

Revised: June 2, 2026

Prepare for upgrade

Prepare for upgrade

Before you start the upgrade process, complete these tasks:

Health check

Run a health check on your Cisco ISE deployment before upgrading to identify and resolve critical issues that may cause downtime. For more information, refer to "Health Check" in the [“Troubleshoot”](#) chapter in the *Cisco ISE Administrator Guide, Release 3.5*.

Optimize upgrade duration

Follow these guidelines to address issues in your current deployment during the upgrade process. This will help reduce overall downtime.

- Upgrade to the latest patch in the existing version before starting the upgrade.



Note

If you are upgrading from earlier releases and have an SSM On-Prem server configured, you must disconnect the SSM On-Prem server before you begin the upgrade process.

- Test the upgrade in a staging environment to identify and address any issues without impacting the live system.
 - All the nodes in the Cisco ISE deployment should be at the same patch level in order to exchange data.



Note

If the nodes in your deployment are not running the same Cisco ISE version and patch level, you will get a warning message: **Upgrade cannot begin**. This means the upgrade is blocked. Make sure all nodes have the same version and patch installed before starting the upgrade.

- Follow these guidelines if you are upgrading from a Cisco ISE release earlier than Cisco ISE release 3.2 patch 3.
 - Depending on the number of PSNs in your deployment and the staff available, install the required final version of Cisco ISE, apply the latest patch, and prepare the system for use.
 - If you want to retain the MnT logs, complete the tasks for MnT nodes and join them to the new deployment as MnT nodes. However, if you do not need to retain the operational logs, you can skip the step by reimaging the MnT nodes.
 - Cisco ISE installation can be performed in parallel in a multi-node deployment without impacting the production environment. Installing Cisco ISE servers 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 policies during the registration process from the PAN.
- It is best practice to archive old logs instead of transferring them to new deployments. Restoring operational logs on the MnT nodes does not synchronize them with other nodes if you change MnT roles later.

- If you have two data centers with full distributed deployment, first upgrade the backup data center. Then test the use cases before upgrading the primary data center.
- Download and store the upgrade software in a local repository before the upgrade to speed up the process.
- If you are currently upgrading to a recent Cisco ISE release, you can either use Health Check or Upgrade Readiness Tool (URT) to run system diagnosis before you initiate the upgrade process.
- Use the URT to detect and fix any configuration data upgrade issues before you start the upgrade process. Most upgrade failures occur due to configuration data issues during the upgrade. The URT validates the data to identify issues before the upgrade and fixes or reports them whenever possible. The URT is available as a separate downloadable bundle that can be run on a Secondary PAN or standalone node. There is no downtime to run this tool. This video explains how to use the URT: <https://video.cisco.com/detail/video/5797832452001>.



Warning

Do not run the URT on the Primary PAN. The URT tool does not simulate MnT operational data upgrades.

- When you upgrade Cisco ISE using the GUI, it shows a system generated timestamp on each node. If the URT takes additional time to complete the upgrade, we recommend using the CLI instead.
- Back up the 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 the heartbeat between PANs during the upgrade.
- Review the existing policies and eliminate any outdated or redundant 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 these 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 to filter incoming logs and avoid duplication of entries in AAA logs. To view this window, navigate to **Administration > System > Logging > Collection Filters** in the Cisco ISE GUI.
- You can create remote logging targets by navigating to **Administration > System > Logging > Remote Logging Targets** in the Cisco ISE GUI. You can then route each logging category to a specific logging target by navigating to **System > Logging > Logging categories** in the Cisco ISE GUI.
- Enable the **Ignore Repeated Updates** options to avoid repeated accounting updates. To view this window, navigate to **Administration > System > Settings > Protocols > RADIUS** in the Cisco ISE GUI.
- Download and use the latest upgrade bundle for upgrade. Use this 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

Cisco ISE includes URT. You can run this tool to detect and resolve data upgrade issues before starting the upgrade process.

Most upgrade failures occur because of data upgrade issues. Use URT to validate your data before an upgrade, identify and report issues, and fix issues when possible.

The URT is available as a separate downloadable bundle. Run the URT on a Secondary Administration Node (SAN) to provide high availability and support deployments with multiple nodes, or run it on the standalone node for a single-node deployment.



