Cisco ISE 2.7 Upgrade Guide: Prepare for Upgrade

Prepare for Upgrade

Before you start the upgrade process, ensure that you perform the following tasks:

Note In a multinode deployment with Primary and Secondary PANs, monitoring dashboards and reports might fail after upgrade because of a caveat in the data replication. See CSCvd79546 for details. As a workaround, perform a manual synchronization from the Primary PAN to the Secondary PAN before initiating upgrade.

Note If you are currently on Release 2.3, you cannot upgrade to Release 2.3 Patch 1 because of an exception. See CSCvd79546 for details. As a workaround, synchronize the Primary PAN and Secondary PAN before upgrade.

Guidelines to Minimize Upgrade Time and Maximize Efficiency during Upgrade

The following guidelines help you address the issues in your current deployment that you might encounter during the upgrade process. Thus, reducing the overall upgrade downtime with increased efficiency.

- Upgrade to the latest patch in the existing version before starting the upgrade.
- We recommend that you test the upgrade in a staging environment to identify and fix any upgrade issues before upgrading the production networks.
  - All the nodes in the Cisco ISE deployment should be in the same patch level in order to exchange data.

    Note If all the nodes in your deployment are not on the same Cisco ISE version and patch version, you will get a warning message: **Upgrade cannot begin**. This message indicates that the upgrade is in a blocked state. Ensure that all the nodes in the deployment are in the same version (including the patch version, if any) before you begin the upgrade process.

  - Based on the number of PSNs in your deployment and availibilty of personnels, you can install the final version of Cisco ISE you need to upgrade to, apply latest patch, and keep it ready.
  - In case you want to reatain the MnT logs, perform the above tasks for MnT nodes and join the new deployment as MnT nodes. However, if you do not need to retain the operational logs, you can skip the step by re-imaging the MnT nodes.

- Cisco ISE installation can be done in parallel if you have multi-node deployment without impact to the production deployment. Installing ISE server's in-parallel saves time especially when you are using backup and restore from a previous release.
- PSN can be added to the new deployment to download the existing polices during the registration process from the PAN. Use ISE latency and bandwidth calculator to understand the latency and bandwidth requirement in Cisco ISE deployment.
- It is a best practice to archive the old logs and not transit them to the new deployments. This is because operational logs restored in the MnTs are not synchronized to different nodes in case you change the MnT roles later.
- If you have two Data Centers (DC) with full distributed deployment, upgrade the backup DC and test the use cases before upgrading primary DC.

- Download and store the upgrade software in a local repository before upgrade to speed up the process.
- Use the Upgrade Readiness Tool (URT) to detect and fix any configuration data upgrade issues before you start the upgrade process. Most of the upgrade failures occur because of configuration data upgrade issues. The URT validates 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 Policy Administration node or standalone node. There is no downtime to run this tool. The following video explains how to use the URT:
https://www.cisco.com/c/en/us/td/docs/security/ise/videos/urt/v1-0/cisco-urt.html

Warning Do not run the URT on the Primary Policy Administration Node. The URT tool does not simulate MnT operational data upgrades.

- When upgrading Cisco ISE using the GUI, note that the timeout for the process per node is four hours. If the process takes more than four hours, the upgrade fails. If upgrading with the Upgrade Readiness Tool (URT) will take you more than four hours, Cisco recommends that you use CLI for this process.
- Take the backup of load balancers before changing the configuration. You can remove the PSNs from the load balancers during the upgrade window and add them back after the upgrade.
- Disable automatic PAN Failover (if configured) and disable Heartbeat between PANs during the upgrade.
- Review the existing policies and rules and remove outdated, redundant, and stale policy and rules.
- Remove unwanted monitoring logs and endpoint data.
- You can take a backup of configuration and operations logs and restore it on a temporary server that is not connected to the network. You can use a remote logging target during the upgrade window.

  You can use the following options after the upgrade to reduce the number of logs that are sent to MnT nodes and improve the performance:

  - Use the MnT collection filters (**Administration > System > Logging > Collection Filters**) to filter incoming logs and avoid duplication of entries in AAA logs.
  - You can create Remote Logging Targets (**Administration > System > Logging > Remote Logging Targets**) and route each individual logging category to specific Logging Target (**System > Logging > Logging categories**).

- Enable the Ignore Repeated Updates options in the **Administration > System > Settings > Protocols > RADIUS** window to avoid repeated accounting updates.

- Download and use the latest upgrade bundle for upgrade. Use the following query in the Bug Search Tool to find the upgrade related defects that are open and fixed: http://cs.co/ise-upgrade-bugsearch
- Test all the use cases for the new deployment with fewer users to ensure service continuity.

Validate Data to Prevent Upgrade Failures

Cisco ISE 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 and other deployments with multiple nodes, 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 Policy Administration Node.

