The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

Before You Begin 1
Supported Upgrade Paths 1
Cisco Secure ACS to Cisco ISE Migration 2
Available Upgrade Bundles 2
Time Taken for Upgrade 2
Firewall Ports That Must be Open for Communication 3
Sequence Network Interface Cards (NICs) for UCS and IBM Appliances 3
  Pre-Upgrade Check of NICs for UCS and IBM Appliances 3
  Sequence NICs After Pre-Upgrade Check 4
  Troubleshooting Network Outage and Application Startup Failure After Upgrade 4
VMware Virtual Machine Settings 5
Export Certificates and Private Keys 5
Create Repository and Copy the Upgrade Bundle 5
Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node 6
Back Up System Logs from the Primary Administration Node 7
Obtain Active Directory and Internal Administrator Account Credentials 7
Review Custom Portal Migration in a Lab Setting Before Using Them in Production Environment 7
Activate MDM Vendor Before Upgrade 8
Record Profiler Configuration 8

CHAPTER 2

Upgrade Methods for Different Types of Deployments 9
Upgrade a Standalone Node 9
Upgrade a Two-Node Deployment 11
Upgrade a Distributed Deployment 12
Verify the Upgrade Process 17
CHAPTER 3  
Guest Service Changes  19  
  Admin Portal Changes  19  
  Other Portal-Related Changes  29  
  Policy-Related Changes  31  

CHAPTER 4  
Post-Upgrade Tasks  33  
  Post-Upgrade Tasks  33  

CHAPTER 5  
Recover from Upgrade Failures  43  
  Upgrade Failures  43  
  Upgrade Fails During Binary Install  45
Before You Begin

Read the following information carefully, and record these configurations (back up, export, obtain screen shots) wherever possible before you begin an upgrade:

- Supported Upgrade Paths, page 1
- Cisco Secure ACS to Cisco ISE Migration, page 2
- Available Upgrade Bundles, page 2
- Time Taken for Upgrade, page 2
- Firewall Ports That Must be Open for Communication, page 3
- Sequence Network Interface Cards (NICs) for UCS and IBM Appliances, page 3
- VMware Virtual Machine Settings, page 5
- Export Certificates and Private Keys, page 5
- Create Repository and Copy the Upgrade Bundle, page 5
- Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node, page 6
- Back Up System Logs from the Primary Administration Node, page 7
- Obtain Active Directory and Internal Administrator Account Credentials, page 7
- Review Custom Portal Migration in a Lab Setting Before Using Them in Production Environment, page 7
- Activate MDM Vendor Before Upgrade, page 8
- Record Profiler Configuration, page 8

Supported Upgrade Paths

You can directly upgrade to Cisco ISE, Release 1.4, from any of the following releases:

- Cisco ISE, Release 1.2 patch 14 or later
- Cisco ISE, Release 1.2.1 patch 5 or later
If you are on a version earlier than Cisco ISE, Release 1.2 patch 14, you must first upgrade to one of the releases listed above and then upgrade to Release 1.4.

Cisco Secure ACS to Cisco ISE Migration

You can directly migrate to Cisco ISE, Release 1.4 only from Cisco Secure ACS, Releases 5.5 and 5.6. For information about migrating from Cisco Secure ACS, Releases 5.5 and 5.6 to Cisco ISE, Release 1.4, see the Cisco Identity Services Engine Migration Tool Guide.

You cannot migrate to Release 1.4 from Cisco Secure ACS 4.x or earlier versions, Cisco Secure ACS 5.1, 5.2, 5.3, or 5.4, or from Cisco Network Admission Control (NAC) Appliance. From Cisco Secure ACS, Releases 4.x, 5.1, 5.2, 5.3, and 5.4, you must upgrade to ACS, Release 5.5 or 5.6 and then migrate to Cisco ISE, Release 1.4.

Available Upgrade Bundles

You can choose one of the following upgrade bundles to upgrade to Release 1.4:

- To upgrade from Release 1.2 or 1.2.1 to 1.4, use ise-upgradebundle-1.2.x-to-1.4.0.253.x86_64.tar.gz. MD5 checksum is 6c12533aee5f5e6995fe0518d086fbb8.

- To upgrade from Release 1.3 to 1.4, use ise-upgradebundle-1.4.0.253.x86_64.tar.gz. MD5 checksum is 35a159416afd0900c9da7b3de6c72043.

Time Taken for Upgrade

Upgrade Time Estimation

Actual time taken for upgrade varies depending on a number of factors. Your production network continues to function without any downtime during the upgrade process if you have multiple PSNs as part of a node group.

Factors That Affect Upgrade Time

- Number of endpoints in your network
- Number of users and guest users in your network
- Amount of logs in a Monitoring or Standalone node
- Profiling service, if enabled

Note: Cisco ISE nodes on virtual machines might take a longer time to upgrade than physical appliances.
Firewall Ports That Must be Open for Communication

If you have a firewall deployed between your primary Administration node and any other node, the following ports must be open before you upgrade:

- TCP 1521—For communication between the primary administration node and monitoring nodes.
- TCP 443—For communication between the primary administration node and all other secondary nodes.
- TCP 12001—For global cluster replication.
- TCP 7800 and 7802—(Applicable only if the policy service nodes are part of a node group) For PSN group clustering.

For a full list of ports that Cisco ISE uses, see the Cisco Identity Services Engine Hardware Installation Guide.

Sequence Network Interface Cards (NICs) for UCS and IBM Appliances

This section is applicable if you are directly upgrading from Cisco ISE, Release 1.2 or 1.2.1 to any later release.

The order in which the Network Interface Cards (NICs) are connected to Cisco UCS SNS 3415 and Cisco UCS SNS 3495, and IBM Cisco ISE 3315 appliances might affect the upgrade. You should ensure that a pre-upgrade check is performed, followed by sequencing of the NICs.

Pre-Upgrade Check of NICs for UCS and IBM Appliances

During upgrade, potential problems may arise with the sequencing of NICs on UCS and IBM appliances. For UCS appliances, the Intel NICs should be eth0 and eth1, and Broadcom NICs should be eth2 and eth3. For IBM appliances, the Broadcom NICs should be eth0 and eth1, and Intel NICs should be eth2 and eth3.

- Use the `show inventory` command to check the sequence of NICs for UCS appliances. In case of incorrect ordering, the `show inventory` command will display the following output.

```
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 600.10 GB
Disk 0: Geometry: 255 heads 63 sectors/track 72961 cylinders
NIC count: 4
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:10:18:D4:FC:EC
NIC 0: Driver Descr: Broadcom NetXtreme II BCM5706/5708/5709/5716 Driver
NIC 1: Device Name: eth1
NIC 1: HW Address: 00:10:18:D4:FC:EE
NIC 1: Driver Descr: Broadcom NetXtreme II BCM5706/5708/5709/5716 Driver
NIC 2: Device Name: eth2
NIC 2: HW Address: 60:73:5C:69:59:26
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3
NIC 3: HW Address: 60:73:5C:69:59:27
```
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver

(*) Hard Disk Count may be Logical

• Use the show inventory command to check the sequencing of NICs for IBM appliances. In case of incorrect ordering, the show inventory command will display the following output.

Cisco Identity Service Engine
=====================================================================
Version : 1.2.0.899
Build Date : Wed Jul 24 01:37:31 2013
Install Date : Thu Nov 20 04:12:01 2014

acsview-srv11/admin# sh inventory | include NIC
NIC count: 4
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:15:17:CA:D8:62
NIC 0: Driver Descr: Intel(R) PRO/1000 Network Driver
NIC 1: Device Name: eth1
NIC 1: HW Address: 00:15:17:CA:D8:63
NIC 1: Driver Descr: Intel(R) PRO/1000 Network Driver
NIC 2: Device Name: eth2
NIC 2: HW Address: 00:21:5E:95:7F:44
NIC 2: Driver Descr: Broadcom Tigon3 ethernet Driver
NIC 3: Device Name: eth3
NIC 3: HW Address: 00:21:5E:95:7F:45
NIC 3: Driver Descr: Broadcom Tigon3 ethernet Driver
acsview-srv11/admin#

Sequence NICs After Pre-Upgrade Check

After the pre-upgrade check, if you need to swap the NICs, ensure that you have physical access to the appliance. In addition, ensure that you have backed up all the latest configuration and operation files before you start the upgrade.

Refer to the Upgrade Methods for Different Types of Deployments chapter for additional information. As mentioned in the guide, the appliance reboots twice as part of the upgrade. During this time, the following message is displayed.

% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time progress of the upgrade is visible on console.
It could take up to 30 minutes for this to complete. Rebooting to do Identity Service Engine upgrade...

On seeing the above notice, the Ethernet cables should be swapped on the following interfaces without switching off the power.

eth0 <> eth2
eth1 <> eth3

If you are unable to swap the Ethernet cables, during the time the notice is displayed, wait for the upgrade to complete. Following two reboots, the login prompt appears. You can execute the show application status command to verify that the upgrade is complete. You can view the complete verification steps in the section, Verify the Upgrade Process, on page 17. Once you have confirmed that the upgrade is complete, you can swap the Ethernet cables, as mentioned above, and reboot the appliance using the reload command.

