APPENDIX A

User Interface Reference

This chapter is a reference for Cisco Identity Services Engine (Cisco ISE) user interface elements, and contains the following sections:

Operations

This section contains the following topics:

Authentications

Choose **Operations > Authentications** to display the Authentications page. Authentications data categories are described in the following table.

Table A-1 Authentications

Option	Description
Time	Shows the time that the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication was successful or a failure. 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 on the selected authentication scenario. This column is required and cannot be deselected.
Username	Shows the username that is associated with the authentication.

Table A-1 Authentications (continued)

Option	Description
Calling Station ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
IP Address	Shows the IP address of the endpoint device.
NAD	IP address of the Network Access Device.

Optionally, you can choose to show the categories in the following table:

Table A-2 Optional Authentications Categories

Option	Description
Server	Indicates the policy service ISE node from which the log was generated.
NAS Port ID	Network access server (NAS) port at which the endpoint is connected.
Failure Reason	Shows a detailed reason for failure, if the authentication failed.
SGA Security Group	Shows a security profile for the authentication.
Authorization Profiles	Shows an authorization profile that was used for authentication.
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 the like.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
SGA Security Group	Shows the trust group that is identified by the authentication log.
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.

Alarms

This section contains the following topics:

Alarms Inbox

This section contains the following topics:

Inbox

The following table describes the Operations > Alarms > Inbox options:

Table A-3 Inbox

Option	Description
Severity	*Display only*. Indicates the severity of the associated alarm: • Critical • Warning • Info
Name	Indicates the name of the alarm. Click to display the Alarms: Properties page and edit the alarm.
Time	*Display only*. Indicates the time of the associated alarm generation in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = Day of the month, from 01 to 31. • hh = Hour of the day, from 00 to 23. • mm = Minute of the hour, from 00 to 59. • ss = Second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit year.
Cause	*Display only*. Indicates the cause of the alarm.
Assigned To	*Display only*. Indicates who is assigned to investigate the alarm.

Table A-3 Inbox (continued)

Option	Description
Status	*Display only*. Indicates the status of the alarm: • New—The alarm is new. • Acknowledged—The alarm is known. • Closed—The alarm is closed.
Edit	Check the check box next to the alarm that you want to edit, and click **Edit** to edit the status of the alarm and view the corresponding report.
Close	Check the check box next to the alarm that you want to close, and click **Close** to close the alarm. You can enter closing notes before you close an alarm. **Note** Closing an alarm only removes the alarm. It does not delete the alarm.
Delete	Check the check box next to the alarm that you want to delete, and click **Delete** to delete the alarm.

Edit > Alarm

Click **Edit** in the Inbox to view the Edit tab that provides information on the event that triggered the alarm. You cannot edit any of the fields on the Alarm tab. The options are shown in the following table.

Table A-4 Edit Alarm

Option	Description
Occurred At	Date and time when the alarm was triggered.
Cause	The event that triggered the alarm.
Detail	Additional details about the event that triggered the alarm. ISE usually lists the counts of items that exceeded the specified threshold.
Report Links	Wherever applicable, one or more hyperlinks are provided to the relevant reports that allow you to further investigate the event.
Threshold	Information on the threshold configuration.

Edit > Status

Click **Edit** in the Inbox and click the Status tab to edit the status of the alarm and add a description to track the event. The options are shown in the following table.

Table A-5 Edit Status

Option	Description
Status	Status of the alarm. When an alarm is generated, its status is New. After you view the alarm, change the status of the alarm to Acknowledged or Closed to indicate the current status of the alarm.
Assigned To	(Optional) Specify the name of the user to whom this alarm is assigned.
Notes	(Optional) Enter any additional information about the alarm that you want to record.

Rules

Choose **Operations > Alarms > Rules** page to specify the alarm rule parameters. This section contains the following topics:

Passed Authentications

Modify the fields described in the following table to create a threshold with the passed authentication criteria.

Table A-6 Passed Authentications

Option	Description
Passed Authentications	Greater than <*count*> <**occurrences** | **%**> in the past *time* ***Minutes*** | ***Hours*** for a *object*, where: • *count* values can be the absolute number of occurrences or percent. The valid values are as follows: – *count* must be in the range 0 to 99 for greater than. – *count* must be in the range 1 to 100 for lesser than. • **occurrences** | **%** value can be occurrences or %. • *time* values can be 1 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be any of the following: – ISE Instance – User – Identity Group – Device IP – Identity Store – Allowed Protocol – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel **Note** In a distributed deployment, if there are two instances, the count is calculated as an absolute number or as a percentage for each of the instances. An alarm is triggered only when the individual count of any instance exceeds the threshold.
Filter	
ISE Instance	Choose a valid Cisco ISE instance for the threshold.
User	Choose or enter a valid username for the threshold.
Identity Group	Choose a valid identity group name for the threshold.
Device Name	Choose a valid device name for the threshold.
Device IP	Choose or enter a valid device IP address for the threshold.
Device Group	Choose a valid device group name for the threshold.
Identity Store	Choose a valid identity store name for the threshold.

Table A-6 Passed Authentications (continued)

Option	Description
Allowed Protocol	Choose a valid allowed protocol name for the threshold.
MAC Address	Choose or enter a valid MAC address for the threshold. This filter is available only for RADIUS authentications.
NAD Port	Choose a port for the network device for the threshold. This filter is available only for RADIUS authentications.
AuthZ Profile	Choose an authorization profile for the threshold. This filter is available only for RADIUS authentications.
AuthN Method	Choose an authentication method for the threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Choose an EAP authentication value for the threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Choose an EAP tunnel value for the threshold. This filter is available only for RADIUS authentications.
Protocol	Configure the protocol that you want to use for your threshold.

Failed Authentications

Modify the fields described in the following table to create a threshold with the passed authentication criteria.

Table A-7 Failed Authentications

Option	Description
Failed Authentications	Greater than *count* **occurrences | %** in the past *time Minutes|Hours* for a *object*, where: • *count* values can be the absolute number of occurrences or percent. Valid values must be in the range 0 to 99. • **occurrences | %** value can be occurrences or %. • *time* values can be 1 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be any of the following: – ISE Instance – User – Identity Group – Device IP – Identity Store – Allowed Protocol – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel **Note** In a distributed deployment, if there are two instances, the count is calculated as an absolute number or as a percentage for each of the instances. An alarm is triggered only when the individual count of any instance exceeds the specified threshold.
Filter	
Failure Reason	Enter a valid failure reason name for the threshold.
ISE Instance	Choose a Cisco valid ISE instance for the threshold.
User	Choose or enter a valid username for the threshold.
Identity Group	Choose a valid identity group name for the threshold.
Device Name	Choose a valid device name for the threshold.
Device IP	Choose or enter a valid device IP address for the threshold.
Device Group	Choose a valid device group name for the threshold.
Identity Store	Choose a valid identity store name for the threshold.
Allowed Protocol	Choose a valid allowed protocol name for the threshold.
MAC Address	This filter is available only for RADIUS authentications.

Table A-7 Failed Authentications (continued)

Option	Description
NAD Port	This filter is available only for RADIUS authentications.
AuthZ Profile	This filter is available only for RADIUS authentications.
AuthN Method	This filter is available only for RADIUS authentications.
EAP AuthN	This filter is available only for RADIUS authentications.
EAP Tunnel	This filter is available only for RADIUS authentications.
Protocol	Configure the protocol that you want to use for your threshold.

Authentication Inactivity

Modify the fields described in the following table to define threshold criteria based on authentications that are inactive.

Table A-8 Authentication Inactivity

Option	Description
ISE Instance	Choose a valid instance for the threshold.
Device	Choose a valid device for the threshold.
Protocol	Choose the protocol for threshold.
Inactive for	Select one of the following options: • Hours—Number of hours, from 1 to 744. • Days—Number of days, from 1 to 31.

ISE Configuration Changes

Modify the fields described in the following table to define threshold criteria based on system diagnostics in the Cisco ISE instance.

Table A-9 ISE Configuration Changes

Option	Description
Administrator	Choose a valid administrator username for the threshold.
Object Name	Enter the name of the object for the threshold.
Object Type	Choose a valid object type for the threshold.
Change	Select a administrative change for the threshold: • Any • Create—Includes “duplicate” and “edit” administrative actions. • Update • Delete
Filter	
ISE Instance	Choose a valid Cisco ISE instance for the threshold.

ISE System Diagnostics

Modify the fields described in the following table to define threshold criteria based on system diagnostics in the Cisco ISE instance.

Table A-10 ISE System Diagnostics

Option	Description
Severity at and above	Choose the severity level for the threshold. This setting captures the indicated severity level and those that are higher within the threshold: • **Fatal** • **Error** • **Warning** • **Info** • **Debug**
Message Text	Enter the message text for the threshold. Maximum character limit is 1024.
Filter	
ISE Instance	Choose a valid Cisco ISE instance for the threshold.

ISE Process Status

Modify the fields described in the following table to define rule criteria based on Cisco ISE process status.