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

1. Checks if the URT is run on a supported version of Cisco ISE. The supported versions are Releases 2.2, 2.3, 2.4 and 2.6.
2. Verifies that the URT is run on a standalone Cisco ISE node or a Secondary Policy Administration Node (secondary PAN)
3. 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
4. Checks if all the prerequisites are met.

   The following prerequisites are checked by the URT:

   - Version compatibility
   - Persona checks
   - 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

5. Clones the configuration database
6. 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.

7. 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.

Before you begin

While running the URT, ensure that you simultaneously do not:

- Back up or restore data
- Perform any persona changes

Procedure

Step 1 Create a Repository and Copy the URT Bundle, on page 4

Step 2 Run the Upgrade Readiness Tool, on page 5

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.

Procedure

Step 1 Download the URT bundle from Cisco.com (ise-urtbundle-2.7.0.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 node using the following command:

```
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.

Procedure

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

```
application install 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.

Change the Name of Authorization Simple Condition if a Predefined Authorization Compound Condition with the Same Name Exists

Cisco ISE comes with several predefined authorization compound conditions. If you have an authorization simple condition (user defined) in the old deployment that has the same name as that of a predefined authorization compound condition, then the upgrade process fails. Before you upgrade, ensure that you rename the authorization simple conditions that have any of the following predefined authorization compound condition names:

- Compliance_Unknown_Devices
- Non_Compliant_Devices
- Compliant_Devices

- Non_Cisco_Profiled_Phones
- Switch_Local_Web_Authentication
- Catalyst_Switch_Local_Web_Authentication
- Wireless_Access
- BYOD_is_Registered
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed

Change VMware Virtual Machine Guest Operating System and Settings

If you are upgrading Cisco ISE nodes on virtual machines, ensure that you change the Guest Operating System to supported Red Hat Enterprise Linux (RHEL) version. To do this, you must power down the VM, update the Guest Operating System, 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.

Remove Non-ASCII Characters From Sponsor Group Names

Prior to release 2.2, if you have created sponsor groups with non-ASCII characters, before upgrade, be sure to rename the sponsor groups and use only ASCII characters.

Cisco ISE, Release 2.2 and later does not support non-ASCII characters in sponsor group names.

Firewall Ports that Must be Open for Communication

If you have a firewall that is 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.

For a full list of ports that Cisco ISE uses, see the Cisco ISE Ports Reference.

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

Obtain a backup 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 runs 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 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 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 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.

   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.

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.

Note Cisco ISE allows you to obtain a backup from an ISE node (A) and restore it on another ISE 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 and portal group tags.

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*

CA Certificate Chain

Before upgrading to Cisco ISE 2.7 , ensure that the internal CA certificate chain is valid.

1. Choose **Administration** > **System** > **Certificates** > **Certificate Authority Certificates**.
2. For each node in the deployment, select the certificate with `Certificate Services Endpoint Sub CA` in the **Friendly Name** column. Click **View** and check if the `Certificate Status is Good` message is visible.
3. If any certificate chain is broken, you must fix the issue before upgrading Cisco ISE. Choose **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Requests** > **ISE Root CA**

Check Certificate Validity

The upgrade process fails if any certificate in the Cisco ISE 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.

Delete a Certificate

In order to delete an expired certificate, perform the following steps:

Procedure

Step 1	Choose **Administration > System > Certificates > Certificate Management > System Certificates**.
Step 2	Select the expired certificate.
Step 3	Click **Delete**.
Step 4	Choose **Administration > System > Certificates > Certificate Management > Trusted Certificates**.
Step 5	Select the expired certificate.
Step 6	Click **Delete**.

Step 7 Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.

Step 8 Select the expired certificate.

Step 9 Click **Delete**.

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).

Procedure

Step 1 Choose **Administration > System > Certificates > Certificate Management > System Certificates**.

Step 2 Select the certificate and click **Export**.

Step 3 Select **Export Certificates and Private Keys** radio button.

Step 4 Enter the **Private Key Password** and **Confirm Password**.

Step 5 Click **Export**.

- All certificates from the Trusted Certificates Store of the Primary Administration Node. Record the certificate configuration (what service the certificate was used for).

Procedure

Step 1 Choose **Administration > System > Certificates > Certificate Management > Trusted Certificates**.

Step 2 Select the certificate and click **Export**.

Step 3 Click **Save File** to export the certificate.

Step 4 Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.

Step 5 Select the certificate and click **Export**.

Step 6 Select **Export Certificates and Private Keys** radio button.

Step 7 Enter the **Private Key Password** and **Confirm Password**.

Step 8 Click **Export**.

Step 9 Click **Save File** to export the certificate.

