Preface

Revised: May 2017, OL-27087-01

This preface provides the following information about the Cisco Identity Services Engine (ISE) 3300 Series appliance:

Overview of Cisco Identity Services Engine

Cisco Identity Services Engine (ISE), as a next-generation identity and access control policy platform enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE's unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices in order to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches.

Cisco ISE is a key component of the Cisco Security Group Access Solution. Cisco ISE is a consolidated policy-based access control solution that:

- Combines authentication, authorization, accounting (AAA), posture, profiler, and guest management services into one appliance
- Enforces endpoint compliance by checking the device posture of all endpoints accessing the network, including 802.1X environments
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments allowing services to be delivered where they are needed

- Employs advanced enforcement capabilities including Security Group Access (SGA) through the use of Security Group Tags (SGTs) and Security Group (SG) Access Control Lists (ACLs)
- Supports scalability to support a number of deployment scenarios from small office to large enterprise environments

The Cisco ISE software comes preinstalled on a range of physical appliances with various performance characterizations. The inherent scalability of Cisco ISE allows you to add appliances to a deployment and increase performance and resiliency, as needed. The Cisco ISE architecture supports standalone and distributed deployments, along with high-availability options. Cisco ISE allows you to configure and manage your network from a centralized portal for efficiency and ease of use.

Cisco ISE also incorporates distinct configurable roles and services, so that you can create and apply Cisco ISE services where they are needed in the network. The result being a comprehensive Cisco ISE deployment that operates as an fully functional and integrated system.

This current maintenance release, Cisco ISE Release 1.1.4, provides support for Cisco SNS-3400 Series appliances. In addition to the Cisco SNS appliances, Cisco ISE 1.1.4 also supports all the platforms and features that are supported in the ISE Release 1.1.3.

Purpose

This document describes how to upgrade a Cisco Identity Services Engine software image on Cisco ISE Series appliances and VMware virtual machines.

You can upgrade the Cisco Identity Services Engine (ISE) from a previous major release or maintenance release to the latest Cisco ISE Maintenance Release 1.1.x. You can also migrate from the Cisco Secure Access Control System (ACS) Releases 5.1 and 5.2 to the latest Cisco ISE Maintenance Release 1.1.x.

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, Releases 5.1 and 5.2 to the latest Cisco ISE release, see the *Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x*.

Note You can migrate to the latest Cisco ISE release only from Cisco Secure ACS 5.1 and 5.2 releases. You must upgrade to Cisco Secure ACS 5.1 or 5.2 release before you plan to migrate to the latest Cisco ISE release.

Audience

This guide is designed for network administrators, system integrators, and network deployment personnel who upgrade and configure the Cisco ISE software on Cisco ISE 3300 Series appliances, Cisco SNS-3400 Series appliances, or on the VMware servers. As a prerequisite to using this upgrade guide, you should be familiar with networking equipment and cabling and have a basic knowledge of electronic circuitry, wiring practices, and equipment rack installations.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Document Organization

Table 1 lists the organization of the *Cisco ISE Upgrade Guide, Release 1.1.x*.

Table 1 Cisco ISE Upgrade Guide Organization

Chapter/Appendix and Title	Description
Chapter 1, "Upgrading Cisco ISE"	Describes how to upgrade Cisco ISE from any previous release.
Chapter 2, "Upgrading a Standalone Node"	Describes how to upgrade a Cisco ISE standalone node.
Chapter 3, "Upgrading a Two-Admin Node Deployment"	Describes how to upgrade a Cisco ISE Two-node deployment.
Chapter 4, "Upgrading Distributed Deployment"	Describes how to upgrade Cisco ISE in a distributed deployment.
Chapter 5, "Recovering from Upgrade Failures"	Describes the procedures of how to recover from upgrade failures.

Document Conventions

This guide uses the following conventions to convey instructions and information.

Item	Convention
Commands, keywords, special terminology, and options that should be chosen during procedures	**boldface** font
Variables for which you supply values and new or important terminology	*italic* font
Displayed session and system information, paths, and file names	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Indicates menu items to choose, in the order in which you choose them.	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material that is not covered in this guide

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Release-Specific Documents

Table 2 lists the product documentation available for the Cisco ISE Release. General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Table 2 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco Identity Services Engine User Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Upgrade Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

- Cisco ISE
  http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html

- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

Documentation Updates

Table 3 lists the documentation updates for this Cisco ISE product release.