Table A-11 ISE Process Status

Option	Description
Monitor Processes	
ISE Database	Adds the ISE database to the configuration.
ISE Database Listener	Adds the ISE management to the configuration.
ISE Application server	Adds the ISE runtime to the configuration.
ISE M&T Session	Monitors this process. If this process goes down, an alarm is generated.
ISE M&T Log Collector	Monitors this process. If this process goes down, an alarm is generated.
ISE M&T Alert Process	Monitors this process. If this process goes down, an alarm is generated.
ISE M&T Log Processor	Monitors this process. If this process goes down, an alarm is generated.
Filter	
ISE Instance	Choose a valid Cisco ISE instance for the threshold.

ISE System Health

Modify the fields described in the following table to define threshold criteria for Cisco ISE system health.

Table A-12 ISE System Health

Option	Description
Average over the past	Select the amount of time, where <min> minutes values are: 15, 30, 45, 60
Load Average	Enter an integer value of Load Average. The default threshold for load average is 2 and it may trigger many false alarms in the Cisco ISE, Release 1.1.x. You must manually adjust this threshold according to the number of cores that are available to Cisco ISE nodes. The load average is different from the CPU percentage in two significant ways: • Load averages are an instantaneous snapshot, and measure the trend in the CPU utilization. • Load averages include all the demand for the CPU, and shows how much the CPU was active at the time of measurement. If the load average increases above the number of cores (not physical CPUs), it means that the CPU is heavily loaded, and there is more demand for the CPU. If the load average recedes, there is less demand for the CPU.
Memory	Enter the percentage of memory usage (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk I/O	Enter the percentage of disk usage (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/local disk	Enter the percentage of local disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/	Enter the percentage of the / disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/tmp	Enter the percentage of temporary disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Filter	
ISE Instance	Choose a valid Cisco ISE instance.

ISE AAA Health

Modify the fields described in the following table to define threshold criteria for Cisco ISE AAA Health.

Table A-13 ISE AAA Health

Option	Description
Average over the past	Select the amount of time, where <min> minutes values are: 15, 30, 45, 60
RADIUS Throughput	Enter the number of RADIUS transactions per second (lesser than or equal to the specified value). The valid range is from 1 to 999999.
RADIUS Latency	Enter the number in milliseconds for RADIUS latency (greater than or equal to the specified value). The valid range is from 1 to 999999.
Filter	
ISE Instance	Choose a valid Cisco ISE instance for the threshold.

Authenticated But No Accounting Start

Modify the fields described in the following table to define the threshold rule criteria for a specified number of authenticated sessions for a device IP.

Table A-14 Authentication But No Accounting Start

Option	Description
More than <*num*> authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	<*num*>—A count of authenticated sessions in the past 15 minutes.
Filter	
Device IP	Choose or enter a valid device IP address.

Unknown NAD

Modify the fields described in the following table to define threshold criteria based on authentications that have failed because of an unknown NAD.

Table A-15 Unknown NAD

Option	Description
Unknown NAD count	Greater than *num* in the past *time Minutes|Hours* for a *object*, where: • *num* values can be any five-digit number greater than or equal to zero (0). • *time* values can be 1 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – ISE Instance – Device IP
Filter	

Table A-15 Unknown NAD

Option	Description
ISE Instance	Choose a valid Cisco ISE instance.
Device IP	Choose or enter a valid device IP address .
Protocol	Select a protocol for the threshold. The valid option is RADIUS.

External DB Unavailable

Modify the fields described in the following table to define threshold criteria based on an external database that Cisco ISE is unable to connect to.

Table A-16 External DB Unavailable

Option	Description
External DB Unavailable	*percent|count* greater than *num* in the past *time Minutes|Hours* for a *object*, where: • Percent|Count value can be Percent or Count. • *num* values can be any one of the following: – 0 to 99 for percent – 0 to 99999 for count • *time* values can be 1 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – ISE Instance – Identity Store
Filter	
ISE Instance	Choose a valid Cisco ISE instance.
Identity Group	Choose a valid identity group name.
Identity Store	Choose a valid identity store name.
Allowed Protocol	Choose a valid allowed protocol name.
Protocol	Select a protocol. The valid option is RADIUS.

RBACL Drops

Modify the fields described in the following table to define the RBACL Drops threshold.

Table A-17 RBACL Drops

Option	Description
RBACL drops	Greater than *num* in the past *time Minutes|Hours* by a <*object*>, where: • *num* values can be any five-digit number greater than or equal to zero (0). • *time* values can be 1 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – SGT – DGT – DST_IP
Filter	
SGT	Choose or enter a valid source group tag.
DGT	Choose or enter a valid destination group tag.
Destination IP	Choose or enter a valid destination IP address.

NAD-Reported AAA Downtime

Modify the fields described in the following table to define threshold criteria based on the AAA downtime that a network access device reports.

Table A-18 NAD-Reported AAA Downtime

Option	Description
AAA down	Greater than *num* in the past *time Minutes|Hours* by a *object*, where: • *num* values can be any five-digit number greater than or equal to zero (0). • *time* values can be 1 to 1440 minutes, or 1to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – Device IP – Device Group
Filter	
ISE Instance	Choose a valid ISE instance.
Device IP	Choose or enter a valid device IP address.
Device Group	Choose a valid device group name.

Schedules

Click **Operations > Alarms > Schedules** to establish schedules for alarm rules.

Table A-19 Schedules

Option	Description
Filter	Enter a text string on which to filter for a schedule.
Go	Click to filter on the text string.
Clear Filter	Click to clear the filter field.
Name	The name of the schedule. Click the name link to view and/or edit schedule details.
Description	Description of the schedule.
Create	Click to create a new schedule. Specify the following: • Name • Description • Schedule—Click a square to select/deselect that hour. • Select All—Click to select all hours. • Clear All—Click to clear all selected hours. • Undo All—Click to clear all fields on this page. • Submit—Click to create the schedule. • Cancel—Click to cancel to exit without saving the schedule.
Edit	Select a schedule and click Edit to make changes to the schedule. Edit options are the same as the Create options.
Delete	Select a schedule and click Delete to delete the schedule. Confirm you choice by clicking Yes in the Confirm Deletion dialog, or No to exit without deleting the schedule.

Reports

This section covers the following user interface elements:

Catalog

Select **Operations > Reports > Catalog.** Preconfigured system reports are grouped in categories, as shown in Report Type by Category, page A-16.

Report Type by Category

Table A-20 Report Type by Category

Report Name	Description	Logging Category
AAA Protocol		
AAA_Diagnostics	Provides AAA diagnostic details based on severity for a selected time period.	Policy diagnostics, Identity Stores Diagnostics, Authentication Flow Diagnostics, RADIUS Diagnostics
Authentication_Trend	Provides RADIUS authentication summary information for a selected time period; along with a graphical representation.	Passed authentications, Failed attempts
RADIUS_Accounting	Provides user accounting information based on RADIUS for a selected time period.	RADIUS accounting
RADIUS_Authentication	Provides RADIUS authentication details for a selected time period.	Passed authentications, Failed attempts
Allowed Protocol		
Allowed_Protocol_Authentication_Summary	Provides RADIUS authentication summary information for a particular allowed protocol for a selected time period; along with a graphical representation.	Passed authentications, Failed attempts
Top_N_Authentications_By_Allowed_Protocol	Provides the top N passed, failed, and total authentication count for RADIUS authentications with respect to the allowed protocol for a selected time period.	Passed authentications, Failed attempts
Server Instance		
OCSP Monitoring	Provides a summary of all the OCSP certificate validation operations performed by Cisco ISE.	System statistics
Server_Administrator_Entitlement	Provides a list of administrators and their assigned entitlement roles.	Resources and privileges, configuration changes, logins
Server_Administrator_Logins	Provides access-related events for administrators that includes login, logout, events, and information about excessive failed login attempts over standalone, and other distributed nodes when the account is locked or disabled in Cisco ISE.	Administrative and operational audit

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Server_Authentication_Summary	Provides RADIUS authentication summary information for a particular ISE instance for a selected time period, along with a graphical representation. This report could take several minutes to run depending on the number of records in the database. **Note** When you reload this report, if rate of incoming syslog messages is around 150 messages per second or more, the total number of passed and failed authentications that appear above the graph and the passed and failed authentication count that is displayed in the table do not match.	Passed authentications, Failed attempts
Server_Configuration_Audit	Provides all the configuration changes done in ISE by the administrator for a selected time period.	Administrative and operational audit
Server_Health_Summary	Provides the CPU, memory utilization, RADIUS and throughput (in tabular and graphical formats) and also process status, process downtime, and disk space utilization for a particular ISE instance in a selected time period.	System statistics
Server_Operations_Audit	Provides all the operational changes done in ISE by the administrator for a selected time period.	Administrative and operational audit
Server_System_Diagnostics	Provides system diagnostic details based on severity for a selected time period.	Internal Operations Diagnostics, distributed management, administrator authentication and authorization
Top_N_Authentications_By_Server	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to a particular ISE instance for a selected time period.	Passed authentications, Failed attempts
User_Change_Password_Audit	Provides the username of the internal user, identity store name, name of the ISE instance, and time when the user password was changed. Helps to keep track of all changes made to internal user passwords across all ISE interfaces.	Administrative and operational audit
Endpoint		
Endpoint_MAC_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular MAC or MAB for a selected time period, along with a graphical representation.	Passed authentications, Failed attempts
Endpoint_Profiler_Summary	Provides the endpoint profiler summary information for a particular MAC address for a selected time period.	Profiler
Endpoint_Time_To_Profile	Provides information on time taken to an endpoint that has an Unknown profile by using a particular MAC address for a selected time period.	Profiler
Top_N_Authentications_By_ Endpoint_Calling _Station_ID	Provides the top N passed, failed, and total authentication count with respect to endpoint calling station IDs.	Passed authentications, Failed attempts