Warning

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

You can run the URT from the CLI of the Cisco ISE node. The URT

1. checks whether it is run on a supported version of Cisco ISE (supported versions are Cisco ISE release 3.2, 3.3, and 3.4),
2. verifies that URT is run on either 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 to ensure you use the most recent URT bundle, and
4. checks all these prerequisites are met:
 - Version compatibility
 - Persona checks
 - Disk space



Note

Verify the available disk size with Disk Requirement Size (refer to "[Cisco Secured Network Server Series Appliances and Virtual Machine Requirements](#)" chapter in the *Cisco ISE Installation Guide, Release 3.5*. If you need to increase the disk size, reinstall Cisco ISE and restore a configuration backup.

- NTP server
 - Memory
 - System and trusted certificate validation
5. clones the configuration database,
 6. copies the latest upgrade files to the upgrade bundle, and



Note

If there are no patches in the URT bundle, the output returns N/A. This is expected behavior during the installation of a hot patch.

7. performs a schema and data upgrade on the cloned database.

If the upgrade on the cloned database is successful, it provides an estimate of the time required for the upgrade to complete.

If the upgrade is successful, the tool removes the cloned database.

If the upgrade on the cloned database fails, the tool collects the required logs, prompts for an encryption password, generates a log bundle, and stores the bundle on the local disk.

Download and run the URT

The URT checks the configuration data before the upgrade to identify issues that could cause an upgrade failure.

While running the URT, do not simultaneously :

- Back up or restore data
- Make any persona changes

Step 1 [Create a repository, on page 4](#)

Step 2 [Install the URT, on page 4](#)

Create a repository

Create a repository, then copy the URT bundle. For more information about creating a repository, refer to “[Create repositories](#)” in the chapter “Maintain and Monitor” in the *Cisco ISE Administrator Guide, Release 3.5*.

To improve performance and reliability, use FTP. Avoid using repositories located across slow WAN links. Choose a local repository near your nodes.

Make sure your connection to the repository has enough bandwidth.

Step 1 Download the URT bundle from the [Cisco ISE Download Software Center](#) (ise-urtbundle-3.5.0.<build#>-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 command:

```
copy repository_url/path/ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz disk:/
```

To copy the upgrade bundle using SFTP, perform these steps:

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz disk:/
```

The value "aaa.bbb.ccc.ddd" represents the IP address or hostname of the SFTP server;
"ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz" is the name of the URT bundle.

Install the URT

The URT identifies data issues that might cause an upgrade failure. It reports or fixes these issues where possible. To install the URT:

Storing the URT bundle on the local disk allows the installation process to complete more quickly.

Step 1 Enter this command to install the tool:

```
application install ise-urtbundle-3.5.0.<build#>-1.0.0.SPA.x86_64.tar.gz reponame
```



Note

If the application is not installed successfully, URT provides the reason for the upgrade failure. Fix any reported issues, then install the URT again.

Step 2 Remove the 5G attribute if you are upgrading to Cisco ISE release 3.5. For more information, refer to "[Configure Cisco Private 5G as a Service](#)" section in the "Secure Access" chapter in the *Cisco ISE Administrator Guide, Release 3.5*.



Note

If you do not remove the 5G attribute, you will get this error:

```
Error Occurred while adding 5G field to access service
```

```
Error while applying changes in version: 3.5.0.100 class: com.cisco.cpm.acs.nsf.im.NetworkAccessUpgrade
```

```
com.cisco.cpm.infrastructure.upgrade.api.UpgradeFailureException:
com.cisco.cpm.nsf.api.exceptions.NSFEntityAttributeException: AccessService FIVEG
DuplicateAttributeException~AttributeName : FIVEG already exists as FIVEG
```

```

        at
com.cisco.cpm.acs.nsf.im.NetworkAccessUpgrade.upgradeAllowFiveG(NetworkAccessUpgrade.java:2671)

        at com.cisco.cpm.acs.nsf.im.NetworkAccessUpgrade.upgrade(NetworkAccessUpgrade.java:585)

        at
com.cisco.cpm.infrastructure.upgrade.impl.UpgradeServiceRegistrar.UpgradeServices(UpgradeServiceRegistrar.java:132)

        at
com.cisco.cpm.infrastructure.upgrade.impl.UpgradeServiceRegistrar.main(UpgradeServiceRegistrar.java:185)

