Maintain and Monitor

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node. This service monitors and controls network access of endpoints. ANC is invoked by the ISE administrator on the admin GUI, and also can be invoked through pxGrid from third-party systems. ANC supports wired and wireless deployments and requires an Advantage License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint. As a result, the established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time. Also, there are no time constraints on the quarantine period length.

You can perform the following operations to monitor and control network access through ANC:

- Quarantine: Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.
- Unquarantine: Allows you to reverse the quarantine status that permits full access to the network for an endpoint. This happens by returning the endpoint to its original VLAN.
- Shutdown: Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shut down on the NAS to which an endpoint is connected, manually reset the port on the NAS again. This allows an endpoint to connect to the network, which is not available for wireless deployments.

Quarantine and unquarantine operations can be triggered from the session directory reports for active endpoints.

Note If a quarantined session is unquarantined, the initiation method for a newly unquarantined session depends on the authentication method that is specified by the switch configuration.

Enable Adaptive Network Control in Cisco ISE

ANC is disabled by default. ANC gets enabled only when pxGrid is enabled, and it remains enabled until you manually disable the service in the Admin portal.

Configure Network Access Settings

ANC allows you to reset the network access status of an endpoint to quarantine, unquarantine, or shut down a port. These define the degree of authorization for the endpoints in the network.

You can quarantine or unquarantine endpoints, or shut down the network access server (NAS) ports to which endpoints are connected, by using their endpoint IP addresses or MAC addresses. You can perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously. If you discover a hostile endpoint on your network, you can shut down the endpoint's access, using ANC to close the NAS port.

To assign an ANC policy to an endpoint:

Before you begin

- Enable ANC.
- Create authorization profiles and exception type authorization policies for ANC.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Adaptive Network Control** > **Policy List**.

Step 2 Click **Add**.

Step 3 Enter a name for the ANC policy and specify the ANC action. The following options are available:

- Quarantine
- Shut_Down
- Port_Bounce

You can select one or multiple actions, but you cannot combine Shut_Down and Port_Bounce with the other ANC actions .

Quarantine and Re_Authenticate are the only two actions that can be combined.

When an ANC policy with Quarantine, Port_Bounce, or Re_Authenticate is assigned or unassigned to an active endpoint, a CoA is triggered for that endpoint.

When an ANC policy with Shut_Down action is assigned to an active endpoint, a CoA is triggered to shutdown the switch interface. However, CoA is not triggered when an ANC policy with Shut_Down action is unassigned.

Step 4 Choose **Policy > Policy Sets**, and expand the policy set.

Step 5 Associate the ANC policy with the corresponding authorization policy by using the ANCPolicy attribute.

Step 6 Choose **Operations > Adaptive Network Control > Endpoint Assignment**.

Step 7 Click **Add**.

Step 8 Enter the IP address or MAC address of the endpoint and select the policy from the **Policy Assignment** drop-down list.

Step 9 Click **Submit**.

Create Authorization Profiles for Network Access through ANC

You need to create an authorization profile that should be use with ANC. you can view the authorization profile in the list of Standard Authorization Profiles. An endpoint can be authenticated and authorized in the network, but restricted to access network.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Policy** > **Policy Elements** > **Authorization** > **Authorization Profiles**.

Step 2 Click **Add**.

Step 3 Enter a unique name and description for the authorization profile, and update the **Access Type** as **ACCESS_ACCEPT**.

Step 4 Check the **DACL Name** check box, and choose **DENY_ALL_TRAFFIC** from the drop-down list.

Step 5 Click **Submit**.

Exception authorization polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. For ANC authorization, you need to create a quarantine exception policy that is processed before all standard authorization policies. You need to create an exception rule with the following condition:

Session:ANCPolicy EQUALS Quarantine.

ANC NAS Port Shutdown Flow

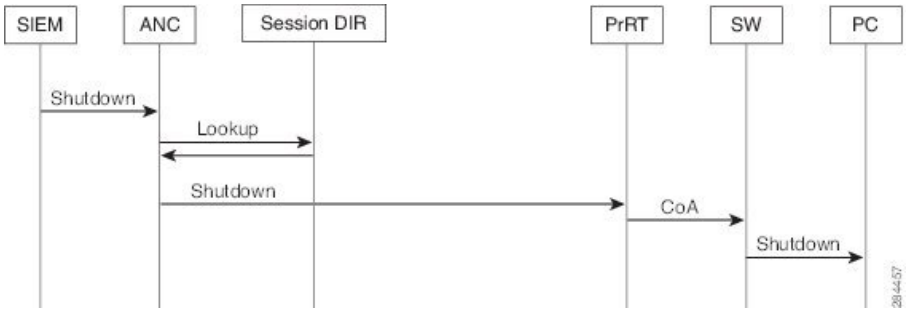
You can shut down the NAS port to which an endpoint is connected by using the endpoint IP address or MAC address.

Shutdown allows you to close a NAS port based on a specified IP address for a MAC address. You have to manually reinstate the port to bring the endpoint back into the network, which is effective only for endpoints that are connected through wired media.

Shutdown may not be supported on all devices. Most switches should support the shutdown command, however. You can use the getResult() command to verify that the shutdown is executed successfully.

This figure illustrates the ANC shutdown flow. For the client device, the shutdown operation is performed on the NAS that the client device uses to access the network.

Figure 1: ANC Shutdown Flow



Endpoints Purge Settings

You can define the endpoint purge policy by configuring rules, based on identity groups and other conditions. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **Identity Management** > **Settings** > **Endpoint Purge**. You can choose not to purge specified endpoints and to purge endpoints based on selected profiling conditions.

You can schedule an endpoint purge job. This endpoint purge schedule is enabled by default. Cisco ISE, by default, deletes endpoints and registered devices that are older than 30 days. The purge job runs at 1:00 a.m. (midnight) every day based on the time zone configured in the primary PAN.

Endpoint purge deletes over five thousand endpoints every 3 minutes.

The following are some of the conditions with examples you can use for purging the endpoints:

- InactivityDays— Number of days since last profiling activity or update on endpoint
  - This condition purges stale devices that have accumulated over time, commonly transient guest or personal devices, or retired devices. These endpoints tend to represent noise in your deployment as they are no longer active on network or not likely to be seen in near future. If they do happen to connect again, then they will be rediscovered, profiled, registered, etc as needed.
  - When there are updates from endpoint, InactivityDays will be reset to 0 only if profiling is enabled.
- ElapsedDays—Numbers days since object is created.
  - This condition can be used for endpoints that have been granted unauthenticated or conditional access for a set time period, such as a guest or contractor endpoint, or employees leveraging webauth for network access. After the allowed connect grace period, they must be fully reauthenticated and registered.
- PurgeDate—Date to purge the endpoint.
  - This option can be used for special events or groups where access is granted for a specific time, regardless of creation or start time. This allows all endpoints to be purged at same time. For example, a trade show, a conference, or a weekly training class with new members each week, where access is granted for specific week or month rather than absolute day, week, or month.

Note If the endpoint count to be purged is more than 10000, only the first 10000 endpoints are purged during the initial purge. After 1 hour, another purge is initiated to delete the next set of 10000 endpoints. This purge cycle will continue until all the endpoints are purged based on purge condition that is matched. This behavior optimizes system performance.

Quarantined Endpoints Do Not Renew Authentication Following Policy Change

Problem

Authentication has failed following a change in policy or additional identity and no reauthentication is taking place. Authentication fails or the endpoint in question remains unable to connect to the network. This issue often occurs on client machines that fails posture assessment per the posture policy that is assigned to the user role.

Possible Causes

The authentication timer setting is not correctly set on the client machine, or the authentication interval is not correctly set on the switch.

Solution

There are several possible resolutions for this issue:

1. Check the **Session Status Summary** report in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured.
2. Enter “show running configuration” on the NAD/switch and ensure that the interface is configured with an appropriate “authentication timer restart” setting. (For example, “authentication timer restart 15,” and “authentication timer reauthenticate 15.”)
3. Enter “interface shutdown” and “no shutdown” to bounce the port on the NAD/switch and force reauthentication following a potential configuration change in Cisco ISE.

Note Because CoA requires a MAC address or session ID, we recommend that you do not bounce the port that is shown in the Network Device SNMP report.

ANC Operations Fail when IP Address or MAC Address is not Found

An ANC operation that you perform on an endpoint fails when an active session for that endpoint does not contain information about the IP address. This also applies to the MAC address and session ID for that endpoint.

Note When you want to change the authorization state of an endpoint through ANC, you must provide the IP address or the MAC address for the endpoint. If the IP address or the MAC address is not found in the active session for the endpoint, then you will see the following error message:

```
No active session found for this MAC address, IP Address or Session ID
```

.

Externally Authenticated Administrators Cannot Perform ANC Operations

If an externally authenticated administrator tries to issue CoA-Quarantine from a live session, Cisco ISE returns the following error message:

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User
 not found internally. Possible use of unsupported externally authenticated user
```

If an externally authenticated administrator performs an ANC operation from **Operations** in the Cisco ISE using the IP address or MAC address of the endpoint, Cisco ISE returns the following error message:

