Upgrade Cisco ISE-PIC

Cisco ISE-PIC Upgrade Overview

This chapter describes how to upgrade Cisco ISE-PIC software on virtual machines from Release 2.2 and 2.4 to Release 2.6.

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 can download the upgrade bundle from Cisco.com. The following upgrade bundle is available for Release 2.6:

- ise-upgradebundle-2.*x*-to-2.6.0.*xxx*.SPA.x86_64.tar.gz

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. Refer to Back Up Cisco ISE-PIC Configuration and Operational Data from the Primary Administration Node, on page 5.
2. Choose the upgrade process based on your deployment:
    - Standalone deployment

1. Upgrade the node. Refer to Upgrade a Standalone Node, on page 8.
2. Run upgrade verification and network tests after you upgrade the node. Refer to Verify the Upgrade Process, on page 9.

- **Note** For details about the parts of this step, refer to:
  - Upgrade a Two-Node Deployment, on page 7
  - Verify the Upgrade Process, on page 9

High availability (two nodes) deployment

1. 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.
2. Run upgrade verification and network tests after you upgrade the seconary node.
3. 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.
4. Re-run the upgrade verification and network tests after you upgrade the Primary Administration Node.
5. 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.

Prepare for Upgrade

Prior to upgrade, perform the following tasks as necessary depending on your deployment.

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.

Note 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
6. Performs a schema and data upgrade on the cloned database
7. - (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 4

Step 2 Run the Upgrade Readiness Tool, on page 4

Create a Repository and Copy the URT Bundle

Create a repository and copy the URT 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.

Before you begin

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

Step 1 Download the URT bundle from Cisco.com (ise-urtbundle-2.6.0.*xxx*-1.0.0.SPA.x86_64.tar.gz).

Step 2 Optionally, to save time, copy the URT bundle to the local disk on the Cisco ISE-PIC node using the following command:

```
copy repository_url/path/ise-urtbundle-2.6.0.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-2.6.0.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-2.6.0.*xxx*-1.0.0.SPA.x86_64.tar.gz is the name of the URT bundle.

Having the URT bundle in the local disk saves time.

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-2.6.0.x.SPA.x86_64.tar.gz reponame
```

Change VMware Virtual Machine Guest Operating System and Settings

If you are upgrading Cisco ISE-PIC nodes on virtual machines, ensure that you change the Guest Operating System to Red Hat Enterprise Linux (RHEL) 7. To do this, you must power down the VM, change the Guest Operating System to RHEL 7, and power on the VM after the change. RHEL 7 supports only E1000 and VMXNET3 network adapters. Be sure to change the network adapter type before you upgrade.

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.

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 of the certificates in the Trusted Certificate and System Certificates store, 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.

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.

To upgrade to Release 2.6, use the following upgrade bundle:
ise-upgradebundle-2.x-to-2.6.0.*xxx*.SPA.x86_64.tar.gz

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-2.x-to-2.6.0.xxx.SPA.x86_64.tar.gz* **disk:/**

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

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.

Upgrade a Two-Node Deployment

Use the **application upgrade prepare** 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 9

Upgrade a Standalone Node

You can use the **application upgrade** command directly, or the application upgrade **prepare** and **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 **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-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** and **proceed** commands as described below.

Before you begin

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

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** 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 9

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**
- 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 of ISO Image

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. For more information about the backup and upgrade processes, see Cisco ISE-PIC Upgrade Overview, on page 1.

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 2.6 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 version:
  - 52.6 ESR
  - 56 and above
- Google Chrome latest version
- Microsoft Internet Explorer 10.*x* and 11.*x*

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.