Cisco Identity Services Engine Passive Identity Connector Installation and Upgrade Guide, Release 2.7

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 1

Cisco ISE-PIC Install and Upgrade Overview

This guide describes how to:

- Install and configure any of the Cisco ISE-PIC releases for the first time. Refer to Install Cisco ISE-PIC , on page 5.
- Upgrade from an older release to a newer release. Refer to Upgrade Cisco ISE-PIC , on page 11.

The rest of this chapter provides an overview of the ISE-PIC terminology and infrastructure. For additional information and detail about configuring and using ISE-PIC, refer to *Identity Services Engine Passive Identity Connector (ISE-PIC) Administrator Guide*.

Cisco ISE-PIC Terminology

This guide uses the following terms when discussing Cisco ISE-PIC:

Term	Definition
GUI	Graphic user interface. GUI refers to any of the screens and tabs in the software installation of ISE-PIC.
NIC	Network interface card.
Node	An individual physical or virtual Cisco ISE-PIC appliance.
PAN	The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN).

Term	Definition
Parser	The ISE-PIC backend component that receives syslog messages and breaks that input up into parts that can then be managed, mapped and published to ISE-PIC. The parser goes through each line of information of a syslog message as it arrives, looking for key information. For example, if a parser is configured to look for “mac=”, the parser then parses each line while looking for that phrase. The parser is set up to then communicate the defined information to ISE once it has found the key phrase that was configured.
Primary node	The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN).
Probe	Probes are mechanisms that collect data from a given source. Probe is a generic term that describes any mechanism, but does not specifically describe how the data is collected or what is collected. For example, an Active Directory (AD) probe helps ISE-PIC collect data from AD while a syslog probe collects data from a parser that reads syslog messages.
Provider	Clients or sources from which ISE-PIC receives, maps and publishes user identity information.
Secondary node	The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN).
Subscriber	Systems that subscribe to the ISE-PIC services in order to receive user identity information.

Cisco ISE-PIC Architecture, Deployments, and Nodes

Cisco ISE-PIC architecture includes the following components:

- Nodes—in a Cisco ISE-PIC deployment, up to two nodes can be configured as described below
- Network resources
- Endpoints

A deployment that has a single Cisco ISE-PIC node is called a *standalone deployment*.

A deployment that has two Cisco ISE-PIC nodes is called a *high availability deployment*, where one node functions as the primary appliance (the primary administration node, or the PAN). A high availability deployment improves service availability.

The PAN provides all the configuration capabilities that are required for this network model, and the secondary Cisco ISE node (the secondary PAN) functions in a backup role. The secondary node supports the primary node and resumes functionality whenever connectivity is lost with the primary node.

Cisco ISE-PIC synchronizes or replicates all of the content that resides on the primary Cisco ISE-PIC node with the secondary Cisco ISE-PIC node in order to ensure that your secondary node is current with the state of your primary node (and therefore can be used as a backup).

ISE Community Resource

For information about deployment and scaling, see ISE Deployment Journey.

Prerequisites and Virtual Appliance Requirements

ISE-PIC supports only virtual machines. Virtual machines should be based on the Cisco SNS 3500 or 3600 series appliance specifications.

For SNS-3500 series appliances, see Cisco SNS-3500 Series Appliance Hardware Installation Guide.

For SNS-3600 series appliances, see Cisco SNS-3600 Series Appliance Hardware Installation Guide.

Additional prerequisites and system requirements for installation of Cisco ISE-PIC are as outlined in the following table.

Table 1: Virtual Appliance Requirements and Prerequisites

Type	Description
Virtual Appliance	Virtual machine requirements, prerequisites, and associated procedures for Cisco ISE-PIC node are same as that of normal Cisco ISE node. Cisco ISE-PIC supports Small, Medium, and Large deployment models similar to Cisco ISE. To achieve optimal performance, ensure that you assign the equivalent resource reservations when you manually install Cisco ISE-PIC using the ISO image. Cisco ISE-PIC can be installed on the following virtual platforms: • VMware virtual machine • Linux KVM • Microsoft Hyper-V For more information about the virtual machine requirements, see *Cisco Identity Services Engine Installation Guide*. It is essential that you follow the prerequisite configuration and setup procedures outlined in the *Cisco Identity Services Engine Installation Guide* to ensure proper installation of ISE or ISE-PIC.