Troubleshooting Network Outage and Application Startup Failure After Upgrade

If you encounter a problem, such as network outage or application startup failure, even after sequencing the NICs, check the downloaded version of the bundle. It is possible that you might have downloaded a previous
version of the bundle that resulted in the inconsistent state of the NICs. Verify that the bundle has the following MD5 checksum:

- ise-upgradebundle-1.2.x-to-1.4.0.253.x86_64.tar.gz—MD5: 6c12533aee5f5e6995fe0518d086f8be
- ise-upgradebundle-1.4.0.253.x86_64.tar.gz—MD5: 35a159416afd0900c9da7b3dc6c72043

If there is network outage or application startup failure following upgrade, as a result of using an older bundle, you can re-image the failed node with Cisco ISE 1.2 software, register it to the old deployment, and restore the operations backup (if the node had a Monitoring persona). Then, you can attempt to perform the upgrade using the latest bundle again. This recovery step is suitable for a Secondary Administration Node, which is the first node to be upgraded in a deployment.

For other nodes in the deployment, you could use the same step or directly reimage the node with Cisco ISE 1.4 software, register it to the new deployment, and restore the operational backup, if applicable.

Ensure that you follow the steps mentioned in the Sequence Network Interface Cards (NICs) after Pre-Upgrade Check section.

If it is a standalone node, you can re-image the node with Cisco ISE 1.4 software and restore the configuration and operations backup.

If all the above steps fail and you encounter failed network connectivity for ISE post upgrade, contact Cisco TAC.

**VMware Virtual Machine Settings**

If you are upgrading a Cisco ISE node on a virtual machine (VM) from Release 1.2 or 1.2.1, after you upgrade, ensure that you power down the VM and change the Guest Operating System to Red Hat Enterprise Linux 6 (64-bit), and power the VM on after the change.

**Export Certificates and Private Keys**

We recommend that you export:

- All local certificates (from all the nodes in your deployment) along with their private keys to a secure location. Record the certificate configuration (what service the certificate was used for).
- All certificates from the Trusted Certificates Store of the Primary Administration Node. Record the certificate configuration (what service the certificate was used for).

**Create Repository and Copy the Upgrade Bundle**

Create a repository to obtain backups and copy the upgrade bundle. We recommend that you use FTP for better performance and reliability. Do not use repositories that are located across slow WAN links. We recommend that you use a local repository that is closer to the nodes.

Download the upgrade bundle from Cisco.com.

For upgrade, you can copy the upgrade bundle to the Cisco ISE node's local disk using the following command:

```
copy repository_url/path/ise-upgradebundle-1.4.0.253.x86_64.tar.gz disk:
```
For example, if you want to use SFTP to copy the upgrade bundle, you can do the following:

1. (Add the host key if it does not exist) `crypto host_key add host mySftpserver`
2. `copy sftp://aaa.bbb.ccc.ddd/ise-upgradebundle-1.4.0.253.x86_64.tar.gz disk:/`

   where `aaa.bbb.ccc.ddd` is the IP address or hostname of the SFTP server and `ise-upgradebundle-1.4.0.253.x86_64.tar.gz` is the name of the upgrade bundle.

Having the upgrade bundle in the local disk saves time during upgrade. Alternatively, you can use the `application upgrade prepare` command to copy the upgrade bundle to the local disk and extract it.

---

**Note**
Ensure that you have a good bandwidth connection with the repository. When you download the upgrade bundle from the repository to the node, the download times out if it takes more than 35 minutes to complete.

---

**Back Up Cisco ISE Configuration and Operational Data from the Primary Administration Node**

Obtain a back up of the Cisco ISE configuration and operational data from the Command Line Interface (CLI) or the GUI. The CLI command is:

```
backup backup-name repository repository-name {ise-config | ise-operational} encryption-key {hash | plain} encryption-keyname
```

**Note**
When Cisco ISE is run on VMware, Vmware snapshots are not supported for backing up ISE data.

VMware snapshot saves the status of a VM at a given point of time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. Cisco recommends that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

You can also obtain the configuration and operational data backup from the Cisco ISE Admin Portal. Ensure that you have created repositories for storing the backup file. Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node. 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.

1. Choose **Administration > System > Backup and Restore**.
2. Click **Backup Now**.
3. Enter the values as required to perform a backup.
4. Click **OK**.
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.

---

### Back Up System Logs from the Primary Administration Node

Obtain a backup of the system logs from the Primary Administration Node from the Command Line Interface (CLI). The CLI command is:

```
backup-logs backup-name repository repository-name encryption-key { hash | plain} encryption-key name
```

### Obtain Active Directory and Internal Administrator Account Credentials

If you use Active Directory as your external identity source, ensure that you have the Active Directory credentials and a valid internal administrator account credentials on hand. After upgrade, you might lose Active Directory connections. If this happens, you need the ISE internal administrator account to log in to the Admin portal and Active Directory credentials to rejoin Cisco ISE with Active Directory.

### Review Custom Portal Migration in a Lab Setting Before Using Them in Production Environment

---

**Note**

This section is applicable only when you directly upgrade from Release 1.2 or 1.2.1 to a later release of Cisco ISE.

Cisco ISE provides a new streamlined guest and employee on-boarding experience as well as a new portal customization experience with a host of new features from multi-language support to WYSIWYG customization. When you upgrade to the new release, all custom portals are migrated to the new ISE experience. Here are a few considerations that you must be aware of:

- The basic look and feel customizations that were done using CSS & HTML in previous releases of ISE are migrated by the upgrade process into the new Guest and Personal Devices flows.

- Customizations done using basic html and native administration tools should migrate properly. Customizations that use custom JavaScript to alter the Guest flow might not migrate properly. After upgrade, you can recreate these portals from the ISE Admin portal.

- You cannot edit any of the custom portals that are migrated to the new release. If you want to make changes to the look and feel, flow, or function, you must create a new portal (after upgrade, from the ISE Admin portal).
• ISE 1.2 and 1.2.1 customers were capable of making a wide variety of portal customizations. Some of those customizations might not migrate to the new release predictably. We recommend that you review your newly migrated portals in a lab setting before using them in a production environment.

• After upgrade, ISE fails to create a guest account when you:
  1  Configured your guest portal in ISE 1.2 or 1.2.1 to allow self-service
  2  Hardcoded the time zone value during portal customization
  3  Migrated the customized portal to the new release through the ISE upgrade process

This occurs because the hardcoded time zone value in your customized portal might not match the Guest Location names in the new release. "Time zones" in ISE 1.2 and 1.2.1 are renamed as “Guest Locations” in the new release.

As a workaround, after you upgrade to the new release, add the same time zone that you hardcoded in 1.2 or 1.2.1, as a Guest Location in the new release. To do this, from the ISE Admin portal, choose Guest Access > Settings > Guest Locations and SSIDs, add the time zone in the Location name text box, choose the corresponding time zone, click Add, and save the settings.

### Activate MDM Vendor Before Upgrade

If you use the MDM feature, then before upgrade, ensure that the MDM vendor status is active. Otherwise, the existing authorization profiles for MDM redirect are not updated with the MDM vendor details. After upgrade, you must manually update these profiles with an active vendor and the users will go through the onboarding flow again.

### Record Profiler Configuration

If you use the Profiler service, ensure that you record the profiler configuration for each of your Policy Service nodes from the Admin portal (Administration > System > Deployment > `<node>` > Profiling Configuration). You can make a note of the configuration or obtain screen shots.
Upgrade Methods for Different Types of Deployments

Review the following sections in this chapter for information on how to perform an upgrade on the following different types of deployments:

- Upgrade a Standalone Node, page 9
- Upgrade a Two-Node Deployment, page 11
- Upgrade a Distributed Deployment, page 12
- Verify the Upgrade Process, page 17

Upgrade a Standalone Node

You can use the `application upgrade` command directly, or the `application upgrade prepare` and `proceed` commands in sequence to upgrade a standalone node.

You can run the `application upgrade` command from the CLI on a standalone node that assumes the Administration, Policy Service, pxGrid, and Monitoring personas. If you choose to run this command directly, we recommend that you copy the upgrade bundle from the remote repository to the Cisco ISE node's local disk before you run the `application upgrade` command to save time during upgrade.

Alternatively, you can use the `application upgrade prepare` and `application upgrade proceed` commands. The `application upgrade prepare` command downloads the upgrade bundle and extracts it locally. This command copies the upgrade bundle from the remote repository to the Cisco ISE node's local disk. After you have prepared a node for upgrade, run the `application upgrade proceed` command to complete the upgrade successfully.

We recommend that you run the `application upgrade prepare` and `proceed` commands described below.

Before You Begin

Ensure that you have read the instructions in the Before You Upgrade chapter.
Procedure

Step 1  Create a repository on the local disk. For example, you can create a repository called "upgrade."

