Reporting

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. For more information, see Chapter 25, "Monitoring and Troubleshooting."

This chapter explains the types of reports that are available in Cisco ISE. It also discusses the various ways that you can use report data, and organize it for more effective use.

This chapter covers the following topics:

Cisco ISE Reports

Cisco ISE collects log and configuration data from across the 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 preconfigured and e grouped into logical categories with information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting. For a complete list of Cisco ISE reports, see Available Reports, page 26-6.

This section covers the following topics:

Running and Viewing Reports

This section describes how to run, view, and navigate reports using Reports View. You can specify time increments over which to display data in a report.

Step 1 Choose **Operations > Reports > ISE Reports**.

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 that are case sensitive, of which some are mandatory and some are optional.

Step 4 Enter an appropriate value for the filters.

Step 5 Run the report.

Related Topics

- Exporting Reports, page 26-2
- Scheduling and Saving ISE Reports, page 26-3
- Adding Favorite Reports, page 26-4
- Available Reports, page 26-6

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.

Exporting Reports

You can export report data to an Excel spreadsheet as a comma-separated values (.csv) file. After you export the data, you will receive an email detailing the location of the report.

Note You can export report data to a .csv format only by using the Primary PAP nodes.

Step 1 Run a report, as described in Running and Viewing Reports, page 26-2.

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

Step 3 Specify the data columns that you want to export.

Step 4 Choose a repository from the drop-down list.

Step 5 Click **Export**.

Note To view the non-English characters correctly after exporting a report, you must import the file into Microsoft Excel by enabling UTF-8 character encoding. If you choose to open the exported .csv file directly in Microsoft Excel without enabling UTF-8 character encoding, the non-English characters in the report appear in some garbage form.

You cannot export the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary
- Guest Sponsor summary
- End point Profile Changes
- Network Device Session Status

Related Topics

Configuring the SMTP Server to Support Notifications, page 5-5

Scheduling and Saving ISE Reports

You can customize a report and save the changes as a new report, or restore the default report settings.

You can also customize and schedule ISE reports to run and re-run at specific time or time intervals. You can also send and receive email notifications once the reports are generated.

Note You can save or schedule (customize) ISE reports only by using the Primary PAP nodes.

Step 1 Run a report as described in Running and Viewing Reports, page 26-2.

Step 2 Click **Save As** in the top right-hand corner of the report summary page.

Step 3 Choose **Report** or **Scheduled Report**.

Step 4 Enter the required details in the dialog box.

Step 5 Click **Save as New**.

You cannot schedule the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary
- Guest Sponsor summary

- End point Profile Changes
- Network Device Session Status

Adding Favorite Reports

You can add preconfigured system reports to your favorites list, as well as reports that you have customized.

You can add reports that you use frequently to a list of favorites to make them easier to find, similar to how you bookmark favorite websites in a browser. You can view and edit the parameters of your favorite reports, and then save the customized reports for reuse.

Note Every administrator account is assigned one or more administrative roles. Depending on the roles that are assigned to your account, you may not be able to perform the tasks that are described in this section.

Step 1 Run a report, as described in Running and Viewing Reports, page 26-2.

Step 2 Click **Favorite** in the top right-hand corner of the report summary page.

The report appears in your Favorites list.

Note You can add preconfigured system reports to your favorites list only by using the Primary PAP nodes.

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. For more information, see Chapter 14, "Managing Users and External Identity Sources."

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 Topic

Changing Authorization for RADIUS Sessions, page 26-5

Changing 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 Choose **Operations > Authentications**.

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:

Note For Inline Posture nodes and where wireless LAN controllers (WLC) are in use, only two options are available: Session reauthentication and Session termination.

- **SAnet Session Query—**Use this to query information about sessions from SAnet supported devices.
- **Session reauthentication**—Reauthenticate session.
- **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.

Step 5 To save your changes, see Scheduling and Saving ISE Reports, page 26-3.

Related Topics

See Troubleshooting Unexpected RADIUS Authentication Results, page 25-18. A failed dynamic CoA will be listed under failed RADIUS authentications.

For information on CoA, policies, and profiles, see the following:

- Authorization Policies and Supported Dictionaries, page 20-4
- Configuring Authorization Policies, page 20-8
- Chapter 21, “Cisco ISE Endpoint Profiling Policies”
- Chapter 23, “Configuring Client Posture Policies”
- Cisco ISE Does Not Issue CoA Following Authentication, page G-33
- CoA Not Initiating on Client Machine, page G-3
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page G-18
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page G-19

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.

Table 26-1 Available Reports

Report Name	Description	Logging Category
Auth Services Status		
AAA Diagnostics	The AAA Diagnostics report provides details of all 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.	Choose **Administration > Logging > Logging Categories** and select these logging categories: Policy Diagnostics, Identity Stores Diagnostics, Authentication Flow Diagnostics, and RADIUS Diagnostics.
RADIUS Authentication	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.	Choose **Administration > Logging > Logging Categories** and select these logging categories: Passed Authentications and Failed Attempts.