Caused by: com.cisco.cpm.nsf.api.exceptions.NSFEntityAttributeException: AccessService FIVEG
DuplicateAttributeException~AttributeName : FIVEG already exists as FIVEG

```

Remove the URT

Uninstall URT if the installation failed or if the installed version is outdated. Follow these steps to uninstall URT.

Make sure URT appears in the installed programs list.

Step 1 Enter this command in the CLI:

```
application remove urt
```

Step 2 At the prompt, enter **Y**:

```
Continue with application removal? (y/n)
```

This message is displayed when the uninstallation is complete:

```
Application successfully uninstalled
```

What's next

After the uninstallation is successful, you can install URT, if required.

Rename authorization simple condition to avoid compound condition name conflict

Cisco ISE comes with several predefined authorization compound conditions. The upgrade process fails if your old deployment contains an authorization simple condition with the same name as a predefined authorization compound condition. Rename your authorization simple condition before the upgrade to prevent a name conflict with a predefined compound condition.

Here is a list of predefined authorization compound condition names that must not conflict with any authorization simple condition names during an upgrade to prevent upgrade failures:

- 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

Update VMware settings

If you are upgrading Cisco ISE nodes on VMs,

1. change the guest OS to RHEL 7,
2. power down the VM,
3. change the guest OS to RHEL 7, and
4. power on the VM.

RHEL 7 supports only E1000 and VMXNET3 network adapters. Change the network adapter type before you upgrade.

Update the sponsor group names

Before upgrading, rename any sponsor groups with non-ASCII characters to use only ASCII characters.

Cisco ISE does not support non-ASCII characters in sponsor group names.

Enable key firewall ports

If you have a firewall deployed between your PAN and any other node, you must open these ports before upgrading:

- TCP 1521: For communication between the PAN and monitoring nodes.
- TCP 443: For communication between the PAN and all other secondary nodes.
- TCP 12001: For global cluster replication.
- TCP 7800 and 7802: Required for PSN group clustering when PSNs are part of a node group.

For a full list of ports that Cisco ISE uses, refer to chapter "[Cisco ISE Ports Reference](#)" in the *Cisco ISE Installation Guide, Release 3.5*.

Back up Cisco ISE configuration and operational data from the PAN

Obtain a backup of the Cisco ISE configuration and operational data from either the CLI or the GUI. To back up the configuration and operational data using the CLI, enter this command:

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 Cisco ISE data.

A VMware snapshot saves the status of a VM at a specific point in time. In a multi-node Cisco ISE deployment, all nodes continuously synchronize data with the current database. Restoring a snapshot might cause database replication and synchronization issues. Use the Cisco ISE backup functionality for data archival and restoration.

If you use VMware snapshots to back up Cisco ISE data, Cisco ISE services stop. To restore the ISE node, reboot it.

You can also obtain the configuration and operational data backup from the Cisco ISE Admin Portal. Ensure that you

- have created repositories that store the backup file
- do not use a local repository to back up data, and

You cannot back up the monitoring data in the local repository of a Remote Monitoring node.

- do not use CD-ROM, HTTP, HTTPS, or TFTP repositories, because they are read-only or do not support file listing.

Perform these steps to obtain the back up from Cisco ISE GUI:

1. In the Cisco ISE GUI, navigate to **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.

Wait for the backup to finish before changing or promoting node roles. Changing node roles during backup shuts down all processes and may cause data inconsistencies.

After backup, verify the backup file exists in the specified repository. Cisco ISE appends the backup filename with a timestamp and adds a CFG tag for configuration backups and an OPS tag for operational backups.



Note

Cisco ISE allows you to obtain a backup from a Cisco ISE node (A) and restore it to another Cisco 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 PAN

Obtain a backup of the system logs from the PAN using the CLI. Use this CLI command:

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

CA certificate chain

Before upgrading to Cisco ISE release 3.5, ensure that the internal CA certificate chain is valid. Follow these steps to check if the internal CA certificate is valid:

1. In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.

2. For each node in the deployment, select the certificate labeled **Certificate Services Endpoint Sub CA** in the **Friendly Name** field.
3. Click **View**.
4. Check if the `Certificate Status is good` message is visible.
5. Fix any broken certificate chains before upgrading Cisco ISE by navigating to **Administration > System > Certificates > Certificate Management > Certificate Signing Requests > ISE Root CA** in the Cisco ISE GUI.

Check certificate validity

If any certificate in the Cisco ISE Trusted Certificates or System Certificates store has expired, the upgrade fails.

Before you upgrade, follow these steps to check the validity of trusted certificates.

1. In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Management > Trusted Certificates**.
2. Check the **Expiration Date** field of the certificate. Renew the certificate if its validity has expired or is about to expire.

Similarly, follow these steps to check the validity of system certificates.

1. In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.
2. Check the **Expiration Date** field of the certificate. Renew the certificate if its validity has expired or is about to expire.

Update a certificate

Before upgrading to Cisco ISE release 3.5, replace any SHA1 certificates used for Admin services with certificates that use a secure algorithm, such as SHA256 or later. SHA1 is no longer supported for Admin services under the latest CiscoSSL security requirements. Update these certificates to ensure Admin services work correctly. Import SHA1 certificates only for other services, not for Admin services.