```
Server failure: User not found internally. Possible use of unsupported externally
 authenticated user
```

Backup Data Type

Cisco ISE allows you to back up data from the primary PAN and from the Monitoring node. Backup can be done from the CLI or user interface.

Cisco ISE allows you to back up the following type of data:

- Configuration data—Contains both application-specific and Cisco ADE operating system configuration data. Backup can be done via the primary PAN using the GUI or CLI.
- Operational Data—Contains monitoring and troubleshooting data. Backup can be done via the primary PAN GUI or using the CLI for the Monitoring node.

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

Note Cisco ISE does not support VMware snapshots for backing up ISE data because a VMware snapshot saves the status of a VM at a given point in time. In a multinode Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. We recommend that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots or any third-party backup service to back up Cisco ISE data might result in interrupting Cisco ISE services. When a backup is initiated by VMware or any other third-party backup service like CommVault SAN level backup, it quiesces the file system to maintain crash consistency, which can cause your Cisco ISE functionalities to freeze. A reboot is required to resume the services on your Cisco ISE deployment.

The restore operation can be performed with the backup files of previous versions of Cisco ISE and restored on a later version, as long as the previous versions are in the supported direct upgrade path for the later version.

Cisco ISE, Release 3.0 supports restore from backups obtained from Release 2.4 and later.

Note While recreating a deployment after backing up and restoring data, a **Context Visibility Reset** of both the Primary PAN and Secondary PAN are required to ensure that data on both the nodes are synced.

Backup and Restore Repositories

Cisco ISE allows you to create and delete repositories through the administrator portal. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

Note Repositories are local to each device.

We recommend that you have a repository size of minimum 100 GB for all types of deployment (small, medium, and large).

The following table shows the supportability information between the Cisco ISE operations and the type of external repositories:

Table 1: Supportability Matrix for External Repositories

Repository Type	Config Backup	Config Restore	Upgrade	Operational Backup	Operational Restore	Support Bundle	Validation from the User Interface	Exporting Reports from the User Interface	Exporting Policies from the User Interface
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	X	X	X	X	X	X	X	X	X
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

Create Repositories

You can use the CLI and GUI to create repositories. We recommend that you use the GUI due to the following reasons:

- Repositories that are created through the CLI are saved locally and do not get replicated to the other deployment nodes. These repositories do not get listed in the GUI's repository page.
- Repositories that are created on the primary PAN get replicated to the other deployment nodes.

The keys are generated only at the primary PAN on GUI, and so during upgrade you need to generate the keys again at GUI of new primary admin and export it to the SFTP server. If you remove the nodes from your deployment, you need to generate the keys on GUI of non-admin nodes and export it to the SFTP server.

You can configure an SFTP repository in Cisco ISE with RSA public key authentication. Instead of using an administrator-created password to encrypt the database and logs, you can choose the RSA public key authentication that uses secure keys. In case of SFTP repository created with RSA public key, the repositories created through the GUI do not get replicated in the CLI and the repositories created through the CLI do not get replicated in the GUI. To configure same repository on the CLI and GUI, generate RSA public keys on both CLI and GUI and export both the keys to the SFTP server.

Note Cisco ISE initiates outbound SSH or SFTP connections in FIPS mode even if FIPS mode is not enabled on ISE. Ensure that the remote SSH or SFTP servers that communicate with ISE allow FIPS 140 approved cryptographic algorithms.

Cisco ISE uses embedded FIPS 140 validated cryptographic modules. For details of the FIPS compliance claims, see the FIPS Compliance Letter.

Before you begin

- To perform the following task, you must have the privileges of either a Super Admin or System Admin.

- If you want to create an SFTP repository with RSA public key authentication, perform the following steps:
  - Enable RSA public key authentication in the SFTP repository.
  - You must log in as the Admin CLI user. Enter the host key of the SFTP server from the Cisco ISE CLI using the **crypto host_key add** command. The host key string should match the hostname that you enter in the **Path** field of the repository configuration page.
  - Generate the key pairs and export the public key to your local system from the GUI. From the Cisco ISE CLI, generate the key pairs using the **crypto key generate rsa passphrase** *test123* command, where, passphrase must be greater than four letters, and export the keys to any repository (local disk or any other configured repository).
  - Copy the exported RSA public key to the PKI-enabled SFTP server and add it to the "authorized_keys" file.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Repository**.

Step 2 Click **Add** to add a new repository.

Step 3 Enter the values as required to set up new repository. See Repository Settings, on page 10 for a description of the fields.

Step 4 Click **Submit** to create the repository.

Step 5 Verify that the repository is created successfully by clicking **Repository** from the **Operations** navigation pane on the left or click the **Repository List** link at the top of **Repository** window to go to the repository listing page.

What to do next

- Ensure that the repository that you have created is valid. You can do so from the **Repository Listing** window. Select the corresponding repository and click **Validate**. Alternatively, you can execute the following command from the Cisco ISE command-line interface:

  show repository *repository_name*

  where *repository_name* is the name of the repository that you have created.

Note If the path that you provided while creating the repository does not exist, then you will get the following error:

```
%Invalid Directory
```

- Run an on-demand backup or schedule a backup.

Repository Settings

The following table describes the fields on the **Repository List** window, which you can use to create repositories to store your backup files. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Maintenance** > **Repository**.

Table 2: Repository Settings

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Server Name	(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IP address (IPv4 or IPv6) of the server where you want to create the repository. **Note** Ensure that the ISE eth0 interface is configured with an IPv6 address if you are adding a repository with an IPv6 address.
Path	Enter the path to your repository. The path must be valid and must exist at the time you create the repository. This value can start with two forward slashes (//) or a single forward slash (/) denoting the root directory of the server. However, for the FTP protocol, a single forward slash (/) denotes the FTP of the local device home directory and not the root directory.
Enable PKI authentication	(Optional; applicable only for SFTP repository) Check this check box if you want to enable RSA Public Key Authentication in SFTP repository.
User Name	(Required for FTP, SFTP) Enter the username that has write permission to the specified server. A username can contain alphanumeric and _-. /@\$ characters.
Password	(Required for FTP, SFTP) Enter the password that will be used to access the specified server. Passwords can consist of the following characters: 0 to 9, a to z, A to Z, -, ., |, @, #,$, ^, &, *, (,), +, and =.

Related Topics

Backup and Restore Repositories, on page 8
Create Repositories, on page 9

Enable RSA Public Key Authentication in SFTP Repository

In the SFTP server, each node must have two RSA public keys, one each for CLI and for GUI. To enable RSA public key authentication in SFTP repository, perform the following steps:

Note After you enable RSA public key authentication in SFTP repository, you will not be able to log in using SFTP credentials. You can either use PKI-based authentication or credential-based authentication. If you want to use credential-based authentication again, you must remove the public key pair from the SFTP server.

Step 1 Log in to SFTP server with an account that has permission to edit the */etc/ssh/sshd_config.file*.

Note The location of the *sshd_config* file might vary based on the operating system installation.

Step 2 Enter the **vi /etc/ssh/sshd_config** command.

The contents of the sshd_config file is listed.

Step 3 Remove the "#" symbol from the following lines to enable RSA public key authentication:

- RSAAuthentication yes
- PubkeyAuthentication yes

  Note If Public Auth Key is no, change it to yes.

- AuthorizedKeysFile ~/.ssh/authorized_keys

On-Demand and Scheduled Backups

You can configure on-demand backups of the primary PAN and the primary monitoring node. Perform an on-demand backup when you want to back up data immediately.

You can schedule system-level backups to run once, daily, weekly, or monthly. Because backup operations can be lengthy, you can schedule them so they are not a disruption. You can schedule a backup from the Admin portal.

Note If you are using the internal CA, you should use the CLI to export certificates and keys. Backup using in the administration portal does not back up the CA chain.

For more information, see the "Export Cisco ISE CA Certificates and Keys" section in the "Basic Setup" chapter *Cisco Identity Services Engine Administrator Guide* .

Configurational and operational backups on Cisco ISE can overload your system for a short time. This expected behaviour of temporary system overload will depend on the configuration and monitoring database size of your system.

Related Topics

Maintenance Settings

Perform an On-Demand Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE to the configuration state that existed at the time of obtaining the backup.

Important When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you have to choose from one of these options to avoid errors:

- **Option 1:**

  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.

  Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA.

  Pros: This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system continues to be trusted.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Before you begin

- Before you perform an on-demand backup, you should have a basic understanding of the backup data types in Cisco ISE.
- Ensure that you have created repositories for storing the backup files.
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- Ensure that you perform all certificate-related changes before you obtain the backup.
- To perform the following task, you must be a Super Admin or System Admin.

Note For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing. To restore a backup, choose the repository and click **Restore**.

Step 1 Choose **Administration** > **System** > **Backup and Restore**.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Step 3 Choose the type of backup: Configuration or Operational.

Step 4 Click **Backup Now**.

Step 5 Enter the values as required to perform a backup.

Step 6 Click **Backup**.

Step 7 Verify that the backup completed successfully.

Cisco ISE appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository.

In a distributed deployment, do not change the role of a node or promote a node when the backup is running. Changing node roles does not 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.

Do not promote a node when the backup is running. This 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 changes.

Note High CPU usage might be observed and High Load Average alarm might be seen when the backup is running. CPU usage will be back to normal when the backup is complete.

Related Topics

Cisco ISE Restore Operation, on page 18
Export Authentication and Authorization Policy Configuration, on page 23

On-Demand Backup Settings

The following table describes the fields on the **On-Demand Backup** window, which you can use to obtain a backup at any point of time. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup & Restore**.

Table 3: On-Demand Backup Settings

Field Name	Usage Guidelines
Type	Choose one of the following: • **Configuration Data Backup**: Includes both application-specific and Cisco ADE operating system configuration data • **Operational Data Backup**: Includes monitoring and troubleshooting data
Backup Name	Enter the name of your backup file.
Repository Name	Repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	This key is used to encrypt and decrypt the backup file.

Related Topics

Backup Data Type, on page 7
On-Demand and Scheduled Backups, on page 12
Backup History, on page 17
Backup Failures, on page 17
Cisco ISE Restore Operation, on page 18
Export Authentication and Authorization Policy Configuration, on page 23
Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 25
Perform an On-Demand Backup, on page 12

Schedule a Backup

You can perform an On-demand backup to instantly back up the configuration or monitoring (operational) data. The restore operation restores Cisco ISE to the configuration state that existed at the time of obtaining the backup.

Important When performing a back up and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a back up and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**

  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.

  Pros: Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**

  After the restore process, generate all new certificates for the internal CA.

  Pros: This option is the recommended and clean method, where the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.

  Cons: Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

Before you begin

- Before you schedule a backup, you should have a basic understanding of the backup data types in Cisco ISE.
- Ensure that you have configured repositories.

- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.

Note For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

Scheduled Backup Settings

The following table describes the fields on the Scheduled Backup window, which you can use to restore a full or incremental backup. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Table 4: Scheduled Backup Settings

Field Name	Usage Guidelines
Type	Choose one of the following: • **Configuration Data Backup**: Includes both application-specific and Cisco ADE operating system configuration data • **Operational Data Backup**: Includes monitoring and troubleshooting data
Name	Enter a name for your backup file. You can enter a descriptive name of your choice. Cisco ISE appends the timestamp to the backup filename and stores it in the repository. You will have unique backup filenames even if you configure a series of backups. On the Scheduled Backup list window, the backup filename will be prepended with "backup_occur" to indicate that the file is an occurrence **kron** job.
Description	Enter a description for the backup.
Repository Name	Select the repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	Enter a key to encrypt and decrypt the backup file.
Schedule Options	Choose the frequency of your scheduled backup and fill in the other options accordingly.

Related Topics

Backup Data Type, on page 7
On-Demand and Scheduled Backups, on page 12
Backup History, on page 17
Backup Failures, on page 17
Cisco ISE Restore Operation, on page 18
Export Authentication and Authorization Policy Configuration, on page 23

Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 25
Backup Using the CLI, on page 17
Schedule a Backup, on page 15

Backup Using the CLI

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI. However, you can perform operational backup on the secondary monitoring node only from the CLI.

Backup History

Backup history provides basic information about scheduled and on-demand backups. It lists the name of the backup, backup file size, repository where the backup is stored, and time stamp that indicates when the backup was obtained. This information is available in the Operations Audit report and on the Backup and Restore page in the History table.

For failed backups, Cisco ISE triggers an alarm. The backup history page provides the failure reason. The failure reason is also cited in the Operations Audit report. If the failure reason is missing or is not clear, you can run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

While the backup operation is in progress, you can use the **show backup status** CLI command to check the progress of the backup operation.

Backup history is stored along with the Cisco ADE operating system configuration data. It remains there even after an application upgrade and are only removed when you reimage the PAN.

Backup Failures

If backup fails, check the following:

- Check if there is any NTP sync or service failure issue. When the NTP service on Cisco ISE is not working, Cisco ISE raises the NTP Service Failure alarm. When Cisco ISE cannot sync with all the configured NTP servers, Cisco ISE raises the NTP Sync Failure alarm. Cisco ISE backup might fail if the NTP services are down or if there is any sync issue. Check the Alarms dashlet and fix the NTP sync or service issue before you retry the backup operation.
- Make sure that no other backup is running at the same time.
- Check the available disk space for the configured repository.
    - Monitoring (operational) backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your Monitoring node is allocated 600 GB, and the monitoring data takes up more than 450 GB of storage, then monitoring backup fails.
    - If the database disk usage is greater than 90%, a purge occurs to bring the database size to less than or equal to 75% of its allocated size.
- Verify if a purge is in progress. Backup and restore operations will not work while a purge is in progress.
- Verify if the repository is configured correctly.

Cisco ISE Restore Operation

You can restore configuration data on a primary or standalone administration node. After you restore data on the Primary PAN, you must manually synchronize the secondary nodes with the Primary PAN.

The process for restoring the operational data is different depending on the type of deployment.

Note The new backup/restore user interface in Cisco ISE makes use of meta-data in the backup filename. Therefore, after a backup completes, you should not modify the backup filename manually. If you manually modify the backup filename, the Cisco ISE backup/restore user interface will not be able to recognize the backup file. If you have to modify the backup filename, you should use the Cisco ISE CLI to restore the backup.

Guidelines for Data Restoration

Following are guidelines to follow when you restore Cisco ISE backup data.

- 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 host names (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.
- If you obtain a backup from the Primary PAN in one timezone and try to restore it on another Cisco ISE node in another timezone, the restore process might fail. This failure happens if the timestamp in the backup file is later than the system time on the Cisco ISE node on which the backup is restored. If you restore the same backup a day after it was obtained, then the timestamp in the backup file is in the past and the restore process succeeds.
- When you restore a backup on the Primary PAN with a different hostname than the one from which the backup was obtained, the Primary PAN becomes a standalone node. The deployment is broken and the secondary nodes become nonfunctional. You must make the standalone node the primary node, reset the configuration on the secondary nodes, and reregister them with the primary node. To reset the configuration on Cisco ISE nodes, enter the following command from the Cisco ISE CLI:
  - **application reset-config ise**
- We recommend that you do not change the system timezone after the initial Cisco ISE installation and setup.
- If you changed the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data from the standalone Cisco ISE node or Primary PAN. Otherwise, if you try to restore data using an older backup, the communication between the nodes might fail.
- After you restore the configuration backup on the Primary PAN, you can import the Cisco ISE CA certificates and keys that you exported earlier.

Note If you did not export the Cisco ISE CA certificates and keys, then after you restore the configuration backup on the Primary PAN, generate the root CA and subordinate CAs on the Primary PAN and Policy Service Nodes (PSNs).

- If you are trying to restore a platinum database without using the correct FQDN (FQDN of a platinum database), you need to regenerate the CA certificates. (To view this window, click the **Menu** icon (☰) and choose **Administration** > **Certificates** > **Certificate Signing Requests** > **Replace ISE Root CA certificate chain**).However, If you restore the platinum database with the correct FQDN, note that the CA certificates regenerated automatically.
- You need a data repository, which is the location where Cisco ISE saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.
- If you have a standalone administration node that fails, you must run the configuration backup to restore it. If the Primary PAN fails, you can use the distributed setup to promote your Secondary Administration Node to become the primary. You can then restore data on the Primary PAN after it comes up.

Note Cisco ISE also provides the **backup-logs** CLI command that you can use to collect log and configuration files for troubleshooting purposes.

Restoration of Configuration or Monitoring (Operational) Backup from the CLI

To restore configuration data through the Cisco ISE CLI, use the **restore** command in the EXEC mode. Use the following command to restore data from a configuration or operational backup:

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

Syntax Description

restore	Type this command to restore data from a configuration or operational backup.
filename	Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. **Note** You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository	Specifies the repository that contains the backup.
repository-name	Name of the repository you want to restore the backup from.
encryption-key	(Optional) Specifies user-defined encryption key to restore backup.
hash	Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.
encryption-key name	Enter the encryption key.
include-adeos	(Optional, applicable only for configuration backup) Enter this command operator parameter if you want to restore ADE-OS configuration from a configuration backup. When you restore a configuration backup, if you do not include this parameter, Cisco ISE restores only the Cisco ISE application configuration data.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you use restore commands in Cisco ISE, the Cisco ISE server restarts automatically.