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Top_N_Authentications_By_Machine	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to machine information for a selected time period.	Passed authentications, Failed attempts
Failure Reason		
Authentication_Failure_Code_Lookup	Provides the description and the appropriate resolution steps for a particular failure reason.	—
Failure_Reason_Authentication_Summary	Provides the RADIUS authentication summary information for a particular failure reason, along with a graphical representation for a selected time period.	Failed attempts
Top_N_Authentications_By_Failure_Reason	Provides the top N failed authentication count for RADIUS protocols with respect to Failure Reason for a selected time period.	Failed attempts
Network Device		
AAA_Down_Summary	Provides the number of AAA unreachable events that a NAD logs within a selected time period.	Passed authentications, Failed attempts
Network_Device_Authentication_Summary	Provides the RADIUS authentication summary information for a particular network device for a selected time period, along with a graphical representation.	Passed authentications, Failed attempts
Network_Device_Log_Messages	Provides you the log information of a particular network device, for a specified time period.	Passed authentications, Failed attempts
Session_Status_Summary	Provides the port sessions and status of a particular network device obtained by SNMP.	—
Top_N_AAA_Down_By_Network_Device	Provides the number of AAA down events encountered by each of the network devices.	Passed authentications, Failed attempts
Top_N_Authentications_By_Network_Device	Provides the top N passed, failed, and total authentication count for RADIUS with respect to network device for a selected time period.	Passed authentications, Failed attempts
User		
Client_Provisioning	Provides a summary of successful and unsuccessful client provisioning evaluation and download events, displayed according to the associated User ID.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Guest_Accounting	Provides session (login and log out) information for selected guests over a specified time period.	Passed authentications, RADIUS accounting
Guest_Activity	Provides guest information for a selected time period.	Passed authentications
Guest_Sponsor_Summary	Provides sponsor information along with a graphical representation, for a selected time period.	Passed authentications
Supplicant_Provisioning	Provides information about a list of endpoints that are registered through the Asset Registration Portal (ARP) for a specific period of time.	—

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Top_N_Authentications_By_User	Provides top N passed, failed, and total authentication count for RADIUS with respect to users for a selected time period.	Passed authentications, Failed attempts
Unique_Users	Provides the count for the number of unique users.	Passed authentications, Failed attempts
User_Authentication_Summary	Provides RADIUS authentication summary information for a particular user for a selected time period; along with the graphical representation.	Passed authentications, Failed attempts
Security Group Access		
PAC Provisioning	Provides a summary of SGA PAC generated.	—
Policy CoA	Provides the summary of the policy change request through policy CoA.	—
RBACL_Drop_Summary	Provides a summary of RBAC drop events.	—
SGT_Assignment_Summary	Provides a summary of SGT assignments for a selected time period.	Passed authentications
Top_N_RBACL_Drops_By_ Destination	Provides the top N RBACL drop event count with respect to destination for a selected time period.	—
Top_N_RBACL_Drops_By_User	Provides the top N RBACL drop event count with respect to the user for a selected time period.	—
Top_N_SGT_Assignments	Provides the top N SGT assignment count for a selected time period.	Passed authentications
Session Directory		
RADIUS_Active_Sessions	Provides information on RADIUS authenticated, authorized, and started sessions. Dynamically control active RADIUS sessions. Send a reauthenticate or disconnect request to a NAD to perform the following CoA actions: • Quarantine • Session reauthentication • Session reauthentication with last • Session reauthentication with rerun • Session termination • Session termination with port bounce • Session termination with port shut down The RADIUS_Active_Sessions report will display WLC Roam status as N (N stands for No) for any wired active session.	Passed authentications, RADIUS accounting
RADIUS_Session_History	Provides a summary of RADIUS session history, such as total authenticated, active, and terminated sessions and total and average session duration and throughput for a selected time period.	Passed authentications, RADIUS accounting

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
RADIUS_Terminated_Sessions	Provides all the RADIUS terminated session information for a selected time period.	Passed authentications, RADIUS accounting
Posture		
Posture_Detail_Assessment	Provides the posture authentication summary information for a particular user for a selected time period.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Posture_Trend	Provides the count of passed or failed, as well as status information for a particular policy for a selected time period; along with the graphical representation.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Endpoint Protection Service		
Endpoint_Operations_History	Provides EPS action history information comprising these values: Timestamp, Endpoint MAC Address, Endpoint IP Address, Operation Type, Operation Status, Operation ID, Audit Session ID, Admin Username, AdminIP Address.	—
MyDevices		
Registered Endpoints	Provides information about a list of endpoints that are registered through the Asset Registration Portal (ARP) by a specific user for a selected period of time.	—

Report Type Page

Select a category name from the Reports navigation pane. The Reports Type page appears.

Table A-21 Report Type Page

Option	Description
Report Name	A list of available report names for the category you selected.
Type	The type of report.

Table A-21 Report Type Page

Option	Description
Modified At	The time the report was last modified by an administrator, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.
Filter	Enter a text string to search for a report in the text field and click **Go**. Click **Clear Filter** to list the Catalog reports.

Report Name Page

Not all options listed in the following table are used in all reports.

Table A-22 Report Name Page

Option	Description
User	Enter a username or click **Select** to enter a valid username on which to configure your threshold.
MAC Address	Enter a MAC address or click **Select** to enter a valid MAC address on which to run your report.
Identity Group	Enter an identity group name or click **Select** to enter a valid identity group name on which to run your report.
Device Name	Enter a device name or click **Select** to enter a valid device name on which to run your report.
Device IP	Enter a device IP address or click **Select** to enter a valid device IP address on which to run your report.
Device Group	Enter a device group name or click **Select** to enter a valid device group name on which to run your report.
Allowed Protocol	Enter an allowed protocol name or click **Select** to enter a valid allowed protocol name on which to run your report
Identity Store	Enter an identity store name or click **Select** to enter a valid identity store name on which to run your report.
ISE Instance	Enter an ISE instance name or click **Select** to enter a valid ISE instance name on which to run your report.
Failure Reason	Enter a failure reason name or click **Select** to enter a valid failure reason name on which to run your report.
Protocol	Use the drop down list box to select which protocol on which you want to run your report. RADIUS is the only option at this time.
Authentication Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: • Pass Or Fail • Pass • Fail
Radius Audit Session ID	Enter the RADIUS audit session identification name on which you want to run a report.
ISE Session ID	Enter the ISE session identification name on which you want to run a report.

Table A-22 Report Name Page

Option	Description
Severity	Use the drop down list box to select the severity level on which you want to run a report. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: • Fatal • Error • Warning • Info • Debug
End Point IP Address	Enter the end point IP address on which you want to run a report.
Command Accounting Only	Check the check box to enable your report to run for command accounting.
Top	Use the drop down list box to select the number of top (most frequent) authentications by allowed protocol on which you want to run your report. Valid options are: • 10 • 50 • 100 • 500 • 1000 • All
By	Use the drop down list box to select the type of authentications on which you want to run your report. Valid options are: • Passed Authentications • Failed Authentications • Total Authentications
Administrator Name	Enter the administrator username, or click Select to select the administrator username, for which you want to run your report.
Object Type	Enter a valid object type on which you want to run your report.
Object Name	Enter the name, or click Select to select the object name, of the object on which you want to run your report.
Authorization Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: • Pass Or Fail • Pass • Fail

Table A-22 Report Name Page

Option	Description
Time Range	Use the drop down list box to select the time range on which you want to run your report. Valid options are: • Last Hour (for the ISE Health Summary report only) • Today • Yesterday • Last 7 Days • Last 30 Days • Custom—You must configure a Start Date and End Date, or a Day. **Note** Some options are not valid for some Time Range entries of the various reports.
Start Date	Enter a date, or click the date selector icon to select a start date for running your report.
End Date	Enter a date, or click the date selector icon to select an end date for running your report.
Day	Enter a date, or click the date selector icon to select an end date for running your report.
Clear	Click to delete the contents of an associate text box.
Run	Click to run the report for which you have made selections.

Favorites

Select **Operations > Reports > Favorites** to display a list of favorite reports. Favorites allows you to bookmark frequently used reports by saving them as favorite reports.

customized.