Table 3 Updates for Cisco Identity Services Engine Upgrade Guide, Release 1.1.x

Date	Description
11/20/2013	Resolved CSCud32400
4/25/13	Cisco Identity Services Engine, Release 1.1.4
2/28/13	Cisco Identity Services Engine, Release 1.1.3
10/31/12	Cisco Identity Services Engine, Release 1.1.2
7/10/12	Cisco Identity Services Engine, Release 1.1.1
9/20/12	Updated the upgrade procedure for two-node and distributed deployments based on CSCub56366.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

CHAPTER 1

Upgrading Cisco ISE

You can upgrade Cisco ISE from any previous release to the next release. The previous release might have patches installed on it or it can be any maintenance release.

If you are upgrading from any one of the Cisco ISE 1.0.x releases, you must follow the instructions listed in the "Obtaining a Valid License" section on page 1-2.

If you are currently running Cisco ISE, Release 1.0.4, then you must apply Cisco ISE 1.0.4 patch 5 before you upgrade to Cisco ISE, Release 1.1.x. Cisco ISE 1.0.4 patch 5 can be applied directly on Cisco ISE, Release 1.0.4 or any previously patched version thereof. Applying this patch ensures that your secondary Cisco Administration ISE node's license is not lost during the upgrade process.

Ensure that you do not delete system default sponsor groups and sponsor group policies when you upgrade Cisco ISE, Release 1.0.4.573 to higher versions of Cisco ISE, Releases (for example, Cisco ISE, Release 1.1, 1.1.x and 1.2) and restore from the Cisco ISE, Release 1.0.4.573 backup in higher versions of Cisco ISE.

If you are currently running Cisco ISE, Release 1.1, then you must apply Cisco ISE 1.1 patch 3 before you upgrade to Cisco ISE, Release 1.1.x. Cisco ISE 1.1 patch 3 can be applied directly on Cisco ISE, Release 1.1 or any previously patched version thereof. Applying this patch ensures that your secondary Cisco Administration ISE node's license is not lost during the upgrade process.

This chapter contains the following sections:

Note When you upgrade to Cisco ISE, Release 1.1.x, you may be required to open some network ports you may not have been using in previous releases of Cisco ISE. Ensure you consult the table of required ports to open in Cisco ISE in the "Cisco ISE 3300 Series Appliance Ports Reference" appendix of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

Before You Begin

Before you upgrade your deployment, you must do the following:

- If you are upgrading from Release 1.0, follow the instructions listed in "Obtaining a Valid License" section on page 1-2.
- If you are running Cisco ISE, Release 1.1, then you must apply ISE 1.1 patch 3 before you can upgrade to Cisco ISE, Release 1.1.x. Applying this patch ensures that your secondary Cisco Administration ISE node's license is not lost during the upgrade process.
- If you are performing a split deployment upgrade and you have a secondary Cisco ISE Administration node in your deployment, you must have a valid license for the secondary Cisco ISE Administration node (ISE Node B) based on its UDI.

  If your secondary Admin node has been operational for more than 90 days, its license will be lost after it has been deregistered. In this case, you must obtain a valid license for the secondary Cisco ISE Administration node (ISE Node B) based on its UDI: Serial Number, Version ID, and Product ID. See Obtaining a Valid License, page 1-2 for more information.

  You cannot preinstall or install a license on the secondary Cisco ISE Administration node at runtime. You can install the license only after the node has been promoted to become the primary Cisco ISE Administration node. All licenses are applied on the primary Administration ISE node only.
- Obtain a backup of Cisco ISE configuration data and Cisco ADE operating system data. See Performing an On-Demand Backup, page 1-3 for more information.

This section contains the following topics:

Obtaining a Valid License

You can request a license from the Cisco Global Licensing Organization (GLO). GLO is staffed 24x7x365 and you can contact them when you are unable to perform the licensing activity online at:

https://tools.cisco.com/SWIFT/LicensingUI/Home

If you have issues in obtaining the license, you can open a case with GLO in any one of the following three ways:

- The online portal at http://cisco.com/tac/caseopen. After you select the technology and subtechnology, ensure that you select *Licensing* from the Type of Problem list box. This option is the preferred and most efficient method for you to open severity 3 service requests.
- Call 800-553-2447 (in the US and Canada). Use the following link for global numbers:

  http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html. This option should be used for urgent situations such as a network downtime or severe degradation to reach someone quickly.
- E-mail GLO at licensing@cisco.com. You must include the UDI of the secondary Admin node in the case to request a new license. You can obtain the UDI by entering the following command:

  psn1/admin# show udi

  You must also include the sales order number and if available, the PAK number of the original license.

Performing an On-Demand Backup

You can perform an on-demand backup of the Cisco ISE configuration data and Cisco ADE operating system data. You can do the backup in the following two ways:

- Backup from the Cisco ISE UI, page 1-3
- Backup from the Cisco ISE CLI, page 1-4

Backup from the Cisco ISE UI

Cisco ISE user interface (UI) provides an option to obtain an on-demand backup of the primary administration node. You can obtain a backup of the Cisco ISE application-specific configuration data, or application and Cisco ADE operating system data.