Example:
ise/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# repository upgrade
ise/admin(config-Repository)# url disk:
% Warning: Repositories configured from CLI cannot be used from the ISE web UI and are not
replicated to other ISE nodes. If this repository is not created in the ISE web UI, it will be deleted when ISE services
restart.
ise/admin(config-Repository)# exit
ise/admin(config)# exit

Step 2  From the Cisco ISE command line interface (CLI), enter application upgrade prepare command.
This command copies the upgrade bundle to the local repository "upgrade" that you created in the previous
step and lists the MD5 and SHA256 checksum.

Example:
ise/admin# application upgrade prepare ise-upgradebundle-1.4.0.253.x86_64.tar.gz upgrade
Getting bundle to local machine...
md5: 35a1594164af90900ca9730c6730f243
sha256: e358cae24977af67f8b2bb3574b3e559ce9578d2f36c444cd8ba9e6ddefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?

Step 3  Enter Y to continue.
The upgrade package is extracted. The following message appears.

Example:
Getting bundle to local machine...
md5: 35a1594164af90900ca9730c6730f243
sha256: e358cae24977af67f8b2bb3574b3e559ce9578d2f36c444cd8ba9e6ddefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?

Step 4  From the Cisco ISE CLI, enter the application upgrade proceed command.

Example:
ise45/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Registering this node to primary of new deployment...
STEP 6: Downloading configuration data from primary of new deployment...
STEP 7: Importing configuration data...
STEP 8: Running ISE configuration data upgrade for node specific data...
STEP 9: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
Gathering Config schema(CEPM) stats ..... 
Gathering Operational schema(MNT) stats .......... 
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
% This application Install or Upgrade requires reboot, rebooting now...
The upgrade is now complete.

What to Do Next
Verify the Upgrade Process, on page 17

Upgrade a Two-Node Deployment

Use the application upgrade prepare and proceed commands to upgrade a two-node deployment. You do not have to manually deregister the node and register it again. The upgrade software automatically deregisters the node and moves it to the new deployment. When you upgrade a two-node deployment, you should initially upgrade only the Secondary Administration Node (node B). When the secondary node upgrade is complete, you upgrade the primary node (node A). If you have a deployment set up as shown in the following figure, you can proceed with this upgrade procedure.

Before You Begin

- Perform an on-demand backup (manually) of the configuration and operational data from the Primary Administration Node.

- Ensure that the Administration and Monitoring personas are enabled on both the nodes in the deployment. If the Administration persona is enabled only on the Primary Administration Node, enable the Administration persona on the secondary node because the upgrade process requires the Secondary Administration Node to be upgraded first.

  Alternatively, if there is only one Administration node in your two-node deployment, then deregister the secondary node. Both the nodes become standalone nodes. Upgrade both the nodes as standalone nodes and set up the deployment after the upgrade.

- If the Monitoring persona is enabled only on one of the nodes, ensure that you enable the Monitoring persona on the other node before you proceed.
Procedure

**Step 1** Upgrade the secondary node (node B) from the CLI. The upgrade process automatically removes node B from the deployment and upgrades it. Node B becomes the primary node when it restarts.

**Step 2** Upgrade node A. The upgrade process automatically registers node A to the deployment and makes it the secondary node.

**Step 3** Promote node A to be the primary node in the new deployment. After the upgrade is complete, if the nodes contain old Monitoring logs, ensure that you run the `application configure ise` command and choose 5 (Refresh Database Statistics) on those nodes.

---

What to Do Next

Verify the Upgrade Process, on page 17

---

Upgrade a Distributed Deployment

You must first upgrade the Secondary Administration Node to the new release. For example, if you have a deployment setup as shown in the following figure, 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), one Primary Monitoring Node (node H), and one Secondary Monitoring Node (node I), you can proceed with the following upgrade procedure.

*Figure 2: Cisco ISE Deployment Before Upgrade*
Do not manually deregister the node before an upgrade. Use the `application upgrade prepare` and `proceed` commands to upgrade to the new release. The upgrade process deregisters the node automatically and moves it to the new deployment. If you manually deregister the node before an upgrade, ensure that you have the license file for the Primary Administration 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 the Cisco Technical Assistance Center for assistance.

To upgrade your deployment with minimum possible downtime while providing maximum resiliency and ability to roll back, the upgrade order should be as follows:

1. Secondary Administration Node (the Primary Administration Node at this point remains at the previous version and can be used for rollback, if upgrade fails).
2. Primary Monitoring Node
3. Policy Service Nodes
   At this point, verify if the upgrade is successful and also run the network tests to ensure that the new deployment functions as expected. See [Verify the Upgrade Process](#) on page 17 for more information. If the upgrade is successful, proceed to upgrade the following nodes:
4. Secondary Monitoring Node
5. Primary Administration Node
   Re-run the upgrade verification and network tests after you upgrade the Primary Administration Node.

**Before You Begin**

- If you do not have a Secondary Administration Node in the deployment, configure a Policy Service Node to be the Secondary Administration Node before beginning the upgrade process.
- Ensure that you have read and complied with the instructions given in the Before You Upgrade chapter.
- When you upgrade a complete Cisco ISE deployment, Domain Name System (DNS) server resolution (both forward and reverse lookups) is mandatory; otherwise, the upgrade fails.

**Procedure**

**Step 1**
Upgrade the Secondary Administration Node (node B) from the CLI.
The upgrade process automatically deregisters node B from the deployment and upgrades it. Node B becomes the primary node of the new deployment when it restarts. Because each deployment requires at least one Monitoring node, the upgrade process enables the Monitoring persona on node B even if it was not enabled on this node in the old deployment. If the Policy Service persona was enabled on node B in the old deployment, this configuration is retained after upgrading to the new deployment.

**Step 2**
Upgrade one of your Monitoring nodes (node H) to the new deployment.
We recommend that you upgrade your Primary Monitoring Node before the Secondary Monitoring Node (this is not possible if your Primary Administration Node in the old deployment functions as your Primary Monitoring Node as well). Your primary Monitoring node starts to collect the logs from the new deployment and you can view the details from the Primary Administration Node dashboard.
If you have only one Monitoring node in your old deployment, before you upgrade it, ensure that you enable the Monitoring persona on node A, which is the Primary Administration Node in the old deployment. Node persona changes result in a Cisco ISE application restart. Wait for node A to come up before you proceed. Upgrading the Monitoring node to the new deployment takes longer than the other nodes because operational data has to be moved to the new deployment.

If node B, the Primary Administration Node in the new deployment, did not have the Monitoring persona enabled in the old deployment, disable the Monitoring persona on it. Node persona changes result in a Cisco ISE application restart. Wait for the Primary Administration Node to come up before you proceed.

**Step 3** Upgrade the Policy Service Nodes (nodes D, E, F, and G) next. You can upgrade several PSNs in parallel, but if you upgrade all the PSNs concurrently, your network will experience a downtime. If your PSN is part of a node group cluster, you must deregister the PSN from the PAN, upgrade it as a standalone node, and register it with the PAN in the new deployment.

After the upgrade, the PSNs are registered with the primary node of the new deployment (node B), and the data from the primary node (node B) is replicated to all the PSNs. The PSNs retain their personas, node group information, and profiling probe configurations.

**Step 4** Deregister the IPN node (node C) from the Primary Administration Node.

**Step 5** Register the IPN node (node C) to the Primary Administration Node (node B) of the new deployment.

**Step 6** If you have a second Monitoring node (node I) in your old deployment, you must do the following:

a) Enable the Monitoring persona on node A, which is the primary node in your old deployment. A deployment requires at least one Monitoring node. Before you upgrade the second Monitoring node from the old deployment, enable this persona on the primary node itself. Node persona changes result in a Cisco ISE application restart. Wait for the primary ISE node to come up again.

b) Upgrade the Secondary Monitoring Node (node I) from the old deployment to the new deployment. Except for the Primary Administration Node (node A), you must have upgraded all the other nodes to the new deployment.

**Step 7** Finally, upgrade the Primary Administration Node (node A). This node is upgraded and added to the new deployment as a Secondary Administration Node. You can promote the Secondary Administration Node (node A) to be the primary node in the new deployment.