Table 26-1 Available Reports (continued)

Report Name	Description	Logging Category
RADIUS Errors	The RADIUS Errors report enables you to check for RADIUS Requests Dropped (authentication/accounting requests discarded from unknown Network Access Device), EAP connection time outs and unknown NADs.	Choose **Administration > Logging > Logging Categories** and select Failed Attempts.
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.	Choose **Administration > Logging > Logging Categories** and select RADIUS Accounting.
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 any authentication failures. 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** As 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.	—
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. Provides a summary of all the OCSP certificate validation operations performed by Cisco ISE.	Choose **Administration > Logging > Logging Categories** and select System Diagnostics.
Deployment Status		
Administrator Logins	The Administrator Logins report provides an audit trail of all administrator logins.	Choose **Administration > Logging > Logging Categories** and select Administrative and Operational audit.
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.	—

Table 26-1 Available Reports (continued)

Report Name	Description	Logging Category
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.	Choose **Administration > Logging > Logging Categories** and select Administrative and Operational audit.
Secure Communications Audit	The Secure Communications Audit report provides auditing details about all communications that occur over a secure channel. This report aligns with Cisco Common Criteria requirements.	—
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.	Choose **Administration > Logging > Logging Categories** and select Administrative and Operational audit.
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.	Choose **Administration > Logging > Logging Categories** and select these logging categories: Internal Operations Diagnostics, Distributed Management, Administrator Authentication and Authorization.
Health Summary	The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours, and 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.	—
Network Device Session Status	The Network Device Session Status Summary report enables you to display the switch configuration without logging into the switch directly. Cisco ISE accesses these details using an SNMP query and requires that your network devices are configured with SNMP v1/v2c. If a user is experiencing network issues, this report can help you identify if the issue is related to the switch configuration rather than with Cisco ISE.	—

Table 26-1 Available Reports (continued)

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 4AM daily, Cisco ISE checks whether there are any logging files that meet the criteria you have set on the Administration > Maintenance > Data Purging page. If so, the files are deleted and recorded in this report. Additionally, Cisco ISE continually maintains a maximum of 80% used storage space for the log files. Every hour, Cisco ISE verifies this percentage and deletes the oldest data until it reaches the 80% threshold again. This information is also recorded in this report.	—
Misconfigured Supplicants	The Misconfigured Supplicants report provides a list of mis-configured supplicants along with the statistics due to failed attempts that are performed by a specific supplicant. If you have taken corrective actions and fix the mis-configured supplicant, the report displays fixed acknowledgement in the report. **Note** RADIUS Suppression should be enabled to run this report.	—
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 mis-configured NADs, the report displays fixed acknowledgment in the report. **Note** RADIUS Suppression should be enabled to run this report.	—
Endpoints and Users		
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 to verify whether the endpoints have been correctly provisioned.	Choose **Administration > 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 was currently 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.	—

Table 26-1 Available Reports (continued)

Report Name	Description	Logging Category
Guest Activity	The Guest Activity report 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.	Choose **Administration > Logging > Logging Categories** and select Passed Authentications.
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.	—
Guest Sponsor Mapping	The Guest Sponsor Mapping report displays the list of sponsors along with the details of guest users created by them.	—
Guest Sponsor Summary	The Guest Sponsor Summary report displays all guest users created by each sponsor. Click on a sponsor name to display details about the guest users.	—
Endpoint Protection Service Audit	The Endpoint Protection Service Audit report is based on the RADIUS accounting. It displays historical reporting of all network sessions for each endpoint.	Choose **Administration > Logging > Logging Categories** and select Passed Authentications and RADIUS Accounting.
Mobile Device Management	The 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.	—
Posture Detail Assessment	The Posture Detail Assessment report provides details about posture compliancy for a particular endpoint. If an endpoint previously had network access and then suddenly was unable to access the network, you can use this report to determine if a posture violation occurred.	Choose **Administration > Logging > Logging Categories** and select Posture and Client Provisioning Audit and Posture and Client Provisioning Diagnostics.
Profiled Endpoint Summary	The Profiled Endpoint 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.	Choose **Administration > Logging > Logging Categories** and select Profiler.

Table 26-1 Available Reports (continued)

Report Name	Description	Logging Category
Endpoint Profile Changes	The Endpoint Profile Change report serves two purposes: • Compares the profile changes for a particular endpoint to verify that the latest and most current profile has been applied. • Displays profile changes initiated by the profiler feed service (which is available with a Cisco ISE Advanced license).	
Top Authorization by Endpoint (MAC address)	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 Authorization 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
User Change Password Audit	The User Change Password Audit report displays verification about employee's password changes.	Administrative and Operational audit
Supplicant Provisioning	The Supplicant Provisioning report provides details about the supplicants provisioned to employee's personal devices.	Posture and Client Provisioning Audit
Registered Endpoints	The Registered Endpoints report displays all personal devices registered by employees.	—
Security Group Access		
RBACL Drop Summary	The RBACL Drop Summary report is specific to the Security Group Access (SGA) 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.	—
Top N RBACL Drops By User	The Top N RBACL Drops By User report is specific to the Security Group Access (SGA) 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.	—