Prerequisites:

1. Before you perform this task, you should have a basic understanding of the Backup and Restore operations in Cisco ISE.
2. Ensure that you have configured repositories. See the "Configuring Repositories" section in the *Cisco Identity Services Engine User Guide, Release 1.1.x*, for more information.
3. Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See "Cisco ISE Admin Group Roles and Responsibilities" section in the *Cisco Identity Services Engine User Guide, Release 1.1.x*, for more information on the various administrative roles and the privileges associated with each of them.

Note For backup and restore operations, you cannot choose the CDROM, HTTP, or HTTPS options because these are read-only repositories.

To perform an on-demand backup, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 From the Operations navigation pane on the left, choose **Data Management > Administration Node > Full Backup On Demand**.

The Backup On Demand page appears.

Step 3 Enter the name of your backup file.

Step 4 Select the repository where your backup file should be saved.

You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.

Step 5 Check the **Application-Only Backup, Excludes OS System Data** check box to obtain a Cisco ISE application data backup. Uncheck this check box if you want the Cisco ADE operating system data as well.

Step 6 Enter the **Encryption Key**. This key is used to encrypt and decrypt the backup file.

Step 7 Click **Backup Now** to run your backup.

Note 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 backup is running concurrently. Wait for the backup to complete before you make any node role changes.

Step 8 Your page is refreshed and the following message appears in the lower right corner of the page, if you are viewing the Backup On Demand page:

Backup is done successfully.

If you have moved to other pages in the Cisco ISE user interface, to check the status of your backup, you must go to the Backup History page. See the "Viewing Backup History" for more information.

Cisco ISE appends the backup filename with the timestamp and stores this file in the specified repository. Check if your backup file exists in the repository that you have specified.

Backup from the Cisco ISE CLI

To perform a backup from the Cisco ISE CLI (including the Cisco ISE and Cisco ADE OS data) and place the backup in a repository, use the **backup** command in the EXEC mode. To perform a backup of only the Cisco ISE application data without the Cisco ADE OS data, use the **application** command.

Note Before attempting to use this **backup** command in the EXEC mode, you must copy the running configuration to a safe location, such as a network server, or save it as the Cisco ISE server startup configuration. You can use this startup configuration when you restore or troubleshoot your Cisco ISE application from the backup and system logs. For more information of copying the running configuration to the startup configuration, see the "copy" command in the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*.

backup *backup-name* **repository** *repository-name* **application** *application-name* **encryption-key hash |plain** *encryption-key name*

The below table provides the syntax description:

backup	The command to perform a backup the Cisco ISE and Cisco ADE OS and place the backup in a repository.
backup-name	Name of backup file. Supports up to 100 alphanumeric characters.
repository	Repository command.
repository-name	Location where the files should be backed up to. Supports up to 80 alphanumeric characters.
application	Application command (application-only backup, excludes the Cisco ADE OS system data).
application-name	Application name. Supports up to 255 alphanumeric characters.
encryption-key	Specifies user-defined encryption key to protect the backup.
hash	Hashed encryption key for protection of backup. Specifies an *encrypted* (hashed) encryption key that follows. Supports up to 40 characters.

plain	Plaintext encryption key for protection of backup. Specifies an *unencrypted* plaintext encryption key that follows. Supports up to 15 characters.
encryption-key name	Specifies encryption key in hash | plain format for backup.

This command performs a backup of the Cisco ISE and Cisco ADE OS data and places the backup in a repository with an encrypted (hashed) or unencrypted plaintext password.

You can encrypt and decrypt the backups by using user-defined encryption keys.

Example 1

```
ise/admin# backup mybackup repository myrepository encryption-key plain Lab12345
% Creating backup with timestamped filename: backup-111125-1252.tar.gpg
ise/admin#
```

Example 2

```
ise/admin# backup mybackup repository myrepository application ise encryption-key plain
Lab12345
% Creating backup with timestamped filename: backup-111125-1235.tar.gpg
ise/admin#
```

Performing an Application Upgrade from the CLI

The Cisco ISE provides the option of application upgrade from the Cisco ISE, Release 1.0.4 patch 5, or 1.1 patch 3 to the latest Cisco ISE Maintenance Release 1.1.x 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

See the "Upgrading the Cisco ISE Standalone Node" section on page 2-1 for more information on how the CLI transcript for a successful upgrade on a standalone node would look like.

Note If your repository is an SFTP location, the upgrade may take significantly longer time. For a secure upgrade, we recommend you to use HTTPS or CD/DVD as a repository.

