CHAPTER 5

Upgrading the Cisco ISE

You can upgrade the Cisco Identity Services Engine (ISE) from a previous major release or maintenance release to the latest Cisco ISE Maintenance Release 1.0.4. You can also migrate from the Cisco Secure Access Control System (ACS) 5.1 and 5.2 releases to the latest Cisco ISE Maintenance Release 1.0.4.

You cannot migrate to the latest Cisco ISE release from Cisco Secure ACS 4.x or lower versions, or from a Cisco Network Admission Control (NAC) Appliance.

For information on migrating from Cisco Secure ACS 5.1 and 5.2 releases to the latest Cisco ISE release, see the *Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4*.

Note You can migrate to the latest Cisco ISE release only from the latest ACS 5.x release. You must upgrade to the latest ACS 5.x release before you plan to migrate to the latest Cisco ISE release.

This chapter describes the following procedures:

- Upgrading the Cisco ISE Node, page 5-1
- Recovering from Upgrade Failures, page 5-8

Upgrading the Cisco ISE Node

Note There is a known issue regarding default "admin" administrator user interface access following an upgrade from the Cisco ISE Release 1.0.3.377 to Cisco ISE Maintenance Release 1.0.4.573. See the "Known Issues" section of the *Release Notes for Cisco Identity Service Engine, Release 1.1*. for details.

You can upgrade Cisco ISE from the previous release to the next release. The previous release may include patches that are already installed on it or it can be any maintenance release.

For example, you can upgrade Cisco ISE, Release 1.1 to the latest Cisco ISE maintenance release and then upgrade the maintenance release to the next future release later.

The following upgrade options are available:

- Perform an application upgrade from the CLI. For more information, see Performing an Application Upgrade from the CLI, page 5-2.
- Perform a split deployment upgrade. For more information, see Performing a Split Deployment Upgrade, page 5-4

- Replace the old Cisco ISE, Release 1.0, 1.0.4 or 1.1 appliance with a new Cisco ISE appliance that runs the latest Cisco ISE Release 1.1.1. For more information, see the Replacing the Cisco ISE Appliance Running ISE 1.1 Software with the Cisco ISE Appliance Running ISE 1.1.1, page 5-6.

Note We strongly recommend that you delay any deployment configuration changes like changing node personas, system synchronization, node registration or deregistration, and so on. until all nodes in your deployment are completely upgraded. (One exception to this recommendation, however, involves steps that are required to recover from a failed upgrade, as described in Recovering from Upgrade Failures on a Standalone Node, page 5-9.)

Note When you upgrade or restore Cisco ISE Monitoring nodes from the older versions of Cisco ISE to Cisco ISE 1.1.1, the active sessions are not retained and are reset to “0”.

Performing an Application Upgrade from the CLI

The Cisco ISE provides the option of application upgrade from the Cisco ISE, Release 1.0, 1.0.4 or 1.1 to the latest Cisco ISE Maintenance Release 1.1.1 directly from the CLI. This option allows you to install the new Cisco ISE software on the appliance and simultaneously upgrade configuration and monitoring information databases.

To perform an application upgrade, from the Cisco ISE CLI, enter:

application upgrade *application-bundle repository-name*

where

- *application-bundle* is the name of the application bundle to upgrade the Cisco ISE application
- *repository-name* is the name of the repository

For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*.

Note Before proceeding, we recommend that you review all of the following sections for information on how to perform an upgrade on different types of nodes.

You can use the **application upgrade** command from the CLI to upgrade the Cisco ISE from the previous version to the current version in the following cases:

- When upgrading the Cisco ISE on a standalone node that assumes Administration, Policy Service, and Monitoring personas.
- When upgrading the Cisco ISE on a distributed deployment.

Note Perform an on-demand backup (manually) of the Primary administration node before upgrading the Cisco ISE.

To validate the upgrade process, do one of the following:

- Check the *ade.log* file for the upgrade process.

  To download the *ade.log* file, see the “Downloading Support Bundles” section in Chapter 23 of the *Cisco Identity Services Engine User Guide, Release 1.1*.

- Run the **show version** CLI command to verify the build version.

Upgrading the Cisco ISE on a Standalone Node

You can execute the **application upgrade** command from the CLI on a standalone Cisco ISE node that assumes the Administration, Policy Service, and Monitoring personas.

To upgrade the Cisco ISE on a standalone node:

Step 1 Perform an on-demand backup (manually) of the Primary Administration ISE node from the admin user interface or CLI and an on-demand backup of the Monitoring node from the admin user interface before upgrading the Cisco ISE.