Delete a certificate

To delete an expired certificate, complete these steps:

- | | |
|---------------|--|
| Step 1 | In the Cisco ISE GUI, navigate to Administration > System > Certificates > Certificate Management > System Certificates . |
| Step 2 | Identify and select the certificate that has expired. |
| Step 3 | Click Delete to remove the selected certificate. |
| Step 4 | In the Cisco ISE GUI, navigate to Administration > System > Certificates > Certificate Management > Trusted Certificates . |
| Step 5 | Select the expired certificate. |
| Step 6 | Click Delete . |
| Step 7 | In the Cisco ISE GUI, navigate to Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates . |
| Step 8 | Select the expired certificate. |
| Step 9 | Click Delete . |

Export certificates from all nodes

Export all local certificates and their private keys from every node in your deployment to a secure location. Record the configuration for each certificate, including the service with which it is used.

- Step 1** In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Management > System Certificates**.
- Step 2** Select the certificate and click **Export**.
- Step 3** Select the **Export Certificate and Private Key** radio button.
- Step 4** Set a **Private Key Password** and then **Confirm Password**.
- Step 5** Click **Export**.

The local certificates and their private keys are downloaded to your system.

Export certificates from Trusted Certificates Store

Export all certificates from the Trusted Certificates Store of the PAN. Record the configuration for each certificate, including the service with which the certificate is used.

- Step 1** In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Management > Trusted Certificates**.
- Step 2** Select the certificate and click **Export**.

Disable automatic failover and scheduled backups for upgrade

You cannot perform deployment changes when running a backup in Cisco ISE. Disable automatic configurations to ensure your upgrade goes smoothly. You should disable these configurations before you upgrade Cisco ISE:

- PAN Automatic Failover: Disable this option in the PAN before upgrading Cisco ISE.
- Scheduled backups: Disable all backup schedules before upgrading. After the upgrade, reschedule and recreate the backup schedules.

Backups scheduled to run **once** are triggered every time the Cisco ISE application restarts. If you have a backup schedule set to run only once, disable it before upgrading.

Configure NTP server and verify availability

During upgrade, the Cisco ISE nodes reboot, migrate, and replicate data from the PAN to the SAN. 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 throughout the upgrade process.

Earlier versions of Cisco ISE use chrony instead of the 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 of less than 3 seconds. Therefore, we recommend that you use an NTP server with low root dispersion before upgrading to required Cisco ISE version to avoid NTP service disruption.

Upgrade your VM

Cisco ISE software must synchronize with both the chip and appliance capacity so that it can support the latest CPU and memory resources in UCS hardware.

As Cisco ISE versions progress,

- support for older hardware is phased out, and
- newer hardware is introduced.

It is recommended to upgrade your VM capacity to improve performance.

When planning VM upgrades, use OVA files to install the software efficiently. Each OVA file is a package that describes the VM and reserves the hardware resources required to install Cisco ISE software on your appliance.

For more information about the VM and hardware requirements, refer to "Hardware and Virtual Appliance Requirements for Cisco ISE" in the "[Cisco Secured Network Server Series Appliances and Virtual Machine Requirements](#)" chapter in the *Cisco ISE Installation Guide, Release 3.5*.

Cisco ISE VMs require dedicated resources in the VM infrastructure. These include an adequate number of CPU cores, comparable to hardware appliances, to ensure performance and scalability.

Resource sharing in the VM infrastructure can negatively impact performance. It may cause high CPU usage, delays in user authentication and registration, dropped logs, slow reporting, and reduced dashboard responsiveness.



Note

Use reserved resources for CPU, memory, and hard disk space during upgrades instead of shared resources to avoid performance issues.

The local disk allocation has increased to 29 GB for newer versions of Cisco ISE. Therefore, Cisco ISE requires a minimum disk size of 300 GB for each VM.

Record profiler configuration

If you use the Profiler service, record the profiler configuration for each PSN from the Admin portal.

Follow these steps to find the profiler configuration information:

1. In the Cisco ISE GUI, navigate to **Administration > System > Deployment**.
2. Select the node.
3. On the **Edit Node** page, go to the **Profiling Configuration** tab.
4. Note the configuration information or capture screenshots.

Obtain Active Directory and internal administrator account credentials

If you use Active Directory (AD) as your external identity source, make sure you have your AD credentials and a valid internal administrator account ready. After the upgrade, your AD connection might be lost. If that happens, use your Cisco ISE internal administrator account to log in to the Admin portal and use your Active Directory credentials to rejoin Cisco ISE to AD.

Activate Mobile Device Management vendor

If your deployment works with third-party Mobile Device Management (MDM) solutions, ensure that the MDM vendor status is active before upgrading.

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 these:

1. Enable the MDM server before upgrading.
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 more information, refer to “Create Repositories” in the “[Maintain and Monitor](#)” chapter in the *Cisco ISE Administrator Guide, Release 3.5*.

Perform these steps to create a repository and copy the upgrade bundle:

1. Place the upgrade bundle on the local disk to save time during the upgrade process. You can also use this command to copy and extract the upgrade bundle on the local disk:

```
application upgrade prepare <upgrade bundle name> <repository name>
```



Note

- Ensure your connection to the repository is fast and stable. If the upgrade bundle (about 14 GB) takes more than 35 minutes to download to the node, the process will time out.
- If you store configuration files on a local disk, these files are deleted during the upgrade. Create a Cisco ISE repository and copy them to the repository to keep your files.
- Choose a local repository near your nodes instead of one on a slow WAN link. Use FTP for faster performance and reliability.

2. Download the upgrade bundle from [Cisco.com](#).

To upgrade to Cisco ISE release 3.5, use this upgrade bundle: `ise-upgradebundle-3.2.x-3.4.x-to-3.5.0.<build#>.SPA.x86_64.tar.gz`

3. To perform the upgrade, copy the upgrade bundle to the Cisco ISE node local disk using this command:

```
copy repository_url/path/ise-upgradebundle-3.2.x-3.4.x-to-3.5.0.<build#>.SPA.x86_64.tar.gz disk:/
```

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

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-3.2.x-3.4.x-to-3.5.0.<build#>.SPA.x86_64.tar.gz disk:/**

`aaa.bbb.ccc.ddd` is the IP address or hostname of the SFTP server and

`ise-upgradebundle-3.2.x-3.4.x-to-3.5.0.<build#>.SPA.x86_64.tar.gz` is the name of the upgrade bundle.

Check the available disk space

Ensure that you allocate the required disk space for VMs. For more information, refer to "Disk space requirements for VMs in a Cisco ISE deployment" in [Cisco Secured Network Server Series Appliances and Virtual Machine Requirements](#) chapter in the *Cisco ISE Installation Guide, Release 3.5*.

If you need to increase the disk size, reinstall Cisco ISE and restore a configuration backup.

Check load balancer configuration

If you use a load balancer between the PAN and the PSN, set the session timeout on the load balancer high enough so it does not disrupt the upgrade process. A session timeout that is too short can interrupt the upgrade on PSNs. For instance, if a session ends during a database transfer from the PAN to a PSN, the upgrade on the PSN fails.

Resizing MnT hard disk

Upgrading does not require changes to the MnT disk capacity. If your logs consistently reach capacity and you need additional hardware resources, plan the MnT hard disk size based on your log retention needs. Log retention capacity has increased significantly over recent Cisco ISE releases.

You can activate collection filters to remove unnecessary logs from different devices. Excess logs may overwhelm your Cisco ISE MnT.

In the Cisco ISE GUI, navigate to **Administration > System > Logging > Collection filters**.

Refer to the Cisco ISE storage requirements on the [Cisco ISE Performance and Scalability community page](#). The table provides log retention information that is based on the number of endpoints for RADIUS and the number of network devices for TACACS+. Calculate log retention separately for TACACS+ and RADIUS.