The following preconfigured catalog system reports are available in **Operations > Reports > Favorites** by default:

- Authentications - RADIUS - Today—A report that is preconfigured from AAA Protocol > RADIUS_Authentication to run for the current system date.
- Authentications - RADIUS - Yesterday—A report that is preconfigured from AAA Protocol > RADIUS_Authentication to run for the previous day from the current system date.
- ISE-Server Configuration Audit - Today—A report that is preconfigured from Server Instance > Server_Configuration_Audit to run for the current system date.
- ISE-System Diagnostics -Today—A report that is preconfigured from Server Instance > Server_System_Diagnostics to run for the current system date.

For a list of all available reports, see Report Type by Category, page A-16.

Favorites Page

Table A-23 Favorites Page

Option	Description
Favorite Name	The name of the favorites report. Click to open a summary of an associated report.
Report Name	The report name associated with a Catalog (Report) type.
Report Type	The general category name associated with the report.

Report Context Menus

Use context menus as shortcuts to performing data formatting and organizing tasks from the Interactive Viewer. To bring up a context menu, right click an element in a report. The context menu options that are displayed are unique to the element selected.

For more information, see Organizing and Formatting Report Data, page 25-11.

Related Topics

- Data Formatting, page A-27
- Filters, page A-39

Table A-24 Report Context Menus

Option	Description
Aggregation	Opens a dialog box that supports creating an aggregate row for this column.
Alignment	Opens a submenu that contains: • Align Left. Aligns the column data to the left. • Align Center. Centers the column data. • Align Right. Aligns the column data to the right.
Calculation	Opens a submenu that supports creating a calculated column based on this column.
Chart	Opens a submenu that supports inserting a chart.
Column	Opens a submenu that contains: • Delete Column. Deletes the selected column. • Reorder Columns. Opens a dialog box that supports changing the order of columns in the report design. • Column Width. Opens the Column Properties dialog box, which supports setting the column width. • Do Not Repeat Values. Suppresses consecutive duplicate data values in a column. If the column is already set to Do Not Repeat Values, this menu item changes to Repeat Values.
Data Fields	Opens a dialog box that displays the report columns. Supports adding or removing data fields.

Table A-24 Report Context Menus (continued)

Option	Description
Filter	Opens a submenu that contains: • Filter. Opens a dialog box that supports creating filters based on this column. • Top or Bottom N. Opens a dialog box that supports displaying the highest or lowest *n* values or the highest or lowest *n* percent in the column.
Format Data	Opens a dialog box that supports formatting the data type. For example, if the column contains numeric data, the Number column format dialog box opens and you can format the data as currency, percentages, and so on.
Group	Opens a submenu that contains: • Add Group. Creates a group based on this column. When you select a grouped column, this menu item changes to Delete Group. • Add Section. Creates a section based on this column. When you select a section column, this menu item changes to Delete Section. • Hide Detail. Hides the group's or section's detail rows. If the detail rows are hidden, this menu item changes to Show Detail. This option is available when you select a grouped column or a section column. • Page Break. Sets a page break before or after a group or section. This option is available when you select a grouped column or a section column.
Sort	Opens a submenu that contains: • Sort Ascending. Sorts the column rows in ascending order. • Sort Descending. Sorts the column rows in descending order. • Advanced Sort. Opens the Advanced Sort dialog box, which supports performing a sort based on additional columns.
Style	Opens a submenu that contains: • Font. Opens the Font dialog box, which supports modifying the font properties of column data. • Conditional Formatting. Opens a dialog box that supports setting conditional formatting rules for data in this column.

Data Formatting

This section describes data formatting for you to format data presented in the reports by using the Interactive Viewer.

Data Types and Formats

Table A-25 Data Types and Formats

Data type	Option	Description
Date and Time	Unformatted	The data retains the default format set by the template or theme.
	General Date	June 5, 2006 12:00:00 AM GMT +00:00
	Long Date	June 5, 2006
	Medium Date	Jun 5, 2006
	Short Date	6/5/06
	Long Time	12:00:00 AM GMT +00:00
	Medium Time	12:00:00 AM
	Short Time	12:00
	Custom	The format depends on a format code you type. For example, typing yyyy/mm results in 2006/10. You learn more about custom formatting later in this chapter.
Number	Unformatted	The number retains the default format set by the template or theme.
	General Number	6066.88 or 6067, depending on the decimal and thousands separator settings
	Currency	$6,067.45 or ¥6067, depending on the locale and optional settings
	Fixed	6067 or 6,067 or 6067.45, depending on optional settings
	Percent	45% or 45.8%, depending on optional settings
	Scientific	2E04 or 2.67E04, where the number after the E represents the exponent of 10, depending on optional settings. For example, 2.67E04 means 2.67 multiplied by 10 raised to the fourth power.
	Custom	The format depends on a format code you type. For example, typing #,### results in a format with a comma as a thousands separator and no decimal points. You learn more about custom formats later in this chapter.
String	Unformatted	The string retains the default format set by the template or theme.
	Uppercase	The string displays in all uppercase, for example GREAT NEWS.
	Lowercase	The string displays in all lowercase, for example great news.
	Custom	The format depends on the format code you type. Use custom formatting for postal codes, telephone numbers, and other data that does not match standard formats.

Custom Number Format Patterns

Table A-26 Custom Number Format Patterns

Format pattern	Data in the data set	Result of formatting
0000.00	12.5 124.5 1240.553	0012.50 0124.50 1240.55
#.000	100 100.25 100.2567	100.000 100.250 100.257
$#,###	2000.00 20000.00	$2,000 $20,000
ID #	15	ID 15

Symbols for Defining Custom String Formats

Symbol	Description
@	Character placeholder. Each @ character displays a character in the string. If the string has fewer characters than the number of @ symbols that appear in the format pattern, spaces appear. Placeholders are filled from right to left, unless you specify an exclamation point (!) at the beginning of the format pattern.
&	Same as @, except that if the string has fewer characters, spaces do not appear.
!	Specifies that placeholders are to be filled from left to right.
>	Converts string characters to uppercase.
<	Converts string characters to lowercase.

Results of Custom String Format Patterns

Table A-27 Results of Custom String Format Patterns

Format pattern	Data in the data source	Results of formatting
(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 ( ) 555-1007
(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 () 555-1007
!(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 (555) 100-7
!(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 (555) 100-7
!(@@@) @@@-@@@@ + ext 9	5551007	(555) 100-7 + ext 9
!(&&&) &&&-&&&& + ext 9	5551007	(555) 100-7 + ext 9
>&&&-&&&&&-&&	D1234567xy	D12-34567-XY
<&&&-&&&&&-&&	D1234567xy	d12-34567-xy

Results of Custom Date Formats

Table A-28 Results of Custom Date Formats

Format	Result of formatting
MM-dd-yy	04-15-06
E, M/d/yyyy	Fri, 4/15/2006
MMM d	Apr 15
MMMM	April
yyyy	2006
W	3 (the week in the month)
w	14 (the week in the year)
D	105 (the day in the year)