For more information on how perform an on-demand backup, see the "On-Demand Backup" section of the *Cisco Identity Services Engine User Guide, Release 1.1*.

Step 2 Launch the **application upgrade** command from the Cisco ISE CLI. This process internally upgrades the application binaries, the Database schema, and the datamodel module. It also handles upgrading any Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS) updates.

If a system reload is required to complete the upgrade process, the Cisco ISE node is restarted automatically following a successful upgrade.

The CLI transcript for a successful upgrade on a standalone node should look like the following:

```
ise-vm29/admin# application upgrade ise-appbundle-1.1.0.xxx.i386.tar.gz disk
Save the current ADE-OS running configuration? (yes/no) [yes]?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
################################################################
NOTICE: ISE upgrade requires you to change the database
administrator and database user password. You will be
prompted to change these passwords after the system reboots.
################################################################
Stopping ISE application before upgrade...
Running ISE Database upgrade...
Upgrading ISE Database schema...
ISE Database schema upgrade completed.
Running ISE Global data upgrade as this node is a STANDALONE...
Running ISE data upgrade for node specific data...

This application Install or Upgrade requires reboot, rebooting now...
```

Step 3 After you upgrade from Cisco ISE Release 1.0.3.377 or Cisco ISE Maintenance Release 1.0.4.573 to Cisco ISE Release 1.1, you may be unable to use the SFTP repository until you accept the host key by using the **host-key host <sftpservername>** command. See the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on the usage of the command.

Step 4 When the reboot process completes, you are prompted to log in with your login credentials and are asked immediately to provide new Cisco ISE internal database administrator and user passwords. (This part of the process is only successful if the user account that you are using to log in has administrator-level access privileges.)

```
login: admin
password:
% NOTICE: ISE upgrade requires you to change the database administrator and user
passwords, before you can start the application.
Enter new database admin password:
Confirm new database admin password:
```

```
Enter new database user password:
Confirm new database user password:
Starting database to update password...

Starting database to update password...
ISE Database processes already running, PID: 3323
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.
```

If there is any failure during an upgrade of application binaries and the Cisco ADE-OS, you can only remove and reinstall the previous version of the application bundle and restore the backup.

See Recovering from Upgrade Failures on a Standalone Node, page 5-9 for details on how to recover from upgrade failures.

Note After you upgrade from Cisco ISE Release 1.0.3.377, Cisco ISE Maintenance Release 1.0.4.573 or Cisco ISE Release 1.1 to Cisco ISE Release 1.1.1, the scheduled backup jobs need to be recreated because the older jobs will not work properly.

Performing a Split Deployment Upgrade

To upgrade the Cisco ISE nodes in a distributed deployment to Release 1.1.1, you must use the split deployment upgrade method.

The configuration changes that are made to the Primary Administration ISE node database are applied to the secondary Administration ISE node, the Inline Posture node, and all the secondary nodes in your deployment. This allows you to replicate the database on all the nodes from the Primary Administration ISE node so that each node has a local copy of the configuration. Replication of configuration data across all nodes may introduce complications in terms of functionality changes that are implemented within the latest version and the required configuration.

For more information on centralized configuration and management of Cisco ISE nodes in a distributed deployment, see *Cisco Identity Services Engine User Guide, Release 1.1,* Chapter 10, “Setting Up ISE in a Distributed Environment”.

Note When you upgrade a complete Cisco ISE deployment, Domain Name System (DNS) server resolution is mandatory; otherwise the upgrade will fail.

Note During the split deployment upgrade, before you register the nodes to the new primary Administration node, you must do the following:

- If you use self-signed certificate, you must import the self-signed certificate of all nodes to your new primary Administration node.
- If you use different CA certificates for the nodes, you must import all the CA certificates into the new primary Administration node.
- If you use the same CA certificate for the nodes, you must import that CA certificate into the new primary Administration node.

Assuming that you have a Primary Administration ISE node, a secondary Administration ISE node, an Inline Posture node, and a few Policy Service nodes in your Cisco ISE deployment, the Cisco ISE can be upgraded by using the split deployment upgrade methodology to overcome deployment issues. You can create a new deployment of the version that you intend to upgrade within your Cisco ISE deployment by splitting your deployment.

First, move the secondary Administration ISE node to the new deployment and then move all the Policy Service nodes to the new deployment in a phased manner. After you upgrade all the Policy Service nodes to the new deployment, your Cisco ISE deployment is complete.