The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the **restore** command without the encryption key.

Examples

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
 Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

Related Commands

	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.
show backup status	Displays the status of the backup operation.
show restore status	Displays the status of the restore operation.

If the sync status and replication status after application restore for any secondary node is *Out of Sync*, you have to reimport the certificate of that secondary node to the Primary PAN and perform a manual synchronization.

Restore Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal.

Before you begin

Ensure that the primary PAN Auto Failover configuration, if enabled in your deployment, is turned off. When you restore a configuration backup, the application server processes are restarted. There might be a delay while these services restart. Due to this delay in restart of services, auto failover of secondary PAN might get initiated.

When your deployment is a dual node deployment at the time configuration backup, ensure the following:

- Source and target nodes for the restore are same as the ones used for the configuration backup, the target node can be either stand-alone or primary.
- Source and target nodes for the restore are different from the ones used in the configuration backup, the target node must be stand-alone.

Note You can restore configuration database backup and regenerate the Root CA on a primary PAN only. However, you cannot restore the configuration database backup on a registered PAN.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Step 2 Select the name of the backup from the list of Configurational backup and click **Restore**.

Step 3 Enter the Encryption Key used during the backup.

Step 4 Click **Restore**.

What to do next

If you are using the Cisco ISE CA service, you must:

1. Regenerate the entire Cisco ISE CA root chain.
2. Obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. This ensures that the secondary PAN can function as the root CA or subordinate CA of an external PKI in case of a Primary PAN failure and you promote the secondary PAN to be the primary PAN.

Restoration of Monitoring Database

The process for restoring the Monitoring database is different depending on the type of deployment. The following sections explain how to restore the Monitoring database in standalone and distributed deployments.

You must use the CLI to restore an on-demand Monitoring database backup from previous releases of Cisco ISE. Restoring a scheduled backup across Cisco ISE releases is not supported.

Note If you attempt to restore data to a node other than the one from which the data was taken, you must configure the logging target settings to point to the new node. This ensures that the monitoring syslogs are sent to the correct node.

Restore a Monitoring (Operational) Backup in a Standalone Environment

The GUI lists only the backups that are taken from the current release. To restore backups that obtained from earlier releases, use the restore command from the CLI.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

Step 1 Choose **Administration** > **System** > **Backup and Restore**.

Step 2 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore**.

Step 3 Select the name of the backup from the list of Operational backup and click **Restore**.

Step 4 Enter the Encryption Key used during the backup.

Step 5 Click **Restore**.

Restore a Monitoring Backup with Administration and Monitor Personas

You can restore a Monitoring backup in a distributed environment with administration and monitor personas.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

Step 1 If you are using a primary and secondary PAN, synchronize the PANs.

When you synchronize the PANs, you must chose a PAN and promote that to be the active primary.

Step 2 Before you deregister the Monitoring node, assign the Monitoring persona to another node in the deployment.

Every deployment must have at least one functioning Monitoring node.

Step 3 Deregister the Monitoring node for backup.

Step 4 Restore the Monitoring backup to the newly deregistered node.

Step 5 Register the newly restored node with the current Administration node.

Step 6 Promote the newly restored and registered node as the active Monitoring node.

Restore a Monitoring Backup with a Monitoring Persona

You can restore a Monitoring backup in a distributed environment with only Monitoring persona.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

Step 1 Prepare to deregister the node to be restored. This is done by assigning the monitoring persona to another node in the deployment.

A deployment must have at least one functioning Monitoring node.

Step 2 Deregister the node to be restored.

Note Wait until the deregistration is complete before proceeding with the restore. The node must be in a standalone state before you can continue with the restore.

Step 3 Restore the Monitoring backup to the newly deregistered node.

Step 4 Register the newly restored node with the current Administration node.

Step 5 Promote the newly restored and registered node as the active Monitoring node.

Restore History

You can obtain information about all restore operations, log events, and statuses from the **Operations Audit Report** window.

Note However, the **Operations Audit Report** window does not provide information about the start times corresponding to the previous restore operations.

For troubleshooting information, you have to run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log file.

While the restore operation is in progress, all Cisco ISE services are stopped. You can use the **show restore status** CLI command to check the progress of the restore operation.

Export Authentication and Authorization Policy Configuration

You can export authentication and authorization policy configuration in the form of an XML file that you can read offline to identify any configuration errors and use for troubleshooting purposes. This XML file includes authentication and authorization policy rules, simple and compound policy conditions, Discretionary Access

control Lists (DACLs), and authorization profiles. You can choose to email the XML file or save it to your local system.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup & Restore**.

Step 2 Click **Policy Export**.

Step 3 Enter the values as needed.

Step 4 Click **Export**.

Use a text editor such as WordPad to view the contents of the XML file.

Schedule Policy Export Settings

The following table describes the fields on the **Schedule Policy Export** window. To view this window, click the **Menu** icon (☰) and choose **Administration** > **System** > **Backup and Restore** > **Policy Export**.

Table 5: Schedule Policy Export Settings

Field Name	Usage Guidelines
Encryption	
Encryption Key	Enter a key to encrypt and decrypt the export data. This field is enabled only if you select the **Export with Encryption Key** option.
Destination	
Download file to local computer	Allows you to download the policy export file to your local system.
Email file to	You can enter multiple email addresses separated by a comma.
Repository	Select the repository to export policy data to. You can't enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before scheduling a policy export.
Export Now	Click this option to export the data to the local computer or send as an email attachment. You can't export to a repository; you can only schedule a repository export.
Schedule	
Schedule Options	Choose the frequency of the export schedule and enter the other details accordingly.

Synchronize Primary and Secondary Nodes in a Distributed Environment

In a distributed environment, sometimes the Cisco ISE database in the primary and secondary nodes are not synchronized automatically after restoring a backup file on the PAN. If this happens, you can manually force a full replication from the PAN to the secondary ISE nodes. You can force a synchronization only from the PAN to the secondary nodes. During the sync-up operation, you cannot make any configuration changes. Cisco ISE allows you to navigate to other Cisco ISE Admin portal pages and make any configuration changes only after the synchronization is complete.

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**.

Step 2 Check the check boxes next to the secondary ISE nodes with an Out of Sync replication status.

Step 3 Click **Syncup** and wait until the nodes are synchronized with the PAN. You will have to wait until this process is complete before you can access the Cisco ISE Admin portal again.

Recovery of Lost Nodes in Standalone and Distributed Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and distributed deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data.

Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to a loss of all the nodes. After recovery, you want to use the existing IP addresses and hostnames.

For example, you have two nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Administration Node or Secondary PAN.) A backup of the N1 node, which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster.

Assumption

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged using the same hostnames and IP addresses.

Resolution Steps

1. You have to replace both the N1 and N2 nodes. N1 and N2 nodes will now have a standalone configuration.
2. Obtain a license with the UDI of the N1 and N2 nodes and install it on the N1 node.
3. You must then restore the backup on the replaced N1 node. The restore script will try to sync the data on N2, but N2 is now a standalone node and the synchronization fails. Data on N1 will be reset to time T1.
4. You must log in to the N1 Admin portal to delete and reregister the N2 node. Both the N1 and N2 nodes will have data reset to time T1.

Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to loss of all the nodes. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

For example, you have two ISE nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Policy Service Node.) A backup of the N1 node which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster. The Cisco ISE nodes are replaced at a new location and the new hostnames are N1A (primary PAN) and N2A (secondary Policy Service Node). N1A and N2A are standalone nodes at this point in time.

Assumptions

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged at a different location using different hostnames and IP addresses.

Resolution Steps

1. Obtain the N1 backup and restore it on N1A. The restore script will identify the hostname change and domain name change, and will update the hostname and domain name in the deployment configuration based on the current hostname.
2. You must generate a new self-signed certificate.
3. You must log in to the Cisco ISE administrator portal on N1A.In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment**, and do the following:

   Delete the old N2 node.

   Register the new N2A node as a secondary node. Data from the N1A node will be replicated to the N2A node.

Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database was taken at time T1. The N1 node goes down because of a physical failure and must be reimaged or a new hardware is required. The N1 node must be brought back up with the same IP address and hostname.

Assumptions

This deployment is a standalone deployment and the new or reimaged hardware has the same IP address and hostname.

Resolution Steps

Once the N1 node is up after a reimage or you have introduced a new Cisco ISE node with the same IP address and hostname, you must restore the backup taken from the old N1 node. You do not have to make any role changes.

Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database taken at time T1 is available. The N1 node is down because of a physical failure and will be replaced by a new hardware at a different location with a different IP address and hostname.

Assumptions

This is a standalone deployment and the replaced hardware has a different IP address and hostname.

Resolution Steps

1. Replace the N1 node with a new hardware. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. No role changes are required.

Configuration Rollback

Problem

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. For example, you may delete several NADs or modify some RADIUS attributes incorrectly and

realize this issue several hours later. In this case, you can revert to the original configuration by restoring a backup that was taken before you made the changes.

Possible Causes

There are two nodes: N1 (primary Policy Administration Node or primary PAN) and N2 (secondary Policy Administration Node or secondary PAN) and a backup of the N1 node is available. You made some incorrect configuration changes on N1 and want to remove the changes.

Solution

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. The restore script will synchronize the data from N1 to N2.

Recovery of Primary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, the PAN fails.

For example, you have two Cisco ISE nodes, N1 (PAN) and N2 (Secondary Administration Node). N1 fails because of hardware issues.

Assumptions

Only the primary node in a distributed deployment has failed.

Resolution Steps

1. Log in to the N2 administrator portal. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Deployment** and configure N2 as your primary node.

   The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 administrator portal, register the new N1 node as a secondary node.

   Now, the N2 node becomes your primary node and the N1 node becomes your secondary node.

If you wish to make the N1 node the primary node again, log in to the N1 administrator portal and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

Recovery of Secondary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, a single secondary node has failed. No restore is required.

For example, you have multiple nodes: N1 (primary PAN), N2 (secondary PAN), N3 (secondary Policy Service Node), N4 (secondary Policy Service Node). One of the secondary nodes, N3, fails.

Resolution Steps

1. Reimage the new N3A node to the default standalone state.

2. Log in to the N1 Admin portal and delete the N3 node.
3. Reregister the N3A node.

   Data is replicated from N1 to N3A. No restore is required.

Cisco ISE Logging Mechanism

Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

You can configure a Cisco ISE node to collect the logs in the local systems using a virtual loopback address. To collect logs externally, you configure external syslog servers, which are called targets. Logs are classified into various predefined categories. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

As a best practice, do not configure network devices to send syslogs to a Cisco ISE Monitoring and Troubleshooting (MnT) node as this could result in the loss of some Network Access Device (NAD) syslogs, and overloads the MnT servers resulting in loading issues. If NAD Syslogs are configured to be sent directly to MnT, session management functionality would break. NAD syslogs can be directed to external syslog servers for troubleshooting but should not be directed to MnT.

The Process Down alarm is no longer triggered when ISE Messaging Service fails on a node. When ISE Messaging Service fails on a node, all the syslogs and the Process Down alarm will be lost until the messaging service is brought back up on that node.

In this case, an administrator must look for the **Queue Link Error** alarm that will be listed in the **Alarms** dashlet on the Cisco ISE **Home** window. Click on the alarm, and a new window will open with a **Suggested Actions** section. Follow these instructions to resolve the issue.

Note If the Monitoring node is configured as the syslog server for a network device, ensure that the logging source sends the correct network access server (NAS) IP address in the following format:

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

Otherwise, this might impact functionalities that depend on the NAS IP address.

Configure Syslog Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Local Log Settings**.

Step 2 In the **Local Log Storage Period** field, enter the maximum number of days to keep the log entries in the configuration source.

Logs may be deleted earlier than the configured **Local Log Storage Period** if the size of the localStore folder reaches 97 GB.

Step 3 Click **Delete Logs Now** to delete the existing log files at any time before the expiration of the storage period.

Step 4 Click **Save**.

Cisco ISE System Logs

In Cisco ISE, system logs are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer them to an external server. Cisco ISE has the following default targets, which are dynamically configured in the loopback addresses of the local system:

- LogCollector—Default syslog target for the Log Collector.
- ProfilerRadiusProbe—Default syslog target for the Profiler Radius Probe.

By default, AAA Diagnostics subcategories and System Diagnostics subcategories logging targets are disabled during a fresh Cisco ISE installation or an upgrade to reduce the disk space. You can configure logging targets manually for these subcategories but local logging for these subcategories are always enabled.

You can use the default logging targets that are configured locally at the end of the Cisco ISE installation or you can create external targets to store the logs.

Note If a syslog server is configured in a distributed deployment, syslog messages are sent directly from the authenticating PSNs to the syslog server and not from the MnT node.

Related Topics

Cisco ISE Message Codes, on page 31

Configure Remote Syslog Collection Locations

You can use the web interface to create remote syslog server targets to which system log messages are sent. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP.

A message is generated when an event occurs. An event may be one that displays a status, such as a message displayed when exiting a program, or an alarm. There are different types of event messages generated from multiple facilities such as the kernel, mail, user level, and so on. An event message is associated with a severity level, which allows an administrator to filter the messages and prioritize it. Numerical codes are assigned to the facility and the severity level. A syslog server is an event message collector and collects event messages from these facilities. The administrator can select the event message collector to which messages will be forwarded based on their severity level.

The UDP syslog (log collector) is the default remote logging target. When you disable this logging target, it no longer functions as a log collector and is removed from the **Logging Categories** window. When you enable this logging target, it becomes a log collector in the **Logging Categories** window.

Note Any changes to the default remote logging target **SecureSyslogCollector** results in the restart of the Cisco ISE Monitoring & Troubleshooting Log Processor service.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Remote Logging Targets**.

Step 2 Click **Add**.

Step 3 Enter the required details.

Step 4 Click **Save**.

Step 5 Go to the Remote Logging Targets page and verify the creation of the new target.

The logging targets can then be mapped to each of the logging categories below. The PSN nodes send the relevant logs to the remote logging targets depending on the services that are enabled on those nodes.

- AAA Audit
- AAA Diagnostics
- Accounting
- External MDM
- Passive ID
- Posture and Client Provisioning Audit
- Posture and Client Provisioning Diagnostics
- Profiler

Logs of the following categories are sent by all nodes in the deployment to the logging targets:

- Administrative and Operational Audit
- System Diagnostics
- System Statistics

Cisco ISE Message Codes

A logging category is a bundle of message codes that describe a function, a flow, or a use case. In Cisco ISE, each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

Logging categories promote logging configuration. Each category has a name, target, and severity level that you can set, as per your application requirement.

Cisco ISE provides predefined logging categories for services, such as Posture, Profiler, Guest, AAA (authentication, authorization, and accounting), and so on, to which you can assign log targets.

For the logging category **Passed Authentications**, the option to allow local logging is disabled by default. Enabling local logging for this category will result in high utilization of operational space, and fill prrt-server.log along with the iseLocalStore.log.

If you choose to enable local logging for **Passed Authentications**, go to **Administration** > **System** > **Logging** > **Logging Categories**, click **Passed Authentications** from the category section, and check the check box against **Local Logging**.

Related Topics

Set Severity Levels for Message Codes, on page 32

Set Severity Levels for Message Codes

You can set the log severity level and choose logging targets where the logs of selected categories will be stored.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**.

Step 2 Click the radio button next to the category that you want to edit, and click **Edit**.

Step 3 Modify the required field values.

Step 4 Click **Save**.

Step 5 Go to the Logging Categories page and verify the configuration changes that were made to the specific category.

Cisco ISE Message Catalogs

You can use the Message Catalog page to view all possible log messages and the descriptions. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Message Catalog**.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. Choose **Export** to export all the syslog messages in the form of a CSV file.

See Cisco ISE Syslogs for a comprehensive list of the syslog messages sent by Cisco ISE, what they mean, and how they are recorded in local and remote targets.

Endpoint Debug Log Collector

To troubleshoot issues with a specific endpoint, you can download debug logs for that particular endpoint based on its IP address or MAC address. The logs from the various nodes in your deployment specific to that particular endpoint get collected in a single file thus helping you troubleshoot your issue quickly and efficiently. You can run this troubleshooting tool only for one endpoint at a time. The log files are listed in the GUI. You can download the logs for an endpoint from a single node or from all the nodes in your deployment.

Download Debug Logs for a Specific Endpoint

To troubleshoot issues related to a specific endpoint in your network, you can use the Debug Endpoint tool from the Admin portal. Alternatively, you can run this tool from the Authentications page. Right-click the

Endpoint ID from the Authentications page and click **Endpoint Debug**. This tool provides all debug information for all services related to the specific endpoint in a single file.

Before you begin

You need the IP address or MAC address of the endpoint whose debug logs you want to collect.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Endpoint Debug**.

Step 2 Click the **MAC Address** or **IP** radio button and enter the MAC or IP address of the endpoint.

Step 3 Check the **Automatic disable after *n* Minutes** check box if you want to stop log collection after a specified amount of time. If you check this check box, you must enter a time between 1 and 60 minutes.

The following message appears: "Endpoint Debug degrades the deployment performance. Would you like to continue?"

Step 4 Click **Continue** to collect the logs.

Step 5 Click **Stop** when you want to manually stop the log collection.

Related Topics

Endpoint Debug Log Collector, on page 32

Collection Filters

You can configure the Collection Filters to suppress the syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Services Node levels based on different attribute types. You can define multiple filters with specific attribute type and a corresponding value.

Before sending the syslog messages to monitoring node or external server, Cisco ISE compares these values with fields in syslog messages to be sent. If any match is found, then the corresponding message is not sent.

Note If you configure a collection filter (**Administration** > **System** > **Logging** > **Collection Filter**) for any **Attribute** and **Filter Type**; and you have also selected the **Disable account after n days of inactivity** check box (**Administration** > **Identity Management** > **User Authentication Settings** > **Disable Account Policy**), your account might be disabled as a result of the syslog messages of successful authentication not being relayed to the monitoring node.

Configure Collection Filters

You can configure multiple collection filters based on various attribute types. It is recommended to limit the number of filters to 20. You can add, edit, or delete a collection filter.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Collection Filters**.

Step 2 Click **Add.**

Step 3 Choose the **Filter Type** from the following list:

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

Step 4 Enter the corresponding **Value** for the filter type you have selected.

Step 5 Choose the **Result** from the drop-down list. The result can be All, Passed, or Failed.

Step 6 Click **Submit.**

Related Topics

Collection Filters, on page 33
Event Suppression Bypass Filter, on page 34

Event Suppression Bypass Filter

Cisco ISE allows you to set filters to suppress some syslog messages from being sent to the Monitoring node and other external servers using the Collection Filters. At times, you need access to these suppressed log messages. Cisco ISE now provides you an option to bypass the event suppression based on a particular attribute such as username for a configurable amount of time. The default is 50 minutes, but you can configure the duration from 5 minutes to 480 minutes (8 hours). After you configure the event suppression bypass, it takes effect immediately. If the duration that you have set elapses, then the bypass suppression filter expires.

You can configure a suppression bypass filter from the Collection Filters page in the Cisco ISE user interface. Using this feature, you can now view all the logs for a particular identity (user) and troubleshoot issues for that identity in real time.

You can enable or disable a filter. If the duration that you have configured in a bypass event filter elapses, the filter is disabled automatically until you enable it again. Cisco ISE captures these configuration changes in the Change Configuration Audit Report. This report provides information on who configured an event suppression or a bypass suppression and the duration of time for which the event was suppressed or the suppression bypassed.

Cisco ISE Reports

Cisco Identity Services Engine (ISE) reports are used with monitoring and troubleshooting features to analyze trends, and, monitor system performance and network activities from a central location.

Cisco ISE collects logs and configuration data from your network. It then aggregates the data into reports for you to view and analyze. Cisco ISE provides a standard set of predefined reports that you can use and customize to fit your needs.

Cisco ISE reports are pre-configured and grouped into categories with information related to authentication, session traffic, device administration, configuration, administration, and troubleshooting.

Related Topics

Run and View Reports, on page 36

Export Reports, on page 37
Available Reports, on page 42

Report Filters

There are two types of reports, single-section and multi-section. Single-section reports contain a single grid (Radius Authentications report) and multi-section reports contain many grids (Authentications Summary report) and represent data in the form of charts and tables. The Filter drop-down menu in the single-section reports contains the **Quick Filter** and **Advanced Filter**. In the multi-section reports, you can specify only advanced filters.

Multi-section reports may contain one or more mandatory advanced filters that require your input. For example, when you click the Health Summary report (**Operations > Reports > Diagnostics** page), it displays two mandatory advanced filters—Server and Time Range. You must specify the operator command, server name, required values for both these filters, and click **Go** to generate the report. You can add new advanced filters by clicking the Plus (+) symbol. You can export multi-section reports only in the PDF format. You cannot schedule Cisco ISE multi-section reports to run and re-run at specific time or time intervals.

Note When you click a report, data for the current date is generated by default. However, some multi-section reports require mandatory input from the user apart from the time range.

By default, the Quick Filter is displayed as the first row in single-section reports. The fields may contain a drop-down list from which you can select the search criteria or may be a text box.

An Advanced Filter contains an outer criteria that contains one or more inner criteria. The outer criteria is used to specify if the search should meet All or Any specified inner criteria. The inner criteria contains one or more conditions that is used to specify the Category (Endpoint ID, Identity Group) Method (operator commands, such as Contains, Does Not Contain), and Time Range for the condition.

When using the **Quick Filter**, you can choose a date or time from the **Logged At** drop-down list to generate reports for a data set logged in the last 30 days or less. If you want to generate a report for a date or time prior to 30 days, use the **Advanced Filter** to set the required time frame in the **From** and **To** fields of the **Custom** option from the drop-down list.

Create the Quick Filter Criteria

The section describes how to create a quick filter criteria. You can create quick filter criteria for only single-section reports.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** and click the required report.

Step 2 From the **Settings** drop-down list, choose the required fields.

Step 3 In the required field, you can choose from the drop-down list or type the specific characters to filter data. The search uses the Contains operator command. For example, to filter by text that begins with “K”, enter K or to filter text that has “geo” anywhere in the text, enter geo. You can also use asterisks (*), for example, the regex starting with *abc and ending with *def.

The quick filter uses the following conditions: contains, starts with, ends with, starts with or ends with, and multiple values with OR operator.

Step 4 Press **Enter**.

Create the Advanced Filter Criteria

The section describes how to create an advanced filter criteria. You can create advanced filters for single- and multi-section reports. The Filter drop-down menu in the single-section reports contains the **Quick Filter** and **Advanced Filter**. In the multi-section reports, you can specify only advanced filters.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** and click the required report.

Step 2 In the **Filters** section, from the **Match** drop-down list, choose one of the options.

a) Choose **All** to match all specified conditions.

b) Choose **Any** to match any one specified condition.

Step 3 From the **Time Range** drop-down list, choose the required category.

Step 4 From the **Operator Commands** drop-down list, choose the required command. For example, you can filter text that begins with a specific character (use Begin With), or specific characters anywhere in the text (use Contains). Or, you can choose the Logged Time and corresponding Custom option and specify the From and To date and time from the calendar to filter data.

Step 5 From the **Time Range** drop-down list, choose the required option.

Step 6 Click **Go**.

You can save a filtered report and retrieve it from the **Filter** drop-down list for future reference.

Run and View Reports

This section describes how to run, view, and navigate reports using Reports View. When you click a report, by default, data for the last seven days is generated. Each report displays 500 rows of data per page. You can specify time increments over which to display data in a report.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **ISE Reports**.

You can also navigate to the **Reports** link under each work center to view the set of reports specific to that work center.

Step 2 Click a report from the **report** categories available.

Step 3 Select one or more filters to run a report. Each report has different filters available, of which some are mandatory and some are optional.

Step 4 Enter an appropriate value for the filters.

Step 5 Click **Go**.

Related Topics

Export Reports, on page 37
Available Reports, on page 42

Reports Navigation

You can get detailed information from the reports output. For example, if you have generated a report for a period of five months, the graph and table will list the aggregate data for the report in a scale of months.

You can click a particular value from the table to see another report related to this particular field. For example, an authentication summary report will display the failed count for the user or user group. When you click the failed count, an authentication summary report is opened for that particular failed count.

Export Reports

You can only export the PDF file format of the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary

Note Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.

- Guest Sponsor summary