Supported Calculation Functions

Table A-29 Supported Calculation Functions

Function	Description	Example of use
ABS(num)	Displays an absolute value for the data in a column.	`ABS([TemperatureCelsius])`
ADD_DAY (date, daysToAdd)	Adds a specified number of days to a date value and displays the result as a date value.	`ADD_DAY([ClosingDate], 30)`
ADD_HOUR (date, hoursToAdd)	Adds a specified number of hours to a time value and displays the result as a time value.	`ADD_HOUR([OpenHour], 8)`
ADD_MINUTE (date, minutesToAdd)	Adds a specified number of minutes to a time value and displays the result as a time value.	`ADD_MINUTE([StartTime], 60)`
ADD_MONTH (date, monthsToAdd)	Adds a specified number of months to a date value and displays the result as a date value.	`ADD_MONTH([InitialRelease], 2)`
ADD_QUARTER (date, quartersToAdd)	Adds a specified number of quarters to a date value.	`ADD_QUARTER([ForecastClosing], 2)`
ADD_SECOND (date, secondsToAdd)	Adds a specified number of seconds to a time value.	`ADD_SECOND([StartTime], 30)`
ADD_WEEK (date, weeksToAdd)	Adds a specified number of weeks to a date value and displays the result as a date value.	`ADD_WEEK([askByDate], 4)`
ADD_YEAR (date, yearsToAdd)	Adds a specified number of years to a date value.	`ADD_YEAR([HireDate], 5)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
AND	Combines two conditions and returns records that match both conditions. For example, you can request records from customers who spend more than $50,000 a year and also have a credit rank of A.	This function is used to connect clauses in an expression and does not take arguments.
AVERAGE(expr)	Displays an average value for the column.	`AVERAGE([CostPerUnit])`
AVERAGE (expr, groupLevel)	Displays the average value at the specified group level.	`AVERAGE([TotalCost], 2)`
BETWEEN(value, upperBound, lowerBound)	For a specified column, displays true if a value is between two specified values and false otherwise. String values and date or time values must be enclose in quotation marks. For dates and times, use the short date and short time formats.	`BETWEEN([PostalCode], 11209, 12701)` `BETWEEN([ReceiptDate], "10/01/06", "12/31/06")`
CEILING (num, significance)	Rounds a number up, away from 0, to the nearest specified multiple of significance. For data that has been converted from a double or float to an integer, displays the smallest integer that is greater than or equal to the float or double.	`CEILING([PortfolioAverage], 1)`
COUNT( )	Counts the rows in a table.	`COUNT( )`
COUNT(groupLevel)	Counts the rows at the specified group level.	`COUNT(2)`
COUNTDISTINCT(expr)	Counts the rows that contain distinct values in a table.	`COUNTDISTINCT([CustomerID])` `COUNTDISTINCT([Volume]*2)`
COUNTDISTINCT (expr, groupLevel)	Counts the rows that contain distinct values at the specified group level.	`COUNTDISTINCT([CustomerID], 3)`
DAY(date)	Displays the number of a day in the month, from 1 to 31, for a date-and-time value.	`DAY([forecastShipping])`
DIFF_DAY(date1, date2)	Displays the difference between two date values, in the number of days.	`DIFF_DAY([checkoutDate], [returnDate])`
DIFF_HOUR(date1, date2)	Displays the difference between two time values, in the number of hours.	`DIFF_HOUR([StartTime],[Finish Time])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
DIFF_MINUTE (date1, date2)	Displays the difference between two time values, in the number of minutes.	`DIFF_MINUTE([StartTime], [FinishTime])`
DIFF_MONTH (date1, date2)	Displays the difference between two date values, in the number of months.	`DIFF_MONTH([askByDate], [shipByDate])`
DIFF_QUARTER (date1, date2)	Displays the difference between two date values, in the number of quarters.	`DIFF_QUARTER([PlanClosing], [ActualClosing])`
DIFF_SECOND (date1, date2)	Displays the difference between two time values, in the number of seconds.	`DIFF_SECOND([StartTime], [FinishTime])`
DIFF_WEEK(date1, date2)	Displays the difference between two weeks as a number.	`DIFF_WEEK([askByDate], [shipByDate])`
DIFF_YEAR(date1, date2)	Displays the difference between two years as a number.	`DIFF_YEAR([HireDate], [TerminationDate])`
false	The Boolean false. This function is used in expressions to indicate that an argument is false.	In the following example, false indicates that the second argument, ascending, is false and therefore the values should be returned in descending order. `RANK([Score], false)`
FIND(strToFind, str)	Displays the index of the first occurrence of specified text. The index is zero-based. The search is case sensitive and the search string cannot include wildcards. The value in the strToFind argument must be enclosed in quotation marks.	`FIND("HQ", [OfficeName])`
FIND(strToFind, str, startPosition)	Similar to FIND(strToFind, str) but supports providing a start position for the search. The index is zero-based.	`FIND("HQ", [OfficeName], 3)`
FIRST(expr)	Places the first value that appears in a specified column into the calculated column. This function supports viewing a row-by-row comparison against a specific value.	`FIRST([customerID])`
FIRST(expr, groupLevel)	Displays the first value that appears in the specified column at the specified group level.	`FIRST([customerID], 3)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
IF(condition, doIfTrue, doIfFalse)	Displays the result of an If...Then...Else statement.	`IF([purchaseVolume] >5 , 7 , 0)` where • [purchaseVolume] is the column name and >5 is the test condition. • 7 is the value to place in the new column if the condition is true. • 0 is the value to place in the new column if the condition is false.

IN(value, check)	Displays true if a data row contains a value specified by the check argument and false otherwise. String values and date or time values must be enclosed in quotation marks. For dates and times, use the short date and short time formats for your locale.	`IN([custID], 101)`
		`IN([city], "New Haven")`
		`IN([FinishTime], "16:09")`

IN(value, check1, ..., checkN)	Displays true if a data row contains any value specified by the check argument list and false otherwise. String values and date or time values must be enclosed in quotation marks. For dates and times, use the short date and short time formats for your locale.	`IN([city], "New Haven", "Baltimore", "Cooperstown")` `IN([ShipDate], "05/01/06", "05/10/06", "05/15/06")`
ISBOTTOMN(expr, n)	Displays true if the value is within the lowest *n* values for the expression, and false otherwise.	`ISBOTTOMN([OrderTotals], 50)`
ISBOTTOMN (expr, n, groupLevel)	Displays true if the value is within the lowest *n* values for the expression at the specified group level, and false otherwise.	`ISBOTTOMN([OrderTotals], 50, 2)`
ISBOTTOMNPERCENT (expr, percent)	Displays the lowest *n* percentage.	`ISBOTTOMNPERCENT([Sales Total], 5)`
ISBOTTOMNPERCENT (expr, percent, groupLevel)	Displays the lowest *n* percentage for the expression at the specified group level.	`ISBOTTOMNPERCENT([Sales Total], 5, 3)`
ISNULL(value)	Displays true if a row does not display a value. Displays false if a row displays a value.	`ISNULL([DepartmentName])`
ISTOPN(expr, n)	Displays true if the value is within the highest *n* values for the expression, and false otherwise.	`ISTOPN([OrderTotals], 10)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
ISTOPN(expr, n, groupLevel)	Displays true if the value is within the highest *n* values for the expression at the specified group level, and false otherwise.	`ISTOPN([OrderTotals], 10, 3)`
ISTOPNPERCENT(expr, percent)	Displays true if the value is within the highest *n* percentage, and false otherwise.	`ISTOPNPERCENT([SalesTotals], 5)`
ISTOPNPERCENT(expr, percent, groupLevel)	Displays true if the value is within the highest *n* percentage values for the expression at the specified group level, and false otherwise.	`ISTOPNPERCENT([SalesTotals], 5, 3)`
LAST(expr)	Displays the last value in a specified column.	`LAST([FinishTime])`
LAST(expr, groupLevel)	Displays the last value for the expression at the specified group level.	`LAST([FinishTime], 3)`
LEFT(str)	Displays the character at the left of the specified string.	`LEFT([city])`
LEFT(str, n)	Displays the specified number of characters in a column's string, counting from the left.	`LEFT([city], 3)`
LEN(str)	Displays the length of a string, including spaces and punctuation marks.	`LEN([Description])`
LIKE(str)	Displays true if the values match, and false otherwise. Use SQL syntax to specify the string pattern. The following rules apply: • Literal pattern characters must match exactly. LIKE is case-sensitive. • A percent character (%) matches zero or more characters. • An underscore character (_) matches any single character. • Escape a literal percent, underscore, or backslash character (\) with a backslash character.	`LIKE([customerName], "D%")` `LIKE([quantityOrdered], "2_")`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
LOWER(str)	Displays the string in a specified column in lowercase.	`LOWER([cityName])`
MAX(expr)	Displays the highest value in the specified column.	`MAX([OrderTotal])`
MAX(expr, groupLevel)	Displays the highest value for the expression at the specified group level.	`MAX([OrderTotal], 2)`
MEDIAN(expr)	Displays the median value in a specified column.	`MEDIAN([HomePrices])`
MEDIAN (expr, groupLevel)	Displays the median value for the expression at the specified group level.	`MEDIAN([HomePrices], 2)`
MIN(expr)	Displays the lowest value in the specified column.	`MIN([OrderTotal])`
MIN(expr, groupLevel)	Displays the lowest value for the expression at the specified group level.	`MIN([OrderTotal], 1)`
MOD(num, div)	Displays the remainder after a number is divided by a divisor. The result has the same sign as the divisor.	`MOD([Salary], 12)`
MONTH(date)	Displays the name of the month for a specified date-and-time value.	`MONTH([ForecastShipDate])`
MONTH(date, option)	Displays the month of a specified date-and-time value, in one of three optional formats: • 1 - Displays the month number of 1 through 12. • 2 - Displays the complete month name in the user's locale. • 3 - Displays the abbreviated month name in the user's locale.	`MONTH([Semester], 2)`
MOVINGAVERAGE (expr, window)	Displays an average value over a specified window, such as an average price or volume over a number of days.	`MOVINGAVERAGE([Price], [Days])`
NOTNULL(value)	For a specified column, displays true if a data value is not empty. Displays false if a data value is empty.	`NOTNULL([DepartmentID])`
NOW( )	Displays the current time stamp.	`NOW([PastDueDate])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
OR	The logical OR operator.	This function is used to connect clauses in an expression and does not take arguments.
PERCENTILE(expr, pct)	Displays a percentile value, a value on a scale of 100 that indicates the percent of a distribution that is equal to or below the specified value. Valid pct argument ranges are 0 to 1. 0 returns the minimum value of the series. 1 returns the maximum value of the series.	`PERCENTILE([Rank], 1)`
PERCENTILE (expr, pct, groupLevel)	Displays a percentile value for the expression at the specified group level. Valid pct argument ranges are 0 to 1. 0 returns the minimum value of the series. 1 returns the maximum value of the series.	`PERCENTILE([Income], 60, 1)`
PERCENTRANK(expr)	Displays the percentage rank of a value.	`PERCENTRANK([TestScores])`
PERCENTRANK(expr, groupLevel)	Displays the percentage rank of a value at the specified group level.	`PERCENTRANK([TestScores], 2)`
PERCENTSUM(expr)	Displays a value as a percentage of a total.	`PERCENTSUM([OrderTotals])`
PERCENTSUM(expr, groupLevel)	Displays a value as a percentage of a total at the specified group level.	`PERCENTSUM([OrderTotals], 3)`
QUARTER(date)	Displays the quarter number, from 1 through 4, of a specified date-and-time value.	`QUARTER([ForecastCloseDate])`
QUARTILE(expr, quart)	Displays the quartile value, where the quart argument is an integer between 0 and 4.	`QUARTILE([OrderTotal], 3)`
QUARTILE (expr, quart, groupLevel)	Displays the quartile value for the expression at the specified group level, where the quart argument is an integer between 0 and 4.	`QUARTER([OrderTotal], 2, 3)`
RANK(expr)	Displays the rank of a number, string, or date-and-time value, starting at 1. Duplicate values receive identical rank but the duplication does not affect the ranking of subsequent values.	`RANK([AverageStartTime])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
RANK(expr, ascending, groupLevel)	Displays the rank of a number, string, or date-and-time value in either ascending or descending order, at the specified group level. To display values in ascending order, use true as the second argument. To display values in descending order, use false as the second argument.	`RANK([Score], false, 3)` `RANK([Score], true, 2)`
RIGHT(str)	Displays the character at the right of a string.	`RIGHT([name])`
RIGHT(str, n)	Displays the specified number of characters in a string, counting from the right.	`RIGHT([name], 3)`
ROUND(num)	Rounds a number.	`ROUND([SalesTarget])`
ROUND(num, dec)	Rounds a number to the specified number of digits. The default value for dec is 0.	`ROUND([StockValue], 2)`
ROUNDDOWN(num)	Rounds a number down.	`ROUNDDOWN([StockPrice])`
ROUNDDOWN(num, dec)	Rounds a number down, away from 0, to the specified number of digits. The default value for dec is 0.	`ROUNDDOWN([StockPrice], 2)`
ROUNDUP(num)	Rounds a number up.	`ROUNDUP([TotalValue])`
ROUNDUP(num, dec)	Rounds a number up, away from 0, to the specified number of digits. The default value for dec is 0.	`ROUNDUP([TotalValue], 2)`
RUNNINGSUM(expr)	Displays a running total, adding the values in successive data rows.	`RUNNINGSUM([StockValue])`
SEARCH(pattern, str)	Case-insensitive search function that can use wildcard characters. An asterisk (*) matches any sequence of characters, including spaces. A question mark (?) matches any single character.	The following search yields New York, New Haven, and so on from the City column: `SEARCH([CustomerData:city], "new*")`
SEARCH (pattern, str, startPosition)	Searches for a specified pattern in a string, starting at a specified position in the string. A case-insensitive search function that can use wildcard characters.	`SEARCH([Location], "new", 1)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
SQRT(num)	Displays the square root of a value.	`SQRT([PrincipalValue])`
STDEV(expr)	Displays the standard deviation.	`STDEV([PurchaseFrequency])`
SUM(expr)	Displays the sum of two specified values.	`SUM([Price]+[Tax])`
TODAY( )	Displays a time stamp value equal to midnight of the current date.	`TODAY([DueDate])`
TRIM(str)	Displays a string with all leading and trailing blank characters removed. Also removes all consecutive blank characters. Leading and trailing blanks can be spaces, tabs, and so on.	`TRIM([customerName])`
TRIMLEFT(str)	Displays a string with all leading blanks removed. Does not remove consecutive blank characters.	`TRIMLEFT([PortfolioName])`
TRIMRIGHT(str)	Displays a string with all trailing blanks removed. Does not remove consecutive blank characters.	`TRIMRIGHT([Comments])`
true	The Boolean true. This function is used in expressions to indicate that an argument is true.	In the following example, true indicates that the second argument, ascending, is true and therefore the values should be returned in ascending order. `RANK([Score], true)`
UPPER(str)	Displays a string in a specified column in all uppercase.	`UPPER([cityName])` `UPPER("new haven")`
VAR(expr)	Displays a variance for the specified expression.	`VAR([EstimatedCost])`
WEEK(date)	Displays the number of the week, from 1 through 52, for a date-and-time value.	`WEEK([LeadQualifyingDate])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
WEEKDAY(date, option)	Displays the day of the week in one of the following format options: • 1 - Returns the day number, from 1 (Sunday) through 7 (Saturday). 1 is the default option. • 2 - Returns the day number, from 1 (Monday) through 7 (Sunday). • 3 - Returns the day number, from 0 (Monday) through 6 (Sunday). • 4 - Returns the weekday name according to the user's locale. • 5 - Returns the abbreviated weekday name according to the user's locale.	`WEEKDAY([DateSold], 4)`
WEIGHTEDAVERAGE (value, weight)	Displays a weighted average of a specified value.	`WEIGHTEDAVERAGE([Score], weight)`
YEAR(date)	Displays the four-digit year value for a date-and-time value.	`YEAR([ClosingDate])`