After the upgrade is complete, if the Monitoring nodes that were upgraded contain old logs, ensure that you run the `application configure ise` command and choose 5 (Refresh Database Statistics) on the Monitoring nodes.
CLI Transcripts of Successful Upgrades

Here is an example CLI transcript of a successful secondary Administration node upgrade.

```
ise74/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
  - Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Running ISE configuration DB schema upgrade...
  - Running db sanity check to fix index corruption, if any...
ISE Database schema upgrade completed.
STEP 7: Running ISE configuration data upgrade...
  - Data upgrade step 1/77, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
  - Data upgrade step 2/77, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
  - Data upgrade step 3/77, ProfilerUpgradeService(1.3.0.187)... Done in 4 seconds.
  - Data upgrade step 4/77, GuestUpgradeService(1.3.0.194)... Done in 0 seconds.
  - Data upgrade step 5/77, NetworkAccessUpgrade(1.3.0.200)... Done in 1 seconds.
  - Data upgrade step 6/77, GuestUpgradeService(1.3.0.208)... Done in 1 seconds.
  - Data upgrade step 7/77, GuestUpgradeService(1.3.0.220)... Done in 0 seconds.
  - Data upgrade step 8/77, RBACUpgradeService(1.3.0.228)... Done in 9 seconds.
  - Data upgrade step 9/77, NetworkAccessUpgrade(1.3.0.230)... Done in 2 seconds.
  - Data upgrade step 10/77, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
  - Data upgrade step 11/77, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
  - Data upgrade step 12/77, RBACUpgradeService(1.3.0.284)... Done in 5 seconds.
  - Data upgrade step 13/77, RBACUpgradeService(1.3.0.335)... Done in 5 seconds.
  - Data upgrade step 14/77, ProfilerUpgradeService(1.3.0.360)... Done in 73 seconds.
  - Data upgrade step 15/77, ProfilerUpgradeService(1.3.0.380)... Done in 2 seconds.
  - Data upgrade step 16/77, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
  - Data upgrade step 17/77, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
  - Data upgrade step 18/77, NSFUpgradeService(1.3.0.410)... Done in 0 seconds.
  - Data upgrade step 19/77, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
  - Data upgrade step 20/77, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
  - Data upgrade step 21/77, RBACUpgradeService(1.3.0.433)... Done in 0 seconds.
  - Data upgrade step 22/77, EgressUpgradeService(1.3.0.437)... Done in 0 seconds.
  - Data upgrade step 23/77, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
  - Data upgrade step 24/77, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
  - Data upgrade step 25/77, CdaRegistration(1.3.0.446)... Done in 1 seconds.
  - Data upgrade step 26/77, RBACUpgradeService(1.3.0.452)... Done in 8 seconds.
  - Data upgrade step 27/77, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
```
- Data upgrade step 28/77, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
- Data upgrade step 29/77, CertMgmtUpgradeService(1.3.0.462)... Done in 0 seconds.
- Data upgrade step 30/77, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
- Data upgrade step 31/77, TokenenUpgradeService(1.3.0.500)... Done in 0 seconds.
- Data upgrade step 32/77, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
- Data upgrade step 33/77, RBACUpgradeService(1.3.0.509)... Done in 8 seconds.
- Data upgrade step 34/77, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
- Data upgrade step 35/77, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
- Data upgrade step 36/77, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
- Data upgrade step 37/77, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
- Data upgrade step 38/77, NetworkAccessUpgrade(1.3.0.561)... Done in 0 seconds.
- Data upgrade step 39/77, CertMgmtUpgradeService(1.3.0.615)... Done in 1 seconds.
- Data upgrade step 40/77, CertMgmtUpgradeService(1.3.0.616)... Done in 0 seconds.
- Data upgrade step 41/77, CertMgmtUpgradeService(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 42/77, OCspServiceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 43/77, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
- Data upgrade step 44/77, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
- Data upgrade step 45/77, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
- Data upgrade step 46/77, RBACUpgradeService(1.3.0.650)... Done in 3 seconds.
- Data upgrade step 47/77, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
- Data upgrade step 48/77, NSFUpgradeService(1.3.0.659)... Done in 0 seconds.
- Data upgrade step 49/77, RBACUpgradeService(1.3.0.670)... Done in 2 seconds.
- Data upgrade step 50/77, ProfilerUpgradeService(1.3.0.670)... Done in 71 seconds.
- Data upgrade step 51/77, NSFUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 52/77, AuthzUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 53/77, GuestAccessUpgradeService(1.3.0.676)... Done in 119 seconds.
- Data upgrade step 54/77, NSFUpgradeService(1.3.0.694)... Done in 0 seconds.
- Data upgrade step 55/77, ProvisioningRegistration(1.3.0.700)... Done in 0 seconds.
- Data upgrade step 56/77, RegisterPostureTypes(1.3.0.705)... Done in 0 seconds.
- Data upgrade step 57/77, CertMgmtUpgradeService(1.3.0.727)... Done in 0 seconds.
- Data upgrade step 58/77, CertMgmtUpgradeService(1.3.0.808)... Done in 0 seconds.
- Data upgrade step 59/77, NSFUpgradeService(1.3.0.810)... Done in 0 seconds.
- Data upgrade step 60/77, RBACUpgradeService(1.3.0.834)... Done in 9 seconds.
- Data upgrade step 61/77, ProfilerUpgradeService(1.3.0.844)... Done in 44 seconds.
- Data upgrade step 62/77, GuestAccessUpgradeService(1.3.0.855)... Done in 1 seconds.
- Data upgrade step 63/77, NSFUpgradeService(1.3.0.859)... Done in 0 seconds.
- Data upgrade step 64/77, NSFUpgradeService(1.3.0.861)... Done in 0 seconds.
- Data upgrade step 65/77, ProvisioningUpgradeService(1.3.0.876)... Done in 0 seconds.
- Data upgrade step 66/77, CertReqMgmtBootstrapService(1.4.0.0)... Done in 0 seconds.
- Data upgrade step 67/77, NSF UpgradeService(1.4.0.110)... Done in 0 seconds.
- Data upgrade step 68/77, NSFUpgradeService(1.4.0.119)... Done in 0 seconds.
- Data upgrade step 69/77, NSFUpgradeService(1.4.0.125)... Done in 0 seconds.
- Data upgrade step 70/77, NSFUpgradeService(1.4.0.157)... Done in 0 seconds.
- Data upgrade step 71/77, GuestAccessUpgradeService(1.4.0.157)... Done in 3 seconds.
- Data upgrade step 72/77, NSFUpgradeService(1.4.0.164)... Done in 0 seconds.
- Data upgrade step 73/77, MDMPartnerUpgradeService(1.4.0.166)... Done in 0 seconds.
- Data upgrade step 74/77, MDMPartnerUpgradeService(1.4.0.167)... Done in 0 seconds.
- Data upgrade step 75/77, ProfilerUpgradeService(1.4.0.175)... Done in 1 seconds.
- Data upgrade step 76/77, CertMgmtUpgradeService(1.4.0.217)... Done in 0 seconds.
- Data upgrade step 77/77, GuestAccessUpgradeService(1.4.0.253)... Done in 0 seconds.

STEP 9: Making this node PRIMARY of the new deployment. When other nodes are upgraded it will be added to this deployment.

STEP 10: Running ISE M4T DB upgrade...
ISE Database Mnt schema upgrade completed.
**Gathering Config schema(CEPM) stats ......
Gathering Operational schema(MNT) stats ......
Stopping ISE Database processes...

% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time progress of the upgrade is visible on console. It could take up to 30 minutes for this to complete.

Rebooting to do Identity Service Engine upgrade...

Here is an example CLI transcript of a successful PSN node upgrade.

ise/admin# application upgrade ise-upgradebundle-1.4.0.253.x86_64.tar.gz sftp
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Please enter yes or no
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Getting bundle to local machine...
md5: 35a159416a4d0900c9a7b3dc6c72043
sha256: 8b3b43057067b0995ecabf5f673c69565c0d0dfaf790dfe58d1e998a9f8c7472a

% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
Unbundling Application Package...
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Registering this node to primary of new deployment...
STEP 7: Downloading configuration data from primary of new deployment...
STEP 8: Importing configuration data...
STEP 9: Running ISE configuration data upgrade for node specific data...
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
No gather stats needed as this is not PAP or MNT node
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.
% This application Install or Upgrade requires reboot, rebooting now...

What to Do Next
Verify the Upgrade Process, on page 17

Verify the Upgrade Process

To verify if an upgrade is successful, do one of the following:

- Check the ade.log file for the upgrade process. To display the ade.log file, enter the following command from the Cisco ISE CLI: show logging system ade/ADE.log
- Enter the show version command to verify the build version.
- Enter the show application status ise command to verify that all the services are running.

We recommend that you run some network tests to ensure that the deployment functions as expected and that users are able to authenticate and access resources on your network.

If upgrade fails because of configuration database issues, the changes are rolled back automatically. Refer to Chapter 4, "Recovering from Cisco ISE Upgrade Failures" for more information.
Verify the Upgrade Process
Chapter 3

Guest Service Changes

This chapter is applicable only when you directly upgrade from Release 1.2 or 1.2.1 to 1.4.

The Guest Services administration is now much simplified. The configuration is centralized in the Admin portal under the Guest Access menu. There are several changes in Cisco ISE Web Portals between the ISE 1.2 and later releases. This chapter provides a list of upgrade considerations and dependencies that you must be aware of when you upgrade from Release 1.2 to later releases.