Type	Description
Software	There are no special operating system or software requirements. The ISO images for ISE-PIC include all necessary software items.

ISE Community Resource

For information about deployment and scaling, see ISE Deployment Journey.

CHAPTER 2

Install Cisco ISE-PIC

Download and Run the ISO Image

Before you begin

Before you install Cisco ISE-PIC on any of the supported appliances, ensure you have:

1. Created and accessed the virtual machine correctly.
2. Complied with all firmware and virtual machine requirements as follows:
   - Virtual Machine—install an OVA template prior to ISE-PIC installation and ensure your virtual machine server is configured correctly.
   - Linux KVM—ensure all virtualization technology and hardware requirements are met.

For more information about requirements, see *Cisco ISE-PIC Administrator Guide*, *Cisco Secure Network Server Data Sheet*, and *Cisco Identity Services Engine Installation Guide*.

Step 1 Boot the virtual machine on which to install ISE-PIC.

a) Map the CD/DVD to an ISO image. A screen similar to the following one appears. The following message and installation menu are displayed.

Example:

```
Please wait, preparing to
boot..................................................................
...................................................................................
```

The following options appear:

```
[1] Cisco ISE-PIC Installation (Keyboard/Monitor)
[2] Cisco ISE-PIC Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
```

Step 2 At the boot prompt, press **2** and **Enter** to install Cisco ISE-PIC using a serial console.

The following message appears.

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
```

Step 3 At the prompt, type **setup** to start the Setup program. See #unique_9 for details about the Setup program parameters.

Step 4 After you enter the network configuration parameters in the Setup mode, the appliance automatically reboots, and returns to the shell prompt mode.

Step 5 Exit from the shell prompt mode. The appliance comes up.

Step 6 Continue with Verify the Installation Process, on page 9.

Run the Setup Program of Cisco ISE

This section describes the setup process to configure the ISE-PIC server.

The setup program launches an interactive command-line interface (CLI) that prompts you for the required parameters. An administrator can use the console or a dumb terminal to configure the initial network settings and provide the initial administrator credentials for the ISE-PIC server using the setup program. This setup process is a one-time configuration task.

Note If you are integrating with Active Directory (AD), it is best to use the IP and subnet addresses from a dedicated Site created specifically for ISE. Consult with the staff in your organization responsible for AD and retrieve the relevant IP and subnet addresses for your ISE nodes prior to installation and configuration.

Note It is not recommended to attempt offline installation of Cisco ISE as this can lead to system instability. When you run the Cisco ISE installation script offline, the following error is shown:

Sync with NTP server failed' Incorrect time could render the system unusable until it is re-installed. Retry? Y/N [Y]:

Choose **Yes** to continue with the installation. Choose **No** to retry syncing with the NTP server.

It is recommended to establish network connectivity with both the NTP server and the DNS server while running the installation script.

To run the setup program:

Step 1 Turn on the appliance that is designated for the installation.

The setup prompt appears:

```
Please type ‘setup’ to configure the appliance
localhost login:
```

Step 2 At the login prompt, enter **setup** and press **Enter**.

The console displays a set of parameters. You must enter the parameter values as described in the table that follows.

Note The eth0 interface of ISE must be statically configured with an IPv6 address if you want to add a Domain Name Server or an NTP Server with an IPv6 address.

Table 2: Cisco ISE-PIC Setup Program Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical (A–Z, a–z, 0–9), and the hyphen (-). The first character must be a letter.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 or Global IPv6 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14/ 2001:420:54ff:4::458:121:119
Netmask	Must be a valid IPv4or IPv6 netmask.	255.255.255.0/ 2001:420:54ff:4::458:121:119/122
Default gateway	Must be a valid IPv4or Global IPv6 address for the default gateway.	10.12.13.1/ 2001:420:54ff:4::458:1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	example.com
Primary name server	Must be a valid IPv4 or Global IPv6 address for the primary name server.	10.15.20.25 / 2001:420:54ff:4::458:118
Add/Edit another name server	Must be a valid IPv4 or Global IPv6 address for the primary name server.	(Optional) Allows you to configure multiple name servers. To do so, enter `y` to continue.
Primary NTP server	Must be a valid IPv4 or Global IPv6 address or hostname of a Network Time Protocol (NTP) server. **Note** Ensure that the primary NTP server is reachable.	**clock.nist.gov** / 10.15.20.25 / 2001:420:54ff:4::458:117
Add/Edit another NTP server	Must be a valid NTP domain.	(Optional) Allows you to configure multiple NTP servers. To do so, enter `y` to continue.

Prompt	Description	Example
System Time Zone	Must be a valid time zone. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or Coordinated Universal Time (UTC) minus 8 hours). **Note** Ensure that the system time and time zone match with the CIMC or Hypervisor Host OS time and time zone. System performance might be affected if there is any mismatch between the time zones. You can run the **show timezones** command from the Cisco ISE-PIC CLI for a complete list of supported time zones.	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE-PIC system. If you choose not to use the default (admin), you must create a new username. The username must be three to eight characters in length and comprise of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE-PIC system. You must create this password in order to continue because there is no default password. The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note When you create a password for the administrator during installation or after installation in the CLI, do not use the $ character in your password, unless it is the last character of the password. If it is the first or one of the subsequent characters, the password is accepted, but cannot be used to log in to the CLI.

If you inadvertently create such a password, reset your password by logging into the console and using the CLI command, or by getting an ISE CD or ISO file. Instructions for using an ISO file to reset the password are explained in the following document: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

After the setup program is run, the system reboots automatically.

Now, you can log in to Cisco ISE-PIC using the username and password that was configured during the setup process.

Verify the Installation Process

To verify that you have correctly completed the installation process:

Step 1 Once the system automatically reboots after installation, enter the username you configured during the setup at the login prompt, and press **Enter**.

Step 2 At password prompt, enter the password you configured during setup, and press **Enter**.

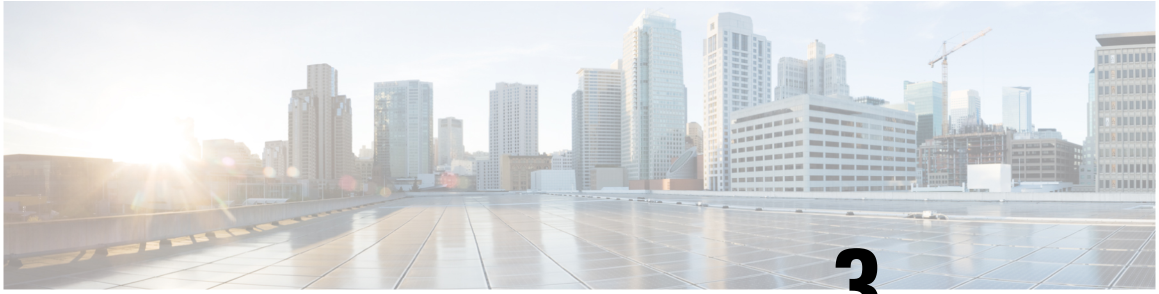
Step 3 Verify that the application has been installed properly by entering the **show application** command, and press **Enter**.

Step 4 Check the status of the ISE-PIC processes by entering the **show application status ise** command, and press **Enter**.

The following message is displayed:

```
ise-server/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          5072
Database Server                        running          90 PROCESSES
Application Server                     running          9117
AD Connector                           running          14187
Certificate Authority Service          running          9947
M&T Session Database                   running          6408
M&T Log Collector                      running          10166
M&T Log Processor                      running          10057
pxGrid Infrastructure Service          running          22303
pxGrid Publisher Subscriber Service    running          22575
pxGrid Connection Manager              running          22516
pxGrid Controller                      running          22625
PassiveID WMI Service                  running          10498
PassiveID Syslog Service               running          11483
PassiveID API Service                  running          12176
PassiveID Agent Service                running          13046
PassiveID Endpoint Service             running          13557
PassiveID SPAN Service                 running          13993
snsbu-c220-ORX/admin#
```



CHAPTER 3

Upgrade Cisco ISE-PIC

Cisco ISE-PIC Upgrade Overview

Upgrading a Cisco ISE-PIC deployment is a multi-step process and must be performed in the order specified in this document. Upgrade is expected to take approximately 240 minutes + 60 minutes for every 15 GB of data.

Factors that may affect upgrade time include the number of:

- Endpoints and users in your network
- Logs in the primary node

You must use the Cisco ISE upgrade bundle to upgrade Cisco ISE-PIC. You can download the upgrade bundle from Cisco.com.

In order to upgrade your deployment with minimum-possible downtime while providing maximum resiliency and ability to roll back, and minimum errors, perform the upgrade in the following order:

1. Back up all configuration data before beginning upgrade in order to ensure you can easily roll back manually if necessary.
2. Choose the upgrade process based on your deployment:
   - Standalone deployment
     a. Upgrade the node. Refer to Upgrade a Standalone Node, on page 18.
     b. Run upgrade verification and network tests after you upgrade the node. Refer to

        Verify the Upgrade Process, on page 19.

Note For details about the parts of this step, refer to:

- Upgrade a Two-Node Deployment, on page 17
- Verify the Upgrade Process, on page 19

   - **High Availability (two nodes) Deployment**
     a. Upgrade the secondary node first, keeping the PAN at the previous version until the secondary node upgrade is confirmed, in order to use the PAN for rollback if the initial upgrade fails.
     b. Run upgrade verification and network tests after you upgrade the seconary node.
     c. Upgrade the PAN.

        After upgrading both nodes, the Secondary Administration Node is now the Primary Administration Node, installed with the upgraded version, and the original Primary Administration Node is now the Secondary Administration Node, also installed with the upgraded version.
     d. Re-run the upgrade verification and network tests after you upgrade the Primary Administration Node.
     e. When you finish upgrading the original primary node (the second upgrade), in the **Edit Node** window from the currently secondary node, click **Promote to Primary** to promote it to become the Primary Administration Node (as was in your old deployment), if required.

Validate Data to Prevent Upgrade Failures

Cisco ISE-PIC offers an Upgrade Readiness Tool (URT) that you can run to detect and fix any data upgrade issues before you start the upgrade process.

Most of the upgrade failures occur because of data upgrade issues. The URT is designed to validate the data before upgrade to identify, and report or fix the issue, wherever possible.

The URT is available as a separate downloadable bundle that can be run on a Secondary Administration Node, for high availability, or on the Standalone Node for a single-node deployment. No downtime is necessary when running this tool.

Warning In multiple-node deployments, do not run the URT on the Primary Administration Node.

You can run the URT from the Command-Line Interface (CLI) of the Cisco ISE-PIC node. The URT does the following:

1. Verifies that the URT is run on a standalone Cisco ISE-PIC node or a Secondary Administration Node
2. Checks if the URT bundle is less than 45 days old—This check is done to ensure that you use the most recent URT bundle
3. Checks if all the prerequisites are met.

   The following prerequisites are checked by the URT:

   - Version compatibility
   - Disk space

   Note Verify the available disk size with Disk Requirement Size. If you are required to increase the disk size, reinstall ISE and restore a config backup.

   - NTP server
   - Memory
   - System and trusted certificate validation
4. Clones the configuration database
5. Copies latest upgrade files to the upgrade bundle

   Note If there are no patches in URT bundle then the output will return: `N/A`. This is an expected behaviour while installing a hot patch.
6. Performs a schema and data upgrade on the cloned database
   - (If the upgrade on the cloned database is successful) Provides an estimate of time it should take for the upgrade to end.
   - (If the upgrade is successful) Removes the cloned database.
   - (If the upgrade on cloned database fails) Collects the required logs, prompts for an encryption password, generates a log bundle, and stores it in the local disk.

Download and Run the Upgrade Readiness Tool

The Upgrade Readiness Tool (URT) validates the configuration data before you actually run the upgrade to identify any issues that might cause an upgrade failure.

Step 1 Create a Repository and Copy the URT Bundle, on page 14

Step 2 Run the Upgrade Readiness Tool, on page 14

Create a Repository and Copy the URT Bundle

Create a repository and copy the URT bundle. For information on how to create a repository, see “Create Repositories” in the Chapter “Maintain and Monitor” in the *Cisco ISE Administrator Guide*.

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.

Before you begin

Ensure that you have a good bandwidth connection with the repository.

Step 1 Download the URT bundle from Cisco.com. You must use the Cisco ISE URT bundle for Cisco ISE-PIC.

Step 2 Optionally, to save time, copy the URT bundle to the local disk on the Cisco ISE-PIC node.