Note Before proceeding, we recommend that you review all of the chapter in this document 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. See Chapter 2, "Upgrading a Standalone Node."
- When upgrading the Cisco ISE on a two-node deployment. See Chapter 3, "Upgrading a Two-Admin Node Deployment."
- When upgrading the Cisco ISE on a distributed deployment. See Chapter 4, "Upgrading Distributed Deployment."

Note Perform an on-demand backup (manually) of the Primary administration node before upgrading the Cisco ISE. See Performing an On-Demand Backup, page 1-3.

Note We strongly recommend that you delay any deployment configuration changes such as changing node personas, system synchronization, node registration or deregistration (required for split deployment upgrade), 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 5-1.)

Note When you upgrade or restore Cisco ISE Monitoring nodes from the older versions of Cisco ISE to Cisco ISE 1.1.x, the active sessions are not retained and are reset to "0".

Validating the Upgrade Process

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

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

  To view the *ade.log* file, issue the following command from the CLI:

  ```
  show logging system
  ```

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

Known Upgrade Issues

This section covers the following upgrade issues:

- Upgrade from Cisco ISE 1.0.4 to 1.1.x with Inline Posture, page 1-7
- Upgrade from Cisco ISE Release 1.0.3.377, page 1-8

Upgrade from Cisco ISE 1.0.4 to 1.1.x with Inline Posture

In Cisco ISE, Release 1.1.x, the Inline Posture node uses certificate based authentication and cannot connect to the Administrative ISE node. Therefore you are required to disconnect the Inline Posture node from the deployment prior to starting the upgrade procedure, then reconfigure the Inline Posture node after the upgrade. To do so, follow the procedure outlined in this section.

Warning **You must have the proper certificates in place for your Inline Posture deployment to mutually authenticate.**

Prerequisite

- If you are currently running Cisco ISE, Release 1.0.4, then you must apply Cisco ISE 1.0.4 patch 5 before you upgrade to Cisco ISE, Release 1.1.x. Cisco ISE 1.0.4 patch 5 can be applied directly on Cisco ISE, Release 1.0.4 or any previously patched version thereof. Applying this patch ensures that your secondary Cisco Administration ISE node's license is not lost during the upgrade process.
- Record all the configuration data for your Inline Posture node *before* you de-register the node. Alternatively, you can save screenshots of each of the Inline Posture tabs (in the Admin user interface) to record the data. Having this data on hand speeds up the process of re-registering the Inline Posture node to complete the following task.

To upgrade to Cisco ISE 1.1.x with Inline Posture, complete the following steps:

Step 1 From the Cisco Administration ISE node, de-register the Cisco Inline Posture node.

Note You can verify that the Inline Posture node has returned to ISE node status by going to the CLI and entering the following command: **show application status ise** If you discover that the node has not reverted to an ISE node, then you can enter the following at the command prompt: **pep switch outof-pep** However, it is recommended that you only do this as a last resort.

Step 2 Upgrade the Cisco Administration ISE node to 1.1.x, as described in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

Step 3 Import CA root certificate, generate CSR, create certificates on the Administration ISE node.

Note Certificates must have extended key usage for both client authentication and server authentication. For an example of this type of extended key usage, see the Microsoft CA Computer template.

Step 4 Perform a fresh installation of ISE 1.1.x on the ISE node (that was the former Inline Posture node), as described in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x*.

Step 5 Import CA root certificate, generate CSR, create certificates on the ISE node (that was the former Inline Posture node), now in standalone mode.

Note Certificates must have extended key usage; client authentication and server authentication. For example, select the computer template from Microsoft CA.

Step 6 Register the newly upgraded ISE Node as an Inline Posture node.

Step 7 Reconfigure the Cisco Inline Posture node.

Upgrade from Cisco ISE Release 1.0.3.377

There is a known issue regarding default "admin" administrator user interface access following upgrade from Cisco Identity Services Engine Release version 1.0.3.377. This issue can affect Cisco ISE customers who have not changed their default "admin" account password for administrator user interface login since first installing Cisco Identity Services Engine Release 1.0.3.377.

Upon upgrading, administrators can be "locked out" of the Cisco ISE administrator user interface when logging in via the default "admin" account where the password has not yet been updated from the original default value.

To avoid this issue, Cisco recommends you do one or more of the following:

1. Verify they have changed password per the instructions in the "Managing Identities" chapter of the *Cisco Identity Services Engine User Guide, Release 1.1.x prior* to upgrade.
2. Disable or modify the password lifetime setting in the **Administration > System > Admin Access > Password Policy** page of the administrator user interface *prior* to upgrade to ensure the upgraded policy behavior does not impact the default "admin" account.
3. Enable password lifetime setting reminders in the **Administration > System > Admin Access > Password Policy** page to alert admin users of imminent expiry. Administrators should change the password when notified.