- Admin Portal Changes, page 19
- Other Portal-Related Changes, page 29
- Policy-Related Changes, page 31

Admin Portal Changes

The following table lists the changes in the Admin portal, provides the UI navigation path, and change information. Refer to the Cisco ISE Administrator Guide for more details.
<table>
<thead>
<tr>
<th>Object Name in Release 1.2</th>
<th>UI Navigation Path in Release 1.2</th>
<th>Object Name in Release 1.4</th>
<th>UI Navigation Path in Release 1.4</th>
<th>Change Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language Template</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Portal &gt; Language Template</td>
<td>Languages</td>
<td>Guest Access &gt; Configure &gt; Guest Portals or Sponsor Portals &gt; Edit &gt; Portal Page Customization &gt; Languages</td>
<td>In Release 1.3 and later, each portal type supports fifteen languages that you can use to display text to the user in the portal. These languages are available as individual properties files bundled together in a single zipped language file. The non-default languages that are created in Release 1.2 are migrated to the new release. However, any new settings that are introduced in the new release are set to their default values in English for these profiles. You must ensure that these values comply with your company policies and standards and update these settings in the respective languages.</td>
</tr>
<tr>
<td>Device Registration</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Multi-Portal Configuration &gt; Guest Portal &gt; Edit &gt; Operations &gt; Guest users should be allowed to do device registration</td>
<td>Guest Device Registration Settings</td>
<td>Guest Access &gt; Configure &gt; Guest Portals &gt; Create /Edit /Duplicate &gt; Portal Behavior and Flow Settings &gt; Guest Device Registration Settings</td>
<td>In the new release, if the <strong>Automatically register guest devices</strong> check box is checked, then the device is automatically added to the endpoint identity group and the guest ID is associated with it automatically.</td>
</tr>
<tr>
<td>Object Name in Release 1.2</td>
<td>UI Navigation Path in Release 1.2</td>
<td>Object Name in Release 1.4</td>
<td>UI Navigation Path in Release 1.4</td>
<td>Change Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Time Profiles and Guest Role</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Time Profiles Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Guest Roles Configuration Administration &gt; Web Portal Management &gt; Sponsor Groups &gt; Sponsor Group &gt; Guest Roles</td>
<td>Guest Types</td>
<td>Guest Access &gt; Configure &gt; Guest Types</td>
<td>In the new release, if the <strong>Automatically register guest devices</strong> check box is checked, then the device is automatically added to the endpoint identity group and the guest ID is associated with it automatically.</td>
</tr>
<tr>
<td>Object Name in Release 1.2</td>
<td>UI Navigation Path in Release 1.2</td>
<td>Object Name in Release 1.4</td>
<td>UI Navigation Path in Release 1.4</td>
<td>Change Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Activated Guest Role</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Guest Roles Configuration</td>
<td>Allow guest to bypass the Guest portal</td>
<td>Guest Access &gt; Configure &gt; Guest Type &gt; Create / Edit</td>
<td></td>
</tr>
</tbody>
</table>
The following Guest Types are available by default in the new release:

- **Daily**—Default settings allow network access for just 1 to 5 days.
- **Weekly**—Default settings allow network access for two weeks.
- **Contractor**—Default settings allow network access for up to a year.

Guest Type in the new release is formed from the following data elements in Release 1.2: Sponsor Groups, Guest Roles, and Time Profiles. Using a combination of these three data elements, Guest Types are created in the new release. If a Guest Role is used in an authorization policy in Release 1.2, a corresponding Guest Type is created in the new release.

If any of these data elements are not used in any policies in Release 1.2, a Guest Type is not created in the new release for that element.

The upgrade process does not migrate time profiles that do not have active guests associated with them. If there are guests whose accounts are expired in 1.2, these guests are not migrated to the new release (irrespective of their status, for example, whether they are in the 'suspended' or 'awaiting initial login' state). Any guest types or sponsor groups that were associated with these guests are not migrated.

If you want a time profile to be available in the new release (Guest Type), then, before upgrade, you must create a guest account, associate it with the required time profile, and activate it.

**Note** The FromFirstLogin time profile in Release 1.2.x is not
<table>
<thead>
<tr>
<th>Object Name in Release 1.2</th>
<th>UI Navigation Path in Release 1.2</th>
<th>Object Name in Release 1.4</th>
<th>UI Navigation Path in Release 1.4</th>
<th>Change Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>available in Release 1.4. This time profile was used to allow the access time to start at first login. In Release 1.2.x, when you create a guest account using the FromFirstLogin time profile, the start date is set to the current date and the expiration date is set to the start date plus the duration configured in the time profile. This configuration is reset when the guest logs in for the first time. The upgrade process does not migrate guest accounts that have expired. You can use the Daily Guest Type instead to allow network access for a day.</td>
</tr>
<tr>
<td>Optional Data 1-5</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Language Template</td>
<td>Custom Fields</td>
<td>Guest Access &gt; Configure &gt; Guest Type &gt; Create / Edit</td>
<td>In Release 1.2, sponsors had the ability to obtain additional information from guests such as an alternate email address or birth dates (optional data). In the new release, the optional data is called custom fields and is available under Guest Type configuration.</td>
</tr>
<tr>
<td>Time Restrictions</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Time Profiles</td>
<td>Maximum Access Time</td>
<td>Guest Access &gt; Configure &gt; Guest Types &gt; Create / Edit &gt; Maximum Access Time</td>
<td>In Release 1.2, you can configure time restrictions (specify the time when guests should not be granted access), but in the new release, you can configure access time (specify the time when guests can be granted access).</td>
</tr>
<tr>
<td>Device Registration</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Portal Policy</td>
<td>Maximum devices guests can register</td>
<td>Guest Access &gt; Configure &gt; Guest Type &gt; Create / Edit &gt; Login Options</td>
<td>—</td>
</tr>
<tr>
<td>Object Name in Release 1.2</td>
<td>UI Navigation Path in Release 1.2</td>
<td>Object Name in Release 1.4</td>
<td>UI Navigation Path in Release 1.4</td>
<td>Change Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| Sponsor Groups            | Administration > Web Portal Management > Sponsor Groups | Sponsor Groups            | Guest Access > Configure > Sponsor Groups | Sponsor Groups in the new release include the following default sponsor groups:  
  • ALL_ACCOUNTS  
  • GROUP_ACCOUNTS  
  • OWN_ACCOUNTS |
<p>|                           |                                  |                           |                                  | AD External Group is present if you have configured Active Directory and joined to the Active Directory domain after you upgrade to the new release. |
|                           |                                  |                           |                                  | The upgrade process does not migrate all the sponsor groups. Sponsor groups that are not used in the creation of guests roles are not migrated. As a result of this change, some sponsors (internal database or Active Directory users) may not be able to log in after upgrade to the new release. You must check the sponsor group mapping for sponsors whose login fails. Map the sponsor to the appropriate sponsor group. |
| Sponsor Group Policy      | Administration &gt; Web Portal Management &gt; Sponsor Group Policy | —                         | —                                | Removed from the new release. Sponsor groups in the new release contain users and AD group mappings and permissions for those users. |</p>
<table>
<thead>
<tr>
<th>Object Name in Release 1.2</th>
<th>UI Navigation Path in Release 1.2</th>
<th>Object Name in Release 1.4</th>
<th>UI Navigation Path in Release 1.4</th>
<th>Change Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsor Group Permissions</td>
<td>Administration &gt; Web Portal Management &gt; Sponsor Groups &gt; Sponsor Group &gt; Authorization Levels</td>
<td>Sponsor Permissions</td>
<td>Guest Access &gt; Configure &gt; Sponsor Groups &gt; Create / Edit &gt; Sponsor Permissions</td>
<td>The following fields have changed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Allow Login—Removed in the new release</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Create Single Account—The Known User option in the new release replaces the Create Single Account option in Release 1.2. Similar to Release 1.2, sponsors can create multiple random accounts and import guest details from a CSV file in the new release.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Send Email—In the new release, this option is available by default in the sponsor portal and all sponsors can send guest credentials through email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Send SMS—In the new release, you have the Send SMS notifications with guest credentials option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Account Start Time—In the new release, you have the Start date cannot be more than n days into the future option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Maximum Duration of Account—In the new release, this option is available under Guest Type configuration (Guest Access &gt; Configure &gt; Guest Types &gt; Create/Edit &gt; Maximum Access Time &gt; Maximum account duration).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Allow Printing Guest Details—In the new release, this option is available by default in the sponsor portal and all sponsors can print the guest details.</td>
</tr>
<tr>
<td>Object Name in Release 1.2</td>
<td>UI Navigation Path in Release 1.2</td>
<td>Object Name in Release 1.4</td>
<td>UI Navigation Path in Release 1.4</td>
<td>Change Information</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Time Profiles</td>
<td>Guest Locations</td>
<td>Guest Access &gt; Settings &gt; Guest Locations and SSIDs</td>
<td>Guest locations in the new release are obtained from the Release 1.2 guest accounts. When you create a guest in Release 1.2, you associate a time zone for the guest. This time zone is used to create the guest location in the new release, and these locations are associated with the respective guest groups.</td>
</tr>
<tr>
<td>Guest Account Purge Settings</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; General &gt; Purge</td>
<td>Schedule purge of expired guest accounts</td>
<td>Guest Access &gt; Settings &gt; Guest Account Purge Policy</td>
<td>—</td>
</tr>
<tr>
<td>Guest Username Policy</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest &gt; Username Policy</td>
<td>Guest Username Policy</td>
<td>Guest Access &gt; Settings &gt; Guest Username Policy</td>
<td>During upgrade, the guest username policy might have changed. You must review the guest username policy and ensure that it conforms to your standards. Any changes that you made to the default guest username policy in Release 1.2 is migrated as a custom policy to the new release. Supported special characters in the guest username are different between Release 1.2 and the new release, and the supported special characters are migrated as custom entries.</td>
</tr>
<tr>
<td>Guest Password Policy</td>
<td>Administration &gt; Web Portal Management &gt; Settings &gt; Guest Password Policy</td>
<td>Guest Password Policy</td>
<td>Guest Access &gt; Settings &gt; Guest Password Policy</td>
<td>During upgrade, the guest password policy might have changed. You must review the guest password policy and ensure that it conforms to your standards. Any changes that you made to the default guest password policy in Release 1.2 is migrated as a custom policy to the new release. Supported special characters in the guest password are different between Release 1.2 and the new release, and the supported special characters are migrated as custom entries.</td>
</tr>
<tr>
<td>Object Name in Release 1.2</td>
<td>UI Navigation Path in Release 1.2</td>
<td>Object Name in Release 1.4</td>
<td>UI Navigation Path in Release 1.4</td>
<td>Change Information</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>SMTP Server Settings</td>
<td>Administration &gt; System &gt; Settings &gt; SMTP Server</td>
<td>Guest Email Settings</td>
<td>Guest Access &gt; Settings &gt; Guest Email Settings Administration &gt; System &gt; Settings &gt; SMTP Server</td>
<td>In Release 1.2, the SMTP server settings and guest email notification settings were in the same UI page. In the new release, the SMTP server settings and email notification to guests are available in two different locations (see the UI navigation path for the new release).</td>
</tr>
</tbody>
</table>
| Personal Devices Portals | Administration > Web Portal Management > Settings | Configure Device Portals  | Administration > Device Portal Management | The following personal devices portals are available by default in the new release:  
  - Blacklist Portal  
  - BYOD Portal  
  - Client Provisioning Portal  
  - MDM Portal  
  - My Devices Portal  
If you changed the default Guest portal interfaces and ports in Release 1.2, new BYOD and Client Provisioning portals are created in the new release that correspond to the 1.2 Guest portals. The authorization profiles are updated accordingly. |
| Portal Theme             | Administration > Web Portal Management > Settings > General > Portal Theme | Portal Theme               | Administration > Device Portal Management > Portal > Edit > Portal Page Customization | In the new release, you can customize the portal theme and view your changes before you save them. |
| Mobile-Optimized Guest Portal | Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration > Edit > Operations > Enable Mobile Portal | —                          | —                                | All portals are mobile optimized by default. Depending on the type of device that is used, the mobile or desktop version is used. |
Other Portal-Related Changes

