deployment

### Scenario

In a distributed 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 nodes: N1 (primary Administration node) and N2 (secondary Policy Service 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 nodes are replaced at a new location and the new hostnames are N1A (primary Administration node) and N2A (secondary Policy Service node). N1A and N2A are standalone nodes at this point in time.

### Assumptions

All Cisco ISE 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. See [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information. 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. See [“Generating a Self-Signed Certificate” section on page 8-18](#) for more information.
3. You must log in to the Cisco ISE Admin portal on N1A, choose **Administration > System > Deployment**, and do the following:
  - a. Delete the old N2 node. See [“Removing a Node from Deployment” section on page 3-19](#) for more information.
  - b. Register the new N2A node as a secondary node. See [“Registering a Secondary Cisco ISE Node” section on page 3-12](#) for more information. 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 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. See [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information.

## 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. See [“Replacing the Cisco ISE Appliance Hardware” section on page 3-20](#) for more information. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. See [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information. No role changes are required.

## Configuration Rollback

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. For example, you may delete several NADs or modify some RADIUS attributes incorrectly and realize this issue several hours later. In this case, you can revert back to the original configuration by restoring a backup that was taken before you made the changes.

### Scenario

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

### Resolution Steps

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. See [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information. The restore script will sync the data from N1 to N2.

## Recovery of Primary Node in Case of Failure in a Distributed Deployment

### Scenario

In a multinode deployment, the primary administration node fails.

For example, you have two Cisco ISE nodes, N1 (primary Administration node) and N2 (secondary Administration node). N1 fails because of hardware issues.

### Assumptions

Only the primary node in a distributed deployment has failed.

### Resolution Steps

1. Log in to the N2 Admin portal. Choose **Administration > System > Deployment** and configure N2 as your primary node. See [“Promoting Secondary Administration Node To Primary” section on page 3-17](#) for more information.

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

2. From the N2 Admin portal, register the new N1 node as a secondary node. See [“Registering a Secondary Cisco ISE Node” section on page 3-12](#) for more information.

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 Admin 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 Distributed Deployment

### Scenario

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

For example, you have multiple nodes: N1 (primary Administration node), N2 (secondary Administration node), N3 (secondary Policy Service node), N4 (secondary Policy Service node). One of the secondary nodes, N3, fails.



**Resolution Steps**

1. Reimage the new N3A node to the default standalone state.
2. Log in to the N1 Admin portal and delete the N3 node. See [“Removing a Node from Deployment” section on page 3-19](#) for more information.
3. Reregister the N3A node. See [“Registering a Secondary Cisco ISE Node” section on page 3-12](#) for more information.

Data is replicated from N1 to N3A. No restore is required.