- End point Profile Changes
- Network Device Session Status

Step 1 Run a report, as described in the Running and Viewing Reports section.

Step 2 Click **Export To** in the top-right corner of the report summary page.

Step 3 Choose one of the following options:

- Repository (CSV): To export the report in CSV file format to a repository
- Local (CSV): To export the report in CSV file format to a local disk
- Local (PDF): To export the report in pdf file format to a local disk

Note

- When you select the local CSV or pdf option, only the first 500 records are exported. You can use the Repository CSV option to export all the records.
- When you export the multi-section reports using the local pdf option, only the first 100 rows are exported for each section.

My Reports

You can add preconfigured system reports and personally filtered reports to the **My Reports** section. Reports saved to the **My Reports** section retain the filters applied to them.

Step 1 On the **Reports** window (**Operations** > **Reports**), click the report that you require from the **Reports** drop-down menu displayed on the left.

Step 2 (Optional) When the selected report opens, add required filters to customize the report.

Step 3 Click the **Add to My Reports** button at the top right-hand corner of the window.

Step 4 The **Save to My Reports** dialog box opens. The name and description of the report is auto populated. You can edit these fields if needed.

Step 5 (Optional) The selected reports are saved with the applicable filters, thus, retaining their customization.

Step 6 Click **Save** to save the report. A dialog box saying that the report has been successfully saved will be displayed.

Step 7 The selected report will now appear in the **My Reports** drop-down list for easy access.

You can remove a report added to the **My Reports** section by clicking the **Remove From My Reports** button at the top right-hand corner of the window. Click **OK** in the Alert dialog box that appears and the report will be removed from your My Reports section.

Scheduling Cisco ISE Reports

You can schedule Cisco ISE reports to run and re-run at specific time or time intervals. You can also apply appropriate filters to your report of choice. You can schedule for reports to run on Cisco ISE with hourly, daily, weekly, monthly, and yearly frequency. It can also be a one-time report scheduling job. You can choose the start dates and end dates of the reports and choose the days of the week when you want to schedule the reports. You get to decide the time when the scheduled report would run.

You can also send and receive email notifications for the reports generated. These email notifications will tell you if the scheduled report has run successfully and will also contain details of the repository, time of scheduled report, and so on.

When scheduling reports with **Hourly** frequency, you can have the report run over multiple days, but the timeframe cannot spread across two days.

For example, when scheduling an hourly report from May 4, 2019, to May 8, 2019, you can set the time interval as between 6:00 a.m. and 11:00 p.m. each day, but not between 6:00 p.m. of one day and 11:00 a.m. of the next. Cisco ISE displays an error message that the time range is invalid in the latter case.

You cannot schedule the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary

Note Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 Series Switches.

- Guest Sponsor summary
- Endpoint Profile Changes
- Network Device Session Status

Step 1 On the **Reports** window (**Operations** > **Reports**), select the report that you want to schedule from the **Reports** drop-down menu displayed on the left.

Step 2 (Optional) When the selected report opens, apply the filters that you want to be applicable to the report.

Step 3 Click the **Schedule** button at the top right-hand corner of the window..

Step 4 The **Save as Schedule** dialog box opens.

Step 5 Fill in the details such as name, description, email, date, and time of the schedule job.

Step 6 From the **Repository** drop-down list, choose the external repository that would save the scheduled report. For more information, see "Table 1. Supportability Matrix for External Repositories" under the Backup and Restore Repositories section of the Cisco ISE Administrator Guide.

Step 7 From the **Frequency** drop-down list, choose the frequency of the schedule as required. For example, if you only need data of the last 12 hours, select the **Last 12 hours** data field while scheduling the report.

Step 8 Select a **Start Date** and **End Date** as required and click **Save**.

Step 9 All the selected filters will automatically apply to the report while scheduling it.

Step 10 You can see the created schedule and applied filters in the **Scheduled Reports** section at the bottom of the window.

You can also edit and delete scheduled reports as needed. Choose the scheduled report of your choice from the **Scheduled Reports** drop-down list (**Operations** > **Reports** > **Scheduled Reports**). Click **Edit Schedule** to make changes to your scheduled reports and click **Save**. Click **Delete Schedule** to delete your scheduled report.

Use Case: Scheduled Reports

To get the previous day's data at 12 AM on the current day, schedule the report following this procedure:

Step 1 On the **Reports** window (**Operations** > **Reports**), select the report that you want to schedule from the **Reports** drop-down menu displayed on the left.

Step 2 (Optional) When the selected report opens, apply the filters that you want to be applicable to the report.

Step 3 In this scenario, to get the data from the previous day, select the **Logged at** field and apply the **Yesterday** filter. This will return the previous day's data whenever the scheduled report runs. If you only need data of the last 12 hours, select the **Last 12 hours data**field in the **Save as Schedule** dialog box while scheduling the report.

Step 4 Click the **Schedule** button at the top right-hand corner of the window.

Step 5 The **Save as Schedule** dialog box opens.

Step 6 Fill in the details such as name, description, email, date, and time of the schedule job.

Step 7 From the **Repository** drop-down list, choose the external repository that would save the scheduled report. For more information, see "Table 1. Supportability Matrix for External Repositories" under the Backup and Restore Repositories section of the Cisco ISE Administrator Guide.

Step 8 From the **Frequency** drop-down list, choose the frequency of the schedule as required. For example, if you only need data of the last 12 hours, select the **Last 12 hours** data field while scheduling the report.

Step 9 Select a **Start Date** and **End Date** as required and click **Save**.

Step 10 All the selected filters will automatically apply to the report while scheduling it.

Step 11 You can see the created schedule and applied filters in the **Scheduled Reports** section at the bottom of the window.

Note

- Most scheduled reports are exported in .csv format. However, the scheduled reports for Radius Authentication, Radius Accounting, TACACS Authentication, TACACS Accounting, and Operations Audit are exported in a .zip folder containing .csv files.
- If an external administrator (for example: Active Directory Administrator) creates a scheduled report without filling the email-id field, no email notifications will be sent.
- An internal or external Cisco ISE user should be deleted only after deleting the scheduled reports created by that particular user to ensure that there are no active schedules running after the user is removed.
- You can save or schedule (with filters) Cisco ISE reports only from the PAN.
- A scheduled report job runs on both Primary MnT and Secondary MnT nodes. If the Primary MnT is down, the Secondary MnT executes the scheduled report job. In such a scenario, the Secondary MnT first pings the Primary MnT. Only if the ping fails, the Secondary MnT runs the scheduled export job.
- Cisco ISE 3.1 Patch 1 onwards, the date format in exported reports has changed from YYYY-MM-DD to DD-MM-YY. The time format has changed from hh:mm:ss.sss to hh:mm:ss.sss AM/PM (24 hour format to 12 hour format).

Cisco ISE Active RADIUS Sessions

Cisco ISE provides a dynamic Change of Authorization (CoA) feature for the Live Sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD) to perform the following tasks:

- Troubleshoot issues related to authentication—You can use the Session reauthentication option to follow up with an attempt to reauthenticate again. However, you must not use this option to restrict access. To restrict access, use the shutdown option.

- Block a problematic host—You can use the Session termination with port shutdown option to block an infected host that sends a lot of traffic over the network. However, the RADIUS protocol does not currently support a method for re-enabling a port that has been shut down.
- Force endpoints to reacquire IP addresses—You can use the Session termination with port bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after a VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Session reauthentication option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the discretion of the administrator. For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the identity and posture of the endpoint are known, it is possible to send the Session reauthentication command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

For CoA commands to be understood by the device, it is important that you configure the options appropriately.

For CoA to work properly, you must configure the shared secret of each device that requires a dynamic change of authorization. Cisco ISE uses the shared secret configuration to request access from the device and issue CoA commands to it.

Note In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.

Related Topics

Change Authorization for RADIUS Sessions, on page 41

Change Authorization for RADIUS Sessions

Some Network Access Devices on your network may not send an Accounting Stop or Accounting Off packet after a reload. As a result, you might find two sessions in the Session Directory reports, one which has expired.

To dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, be sure to choose the most recent session.

Step 1 In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS Livelog**.

Step 2 Switch the view to **Show Live Session**.

Step 3 Click the CoA link for the RADIUS session that you want to issue CoA and choose one of the following options:

- **SAnet Session Query**—Use this to query information about sessions from SAnet supported devices.
- **Session reauthentication**—Reauthenticate session. If you select this option for a session established on an ASA device supporting COA, this will invoke a Session Policy Push CoA.
- **Session reauthentication with last**—Use the last successful authentication method for this session.
- **Session reauthentication with rerun**—Run through the configured authentication method from the beginning.

  Note **Session reauthentication with last** and **Session reauthentication with rerun** options are not currently supported in Cisco IOS software.

- **Session termination**—Just end the session. The switch reauthenticates the client in a different session.

- **Session termination with port bounce**—Terminate the session and restart the port.
- **Session termination with port shutdown**—Terminate the session and shutdown the port.

Step 4 Click **Run** to issue CoA with the selected reauthenticate or terminate option.

If your CoA fails, it could be one of the following reasons:

- Device does not support CoA.
- Changes have occurred to the identity or authorization policy.
- There is a shared secret mismatch.

Available Reports

The following table lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.

To generate syslogs for a logging category, set its **Log Severity Level** to **Info**:

- In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration > System > Logging > Logging Categories**.
- Click the logging category for which syslogs must be generated.
- From the **Log Severity Level** drop-down list, choose **Info**.
- Click **Save**.

Note In Cisco ISE Release 2.6 and later, users with IPv6 addresses will have the following events logged in the audit reports—login/logout, password change, and operational changes made. In Administrator Logins, User Change Password Audit, and Operations Audit reports, you can filter logs by IPv4 and IPv6 records.

Report Name	Description	Logging Category
Audit		
Adaptive Network Control Audit	The Adaptive Network Control Audit report is based on RADIUS accounting. It displays historical reporting of all the network sessions for each endpoint.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Passed Authentications** and **RADIUS Accounting**.

Report Name	Description	Logging Category
Administrator Logins	The Administrator Logins report provides information about all the GUI-based administrator login events as well as successful CLI login events.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
Change Configuration Audit	The Change Configuration Audit report provides details about configuration changes within a specified time period. If you need to troubleshoot a feature, this report can help you determine if a recent configuration change contributed to the problem.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and click **Administrative and Operational Audit**.

Report Name	Description	Logging Category
Data Purging Audit	The Data Purging Audit report records when the logging data is purged. This report reflects two sources of data purging. At 4 a.m. daily, Cisco ISE checks whether there are any logging files that meet the criteria you have set on the **Administration > Maintenance > Data Purging** window. If yes, the files are deleted and recorded in this report. Additionally, Cisco ISE continually maintains a maximum of 80 percent used storage space (threshold) for the log files. Every hour, Cisco ISE verifies this percentage and deletes the oldest data until this threshold is reached again. This information is also recorded in this report. If there is high disk space utilization, an alert message stating `ISE Monitor node(s) is about to exceed the maximum amount allocated` is displayed at 80 percent of the threshold, that is 60 percent of total disk space. Subsequently, an alert message stating `ISE Monitor node(s) has exceeded the maximum amount allocated` is displayed at 90 percent of the threshold, that is 70 percent of the total disk space.	—
Endpoints Purge Activities	The Endpoints Purge Activities report enables a user to review the history of endpoints purge activities. This report requires that the Profiler logging category is enabled. (Note that this category is enabled by default.)	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Profiler**.

Report Name	Description	Logging Category
Internal Administrator Summary	The Internal Administrator Summary report enables you to verify the entitlement of administrator users. From this report, you can also access the Administrator Logins and Change Configuration Audit reports, which enables you to view these details for each administrator.	—
Operations Audit	The Operations Audit report provides details about any operational changes, such as, running backups, registering a Cisco ISE node, or restarting an application.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
pxGrid Administrator Audit	The pxGrid Administrator Audit report provides details of the pxGrid administration actions, such as client registration, client deregistration, client approval, topic creation, topic deletion, publisher-subscriber addition, and publisher-subscriber deletion on the Primary PAN. Every record has the name of the administrator who has performed the action on the node. You can filter the pxGrid Administrator Audit report based on the administrator and message criteria.	—
Secure Communications Audit	The Secure Communications Audit report provides auditing details about security-related events in Cisco ISE Admin CLI, which includes authentication failures, possible break-in attempts, SSH logins, failed passwords, SSH logouts, invalid user accounts, and so on.	—

Report Name	Description	Logging Category
User Change Password Audit	The User Change Password Audit report displays verification about employees' password changes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and click **Administrative and Operational Audit**.
Trustsec Audit	TrustSec Audit logs contains: • Management (Create, Rename, Update, and Delete) of TrustSec components. • Deployments of SGACLs and SGTs to TrustSec-enabled NADs • TrustSec Sessions. If Cisco ISE is integrated with Catalyst Center, and SD Access is managed by Catalyst Center, then this log is empty.	—
Device Administration		