Supported Operator Formats

Table A-30 Supported Operator Formats

Operator	Description
x + y	Addition of numeric values
x - y	Subtraction of numeric values
x * y	Multiplication of numeric values
x / y	Division of numeric values
x%	Percentage of a numeric value
x & y	Concatenation of string values
x = y	Test for equality of two values
x > y	Tests whether x is greater than y
x < y	Tests whether x is less than y
x >= y	Tests whether x is greater than or equal to y
x <= y	Tests whether x is less than or equal to y
x <> y	Tests whether x is not equal to y

Table A-30 Supported Operator Formats (continued)

Operator	Description
x AND y	Tests for values that meet both condition x and condition y
x OR y	Tests for values that meet either condition x or condition y
NOT x	Tests for values that are not x

Aggregate Function Formats

Table A-31 Aggregate Function Formats

Aggregate functions	Description
Average	Calculates the average value of a set of data values.
Count	Counts the data rows in the column.
Count Value	Counts distinct values in the column.
First	Returns the first value in the column.
Last	Returns the last value in the column.
Max	Returns the highest value in the column.
Median	Returns the median value in the column.
Min	Returns the lowest value in the column.
Mode	Returns the most frequently-occurring value in the column.
Quartile	Returns one of four equal-sized sets of data, based on the rank you select. For example, you can request the first quartile to get the top quarter of the data set or the fourth quartile to get the fourth quarter of the data set.
Standard Deviation	Returns the standard deviation, the square root of the variance.
Sum	Adds the values in the column.
Variance	Returns a value that indicates the spread around a mean or expected value.
Weighted average	Returns the weighted average of a numeric field over a set of data rows. In a weighted average, some numbers carry more importance, or weight, than others.

Filters

Conditions for Filters

Table A-32 Conditions for Filters

Condition	Description
Any Of	Returns any of the values you specify.
Between	Returns values that are between two specified values. When you select Between, a second Value field appears for the second default value.

Table A-32 Conditions for Filters (continued)

Condition	Description
Bottom N	Returns the lowest *n* values in the column.
Bottom Percent	Returns the lowest *n* percent of values in the column.
Equal to	Returns values that are equal to a specified value.
Greater Than	Returns values that are greater than a specified value.
Greater Than or Equal to	Returns values that are greater than or equal to a specified value.
Is False	In a column that evaluates to true or false, returns data rows that contain false values.
Is Not Null	Returns data rows that contain values.
Is Null	Returns data rows that do not contain values.
Is True	In a column that evaluates to true or false, returns data rows that contain true values.
Less Than	Returns values that are less than another value.
Less Than or Equal to	Returns values that are less than or equal to another value.
Like	Returns strings that match all or part of the specified string. % matches zero or more characters. _ matches one character.
Not Between	Returns values that are not between two specified values. When you select Not Between, a second Value field appears for the second default value.
Not Equal to	Returns values that are not equal to another value.
Not Like	Returns strings that do not match all or part of the specified string. % matches zero or more characters. _ matches one character.
Top N	Returns the top *n* values in the column.
Top Percent	Returns the top *n* percent of values in the column.