Note Although the above conditions apply to all administrator accounts, the change in behavior from Cisco ISE version 1.0.3.377 only impacts the default "admin" account.

CHAPTER 2

Upgrading a Standalone Node

This chapter describes the following procedures:

Upgrading the Cisco ISE 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 standalone 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 "Performing an On-Demand Backup" section on page 1-3.

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-1.1.1.xxx.i386.tar.gz myrepository
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.x, 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.x* for more information on the usage of the command.

Note 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.x, the scheduled backup jobs need to be recreated, as the older jobs will not work properly.

Note The following Step 4 is applicable only if you are performing an upgrade from the Cisco ISE Release 1.0.3.377 to any future release. You may ignore this step otherwise.

Step 4 After 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 5-1 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.x, the scheduled backup jobs need to be recreated because the older jobs will not work properly.

Replacing Cisco ISE Standalone Appliance Running a Previous Version with an Appliance Running 1.1.4

This upgrade scenario is required only if you are upgrading your Cisco ISE Maintenance Release 1.1.1, 1.1.2, or 1.1.3 software to the Cisco ISE, Release 1.1.4 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.x (not Cisco ISE 1.1.4) software with Cisco ISE appliance that runs the Cisco ISE Release 1.1.4, complete the following steps:

Step 1 Back up the Cisco ISE 1.1.x appliance.

Note Cisco ISE 1.1.x appliance implies an appliance that is currently running Cisco ISE Release 1.1.1, or 1.1.2, or 1.1.3.

Step 2 Start up and configure the new Cisco ISE 1.1.x appliance.

Step 3 Restore the Cisco ISE 1.1.x backup.

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.

For more information on how to perform a backup and restore, see *Cisco Identity Services Engine User Guide, Release 1.1.x,* 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 1.1.x*.

Replacing an ISE Appliance Running a Previous Version with a Cisco SNS-3400 Appliance

This upgrade scenario is required only if you are upgrading your Cisco ISE Maintenance Release 1.1.1, or 1.1.2, or 1.1.3 to the Cisco ISE, Release 1.1.4 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.x (not Cisco ISE 1.1.4) software with a Cisco SNS-3400 appliance, complete the following steps:

Step 1 Upgrade the Cisco standalone node running Cisco ISE 1.1.x to Cisco ISE 1.1.4.

For more information on upgrading the Cisco Standalone node running ISE 1.1.x to Cisco ISE 1.1.4, see Upgrading the Cisco ISE Standalone Node, page 2-1.

Step 2 Back up the upgraded Cisco ISE appliance.

Step 3 Replace the existing Cisco ISE appliance with an SNS appliance by performing a fresh install.

For more information on performing a fresh install of the SNS appliance, refer to the following section in the Cisco ISE 1.1.4 Installation Guide:
http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_app_b-hw_ins_3400.html.

Step 4 Start up and configure the new SNS appliance.

For more information on configuring the new SNS appliance, refer to the following chapter in the Cisco ISE 1.1.4 Installation Guide:
http://www.cisco.com/en/US/docs/security/ise/1.1.1/installation_guide/ise_ins.html.

Step 5 Restore the Cisco ISE 1.1.4 backup onto the new SNS appliance.

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.

For more information on how to perform a backup and restore, see *Cisco Identity Services Engine User Guide, Release 1.1.x,* 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 1.1.x*.

CHAPTER 3

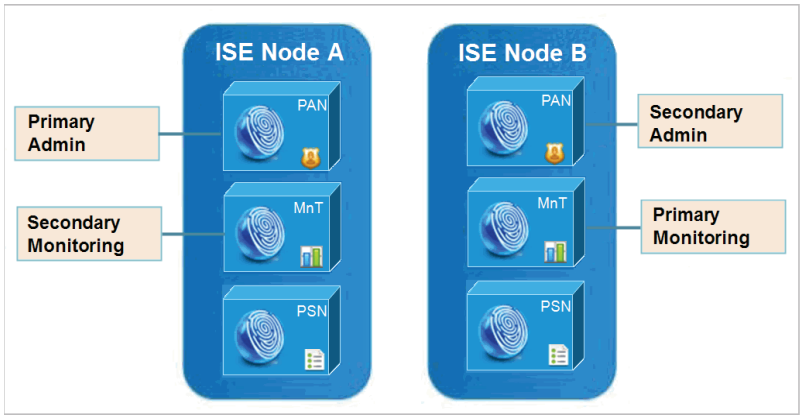
Upgrading a Two-Admin Node Deployment

Performing a Two-Admin Node Deployment 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 set up as shown in Figure 3-1, with one primary Administration node (Node A) and one secondary Administration node (Node B), you can proceed with the following upgrade procedure.