During upgrade, all Cisco ISE portals are migrated to the new release.

- Default Portals—You can edit and make changes to the default portals (Guest, Sponsor, My Devices, and so on) after migration to the new release. Any portal settings that are newly introduced in Release 1.4 are set to their default values. The port, allowed interfaces, and portal theme configuration for the default portals are retained during upgrade.

- Custom Portals for Guest and Personal Devices—This release of Cisco ISE provides a new streamlined guest and employee on-boarding experience as well as a new portal customization experience with a host of new features from multi-language support to WYSIWYG customization. When you upgrade to the new release, all custom portals are migrated to the new experience. Here are a few considerations that you must be aware of:
  - The basic look and feel customizations that were done using CSS & HTML in previous releases of ISE are migrated by the upgrade process in to the new Guest and Personal Devices flows.
  - Customizations done using basic html and native administration tools should migrate properly. Customizations that use custom JavaScript to alter the Guest flow might not migrate properly. After upgrade, you can recreate these portals from the ISE Admin portal.
  - You cannot edit any of the custom portals that are migrated to the new release. If you want to make changes to the look and feel, flow, or function, you must create a new portal after upgrade (from the ISE Admin portal).
  - ISE 1.2 and 1.2.1 customers were capable of making a wide variety of portal customizations. Some of those customizations might not migrate to the new release predictably. We recommend that you review your newly migrated portals in a lab setting before using them in a production environment.

<table>
<thead>
<tr>
<th>Object Name in Release 1.2</th>
<th>UI Navigation Path in Release 1.2</th>
<th>Object Name in Release 1.4</th>
<th>UI Navigation Path in Release 1.4</th>
<th>Change Information</th>
</tr>
</thead>
</table>
| SMS Text Message Notification | Administration > Web Portal Management > Settings > Sponsor > Language Template | SMS Gateway Settings | Administration > System > Settings > SMS Gateway | SMS gateways in the new release enable:  
  - Sponsors to manually send SMS notifications to guests with their login credentials and password reset instructions.  
  - Guests to automatically receive SMS notifications with their login credentials after they successfully register themselves.  
  - Guests to automatically receive SMS notifications with actions to take before their guest accounts expire. |
ISE fails to create a guest account in the new release when you:

1. Configured your guest portal in ISE 1.2 or 1.2.1 to allow self-service
2. Hardcoded the time zone value during portal customization
3. Migrated the customized portal to the new release through the ISE upgrade process

This occurs because the hardcoded time zone value in your customized portal might not match the Guest Location names in the new release. “Time zones” in ISE 1.2 and 1.2.1 are renamed to “Guest Locations” in the new release.

As a workaround, after upgrade, add the same time zone that you hardcoded in 1.2 or 1.2.1, as a Guest Location in the new release. To do this, from the ISE Admin portal, choose Guest Access > Settings > Guest Locations and SSIDs, add the time zone in the Location name text box, choose the corresponding time zone, click Add, and save the settings.

- **Guest Portals**—All guest portals from Release 1.2 or 1.2.1 are migrated to the new release and you will see the following portals upon upgrade. If you do not have the equivalent 1.2 or 1.2.1 guest portal, a default guest portal is created.
  - DRW Portal in Release 1.2 or 1.2.1—Hotspot Portal in the new release
  - Guest Portal with no Self-Service in Release 1.2 or 1.2.1—Sponsored Guest Portal in the new release
  - Guest Portal with Self-Service Enabled in Release 1.2 or 1.2.1—Self-Registered Guest Portal in the new release

- **Sponsor Portals**—In Release 1.2 and 1.2.1, you can customize the following sponsor portal settings from Manage Guest Accounts > My Settings: Language Template, Location, Email Address, Guest Role, Account Duration, Time Zone, Notification Language, and Password Settings. After upgrade, only the sponsor email address gets migrated and the rest of the settings are not migrated. If you have customized your language preference, after upgrade, when you log in to the sponsor portal, your language preference is not retained.

- **BYOD Portals**—The following BYOD portals are migrated from Release 1.2 or 1.2.1:
  - My Devices Portal from Release 1.2 or 1.2.1
  - Guest Portals with BYOD-related configuration

The following default BYOD portals are created after you upgrade to the new release (these portals were not available in Release 1.2 or 1.2.1):
  - Default Blacklist Portal
  - Default BYOD Portal

- **Client Provisioning Portal**—Default Client Provisioning (CP) Portal is created when you upgrade to the new release.

For more information on the new ISE Guest and Personal Devices features and administrative experience, see the Cisco Identity Services Engine Administrator Guide.
Policy-Related Changes

The following policy and policy element changes and enhancements are introduced in this release of Cisco ISE:

- **Sponsor Group Policy**—The sponsor group policy is removed. Sponsor groups in the new release contain users and AD group mappings along with permissions for those users.

- **Authorization Profile**—The redirect URL is formatted according to the new format. For example, the URL redirect for a hotspot portal is:
  

- **Authorization Policy**—A new identity group (Guest Type identity group) is available for use in authorization policy.
Post-Upgrade Tasks

After you upgrade your deployment, perform the tasks listed in this chapter.

- Post-Upgrade Tasks, page 33

### Post-Upgrade Tasks

See the *Cisco Identity Services Engine Administrator Guide* for details about each of these tasks.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you upgraded a Cisco ISE node on a virtual machine (VM) from Release 1.2 or 1.2.1, power down your VM and change the Guest Operating System to Red Hat Enterprise Linux 6 (64-bit), and power the VM on after the change.</td>
<td>—</td>
</tr>
<tr>
<td>After upgrade, ensure that you clear the browser cache, close the browser, and open a new browser session before you access the Cisco ISE Admin portal. Supported browsers are:    • Mozilla Firefox versions 31.x ESR, 36.x, and 37.x  Adobe Flash Player 11.1.0.0 or above must be installed on the system running your client browser. The minimum required screen resolution to view the Cisco ISE Admin portal and for a better user experience is 1280 x 800 pixels.</td>
<td>—</td>
</tr>
</tbody>
</table>
### Task Description

Join all Cisco ISE nodes with Active Directory again, if you use Active Directory as your external identity source and the connection to Active Directory is lost. After rejoining, perform the external identity source call flows to ensure the connection.