Filter Condition Examples

Table A-33 Filter Condition Examples

Type of filter condition	Description	Examples of instructions to data source

Comparison	Compares the value of one expression to the value of another expression using:
	• Equal to
	• Not Equal to
	• Less Than
	• Less Than or Equal to
	• Greater Than
	• Greater Than or Equal to
		`quantity = 10`
		`custName = 'Acme Inc.'`
		`custName > 'P'`
		`custState <> 'CA'`
		`orderDate > {d '2005-06-30'}`

Table A-33 Filter Condition Examples (continued)

Type of filter condition	Description	Examples of instructions to data source

Range	Tests whether the value of an expression falls or does not fall within a range of values using Between or Not Between. The test includes the endpoints of the range.	`price BETWEEN 1000 AND 2000`
		`custName BETWEEN 'E' AND 'K'`
		`orderDate BETWEEN`
		`{d '2005-01-01'} AND {d '2005-06-30'}`

Membership	Tests whether the value of an expression matches one value in a set of values using Any Of.	`officeCode IN (101,103,104)`
		`itemType IN ('sofa', 'loveseat',`
		`'endtable', 'clubchair')`
		`orderDate IN`
		`({d '2005-10-10'}, {d '2005-10-17'})`

Pattern-matching	Tests whether the value of a string field matches or does not match a specified pattern using Like or Not Like. % matches zero or more characters.
	_ matches one character.
		`custName LIKE 'Smith%'`
		`custName LIKE 'Smiths_n'`
		`custState NOT LIKE 'CA%'`

Null value	Tests whether a field has or does not have a null, or missing, value using Is Null or Is Not Null.	`manager IS NULL`
		`shipDate IS NULL`
		`shipDate IS NOT NULL`

Troubleshoot

To bring up Cisco ISE troubleshooting tools, go to **Operations > Troubleshoot > Diagnostic Tools**. Use the following tools to solve problems that may appear on your network:

- General Tools, page A-41
- Security Group Access Tools, page A-48

General Tools

To access the following General Tools for troubleshooting, go to **Operations > Troubleshoot > Diagnostic Tools** and expand **General Tools** in the left panel. Choose from the following tools:

- Connectivity Tests, page A-42
- RADIUS Authentication Troubleshooter, page A-42
- Execute Network Device Command, page A-44
- Evaluate Configuration Validator, page A-45
- Posture Troubleshooting, page A-46
- TCP Dump, page A-48

Connectivity Tests

Perform connectivity tests to troubleshoot failed authentications and other problems.

Table A-34 Connectivity Tests

Option	Description
Hostname or IP Address	Enter the hostname or IP address for a connection you want to test. Click **Clear** to clear the hostname or IP address .
ping	Click **ping** to view the packets sent and received, packet loss (if any) and the time it takes for the test to complete.
traceroute	Click **traceroute** to view the intermediary IP addresses (hops) between the Monitoring persona node and the tested hostname or IP address, and the time it takes for each hop to complete.
nslookup	Click **nslookup** cto view the server and IP address of your tested domain name server hostname or IP address.

RADIUS Authentication Troubleshooter

Check RADIUS authentication results and troubleshoot problems that may occur.

Table A-35 RADIUS Authentication Troubleshooter

Option	Description
Search and select a RADIUS authentication for troubleshooting	
Username	Enter the username of the user whose authentication you want to troubleshoot, or click **Select** to choose the username from a list. Click **Clear** to clear the username.
MAC Address	Enter the MAC address of the device that you want to troubleshoot, or click **Select** to choose the MAC address from a list. Click **Clear** to clear the MAC address.
Audit Session ID	Enter the audit session ID that you want to troubleshoot. Click **Clear** to clear the audit session ID.
NAS IP	Enter the NAS IP address or click **Select** to choose the NAS IP address from a list. Click **Clear** to clear the NAS IP address.
NAS Port	Enter the NAS port number or click **Select** to choose a NAS port number from a list. Click **Clear** to clear the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication from the Authentication Status drop-down list box. The available options are: • Pass or Fail • Pass • Fail
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.

Table A-35 RADIUS Authentication Troubleshooter (continued)

Option	Description
Time Range	Select a time range from the drop-down list. The RADIUS authentication records that are created during this time range are used: • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time	(Only if you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time	(Only if you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the end date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Choose the number of records that you want to fetch from the drop-down list: 10, 20, 50, 100, 200, or 500.

RADIUS Authentication Troubleshooting—Progress Details

Table A-36 RADIUS Authentication Troubleshooting Progress Details

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.

Table A-36 RADIUS Authentication Troubleshooting Progress Details (continued)

Option	Description
Use Console Server	Select this check box to use the console server.
Console IP Address	(If the Use Console Server check box is selected) Enter the console IP address.
Advanced (Use if there is an "Expect timeout error" or the device has non-standard prompt strings)	
Note The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

RADIUS Authentication Troubleshooting—Results Summary

Table A-37 RADIUS Authentication Troubleshooting Results Summary

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Execute Network Device Command

Execute the **show** command on a network device.

Table A-38 Execute Network Device Command

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device on which you want to run the command.
Command	Enter the **show** command.

Evaluate Configuration Validator

Evaluate the configuration of a network device and identify any configuration problems.

Table A-39 Evaluate Configuration Validator

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device whose configuration you want to evaluate.
Select the configuration items below that you want to compare against the recommended template.	
AAA	This option is selected by default.
RADIUS	This option is selected by default.
Device Discovery	This option is selected by default.
Logging	This option is selected by default.
Web Authentication	Select this check box to compare the web authentication configuration.
Profiler Configuration	Select this check box to compare the Profiler configuration.
SGA	Check this check box if you want to compare Security Group Access configuration.
802.1X	Check this check box if you want to compare the 802.1X configuration, and choose one of the following options: • Open Mode • Low Impact Mode (Open Mode + ACL) • High Security Mode (Closed Mode)

Progress Details

Table A-40 Progress Details

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.

Table A-40 Progress Details (continued)

Option	Description
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings)	
Note The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-41 Results Summary

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Posture Troubleshooting

Find and resolve posture problems on the network.

Table A-42 Posture Troubleshooting

Option	Description
Search and Select a Posture event for troubleshooting	
Username	Enter the username to filter on.
MAC Address	Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx-xx

Table A-42 Posture Troubleshooting (continued)

Option	Description
Posture Status	Select the authentication status to filter on: • Any • Compliant • Noncompliant • Unknown
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.
Time Range	Select a time range from the drop-down list . The RADIUS authentication records that are created during this time range are used: • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time:	(Only if you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time:	(Only if you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Select the number of records to display: 10, 20, 50, 100, 200, 500
Search Result	
Time	Time of the event
Status	Posture status
Username	User name associated with the event
MAC Address	MAC address of the system
Failure Reason	Failure reason for the event

TCP Dump

Use the **tcpdump** utility to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear.

Table A-43 TCP Dump

Option	Description
Status:	• Stopped—the tcpdump utility is not running • Start—Click to start the tcpdump utility monitoring the network. • Stop—Click to stop the tcpdump utility
Host Name	Choose the name of the host to monitor from the drop-down list.
Network Interface	Choose the network interface to monitor from the drop-down list.
Promiscuous Mode	• On—Click to turn on promiscuous mode (default). • Off—Click to turn off promiscuous mode. Promiscuous mode is the default packet sniffing mode. It is recommended that you leave it set to On. In this mode the network interface is passing all traffic to the system's CPU.
Filter	Enter a boolean expression on which to filter. Standard tcpdump filter expressions are supported.
Format	Select a format for the tcpdump file from the drop-down list: • Human Readable • Raw Packet Data

Dump File	Displays data on the last dump file, such as the following:
	Last created on Wed Apr 27 20:42:38 UTC 2011 by admin
	`File size: 3,744 bytes`
	`Format: Raw Packet Data`
	`Host Name: Positron`
	`Network Interface: GigabitEthernet 0`
	`Promiscuous Mode: On`
	• Download—Click to download the most recent dump file.
	• Delete—Click to delete the most recent dump file.

Security Group Access Tools

To access the following General Tools for troubleshooting, go to **Operations > Troubleshoot > Diagnostic Tools** and expand **Security Group Access Tools** in the left panel. Choose from the following tools:

- Egress SGACL Policy, page A-49
- SXP-IP Mappings, page A-50
- IP User SGT, page A-52
- Device SGT, page A-54

Egress SGACL Policy

Compare Security Group Access-enabled devices using theEgress policy diagnostic too.

Progress Details

Table A-44 Progress Details for Egress SGACL Policy

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings) **Note** The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-45 Results Summary for Egress SGACL Policy

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

SXP-IP Mappings

Compare SXP-IP mappings between a device and its peers.

Peer SXP Devices

Table A-46 Peer SXP Devices for SXP-IP Mappings

Option	Description
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.
VRF	The VRF instance of the peer device.
Peer SXP Mode	The SXP mode of the peer device; for example, whether it is a speaker or a listener.
Self SXP Mode	The SXP mode of the network device; for example, whether it is a speaker or a listener.
Connection State	The status of the connection.
Common Connection Parameters	
User Common Connection Parameters	Check this check box to enable common connection parameters for all the peer SXP devices. **Note** If the common connection parameters are not specified or if they do not work for some reason, the Expert Troubleshooter again prompts you for connection parameters for that particular peer device.
Username	Enter the username of the peer SXP device.
Password	Enter the password to gain access to the peer device.

Table A-46 Peer SXP Devices for SXP-IP Mappings

Option	Description
Protocol	• Choose the protocol from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	• Enter the port number. The default port number for Telnet is 23 and SSH is 22.
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Check this check box if your enable password is the same as your login password.

Progress Details

Table A-47 Progress Details for SXP-IP Mappings

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings)	
Note The Advanced options appear only for some of the troubleshooting tools.	

Table A-47 Progress Details for SXP-IP Mappings (continued)

Option	Description
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-48 Results Summary for SXP-IP Mappings

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

IP User SGT

Use the IP User SGT diagnostic tool to compare IP-SGT values on a device with an ISE assigned SGT.

Table A-49 IP User SGT

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device.
Filter Results	
Username	Enter the username of the user whose records you want to troubleshoot.
User IP Address	Enter the IP address of the user whose records you want to troubleshoot.
SGT	Enter the user SGT value.