Figure 3-1 Cisco ISE, Release 1.1 Two-Node Administrative Deployment



This supports an upgrade of Cisco ISE, Release 1.0 or 1.1 to Cisco ISE, Release 1.1.x with split domain upgrade only, so that the secondary ISE node has to be deregistered individually from the deployment before upgrade.

Warning **This warning is not applicable if you are upgrading from Cisco ISE, Release 1.1 patch 3.**

If your secondary Admin node has been operational for more than 90 days, its license will be lost after it has been deregistered. In this case, you must obtain a valid license for the secondary Cisco ISE Administration node (ISE Node B) based on its UDI: Serial Number, Version ID, and Product ID. See "Obtaining a Valid License" section on page 1-2 for more information.

To perform a two-adminnode deployment upgrade, complete the following procedure:

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 to Cisco ISE, Release 1.1.x.

For more information on how perform an on-demand backup, see the "Performing an On-Demand Backup" section on page 1-3.

Step 2 Deregister the secondary node (Node B) from the deployment setup. After deregistration, this node becomes a standalone node.

Step 3 Upgrade this standalone node to Cisco ISE, Release 1.1.x.

When you log in to Node B after the upgrade, if the system prompts you for a license, you must install a valid license for the secondary node based on its UDI. See Obtaining a Valid License, page 1-2 for more information.

Step 4 Convert the primary node of the previous deployment (Node A) to a standalone node.

Step 5 Make Node B as the primary node in the new deployment.

Step 6 Upgrade Node A to Cisco ISE, Release 1.1.x and register to Node B in the Cisco ISE, Release 1.1.x deployment setup as the secondary node.

After you upgrade your deployment, all the policies and other data of the previous deployment will be retained in your new deployment.

CHAPTER 4

Upgrading Distributed Deployment

This chapter contains the following topics:

Performing a Split Deployment Upgrade

To upgrade the Cisco ISE nodes in a distributed deployment to Release 1.1.x, 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.x,* 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.

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 you migrate all the nodes to the new deployment.

Split deployment upgrade happens in two phases:

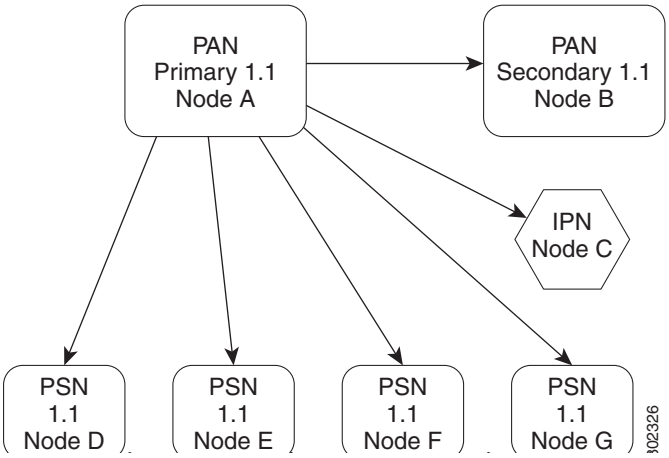
1. Upgrade the Cisco ISE Administration nodes in the distributed deployment
2. Upgrade and register the Policy Service nodes and Inline Posture nodes to the new deployment

Upgrading Cisco ISE Nodes in a Distributed Deployment

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 set up as shown in Figure 4-1, with one primary Administration node (Node A), one secondary Administration node (Node B), one Inline Posture node (IPN) (Node C), and four Policy Service nodes (PSNs) (Node D, Node E, Node F, and Node G), you can proceed with the following upgrade procedure.

Figure 4-1 Cisco ISE, Release 1.1 Administrative Deployment



Cisco ISE supports only a split deployment upgrade from a previous release to Cisco ISE, Release 1.1.x. Secondary ISE nodes and Inline Posture nodes have to be deregistered individually from the deployment before upgrade.

Warning **If your secondary Admin node and the PSN node have been operational for more than 90 days, the licenses of these nodes will be lost after they have been deregistered. In this case, you must obtain valid licenses for the secondary Cisco ISE Administration node (ISE Node B) and the PSN node (ISE Node D) based on their UDIs: Serial Numbers, Version IDs, and Product IDs. See "Obtaining a Valid License" section on page 1-2 for more information. This warning is not applicable if you are upgrading to Cisco ISE, Release 1.1.x from Cisco ISE, Release 1.1 patch 3.**

Prerequisite:

- Make sure you have the license file for your Primary Administration ISE node before beginning the upgrade process. If you do not have the file on hand (if your license was installed by a Cisco partner vendor, for example) contact Cisco TAC for assistance.

- Ensure that you have a copy of the license that you install initially. You need to reinstall the license while completing the upgrade.