TACACS Authentication Summary	The TACACS Authentication Summary report provides details about the most common authentications, and the reason for authentication failures.	—
TACACS Accounting	The TACACS Accounting report provides accounting details for a device session. It displays information related to the generated and logged time of the users and devices.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select TACACS Accounting.
Top N Authentication by Failure Reason	The Top N Authentication by Failure Reason report displays the total number of authentications by failure reason for a specific period, based on the selected parameters.	—

Report Name	Description	Logging Category
Top N Authentication by Network Device	The Top N Authentication by Network Device report displays the number of passed and failed authentications by network device name for a specific period, based on the selected parameters.	—
Top N Authentication by User	The Top N Authentication by User report displays the number of passed and failed authentications by the user name for the specific period based on the selected parameters.	—
Diagnostics		
AAA Diagnostics	The AAA Diagnostics report provides details of all the network sessions between Cisco ISE and users. If users cannot access the network, you can review this report to identify trends and identify whether the issue is isolated to a particular user or indicative of a more widespread problem. **Note** Sometimes ISE will silently drop the Accounting Stop request of an endpoint if user authentication is in progress. However, ISE starts acknowledging all the accounting requests after user authentication is completed.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select the following logging categories: **Policy Diagnostics**, **Identity Stores Diagnostics**, **Authentication Flow Diagnostics**, and **RADIUS Diagnostics**.

Report Name	Description	Logging Category
AD Connector Operations	The AD Connector Operations report provides log of operations performed by the AD Connector, such as Cisco ISE Server password refresh, Kerberos tickets management, DNS queries, DC discovery, LDAP, RPC Connections management, and so on. If some AD failures are encountered, you can review the details in this report to identify the possible causes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **AD Connector**.
Endpoint Profile Changes	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Passed Authentications** and **Failed Attempts**.
Health Summary	The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours. Also, you can review more historical data using this report. You can evaluate this data to see consistent patterns in data. For example, you would expect heavier CPU usage when most employees start their work days. If you see inconsistencies in these trends, you can identify potential problems. The CPU Usage table lists the percentage of CPU usage for the different Cisco ISE functions. The output of the **show cpu usage** CLI command is presented in this table and you can correlate these values with the issues in your deployment to identify possible causes.	—

Report Name	Description	Logging Category
ISE Counters	The ISE Counters report lists the threshold values for various attributes. The values for these different attributes are collected at different intervals and the data is presented in a tabular format; one at 5-minute interval and another after 5 minutes. You can evaluate this data to see the trend, and if you find values that are higher than the threshold, you can correlate this information with the issues in your deployment to identify possible causes. By default, Cisco ISE collects the values for these attributes. You can choose to disable this data collection from the Cisco ISE CLI using the **application configure ise** command. Choose **option 14** to enable or disable counter attribute collection.	—
Key Performance Metrics	The Key Performance Metrics report provides statistical information about the number of endpoints that connect to your deployment and the amount of RADIUS requests that are processed by each of the PSNs on an hourly basis. This report lists the average load on the server, average latency per request, and the average transactions per second.	—

Report Name	Description	Logging Category
Misconfigured NAS	The Misconfigured NAS report provides information about NADs with inaccurate accounting frequency, typically when sending accounting information frequently. If you have taken corrective actions and fix the misconfigured NADs, the report displays fixed acknowledgment in the report. **Note** **RADIUS Suppression** should be enabled to run this report.	—
Misconfigured Supplicants	The Misconfigured Supplicants report provides a list of misconfigured supplicants along with the statistics because of failed attempts that are performed by a specific supplicant. If you have taken corrective actions and fix the misconfigured supplicant, the report displays fixed acknowledgment in the report. **Note** **RADIUS Suppression** should be enabled to run this report.	—
Network Device Session Status	The Network Device Session Status Summary report enables you to display switch configuration without logging in to the switch directly. Cisco ISE accesses these details using an SNMP query and requires that your network devices are configured with SNMP v1 or v2c. If a user is experiencing network issues, this report can help you identify if the issue is related to switch configuration or with Cisco ISE.	—

Report Name	Description	Logging Category
OCSP Monitoring	The OCSP Monitoring Report specifies the status of the Online Certificate Status Protocol (OCSP) services. It identifies whether Cisco ISE can successfully contact a certificate server, and provides certificate status auditing. It also provides a summary of all the OCSP certificate-validation operations performed by Cisco ISE. It retrieves information related to the good and revoked primary and secondary certificates from the OCSP server. Cisco ISE caches the responses and utilizes them for generating subsequent OCSP Monitoring Reports. In the event the cache is cleared, it retrieves information from the OCSP server.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **System Diagnostics**.
RADIUS Errors	The RADIUS Errors report enables you to check for RADIUS Requests Dropped (authentication or accounting requests that are discarded from unknown Network Access Device), EAP connection time outs, and unknown NADs. **Note** You can view the report only for the past 5 days.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Failed Attempts**.

Report Name	Description	Logging Category
System Diagnostics	The System Diagnostic report provides details about the status of the Cisco ISE nodes. If a Cisco ISE node is unable to register, you can review this report to troubleshoot the issue. This report requires that you first enable several diagnostic logging categories. Collecting these logs can negatively impact Cisco ISE performance. So, these categories are not enabled by default, and you should enable them just long enough to collect the data. Otherwise, they are automatically disabled after 30 minutes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select the following logging categories: **Internal Operations Diagnostics**, **Distributed Management**, and **Administrator Authentication and Authorization**.
Endpoints and Users		
Agentless Posture	Lists all the endpoints that ran Agentless posture.	—

Report Name	Description	Logging Category
Authentication Summary	The Authentication Summary report is based on the RADIUS authentications. It enables you to identify the most common authentications and the reason for authentication failures, if any. For example, if one Cisco ISE server is handling significantly more authentications than others, you might want to reassign users to different Cisco ISE servers to better balance the load. **Note** Because the Authentication Summary report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.	—

Report Name	Description	Logging Category
Client Provisioning	The Client Provisioning report indicates the client provisioning agents applied to particular endpoints. You can use this report to verify the policies applied to each endpoint, and in turn, use this to verify whether the endpoints have been correctly provisioned. **Note** The MAC address of an endpoint is not displayed in the **Endpoint ID** column if the endpoint does not connect with ISE (no session is established), or if a Network Address Translation (NAT) address is used for the session.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**, and select **Posture and Client Provisioning Audit** and **Posture and Client Provisioning Diagnostics**.
Current Active Sessions	The Current Active Sessions report enables you to export a report with details about who is on the network within a specified time period. If a user isn't getting network access, you can see whether the session is authenticated or terminated, or if there is another problem with the session.	—
Endpoint Scripts Provisioning Summary	The **Endpoint Scripts Provisioning Summary** window displays details of jobs run through the **Endpoint Scripts** window over the last 30 days.	—

Report Name	Description	Logging Category
External Mobile Device Management	The External Mobile Device Management report provides details about integration between Cisco ISE and the external Mobile Device Management (MDM) server. You can use this report to see which endpoints have been provisioned by the MDM server without logging into the MDM server directly. It also displays information such as registration and MDM-compliance status.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select MDM.
Passive ID	The Passive ID report enables you to monitor the state of WMI connection to the domain controller and gather statistics related to it (such as amount of notifications received, amount of user login/logouts per second etc.) **Note** Sessions authenticated by this method do not have authentication details in the report.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Identity Mapping.
Manual Certificate Provisioning	The Manual Certificate Provisioning report lists all the certificates that are provisioned manually via the certificate provisioning portal.	—
Posture Assessment by Condition	The Posture Assessment by Condition report enables you to view records based on the posture policy condition configured in ISE to validate that the most up-to-date security settings or applications are available on client machines.	—

Report Name	Description	Logging Category
Posture Assessment by Endpoint	The Posture Assessment by Endpoint report provides detailed information, such as the time, status, and PRA Action, of an endpoint. You can click **Details** to view further information of an endpoint. **Note** The Posture Assessment by Endpoint report does not provide posture policy details of applications and hardware attributes of an endpoint. You can view this information only in the Context Visibility page.	—
Profiled Endpoints Summary	The Profiled Endpoints Summary report provides profiling details about endpoints that are accessing the network. **Note** For endpoints that do not register a session time, such as a Cisco IP-Phone, the term Not Applicable is shown in the Endpoint session time field.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Profiler.

Report Name	Description	Logging Category
RADIUS Accounting	The RADIUS Accounting report identifies how long users have been on the network. If users are losing network access, you can use this report to identify whether Cisco ISE is the cause of the network connectivity issues. **Note** Radius accounting interim updates are included in the RADIUS Accounting report if the interim updates contain information about the changes to the IPv4 or IPv6 addresses for the given sessions.	
RADIUS Authentications	The RADIUS Authentications report enables you to review the history of authentication failures and successes. If users cannot access the network, you can review the details in this report to identify possible causes.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select these logging categories: Passed Authentications and Failed Attempts.
Registered Endpoints	The Registered Endpoints report displays all personal devices registered by employees.	—
Rejected Endpoints	The Rejected Endpoints report lists all rejected or released personal devices that are registered by employees.	—
Supplicant Provisioning	The Supplicant Provisioning report provides details about the supplicants provisioned to employee's personal devices.	Posture and Client Provisioning Audit

Report Name	Description	Logging Category
Top Authorizations by Endpoint	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts
Top Authorizations by User	The Top Authorization by User report displays how many times each user was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts
Top N Authentication by Access Service	The Top N Authentication by Access Service report displays the number of passed and failed authentications by the access service type for the specific period based on the selected parameters.	—
Top N Authentication by Failure Reason	The Top N Authentication by Failure Reason report displays the total number of authentications by failure reason for the specific period based on the selected parameters.	—
Top N Authentication by Network Device	The Top N Authentication by Network Device report displays the number of passed and failed authentications by the network device name for the specific period based on the selected parameters.	—
Top N Authentication by User	The Top N Authentication by User report displays the number of passed and failed authentications by the user name for the specific period based on the selected parameters.	—
Guest		
AUP Acceptance Status	The AUP Acceptance Status report provides details of AUP acceptances from all the Guest portals.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Guest.

Report Name	Description	Logging Category
Guest Accounting	The Guest Accounting report is a subset of the RADIUS Accounting report. All users assigned to the Activated Guest or Guest identity groups appear in this report.	—
Primary Guest Report	The Primary Guest Report combines data from various Guest Access reports and enables you to export data from different reporting sources. The Primary Guest report also provides details about the websites that guest users are visiting. You can use this report for security auditing purposes to demonstrate when guest users accessed the network and what they did on it. You must also enable HTTP inspection on the network access device (NAD) used for guest traffic. This information is sent back to Cisco ISE by the NAD. To check when the clients reach the maximum simultaneous sessions limit, from the Admin portal, choose **Administration > System > Logging > Logging Categories** and do the following: **1.** Increase the log level of "Authentication Flow Diagnostics" logging category from WARN to INFO. **2.** Change LogCollector Target from Available to Selected under the "Logging Category" of AAA Diagnostics.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Passed Authentications.

Report Name	Description	Logging Category
My Devices Login and Audit	The My Devices Login and Audit report provides details about the login activities and the operations performed by the users on the devices in My Devices Portal.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select My Devices.
Sponsor Login and Audit	The Sponsor Login and Audit report provides details of guest users' login, add, delete, enable, suspend and update operations and the login activities of the sponsors at the sponsors portal. If guest users are added in bulk, they are visible under the column 'Guest Users.' This column is hidden by default. On export, these bulk users are also present in the exported file.	In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories** and select Guest.
SXP		
SXP Binding	The SXP Binding report provides information about the IP-SGT bindings that are exchanged over SXP connection.	—
SXP Connection	You can use this report to monitor the status of an SXP connection and gather information related to it, such as peer IP, SXP node IP, VPN name, SXP mode, and so on.	—
Trustsec		

Report Name	Description	Logging Category
RBACL Drop Summary	The RBACL Drop Summary report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license. This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE. If a user violates a particular policy or access, packets are dropped and indicated in this report. **Note** Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.	—
Top N RBACL Drops By User	The Top N RBACL Drops By User report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license. This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE. This report displays policy violations (based on packet drops) by specific users. **Note** Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.	—