Progress Details

Table A-50 Progress Details for IP User SGT

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings) **Note** Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-51 Results Summary for IP User SGT

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.

Table A-51 Results Summary for IP User SGT (continued)

Option	Description
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Device SGT

Use the Device SGT diagnostic tool to compare the device SGT with the most recently assigned value.

Table A-52 Device SGT

Option	Description
Enter Information	
Network Device IPs (comma-separated list)	Enter the network device IP addresses (whose device SGT you want to compare with an ISE-assigned device SGT) separated by commas.
Common Connection Parameters	
Use Common Connection Parameters	Select this check box to use the following common connection parameters for comparison: • Username—Enter the username of the network device. • Password—Enter the password. • Protocol—Choose the protocol from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 **Note** Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device. • Port—Enter the port number. The default port number for Telnet is 23 and SSH is 22.
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Select this check box if your enable password is the same as your login password.

Policy

This section covers the following user interface elements:

Authentication

Allowed Protocols Service

Table A-53 Allowed Protocols Service

Option	Description
Allowed Protocols	
Process Host Lookup	Check this check box to configure Cisco ISE to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP).
Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol. When you check the Allow PAP/ASCII check box, you can check the Detect PAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of PAP) request.
Allow CHAP	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	This option enables MS-CHAPv1.
Allow MS-CHAPv2	This option enables MS-CHAPv2.
Allow EAP-MD5	This option enables EAP-based MD5 hashed authentication. When you check the Allow EAP-MD5 check box, you can check the Detect EAP-MD5 as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of EAP-MD5) request.

Table A-53 Allowed Protocols Service (continued)

Option	Description
Allow EAP-TLS	This option enables the EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client. **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. Refer to Chapter 13, "Managing Certificates" for more information on certificates.
Allow LEAP	This option enables Lightweight Extensible Authentication Protocol (LEAP) authentication.
Allow PEAP	This option enables the PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2. When you check the Allow PEAP check box, you can configure the following PEAP inner methods: • Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method.

Table A-53 Allowed Protocols Service (continued)

Option	Description
Allow EAP-FAST	This option enables the EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2. When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method: • Allow EAP-MS-CHAPv2 – Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC • Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. • Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs[1] for EAP-FAST clients. Additional PAC options appear. • Don't use PACs—Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC. When you choose this option, you can configure Cisco ISE to perform machine authentication.

1. PACs = Protected Access Credentials.

PAC Options

Table A-54 PAC Options

Option	Description
Use PAC	• Tunnel PAC Time to Live—The TTL[1] value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days. • Proactive PAC Update When: <n%> of PAC TTL is Left—The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%. • Allow Anonymous In-band PAC Provisioning—Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. **Note** To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning—Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE. When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning. – Server Returns Access Accept After Authenticated Provisioning—Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning. • Allow Machine Authentication—Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the Cisco ISE external identity source. After these details are correctly verified, no further authentication is performed. **Note** Cisco ISE only supports Active Directory as an external identity source for machine authentication. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client).

Table A-54 PAC Options (continued)

Option	Description
	• Enable Stateless Session Resume—Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this check box in the following cases: – If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients – To always perform phase two of EAP-FAST When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication. • Preferred EAP Protocol—Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, and EAP-MD5. By default, LEAP is the preferred protocol to use if you do not enable this field.

1. TTL = Time To Live

Administration

This section covers the following:

System > Settings > Monitoring

To access system monitoring tools go to **Administration > System > Settings**, then expand **Monitoring** in the left panel. This section covers the user interface elements for the following monitoring tools:

Alarm Syslog Targets

Define the destination where alarm syslog messages are sent.

Table A-55 Alarm Syslog Targets

Option	Description
Identification	
Name	Name of the alarm syslog target. The name can be 255 characters in length.
Description	(Optional) A brief description of the alarm that you want to create. The description can be up to 255 characters in length.
Configuration	
IP Address	IP address of the machine that receives the syslog message. This machine must have the syslog server running on it. It is recommended that you use a Windows or a Linux machine to receive syslog messages.
Use Advanced Syslog Options	
Port	Port in which the remote syslog server listens. By default, it is set to 514. Valid options are from 1 to 65535.
Facility Code	Syslog facility code to be used for logging. Valid options are Local0 through Local7.

Email Settings

Define the email address for the mail server and the name that is shown for messages received from the mail server, such as admin@somedomain.com.

Table A-56 Email Settings

Option	Description
Mail Server	Enter a valid email host server.
Mail From	Enter the name that users see when they receive a message from the mail server, such as admin@somedomain.com.

Failure Reasons Editor

View and edit failure reasons.

Viewing Failure Reasons

Table A-57 Viewing Failure Reasons

Option	Description
Failure Reasons	The name of possible failure reasons. Click a failure reason name to open the Failure Reasons Editor page.

Editing Failure Reasons

Table A-58 Editing Failure Reasons

Option	Description
Failure Reason	Display only. The error code and associated failure reason name.
Description	Enter a free text description of the failure reason to assist administrators; use the text tools as needed.
Resolution Steps	Enter a free text description of possible resolution steps for the failure reason to assist administrators; use the text tools as needed.

Results Summary

Table A-59 Results Summary for Failure Reasons

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

System Alarm Settings

Enable, disable, and configure system alarm notification settings.

Table A-60 System Alarm Settings

Option	Description
System Alarm Settings	
Notify System Alarms	Check this check box to enable system alarm notification.
System Alarms Suppress Duplicates	Designate the number of hours that you want to suppress duplicate system alarms from being sent to the Email Notification User List. Valid options are 1, 2, 4, 6, 8, 12, and 24.
Email Notification	

Table A-60 System Alarm Settings (continued)

Option	Description
Email Notification User List	Enter a comma-separated list of e-mail addresses or ISE administrator names or both. Do one of the following: • Enter the e-mail addresses. • Click **Select** and enter valid administrator names. The administrator is notified by e-mail only if e-mail identification is specified in that administrator's account. When a system alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List. Click **Clear** to clear this field.
Email in HTML Format	Select this check box to send e-mail notifications in HTML format, or uncheck to send s plain text.
Syslog Notification	
Send Syslog Message	Select this check box to send a syslog message for each system alarm generates **Note** To send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. See Configuring Alarm Syslog Targets, page 24-59 for more information.

System > Maintenance > Data Management > Monitoring Node

To access monitoring data management tools, go to **Administration > System > Maintenance**, then expand **Data Management > Monitoring Node** in the left panel. This section covers the user interface elements for the following tools:

- Full Backup On Demand, page A-62
- Scheduled Backup, page A-63
- Data Purging, page A-63
- Data Restore, page A-64

Full Backup On Demand

Perform a full backup of the monitoring database on demand.

Table A-61 Full Backup On Demand

Option	Description
Data Repository	Select a repository from the drop-down list, in which to back up the monitoring database. If no repository is selected, a backup will not occur.
Backup Now	Click to perform a full backup of the monitoring database.
Full Backup On Demand Status	Shows the Name, Start Time, End Time, and Status of an on demand backup.

Scheduled Backup

Schedule an incremental or full monitoring database backup.

Table A-62 Scheduled Backup

Option	Description
Incremental Backup	
On	Click the **On** radio button to enable incremental backup.
Off	Click the **Off** radio button to disable incremental backup.
Configure Incremental Monitor Database Backup	
Data Repository	Select a data repository for the backup files.
Schedule	Select the time of the day to perform the incremental backup.
Frequency	Choose the frequency of incremental backups: • Daily • Weekly—Typically occurs at the end of every week. • Monthly—Typically occurs at the end of every month.
Configure Full Monitor Database Backup	
Data Repository	Select a data repositoryused to store the backup files.
Schedule	Select the time of the day to perfrom the database backup.
Frequency	Choose the frequency of the backups: • Daily—Occurs at the specified time each day. • Weekly—Occurs on the last day of every week. • Monthly—Occurs on the last day of every month.

Data Purging

Purge data prior to an incremental or full backup.

Table A-63 Data Purging

Option	Description
Data Purging	
Percentage of Disk Space	Enter a numerical percentage value for allowed disk space usage. This threshold triggers a purge when disk space usage meets or exceeds this value. The default is 80 percent. The maximum value allowed is 100 percent.
Data Repository	Select the data repository to backup data prior to purge.
Maximum Stored Data Period	Enter a value in (30-day) months to be utilized when the disk space usage threshold for purging (Percentage of Disk Space) is met. **Note** For this option, each month consists of 30 days. The default of three months equals 90 days.

Table A-63 Data Purging (continued)

Option	Description
Submit	Click to proceed with the data purge.
Cancel	Click to exit without purging data.

Data Restore

Restore a full or incremental backup.

Table A-64 Data Restore

Column	Description
Available Backups to Restore	Select the radio button next to the name of the backup you want to restore. The backup filename includes the time stamp. For example, ISEViewBackup-20090618_003400.
Date	Shows the date of the backup
Repository	Shows the name of the repository where the backup is stored.
Type	Shows the type of backup, full or incremental
Restore	Click to restore the selected backup of the monitoring database.