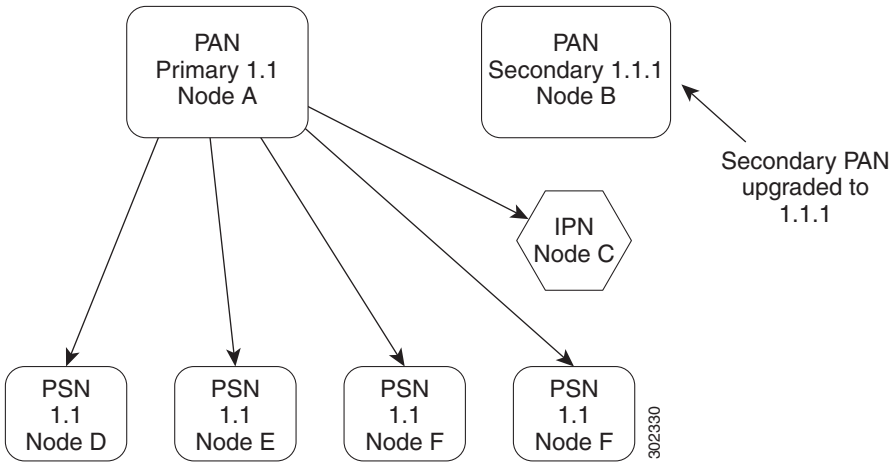
Step 1 Perform an on-demand backup (manually) of the Primary Administration ISE node from the admin user interface or CLI and an on-demand backup of the Monitoring node from the admin user interface before upgrading the Cisco ISE.

For more information on how perform an on-demand backup, see the "Performing an On-Demand Backup" section on page 1-3.

Step 2 Record the Inline Posture Node (IPN) configuration before the upgrade, so that you can reconfigure the IPN node after the upgrade.

Step 3 Deregister the secondary node (Node B) from the deployment setup. After deregistration, this node becomes a standalone node. Upgrade this standalone node to Cisco ISE, Release 1.1.x. See Figure 4-2.

Figure 4-2 Cisco ISE Secondary Node Upgraded



When you log in to Node B after the upgrade, if the system prompts you for a license, you must install a valid license for the secondary node based on its UDI. See Obtaining a Valid License, page 1-2 for more information.

Step 4 Record the Profiling configuration applied on each node before the upgrade, so that you can reconfigure the nodes after the upgrade. You can find the Profiling configuration for a specific node by navigating to **Administration > System > Deployment >** *node-name* **> Profiling Configuration**.

Step 5 Deregister the PSN node (Node D) from the deployment setup. After deregistration, this node becomes a standalone node. Upgrade this standalone node to Cisco ISE, Release 1.1.x.

Step 6 Make Node B as the primary node in the new deployment, and register Node D as the PSN node. If the nodes do not have their own licenses, then they will revert to the default grace period licenses, which are valid only for 100 endpoints. If the deployment is being used by endpoints more than 100, then the functionality of the nodes will be impacted until the Upgrade is complete.

Step 7 Deregister the IPN node (Node C) from the deployment setup, and make it as a standalone node. Upgrade this IPN node to Cisco ISE, Release 1.1.x.

The upgrade process removes the configuration of the IPN. You must reconfigure the IPN after the upgrade.

Note If your IPN node runs version 1.1.0.665 or above, you can deregister and upgrade the node as described in step 6. If your IPN node runs an earlier version (for example, 1.0.0.473), then you have to reimage your IPN appliance and install Cisco ISE 1.1.x on it.

Step 8 Deregister the second PSN node (Node E) from the deployment, and upgrade it to Cisco ISE, Release 1.1.x. Register this node to Node B as the PSN node. Repeat this step for the other PSN nodes (Node F and Node G).

Step 9 Convert the primary node of the previous deployment (Node A) to a standalone node. Upgrade Node A to Cisco ISE, Release 1.1.x and register to Node B in the Cisco ISE, Release 1.1.x deployment setup as the secondary node.

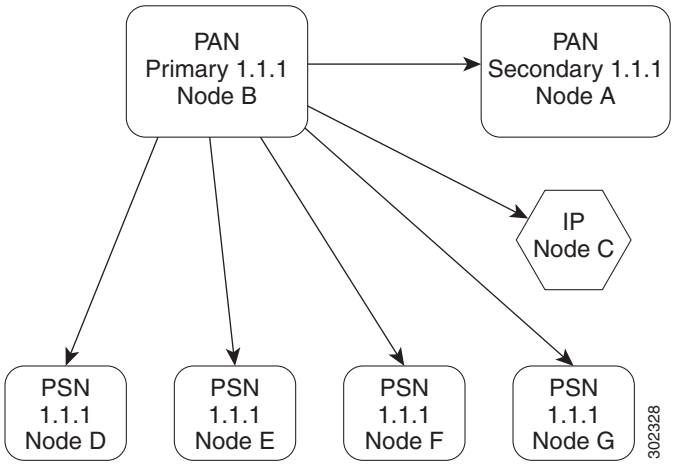
Step 10 Exchange the IPN certificates with the new primary Administration node (Node B) certificates. Similarly, exchange the IPN certificates with the new secondary Administration node (Node A) certificates.