Report Name	Description	Logging Category
TrustSec ACI	This report lists the SGTs and SXP mappings that are synchronized with the IEPGs, EEPGs, endpoints, and subnet configuration of APIC. These details are displayed only if the TrustSec APIC integration feature is enabled.	—

Report Name	Description	Logging Category
TrustSec Deployment Verification		—

Report Name	Description	Logging Category
	You can use this report to verify whether the latest TrustSec policies are deployed on all network devices or if there are any discrepancies between the policies configured in Cisco ISE and the network devices. Click the **Details** icon to view the results of the verification process. You can view the following details: • When the verification process started and completed • Whether the latest TrustSec policies are successfully deployed on the network devices. You can also view the names and IP addresses of the network devices on which the latest TrustSec policies are deployed. • Whether if there are any discrepancies between the policies configured in Cisco ISE and the network devices. It displays the device name, IP address, and the corresponding error message for each policy difference. You can view the TrustSec Deployment Verification alarms in the **Alarms** dashlet (under **Work Centers > TrustSec > Dashboard** and **Home > Summary**). **Note** • The time taken for reporting depends on the number of network devices and TrustSec	

Report Name	Description	Logging Category
	groups in your deployment. • The error message length in the TrustSec Deployment Verification report is currently limited to 480 characters. Error messages with more than 480 characters will be truncated and only the first 480 characters will be displayed in the report.	
Trustsec Policy Download	This report lists the requests sent by the network devices for policy (SGT/SGACL) download and the details sent by ISE. If the Workflow mode is enabled, the requests can be filtered for production or staging matrix.	To view this report, you must do the following: **1.** In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Administration** > **System** > **Logging** > **Logging Categories**. **2.** Choose **AAA Diagnostics** > **RADIUS Diagnostics**. **3.** Set the Log Severity Level to DEBUG for RADIUS Diagnostics.
Threat Centric NAC Service		
Adapter Status	The Adapter Status report displays the status of the threat and vulnerability adapters.	—

Report Name	Description	Logging Category
COA Events	When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.	—
Threat Events	The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured.	—
Vulnerability Assessment	The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.	—

RADIUS Live Logs

The following table describes the fields in the Live logs window that displays the recent RADIUS authentications. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **RADIUS** > **Live Logs**. Note that you can view the RADIUS live logs only in the Primary PAN.

Table 6: RADIUS Live Logs

Field Name	Description
Time	Shows the time at which the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is mandatory and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.

Field Name	Description
Details	Clicking the icon under the **Details** column opens the **Accounting Detail Report** in a new browser window. This report offers information about authentication and related attributes, and authentication flow. Clicking the icon under the **Details** column opens the **Accounting Detail** report if an accounting event is processed for that session. If the session is in authenticated state, **Authentication Detail** report is displayed when you click the icon under the **Details** column. The **Response Time** in the **Authentication Detail** report is the total time taken by Cisco ISE to process the authentication flow. For example, if authentication consists of three roundtrip messages that took 300 ms for the initial message, 150 ms for the next message, and 100 ms for the last, **Response Time** is 300 + 150 + 100 = 550 ms. **Note** You cannot view the details for endpoints that are active for more than 48 hours. You will see a window with the following message when you click the **Details** icon for endpoints that are active for more than 48 hours: `No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.`
Repeat Count	Shows the number of time the authentication requests were repeated in the last 24 hours, without any change in the context of identity, network devices, and authorization.
Identity	Shows the logged in username that is associated with the authentication. If the username is not present in any ID Store, it is displayed as `INVALID`. If the authentication fails due to any other reason, it is displayed as `USERNAME`. **Note** This is applicable only for users. This is not applicable for MAC addresses. To aid debugging, you can force Cisco ISE to display the invalid usernames. To do this, check the **Disclose Invalid Usernames** check box under **Administration** > **System** > **Settings** > **Security Settings**. You can also configure the **Disclose Invalid Usernames** option to time out, so that you do not have to manually turn it off.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows the authorization profile that was used for authentication.

Field Name	Description
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.
Server	Indicates the policy service from which the log was generated.
MDM Server Name	Shows the name of the MDM server.
Event	Shows the event status.
Failure Reason	Shows the detailed reason for failure, if the authentication failed.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Security Group	Shows the group that is identified by the authentication log.
Session ID	Shows the session ID.

Note In the **RADIUS Live Logs** and **TACACS+ Live Logs** window, a Queried PIP entry appears for the first attribute of each policy authorization rule. If all the attributes within the authorization rule are related to a dictionary that was already queried for previous rules, no additional Queried PIP entry appears.

You can do the following in the RADIUS **Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Authentication Latency

Authentication Latency is the average response time of the RADIUS authentication process from the time authetication process is initiated. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Dashboard** > **System Summary** dashlet..

You can select the following authentication latency timeframe from the drop-down list:

- **60 mins:** This option gives you the authentication latency for the authentication that was initiated in last 60 mins.
- **12 hrs:** This option gives you the authentication latency for the authentication process that was initiated in last 24 hrs.

The response time that is displayed is in millisecond (ms). To view a detailed report of authentication latenty, click on the latest log in the **Live Logs** window. To view this window, click the **Menu** icon (☰) and choose **Operations** > **RADIUS**.

RADIUS Live Sessions

The following table describes the fields in the RADIUS **Live Sessions** window, which displays live authentications. To view this window, click the **Menu** icon (☰) and chooseYou can view the RADIUS live sessions only in the Primary PAN.

Table 7: RADIUS Live Sessions

Field Name	Description
Initiated	Shows the timestamp when the session was initiated.
Updated	Shows the timestamp when the session was last updated because of a change.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of an endpoint device.
Action	Click the **Actions** icon to reauthenticate an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times a user or endpoint is reauthenticated.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of an endpoint device.
IP Address	Shows the IP address of an endpoint device.
Audit Session ID	Shows a unique session identifier.
Account Session ID	Shows a unique ID provided by a network device.
Endpoint Profile	Shows the endpoint profile for a device.

Field Name	Description
Posture Status	Shows the status of posture validation and details of the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service node from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and so on.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
Authorization Profiles	Shows an authorization profile that was used for authentication.
NAS IP Address	Shows the IP address of a network device.
Device Port	Shows the connected port to a network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.
ANC Status	Adaptive Network Control status of a device as **Quarantine, Unquarantine**, or **Shutdown**.
WLC Roam	Shows the boolean (Y/N) used to track if an endpoint has been handed off during roaming, from one Wireless Lan Controller (WLC) to another. It has the value of cisco-av-pair=nas-update =Y or N. **Note** Cisco ISE relies on the nas-update=true attribute from WLC to identify whether the session is in roaming state. When the original WLC sends an accounting stop attribute with nas-update=true, the session is not deleted in ISE to avoid reauthentication. If roaming fails, ISE clears the session after five days of inactivity.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.
Bytes Out	Shows the number of bytes sent.
Session Source	Indicates whether it is a RADIUS session or a Passive ID session.
User Domain Name	Shows the registered DNS name of a user.

Field Name	Description
Host Domain Name	Shows the registered DNS name of a host.
User NetBIOS Name	Shows the NetBIOS name of a user.
Host NetBIOS Name	Shows the NetBIOS name of a host.
License Type	Shows the type of license used.
License Details	Shows the license details.
Provider	Endpoint events are learned from different syslog sources. These syslog sources are referred to as providers. • Windows Management Instrumentation (WMI): WMI is a Windows service that provides a common interface and object model to access management information about operating system, devices, applications, and services. • Agent: A program that runs on a client on behalf of the client or another program. • Syslog: A logging server to which a client sends event messages. • REST: A client is authenticated through a terminal server. The TS Agent ID, Source Port Start, Source Port End, and Source First Port values are displayed for this syslog source. • Span: Network information is discovered using span probes. • DHCP: DHCP event. • Endpoint **Note** When two events from different providers are learned or obtained from an endpoint session, the providers are displayed as comma-separated values in the **Live Sessions** window.
MAC Address	Shows the MAC address of a client.
Endpoint Check Time	Shows the time at which an endpoint was last checked by the endpoint probe.
Endpoint Check Result	Shows the result of an endpoint probe. The possible values are: • Unreachable • User Logout • Active User
Source Port Start	(Values are displayed only for the REST provider) Shows the first port number in a port range.

Field Name	Description
Source Port End	(Values are displayed only for the REST provider) Shows the last port number in a port range.
Source First Port	(Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server Agent. A Terminal Server refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address, and therefore, it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a Terminal Server Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port user mapping.
TS Agent ID	(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server Agent that is installed on an endpoint.
AD User Resolved Identities	(Values are displayed only for AD user) Shows the potential accounts that matched.
AD User Resolved DNs	(Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com

TACACS Live Logs

The following table describes the fields in the TACACS Live Logs window that displays the TACACS+ AAA details. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **TACACS** > **Live Logs**. You can view the TACACS live logs only in the Primary PAN.

Table 8: TACACS Live Logs

Field Name	Usage Guidelines
Generated Time	Shows the syslog generation time based on when a particular event was triggered.
Logged Time	Shows the time when the syslog was processed and stored by the Monitoring node. This column is mandatory and cannot be deselected.
Status	Shows if the authentication succeeded or failed. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information about the selected authentication scenario. This column is required and cannot be deselected.
Session Key	Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.

Field Name	Usage Guidelines
Username	Shows the user name of the device administrator. This column is required and cannot be deselected.
Type	Consists of two Types—Authentication and Authorization. Shows names of users who have passed or failed authentication, authorization, or both. This column is mandatory and cannot be deselected.
Authentication Policy	Shows the name of the policy selected for specific authentication.
Authorization Policy	Shows the name of the policy selected for specific authorization.
ISE Node	Shows the name of the ISE node through which the access request is processed.
Network Device Name	Shows the names of network devices.
Network Device IP	Shows the IP addresses of network devices whose access requests are processed.
Network Device Groups	Shows the name of corresponding network device groups to which a network device belongs.
Device Type	Shows the device type policy that is used to process access requests from different network devices.
Location	Shows the location-based policy that is used to process access requests from network devices.
Device Port	Shows the device port number through which the access request is made.
Failure Reason	Shows the reason for rejecting an access request that is made by a network device.
Remote Address	Shows the IP address, MAC address, or any other string that uniquely identifies the end station.
Matched Command Set	Shows the MatchedCommandSet attribute value if it is present, or an empty value if the MatchedCommandSet attribute value is empty or the attribute itself does not exist in the syslog.
Shell Profile	Shows the privileges that were granted to a device administrator for executing commands on the network device.

You can do the following in the **TACACS Live Logs** window:

- Export the data in CSV or PDF format.
- Show or hide the columns based on your requirements.
- Filter the data using the quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

Note All the user customizations are stored as user preferences.

Export Summary

You can view the details of the reports exported by all the users in the last seven days, along with the status. The export summary includes both the manual and scheduled reports. The **Export Summary** window is automatically refreshed every two minutes. Click the **Refresh** icon to refresh the **Export Summary** window manually.

The super admin can cancel the export that is **In-Progess** or in **Queued** state. Other users are allowed only to cancel the export process that they have initiated.

By default, only three manual export of reports can run at a given point of time; the remaining triggered manual export of reports are queued. There are no such limits for the scheduled export of reports.

Note All the reports in the queued state are scheduled again and the reports in the **In-Progress** or **Cancellation-in-progress** state are marked as failed when the Cisco ISE server is restarted. If the primary MnT node is down, the scheduled report export job runs on secondary MnT node.

The following table describes the fields in the **Export Summary** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose **Operations** > **Reports** > **Export Summary**.

Table 9: Export Summary

Field Name	Description
Report Exported	Displays the name of the report.
Exported By	Shows the role of the user who initiated the export process.
Scheduled	Shows whether the report export is a scheduled one.
Triggered On	Shows the time at which the export process has been triggered in the system.
Repository	Displays the name of the repository where the exported data will be stored.
Filter Parameters	Shows the filter parameters selected while exporting the report.

Field Name	Description
Status	Shows the status of the exported reports. It can be one of the following: • Queued • In-progress • Completed • Cancellation-in-progress • Cancelled • Failed • Skipped **Note** Failed status indicates the reason for failure. Skipped status indicates that the scheduled export of reports is skipped because the primary MnT node is down.

You can do the following in the **Export Summary** window:

- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.