When upgrading a complete Cisco ISE deployment to the next release, you create a new deployment that is based on the version to which you want the Cisco ISE to be upgraded and migrate all the nodes to the new deployment.

Split deployment upgrade happens in two phases:

- Upgrading the Secondary Administration ISE Node to a New Deployment, page 5-5
- Upgrading the Policy Service Nodes to the New Deployment, page 5-6

Upgrading the Secondary Administration ISE Node to a New Deployment

Note Before you upgrade any node in a deployment, you must obtain an on-demand backup of the primary Administration ISE node and the Monitoring node. You must also record the Inline Policy Enforcement Point (IPEP) node configuration before the upgrade so that you can reconfigure the IPEP node after the upgrade.

When upgrading to a higher release, you should initially upgrade only the secondary Administration ISE node to the higher version.

For example, if you have a deployment setup with one primary Administration node (Node A), one secondary Administration node (Node B), one IPEP node (Node C), and two PDPs (Node D and Node E), you can proceed with the upgrade procedure as follows:

Step 1 Deregister the secondary node (Node B) from the deployment setup. After deregistration, it becomes a standalone node. Upgrade this standalone node to Cisco ISE Release 1.1.1.

Step 2 Deregister the PDP node (Node D) from the deployment setup. After deregistration, it becomes a standalone node. Upgrade this standalone node to Cisco ISE Release 1.1.1.

Step 3 Promote Node B as the primary node in the new deployment and register Node D as the PDP node.

Step 4 Deregister the PDP node (Node D) from the deployment setup. After deregistration, it becomes a standalone node. Upgrade this standalone node to Cisco ISE Release 1.1.1.

Step 5 Deregister the IPEP node (Node C) from the deployment setup and make it as a standalone node. Upgrade this IPEP node to Cisco ISE Release 1.1.1.

Note The upgrade process removes the IPEP node's configuration. You must reconfigure the IPEP node after the upgrade.

Step 6 Deregister the second PDP node (Node E) from the deployment and upgrade it to Cisco ISE Release 1.1.1. Register to Node B as the PDP node.

Step 7 Convert earlier deployment's primary node (Node A) to a standalone node. Upgrade Node A to Cisco ISE Release 1.1.1 and register to Node B in the the Cisco ISE Release 1.1.1 deployment setup as the secondary node.

Step 8 Exchange the IPEP node certificates with the new primary Administration node (Node B) certificates. Similarly, exchange the IPEP node certificates with the new secondary Administration node (Node A) certificates.

Note Certificates from both the primary and secondary Administration nodes should be installed on each IPEP node to trust the management interface certificate. For more details on certificate provisioning, see "Deploying an Inline Posture Node" section in the *Cisco Identity Services Engine User Guide, Release 1.1*.

Step 9 Register the IPEP node (Node C) to the new deployment setup; that is, to Node B.

Upgrading the Policy Service Nodes to the New Deployment

Any configuration that is applied to the primary Administration ISE node in the previous deployment should also be applied to the secondary Administration ISE node in the new deployment. This allows you to replicate the Policy Service nodes from the secondary Administration ISE node in the new deployment, and these nodes can operate on the new deployment.

You must apply the configuration changes to the upgraded deployment version that are currently applied in the previous version. The changes in the configuration that are applied to the upgraded version need not be applied back to the previous version.

Replacing the Cisco ISE Appliance Running ISE 1.1 Software with the Cisco ISE Appliance Running ISE 1.1.1

Note If you want to replace a Cisco ISE appliance that runs Cisco Identity Services Engine Maintenance Release 1.0.4.558 with a new Cisco ISE that runs Cisco Identity Services Engine Maintenance Release 1.0.4.573, you must upgrade the appliance that runs version 1.0.4.558 to 1.0.4.573 before creating a database backup image, which you can then restore on the new appliance that runs version 1.0.4.573.

Note When you restore data from the backup of a previous version, any existing configuration, regardless of old or new features, will be cleared after the restore.

This section contains the following:

Replacing the Cisco ISE Standalone Appliance Running ISE 1.1 Software with the Cisco ISE Appliance Running Cisco ISE, Release 1.1.1

This upgrade scenario is required only if you are upgrading your Cisco ISE, Release 1.0, Cisco ISE Maintenance Release 1.0.4 or the Cisco ISE, Release 1.1 software to the Cisco ISE, Release 1.1.1 at the same time as you are replacing your existing Cisco ISE chassis.