```
copy repository_url/path/ise-urtbundle-2.7.0.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

For example, if you want to use SFTP to copy the upgrade bundle, you can do the following:

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-2.7.0.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

aaa.bbb.ccc.ddd is the IP address or hostname of the SFTP server and ise-urtbundle-2.7.0.*xxx*-1.0.0.SPA.x86_64.tar.gz is the name of the URT bundle.

Run the Upgrade Readiness Tool

The Upgrade Readiness Tool identifies issues with data that might cause an upgrade failure, and reports or fixes the issues, wherever possible. To run the URT:

Before you begin

Having the URT bundle in the local disk saves time.

Enter the **application install** command to install the URT:

```
application install ise-urtbundle-filename reponame
```

In case the application is not installed successfully during the above execution, URT returns the cause of upgrade failure. You need to fix the issues and re-run the URT.

Firewall Ports that Must be Open for Communication

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

- TCP 1521—For communication between the primary administration node .
- TCP 443—For communication between the primary administration node and secondary nodes.
- 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-PIC uses, see the Cisco ISE Ports Reference.

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

Obtain a backup of the Cisco ISE-PIC configuration and operational data from the Command Line Interface (CLI). The CLI command is:

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

Note When Cisco ISE-PIC runs on VMware, VMware snapshots are not supported for backing up ISE-PIC data.

VMware snapshot saves the status of a VM at a given point of time. In a multi-node Cisco ISE-PIC deployment, data in all the nodes are continuously synchronized with the 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-PIC for archival and restoration of data.

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

You can also obtain the configuration and operational data backup from the Cisco ISE-PIC Admin Portal. Ensure that you have created repositories for storing the backup file. Do not back up using a local repository. The following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because these repository types are all either read-only or their protocol does not support the file listing.

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

Note Cisco ISE-PIC allows you to obtain a backup from an ISE-PIC node (A) and restore it on another ISE-PIC node (B), both having the same hostnames (but different IP addresses). However, after you restore the backup on node B, do not change the hostname of node B because it might cause issues with certificates.

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*

Check Certificate Validity

The upgrade process fails if any certificate in the Cisco ISE-PIC Trusted Certificates or System Certificates store has expired. Ensure that you check the validity in the **Expiration Date** field of the **Trusted Certificates** and **System Certificates** windows (**Administration** > **System** > **Certificates** > **Certificate Management**), and renew them, if necessary, before upgrade.

Also check the validity in the **Expiration Date** field of the certificates in the **CA Certificates** window (**Administration** > **System** > **Certificates** > **Certificate Authority** > **Certificate Authority Certificates**), and renew them, if necessary, before upgrade.

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).

Disable Scheduled Backups before Upgrading

You cannot perform deployment changes when running a backup in Cisco ISE-PIC. Therefore, you must disable automatic configurations in order to ensure that they do not interfere with the upgrade. Ensure that you disable the following configurations before you upgrade Cisco ISE:

- Scheduled Backups—When planning your deployment upgrade, reschedule the backups after the upgrade. You can choose to disable the backup schedules and recreate them after the upgrade.

Backups with a schedule frequency of **once** get triggered every time the Cisco ISE-PIC application is restarted. Hence, if you have a backup schedule that was configured to run only a single time, be sure to disable it before upgrade.

Configure NTP Server and Verify Availability

During upgrade, the Cisco ISE-PIC nodes reboot, migrate, and replicate data from the primary administration node to the secondary administration node. For these operations, it is important that the NTP server in your network is configured correctly and is reachable. If the NTP server is not set up correctly or is unreachable, the upgrade process fails.

Ensure that the NTP servers in your network are reachable, responsive, and synchronized during upgrade.