- After upgrade, if you log in to the Cisco ISE user interface using an Active Directory administrator account, your login fails because Active Directory join is lost during upgrade. You must use the internal administrator account to log in to Cisco ISE and join Active Directory with it.

- If you had enabled certificate-based authentication for administrative access to Cisco ISE (Administration > Admin Access) before upgrade and used Active Directory as your identity source, after upgrade, you will not be able to launch the ISE login page because Active Directory join is lost during upgrade. If you run into this issue, from the Cisco ISE CLI, start the ISE application in safe mode using the following command:

  application start ise safe

  This command brings up the Cisco ISE node in safe mode. Perform the following tasks:

1. Log in to the Cisco ISE user interface using the internal administrator account.
   - If you do not remember your password or if your administrator account is locked, see the [Cisco Identity Services Engine Hardware Installation Guide, Release 2.0](#) for information on how to reset an administrator password.


Obtain a backup of the Cisco ISE CA certificates and keys from the Primary Administration Node and restore it on the Secondary Administration Node. This ensures that the Secondary Administration Node can function as the root CA or subordinate CA of an external PKI in case of a PAN failure and you promote the Secondary Administration Node to be the Primary Administration Node.

### Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide

- [Configure Active Directory as an External Identity Source](#)
- [Backup and Restore of Cisco ISE CA Certificates and Keys](#)
### Task Description

After you upgrade a distributed deployment, the Primary Administration Node's root CA certificates are not added to the Trusted Certificates store when both of the following conditions are met:

- Secondary Administration Node (Primary Administration Node in the old deployment) is promoted to be the Primary Administration Node in the new deployment
- Session services are disabled on the Secondary Administration Node

This might result in authentication failures with the following errors:

- Unknown CA in chain during a BYOD flow
- OCSP unknown error during a BYOD flow

You can see these messages when you click the More Details link from the Live Logs page for failed authentications.

As a workaround, after you upgrade your deployment and you promote the Secondary Administration Node to become the Primary Administration Node in the new deployment, generate a new ISE Root CA certificate chain from the Admin portal (choose Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain).

### Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide

- Generate Root CA and Subordinate CAs on the PAN and PSN

---

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset the RSA node secret if you use RSA SecurID server as your external identity source.</td>
<td>RSA Node Secret Reset</td>
</tr>
<tr>
<td>Perform a posture update from the Primary Administration Node after upgrade if you have enabled the Posture service.</td>
<td>Download Posture Updates to Cisco ISE</td>
</tr>
<tr>
<td>If you had manually configured the Originating Policy Services Node value under SNMP settings, this configuration is lost during upgrade. You must reconfigure this value.</td>
<td>See SNMP Settings under Network Device Definition Settings.</td>
</tr>
<tr>
<td>Task Description</td>
<td>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Update the profiler feed service after upgrade to ensure that the most up-to-date OUIs are installed. | From the Cisco ISE Admin portal:  
1. Choose Administration > FeedService > Profiler. Ensure that the profiler feed service is enabled.  
2. Click Update Now. |
<p>| Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect is hidden, check the <strong>Enable if target network is hidden</strong> check box in the iOS Settings area. | — |
| (Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Check the sponsor group mapping for sponsors whose login fails. Map the sponsor to the appropriate sponsor group. The upgrade process does not migrate all sponsor groups and hence some sponsors might not be able to log in to the sponsor portal. | — |
| (Applicable only when you upgrade directly from Release 1.2 or 1.2.1) The upgrade process migrates the default portals (guest, sponsor, mydevices, and so on) and the custom portals. The ports and allowed interfaces configuration that these portals use are retained during the upgrade. You can edit the default portals, but the custom portals are read-only. You can delete the default portals if you do not need them. | — |
| (Applicable only when you upgrade directly from Release 1.2 or 1.2.1; only for personal devices) If you had statically assigned devices to a particular device group, after you upgrade to the new deployment, ensure that you update the BYOD portal configuration (Administration &gt; Device Portal Management &gt; BYOD &gt; Edit) and choose the appropriate device group in the Endpoint identity group field. Otherwise, after upgrade, when a device connects to the network, it gets assigned to the default RegisteredDevices group. The authorization policy rules are not updated with this device group change and the request is not processed successfully. | — |</p>
<table>
<thead>
<tr>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Check the endpoint purge policy settings (Administration &gt; Identity Management &gt; Settings &gt; Endpoint Purge).</td>
</tr>
<tr>
<td>—</td>
</tr>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Check the guest username, password, and purge policies (Guest Access &gt; Settings).</td>
</tr>
<tr>
<td>—</td>
</tr>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Review the authorization policies for the Guest-related workflows, and update the Guest groups used in policy conditions.</td>
</tr>
<tr>
<td>—</td>
</tr>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Update the Wireless LAN Controller Guest Local Web Authentication configuration. You must replace the web redirect external server URL to https://&lt;ip&gt;:&lt;port&gt;/portal/PortalSetup.action?portal=&lt;portalId&gt;. Click Portal test URL from the Portal Settings and Customization page to obtain this URL (Guest Access &gt; Configure &gt; Portal &gt; Create/Edit &gt; Portal Settings and Customization).</td>
</tr>
<tr>
<td>—</td>
</tr>
<tr>
<td>Reconfigure e-mail settings, favorite reports, and data purge settings.</td>
</tr>
<tr>
<td>See the Monitoring and Troubleshooting section of the Cisco ISE Administrator Guide.</td>
</tr>
<tr>
<td>Check the threshold and/or filters for specific alarms that you need. All the alarms are enabled by default after an upgrade.</td>
</tr>
<tr>
<td>Customize reports based on your needs. If you had customized the reports in the old deployment, the upgrade process overwrites the changes that you made.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you upgraded a Cisco ISE node on a virtual machine (VM) from Release 1.2 or 1.2.1, power down your VM and change the Guest Operating System to Red Hat Enterprise Linux 6 (64-bit), and power the VM on after the change.</td>
</tr>
<tr>
<td>—</td>
</tr>
<tr>
<td>Task Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| After upgrade, ensure that you clear the browser cache, close the browser, and open a new browser session before you access the Cisco ISE Admin portal. Supported browsers are:  
  - Mozilla Firefox versions 31.x ESR, 36.x, and 37.x  
  Adobe Flash Player 11.1.0.0 or above must be installed on the system running your client browser.  
  The minimum required screen resolution to view the Cisco ISE Admin portal and for a better user experience is 1280 x 800 pixels. | —                                                                                                                                                     |
### Task Description

Join all Cisco ISE nodes with Active Directory again, if you use Active Directory as your external identity source and the connection to Active Directory is lost. After rejoining, perform the external identity source call flows to ensure the connection.

- After upgrade, if you log in to the Cisco ISE user interface using an Active Directory administrator account, your login fails because Active Directory join is lost during upgrade. You must use the internal administrator account to log in to Cisco ISE and join Active Directory with it.

- If you had enabled certificate-based authentication for administrative access to Cisco ISE (Administration > Admin Access) before upgrade and used Active Directory as your identity source, after upgrade, you will not be able to launch the ISE login page because Active Directory join is lost during upgrade. If you run into this issue, from the Cisco ISE CLI, start the ISE application in safe mode using the following command:

```
application start ise safe
```

This command brings up the Cisco ISE node in safe mode. Perform the following tasks:

1. Log in to the Cisco ISE user interface using the internal administrator account.

   If you do not remember your password or if your administrator account is locked, see the [Cisco Identity Services Engine Hardware Installation Guide, Release 2.0](https://www.cisco.com/c/en/us/support/unified-collaboration/software-licensing/cisco-identity-services-engine-consumer-product-page.html) for information on how to reset an administrator password.


### Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide

- Configure Active Directory as an External Identity Source
- Backup and Restore of Cisco ISE CA Certificates and Keys

---

Obtain a backup of the Cisco ISE CA certificates and keys from the Primary Administration Node and restore it on the Secondary Administration Node. This ensures that the Secondary Administration Node can function as the root CA or subordinate CA of an external PKI in case of a PAN failure and you promote the Secondary Administration Node to be the Primary Administration Node.
### Task Description

After you upgrade a distributed deployment, the Primary Administration Node's root CA certificates are not added to the Trusted Certificates store when both of the following conditions are met:

- Secondary Administration Node (Primary Administration Node in the old deployment) is promoted to be the Primary Administration Node in the new deployment
- Session services are disabled on the Secondary Administration Node

This might result in authentication failures with the following errors:

- Unknown CA in chain during a BYOD flow
- OCSP unknown error during a BYOD flow

You can see these messages when you click the More Details link from the Live Logs page for failed authentications.