If you are using the same physical appliance or a virtual machine, we recommend that you use Performing an Application Upgrade from the CLI, instead of backup restore.

To replace a Cisco ISE standalone appliance that runs the Cisco ISE 1.1 software with Cisco ISE appliance that runs the Cisco ISE Release 1.1.1, complete the following steps:

Step 1 Back up the Cisco ISE 1.1 appliance.

Step 2 Start up and configure the new Cisco ISE 1.1.1 appliance.

Step 3 Restore the Cisco ISE 1.1 backup.

For more information on how to perform a backup and restore, see *Cisco Identity Services Engine User Guide, Release 1.1,* Chapter 14 “Backing Up and Restoring Cisco ISE Data”.

After you restore data, you must wait until all the application server processes are up and running.

To verify that the Cisco ISE application server processes are running, enter the following command from the Cisco ISE CLI:

show application status ise

For more information on the CLI commands, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*.

Replacing a Subset of Existing Cisco ISE Nodes with Cisco ISE Appliances Running Release 1.1 in a Distributed Deployment

To replace a subset of the Cisco ISE 1.1 nodes with the Cisco ISE appliances that runs 1.1.1 in a distributed deployment, complete the following steps:

Step 1 Perform an application upgrade to the Cisco ISE 1.1 on each node in the existing deployment. See Performing an Application Upgrade from the CLI, page 5-2.

Step 2 Deregister and register the new Cisco ISE 1.1.1 appliances into the deployment.

In this case, the primary Administration ISE node remains on the original hardware. You can promote one of the newer Cisco ISE 1.1.1 appliances to be the new primary Administration ISE node.

Replacing All the Cisco ISE Appliances Running the ISE 1.1 Software with the Cisco ISE Appliances Running Cisco ISE 1.1.1 in a Distributed Deployment

To replace all Cisco ISE appliances that runs Cisco ISE, Release 1..1 of Cisco ISE Maintenance Release 1.0.4 software with Cisco ISE appliances that runs Cisco ISE, Release 1.1.1 in a distributed deployment, complete the following steps:

Step 1 Perform an application upgrade to the Cisco ISE 1.1.1 on each node in the existing deployment. See Performing an Application Upgrade from the CLI, page 5-2.

Step 2 Deregister a secondary appliance and register to the first Cisco ISE 1.1.1 appliance.

Step 3 Repeat Step 2 for the remaining secondary nodes that you want to move from the Cisco ISE 1.0 hardware deployment to the Cisco ISE 1.1.1 hardware deployment.

Step 4 Promote one of the new Cisco ISE 1.1.1 appliances to be the new primary Administration ISE node.

Step 5 Deregister the last Cisco ISE 1.0 appliance and register it to the last Cisco ISE 1.1.1 appliance in the deployment.

Recovering from Upgrade Failures

This section contains:

Recovering from Upgrade Failures on a Standalone Node

Before attempting any rollback or recovery on the node where an upgrade has failed, you must generate an application bundle by using the **backup-logs** CLI command and place it in a remote repository.

Scenario 1: Upgrade failed during database schema or datamodel upgrade

Detection: One of the following messages is shown in the console and ADE.log:

- ISE Database schema upgrade failed!
- ISE Global data upgrade failed!
- ISE data upgrade for node specific data failed!

How to Roll back: Restore from the last backup to roll back.

How to retry the upgrade:

- Analyze the logs.
- To identify and resolve the problem, submit the application bundle that you generated to the Cisco Technical Assistance Center (TAC).
- You need a new application bundle each time you retry an upgrade.

Scenario 2: Upgrade failed during binary install

Detection: An application binary upgrade occurs after the database upgrade. If a binary upgrade failure happens, the following message displays in the console and ADE.log:

% Application install/upgrade failed with system removing the corrupted install

How to Roll back: Reimage the Cisco ISE Appliance by using the previous ISO image and restore from the backup.

How to retry the upgrade:

- Analyze the logs.
- To identify and resolve the problem, submit the application bundle that you generated to the Cisco Technical Assistance Center (TAC).

You need a new application bundle each time you retry an upgrade.

Recovering the Appliance if SSH Session Quit During Upgrade

Detection: The SSH session or console was disconnected or quit during an upgrade.

How to Rollback: Reimage the Cisco ISE Appliance by using the previous ISO image and restore from the backup.

How to retry the upgrade: Continue with the upgrade again. If your appliance is used as a secondary node in the new Cisco ISE version 1.1.1, directly install the new ISO version and register it to the new primary Administration ISE node.