Cisco ISE, Release 2.7 and later uses chrony instead of Network Time Protocol daemon (ntpd). Ntpd synchronizes with servers that have a root dispersion up to 10 seconds whereas, chrony synchronizes with servers that have a root dispersion less than 3 seconds. Therefore, we recommend that you use an NTP server with low root dispersion before upgrading to Cisco ISE, Release 2.7 or later, to avoid NTP service disruption. For more information, see Troubleshoot ISE and NTP Server Synchronization Failures on Microsoft Windows.

Upgrade a Two-Node Deployment

Use the **application upgrade prepare <upgrade bundle name> <repository name>** and **proceed** commands to upgrade a two-node deployment. 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. When the secondary node upgrade is complete, you upgrade the primary node thereafter.

Before you begin

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

Step 1 Upgrade the secondary node from the CLI.

The upgrade process automatically removes the original secondary node from the deployment and upgrades it. The original secondary node becomes the upgraded primary node when it restarts.

Step 2 Upgrade the original primary node.

The upgrade process automatically registers the original primary node to the deployment and makes it the secondary node in the upgraded environment.

Step 3 Promote the secondary node, to be the primary node in the new deployment.

After the upgrade is completeensure that you run the **application configure ise** command and choose 5 (Refresh Database Statistics) on the nodes.

What to do next

Verify the Upgrade Process, on page 19

Upgrade a Standalone Node

You can use the **application upgrade <upgrade bundle name> <repository name>** command directly, or the **application upgrade prepare <upgrade bundle name> <repository name>** and **application upgrade proceed** commands in the specified sequence to upgrade a standalone node.

If you choose to run this command directly, we recommend that you copy the upgrade bundle from the remote repository to the Cisco ISE-PIC node's local disk before you run the command to save time during upgrade.

Alternatively, you can use the **application upgrade prepare <upgrade bundle name> <repository name>** and **application upgrade proceed** commands. The **application upgrade prepare <upgrade bundle name> <repository name>** command downloads the upgrade bundle and extracts it locally. This command copies the upgrade bundle from the remote repository to the Cisco ISE-PIC 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 <upgrade bundle name> <repository name>** and **application upgrade proceed** commands as described below.

Before you begin

Ensure that you have read the instructions in the Prepare for Upgrade section.

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-PIC command line interface (CLI), enter **application upgrade prepare <upgrade bundle name> <repository name>** 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.

Step 3 **Note** After beginning the upgrade, 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...

From the Cisco ISE-PIC CLI, enter the **application upgrade proceed** command.

What to do next

Verify the Upgrade Process, on page 19

Verify the Upgrade Process

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

If an upgrade fails because of configuration database issues, the changes are rolled back automatically.

Perform any of the following options in order to verify whether the upgrade was successful.

- Check the ade.log file for the upgrade process. To display the ade.log file, enter the following command from the Cisco ISE-PIC CLI: **show logging system ade/ADE.log.?**

You can grep for **STEP** to view the progress of the upgrade:

- `info:[application:install:upgrade:preinstall.sh] STEP 0: Running pre-checks`
- `info:[application:operation:preinstall.sh] STEP 1: Stopping ISE application...`
- `info:[application:operation:preinstall.sh] STEP 2: Verifying files in bundle...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 3: Validating data before upgrade...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 4: De-registering node from current deployment.`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 5: Taking backup of the configuration data...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 6: Registering this node to primary of new deployment...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 7: Downloading configuration data from primary  of new deployment...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 8: Importing configuration data...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 9: Running ISE configuration data upgrade for node specific data...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 10: Running ISE M&T database upgrade...`
- `info:[application:install:upgrade:post-osupgrade.sh] POST ADEOS UPGRADE STEP 1: Upgrading Identity Services Engine software...`
- `info:[application:operation:post-osupgrade.sh] POST ADEOS UPGRADE STEP 2: Importing upgraded data to 64 bit database...`
- Search for this string to ensure that the upgrade is successful:

```
Upgrade of Identity Services Engine completed
      successfully.
```

- 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.

Recover from Upgrade Failures

This section describes what you need to do in order to recover if the upgrade fails.

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-PIC configuration data before you start the upgrade. It is important that you back up the configuration data although we automatically try to roll back the changes in case of configuration database failures.

Upgrade Failures

This section describes some of the known upgrade errors and what you must do to recover from them.

Note 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-PIC node to view the upgrade progress. You can use the **show logging application** command from the Cisco ISE-PIC 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:

```
% 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.