As a workaround, after you upgrade your deployment and you promote the Secondary Administration Node to become the Primary Administration Node in the new deployment, generate a new ISE Root CA certificate chain from the Admin portal (choose Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain).

### Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide

- **Generate Root CA and Subordinate CAs on the PAN and PSN**

---

<table>
<thead>
<tr>
<th>Task Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset the RSA node secret if you use RSA SecurID server as your external identity source.</td>
<td>RSA Node Secret Reset</td>
</tr>
<tr>
<td>Perform a posture update from the Primary Administration Node after upgrade if you have enabled the Posture service.</td>
<td>Download Posture Updates to Cisco ISE</td>
</tr>
<tr>
<td>If you had manually configured the Originating Policy Services Node value under SNMP settings, this configuration is lost during upgrade. You must reconfigure this value.</td>
<td>See SNMP Settings under Network Device Definition Settings.</td>
</tr>
</tbody>
</table>
### Task Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
</table>
| Update the profiler feed service after upgrade to ensure that the most up-to-date OUIs are installed. | From the Cisco ISE Admin portal:  
1. Choose Administration > FeedService > Profiler. Ensure that the profiler feed service is enabled.  
2. Click Update Now. |
<p>| Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect is hidden, check the <strong>Enable if target network is hidden</strong> check box in the iOS Settings area. | — |
| (Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Check the sponsor group mapping for sponsors whose login fails. Map the sponsor to the appropriate sponsor group. The upgrade process does not migrate all sponsor groups and hence some sponsors might not be able to log in to the sponsor portal. | — |
| (Applicable only when you upgrade directly from Release 1.2 or 1.2.1) The upgrade process migrates the default portals (guest, sponsor, mydevices, and so on) and the custom portals. The ports and allowed interfaces configuration that these portals use are retained during the upgrade. You can edit the default portals, but the custom portals are read only. You can delete the default portals if you do not need them. | — |
| (Applicable only when you upgrade directly from Release 1.2 or 1.2.1; only for personal devices) If you had statically assigned devices to a particular device group, after you upgrade to the new deployment, ensure that you update the BYOD portal configuration (Administration &gt; Device Portal Management &gt; BYOD &gt; Edit) and choose the appropriate device group in the Endpoint identity group field. Otherwise, after upgrade, when a device connects to the network, it gets assigned to the default RegisteredDevices group. The authorization policy rules are not updated with this device group change and the request is not processed successfully. | — |</p>
<table>
<thead>
<tr>
<th>Task Description</th>
<th>Additional Information/Link to the Relevant Section in the Cisco ISE Administrator Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Check the endpoint purge policy settings (Administration &gt; Identity Management &gt; Settings &gt; Endpoint Purge).</td>
<td>—</td>
</tr>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Check the guest username, password, and purge policies (Guest Access &gt; Settings).</td>
<td>—</td>
</tr>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Review the authorization policies for the Guest-related workflows, and update the Guest groups used in policy conditions.</td>
<td>—</td>
</tr>
<tr>
<td>(Applicable only when you upgrade directly from Release 1.2 or 1.2.1) Update the Wireless LAN Controller Guest Local Web Authentication configuration. You must replace the web redirect external server URL to https://&lt;ip&gt;:&lt;port&gt;/portal/PortalSetup.action?portal=&lt;portalId&gt;. Click Portal test URL from the Portal Settings and Customization page to obtain this URL (Guest Access &gt; Configure &gt; Portal &gt; Create/Edit &gt; Portal Settings and Customization).</td>
<td>—</td>
</tr>
<tr>
<td>Reconfigure e-mail settings, favorite reports, and data purge settings.</td>
<td>See the Monitoring and Troubleshooting section of the Cisco ISE Administrator Guide.</td>
</tr>
<tr>
<td>Check the threshold and/or filters for specific alarms that you need. All the alarms are enabled by default after an upgrade.</td>
<td></td>
</tr>
<tr>
<td>Customize reports based on your needs. If you had customized the reports in the old deployment, the upgrade process overwrites the changes that you made.</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 5

Recover from Upgrade Failures

This section describes what you need to do while recovering from upgrade failures.

The upgrade software performs some validations. If upgrade fails, follow the instructions provided on screen to recover and successfully upgrade to Release 1.4.

At times, upgrade fails because of not following the order in which the nodes have to be upgraded, such as upgrading the secondary Administration node first. If you encounter this error, you can upgrade the deployment again following the order of upgrade specified in this guide.

In rare cases, you might have to reimage, perform a fresh install, and restore data. So it is important that you have a backup of Cisco ISE configuration and monitoring data before you start the upgrade. It is important that you back up the configuration and monitoring data even though we automatically try to roll back the changes in case of configuration database failures.

Note

Upgrade failures that happen because of issues in the monitoring database are not rolled back automatically. You have to manually reimage your system, install Cisco ISE, Release 1.4, and restore the configuration and monitoring data on it.

- Upgrade Failures, page 43
- Upgrade Fails During Binary Install, page 45

Upgrade Failures

This section describes some of the known upgrade errors and what you must do to recover from them.
You can check the upgrade logs from the CLI or the status of the upgrade from the console. Log in to the CLI or view the console of the Cisco ISE node to view the progress of upgrade. You can use the `show logging application` command from the Cisco ISE CLI to view the following logs (example filenames are given in parenthesis):

- DB Data Upgrade Log (`dbupgrade-data-global-20160308-154724.log`)
- DB Schema Log (`dbupgrade-schema-20160308-151626.log`)
- Post OS Upgrade Log (`upgrade-postosupgrade-20160308-170605.log`)

### Configuration and Data Upgrade Errors

During upgrade, the configuration database schema and data upgrade failures are rolled back automatically. Your system returns to the last known good state. If this is encountered, the following message appears on the console and in the logs:

```plaintext
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical Assistance Center for support.
```

### Remediation Errors

If you need to remediate an upgrade failure to get the node back to the original state, the following message appears on the console. Check the logs for more information.

```plaintext
% Warning: Do the following steps to revert node to its pre-upgrade state."
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical Assistance Center for support.
```

### Validation Errors

If there are any validation errors, which is not an actual upgrade failure, the following message appears. For example, you might see this error if you attempt to upgrade a PSN before the secondary PAN is upgraded or if the system does not meet the specified requirements. The system returns to the last known good state. If you encounter this error, ensure that you perform the upgrade as described in this document.

```plaintext
STEP 1: Stopping ISE application...
% Warning: Cannot upgrade this node until the standby PAP node is upgraded and running. If standbyPAP is already upgraded and reachable ensure that this node is in SYNC from current Primary UI.
Starting application after rollback...
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical Assistance Center for support.
```

### Application Binary Upgrade Errors

If the ADE-OS or application binary upgrade fails, the following message appears when you run the `show application status ise` command from the CLI following a reboot. You should reimaged and restore the configuration and operational backups.

```plaintext
% WARNING: An Identity Services Engine upgrade had failed. Please consult logs. You have to reimage and restore to previous version.
```
Other Types of Errors

For any other types of failures (including cancellation of the upgrade, disconnection of the console session, power failure, and so on), you must reimage and restore the configuration and operational backup depending on the personas enabled on the node originally.

Reimage

The term, reimage, refers to a fresh installation of Cisco ISE. For Monitoring database upgrade (schema + data) errors, you must reimage and restore the configuration and operational backups. Before you reimage, ensure that you generate a support bundle by running the `backup-logs` CLI command and place the support bundle in a remote repository in order to help ascertain the cause of failure. You must reimage to the old or new version based on the node personas:

- **Secondary Administration Node**—Reimage to the old version and restore the configuration and operational backup.
- **Monitoring Nodes**—If the nodes are deregistered from the existing deployment, reimage to the new version, register with the new deployment, and enable the Monitoring persona.
- **All Other Nodes**—If there are upgrade failures on the other nodes, the system usually returns to the last known good state. If the system does not roll back to the old version, you can reimage to the new version, register with the new deployment, and enable the personas as done in the old deployment.

Upgrade After Failure

In case of upgrade failures, before you try to upgrade again:

- Analyze the logs. Check the support bundle for errors.
- Identify and resolve the problem by submitting the support bundle that you generated to the Cisco Technical Assistance Center (TAC).

Upgrade Progress

You can view the progress of the upgrade by logging in via SSH and using the `show application status ise` command. The following message appears: %NOTICE: Identity Services Engine upgrade is in progress...

Upgrade Fails During Binary Install

**Problem** An application binary upgrade occurs after the database upgrade. If a binary upgrade failure happens, the following message appears on the console and ADE.log:

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

**Solution** Before you attempt any roll back or recovery, generate a support bundle by using the `backup-logs` command and place the support bundle in a remote repository.

To roll back, reimage the Cisco ISE appliance by using the previous ISO image and restore the data from the backup file. You need a new upgrade bundle each time you retry an upgrade.
• Analyze the logs. Check the support bundle for errors.

• Identify and resolve the problem by submitting the support bundle that you generated to the Cisco Technical Assistance Center (TAC).