Disable PAN Automatic Failover and Disable Scheduled Backups before Upgrading

You cannot perform deployment changes when running a backup in Cisco ISE. 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:

- Primary Administration Node Automatic Failover—If you have configured the Primary Administration Node for an automatic failover, be sure to disable the automatic failover option 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 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 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 Virtual Machine

Cisco ISE software has to be in synchronization with the chip and appliance capacity to support latest CPU/Memory capacity available in the UCS Hardware. As ISE version progresses, support for older hardware will be phased out and newer hardware is introduced. It is a good practice to upgrade Virtual Machine (VM) capacity for better performance. When planning VM upgrades, we highly recommend to use OVA files to install ISE software. Each OVA file is a package that contains files used to describe the VM and reserves the required hardware resources on the appliance for Cisco ISE Software Installation.

For more information about the VM and hardware requirements, see the "Hardware and Virtual Appliance Requirements" in Cisco Identity Services Engine Installation Guide

Cisco ISE VMs need dedicated resources in the VM infrastructure. ISE needs adequate amount of CPU cores akin to hardware appliance for performance and scale. Resource sharing is found to impact performance with high CPU, delays in user authentications, registrations, delay and drops in logs, reporting, dashboard responsiveness, etc. This directly impacts the end-user and admin user experience in your enterprise.

Note It is important that you use reserved resources for CPU, memory and hard disk space during the upgrade instead of shared resources.

Cisco ISE, Release 2.4 and later requires a minimum disk size of 300GB for virtual machines as the local disk allocation is increased to 29GB.

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>** >). Select the node and click **Edit Node**. In the **Edit Node** page, go to the **Profiling Configuration** tab. You can make a note of the configuration information or obtain screen shots.

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.

Activate MDM Vendor Before Upgrade

If you use the MDM feature, then before upgrade, ensure that the MDM vendor status is active.

If an MDM server name is used in an authorization policy and the corresponding MDM server is disabled, the upgrade process fails. As a workaround, you can do one of the following:

1. Enable the MDM server before upgrade.
2. Delete the condition that uses the MDM server name attribute from the authorization policy.

Create Repository and Copy the Upgrade Bundle

Create a repository to obtain backups and copy the upgrade 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.

Ensure that your Internet connection to the repository is good.

Note When you download an upgrade bundle from a repository to a node, the download times out if it takes more than 35 minutes to complete. This issue occurs because of poor Internet bandwidth.

Having the upgrade bundle in the local disk saves time during upgrade. Alternatively, you can use the **application upgrade prepare <upgrade bundle name> <repository name>** 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 (file size is around 9GB) from the repository to the node, the download times out if it takes more than 35 minutes to complete.
- If you are using a local disk to store your configuration files, the files will be deleted when you perform the upgrade. Hence, we recommend that you create a Cisco ISE repository and copy the files to this repository.

Download the upgrade bundle from Cisco.com.

To upgrade to Release 2.7, use the following upgrade bundle:
ise-upgradebundle-2.x-to-2.7.0.*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-2.7.0.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:

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-2.x-to-2.7.0.xxx.SPA.x86_64.tar.gz* **disk:/**

   aaa.bbb.ccc.ddd is the IP address or hostname of the SFTP server and *ise-upgradebundle-2.x-to-2.7.0.xxx.SPA.x86_64.tar.gz* is the name of the upgrade bundle.

Check the Available Disk Size

Ensure that you have allocated the required disk space for virtual machines. See Cisco ISE Installation Guide for more details. If you need to increase the disk size, you will need to reinstall ISE and restore a config backup.

Check Load Balancer Configuration

If you are using any load balancer between the Primary Administration Node (PAN) and the Policy Service node (PSN), ensure that the session timeout that is configured on the load balancer does not affect the upgrade process. If the session timeout is set to a lower value, it might affect the upgrade process on the PSNs located behind the load balancer. For example, if a session times out during the database dump from PAN to a PSN, the upgrade process may fail on the PSN.

Log Retention and Resizing MnT Hard Disk

Upgrade does not need changes to the MnT disk capacity. However, if you are consistently filling up the logs and need greater hardware capacity you can plan out the hard disk size for MnT depending on your log

retention needs. It is important to understand that log retention capacity has increased many folds from Cisco ISE, Release 2.2.

You can also active collection filters (go to **Administration** > **System** > **Logging** > **Collection filters**) for unnecessary logs from different devices that can overwhelm your Cisco ISE MnT.

For more information on collection filter, see "Configure Collection Filters section" in "Maintain & Monitor" Chapter in Cisco Identity Services Engine Administrator Guide

See the ISE storage requirements under Cisco ISE performance and scalability community page. The table lists log retention based on number of endpoints for RADIUS and number of Network devices for TACACS+. Log retention should be calculated for both TACACS+ and/or RADIUS separately.