```
% 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

Validation errors are not an actual upgrade failure. Validations errors may occur. For example, you might see this error 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.

```
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 reimage and restore the configuration and operational backups.

```
% 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 backup.

Reimage

The term, reimage, refers to a fresh installation of Cisco ISE-PIC. 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, as follows:

- Secondary Administration Node—Reimage to the old version and restore the configuration and operational backup.
- Primary Administration Node—If there are upgrade failures on the PAN, 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, and register with the new 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).

Note 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 Failures 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-PIC 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).

Roll Back to the Previous Version

In rare cases, you might have to reimage the Cisco ISE-PIC appliance by using the previous version of ISO image and restoring the data from the backup file. After restoring the data, you can register with the old deployment. Hence, we recommend that you back up the Cisco ISE-PIC configuration data before you start the upgrade process.

Sometimes, upgrade failures that occur because of issues in the configuration database are not rolled back automatically. When this occurs, you get a notification stating that the database is not rolled back, along with an upgrade failure message. In such scenarios, you should manually reimage your system, install Cisco ISE, and restore the configuration data.

Before you attempt to rollback or recovery, generate a support bundle by using the **backup-logs** command, and place the support bundle in a remote repository.

Post-Upgrade Tasks

See the *Identity Services Engine Passive Identity Connector (ISE-PIC) Administrator Guide* for additional details about each of these tasks.

VMware Virtual Machine Guest Operating System Configuration

Ensure that the Guest Operating System on the VMware virtual machine is set to Red Hat Enterprise Linux (RHEL) 7 and the network adapter is set to E1000 or VMXNET3.

Note If you are upgrading to Release 2.7 on an ESXi 5.x server (5.1 U2 minimum), you must upgrade the VMware hardware version to 9 before you can select RHEL 7 as the Guest OS.

Clear Browser Cache

After upgrade, ensure that you clear the browser cache, close the browser, and open a new browser session before you access the Cisco ISE-PIC Admin portal.

Supported browsers are:

- Mozilla Firefox 79 and earlier versions
- Mozilla Firefox ESR 60.9 and earlier versions
- Google Chrome 84 and earlier versions

Reconfigure Active Directory Join Points

The Active Directory join point may be lost during upgrade. Log in to the Admin portal and navigate to check if you need to re-configure a join point.

Configure Active Directory Identity Search Attributes

Cisco ISE-PIC identifies users using the attributes SAM, CN, or both with the sAMAccountName attribute as the default attribute.

You can configure Cisco ISE-PIC to use SAM, CN, or both, if your environment requires it. When SAM and CN are used, and the value of the SAMAccountName attribute is not unique, Cisco ISE-PIC also compares the CN attribute value.

To configure attributes for Active Directory identity search:

1. Choose **Providers** > **Active Directory**. In the **Active Directory** window, click **Advanced Tools**, and choose **Advanced Tuning**. Enter the following details:
    - **ISE Node**—Choose the ISE node that is connecting to Active Directory.
    - **Name**—Enter the registry key that you are changing. To change the Active Directory search attributes, enter: `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`
    - **Value**—Enter the attributes that ISE uses to identify a user:
        - *SAM*—To use only SAM in the query (this option is the default).
        - *CN*—To use only CN in the query.
        - *SAMCN*—To use CN and SAM in the query.
    - **Comment**—Describe what you are changing, for example: Changing the default behavior to SAM and CN
2. Click **Update Value** to update the registry.

    A pop-up window appears. Read the message and accept the change. The AD connector service in ISE restarts.

Configure Reverse DNS Lookup

Ensure that you have Reverse DNS lookup configured for all Cisco ISE-PIC nodes in your two-node deployment from the DNS server(s). Otherwise, you may run into deployment-related issues after upgrade.

Restore Cisco CA Certificates and Keys

Obtain a backup of the Cisco ISE-PIC 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.

Reconfigure Mandatory ISE-PIC System Settings

- Reconfigure e-mail settings, favorite reports, and data purge settings.
- Check the threshold and/or filters for specific alarms that you need. All the alarms are enabled by default after an upgrade.

Additional References

The following link contains additional resources that you can use when working with Cisco ISE: https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.