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

Step 11 Register the IPN node (Node C) to the new deployment setup; that is, to Node B.

After you upgrade and register all the nodes to the new deployment, your Cisco ISE deployment upgrade is complete as shown in Figure 4-3.

Figure 4-3 All Nodes In the Deployment Now Have the New Cisco ISE Release



Step 12 Promote the secondary Administration ISE node (original primary—Node A) to be the primary node in the deployment again. When you are promoting Node A to be the primary node, it would have lost the license. When Node A got registered to Node B, the license would have been removed. You need to reinstall the license for Node A.

Step 13 The upgrade process removes the Profiling configuration, if available. You need to reconfigure the Profiling for each PSN after the upgrade.

Replacing Appliances Running Cisco ISE Release 1.1 with Appliances Running Release 1.1.x in a Distributed Deployment

This section contains the following:

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

The Cisco Secure Network Server is based on the Cisco UCS C220 Rack Server and is configured specifically to support the Cisco Identity Services Engine (ISE), Network Admission Control (NAC), and Access Control System (ACS) security applications. The Secure Network Server supports these applications in two versions. The Cisco Secure Network Server 3415 is designed for small and medium-sized deployments. The Secure Network Server 3495 has several redundant components such as processors, hard disks, and power supplies, making it suitable for large deployments that require highly reliable system configurations.

Note You can run the Cisco ISE version 1.1.4 on the SNS appliances and also on the platforms that are supported in the ISE version 1.1.3.

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

Prerequisite:

- Make sure you have the license file for your Primary Administration ISE node before beginning the upgrade process. If you do not have the file on hand (if your license was installed by a Cisco partner vendor, for example) contact Cisco TAC for assistance.

Step 1 Deregister an existing secondary Cisco ISE 1.1 appliance and upgrade it to Cisco ISE 1.1.x. Make this appliance as the primary node in the new deployment.

Step 2 Deregister the other nodes in the old deployment which you want to move to the new deployment, upgrade them and register them to the new deployment.

Step 3 Register the new Cisco ISE 1.1.x appliances to the new deployment.

In this case, the primary Administration ISE node remains on the original hardware.

Step 4 Promote one of the newer Cisco ISE 1.1.x appliances to be the new primary Administration ISE node.

Replacing All Cisco ISE Appliances Running Release 1.1 with Appliances Running Release 1.1.x in a Distributed Deployment

The Cisco Secure Network Server is based on the Cisco UCS C220 Rack Server and is configured specifically to support the Cisco Identity Services Engine (ISE), Network Admission Control (NAC), and Access Control System (ACS) security applications. The Secure Network Server supports these applications in two versions. The Cisco Secure Network Server 3415 is designed for small and medium-sized deployments. The Secure Network Server 3495 has several redundant components such as processors, hard disks, and power supplies, making it suitable for large deployments that require highly reliable system configurations.

Note You can run the Cisco ISE version 1.1.4 on the SNS appliances and also on the platforms that are supported in the ISE version 1.1.3.

To replace all Cisco ISE appliances that run Cisco ISE Maintenance Release 1.0.4 or the Cisco ISE, Release 1.1 software with Cisco ISE appliances that run Cisco ISE, Release 1.1.x in a distributed deployment, complete the following steps:

Prerequisite:

- Make sure you have the license file for your Primary Administration ISE node before beginning the upgrade process. If you do not have the file on hand (if your license was installed by a Cisco partner vendor, for example) contact Cisco TAC for assistance.

Step 1 Deregister an existing secondary Cisco ISE 1.1 appliance and upgrade it to Cisco ISE 1.1.x. Make this appliance as the primary node in the new deployment.

Step 2 Register the new Cisco ISE 1.1.x appliances to the new deployment.

Step 3 After all the new Cisco ISE 1.1.x appliances are registered to the new deployment, promote one of the new Cisco ISE 1.1.x appliance as the primary node in the new deployment.

Step 4 Deregister the old appliance that was promoted as primary node in Step 1.

CHAPTER 5

Recovering from Upgrade Failures

This chapter contains the following topics:

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 Fails 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 Fails 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 the SSH Session Quits 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, Release 1.1.x, directly install the new ISO version, and register it to the new primary Administration ISE node.

INDEX