Operations User Interface Reference

Recent RADIUS Authentications

The following table describes the fields on the Authentications page, which displays recent RADIUS authentications. The navigation path for this page is: **Operations** > **Authentications** > **Show Live Authentication**.

Table 1: Live Authentications

Option	Usage Guidelines
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.
Repeat Counter	Shows the number of time the authentication requests were repeated in last 24 hours, without any change in the context of identity, network devices, and authorization
Reset Repeat Counts	Click to reset the Retry options for all the endpoints
Identity	Shows the username that is associated with the authentication.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.

Option	Usage Guidelines
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Authorization Profiles	Shows an authorization profile that was used for authentication.
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.
Event	Shows the event status.
Failure Reason	Shows a detailed reason for failure, if the authentication failed.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and the like.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service from which the log was generated.
Session ID	Shows the session ID.

Show Live Sessions

The following table describes the fields on the live sessions page, which displays live authentication sessions. The navigation path for this page is: **Operations** > **Authentications** > **Show Live Sessions**.

Table 2: Live Sessions

Field	Description
Initiated	Shows the timestamp when the authentication session was initiated.
Updated	Shows the timestamp when the session was last updated due to any change, like a CoA action.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of the endpoint device.
CoA Action	Use this to dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times the session has been retried.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of the endpoint device.
IP Address	Shows the IP address of the endpoint device.
Audit Session ID	Shows a unique session identifier provided by NAS.
Account Session ID	Shows a unique ID provided by NAS.
Endpoint Profile	Shows the endpoint profile for the device.
Posture Status	Shows the status of posture validation and details on the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and the like.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
NAS IP Address	Shows IP address of the network devices.
Device Port	Shows the connected port to the network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.

Field	Description
EPS Status ANC Status	Shows the Endpoint Protection Service Adaptive Network Controlstatus of a device as Quarantine, Unquarantine, or Shutdown.
WLC Roam	Shows the boolean (Y/N) used to track that an endpoint has been handed off during roaming, from one WLC to another. It has the value of cisco-av-pair=nas-update =Y or N.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.
Bytes Out	Shows the number of bytes sent.
Session Source	Shows if the endpoint was authenticated via RADIUS or Identity Mapping.

Diagnostic Tools

RADIUS Authentication Troubleshooting Settings

The following table describes the fields on the RADIUS authentication troubleshooting page which allow you to identify and resolve RADIUS authentication problems. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **RADIUS Authentication Troubleshooting**.

Table 3: RADIUS Authentication Troubleshooting Settings

Option	Usage Guidelines
Username	Enter the username of the user whose authentication you want to troubleshoot.
MAC Address	Enter the MAC address of the device that you want to troubleshoot.
Audit Session ID	Enter the audit session ID that you want to troubleshoot.
NAS IP	Enter the NAS IP address.
NAS Port	Enter the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication.
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.

Option	Usage Guidelines
Time Range	Select a time range. The RADIUS authentication records that are created during this time range are used.
Start Date-Time	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	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.

Execute Network Device Command Settings

The following table describes the fields on the Execute Network Device Command page, which you use to execute the **show** command on a network device. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Execute Network Device**.

Table 4: Execute Network Device Command Settings

Option	Usage Guidelines
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 Settings

The following table describes the fields on the Evaluate Configuration Validator page, which you use to evaluate the configuration of a network device and identify any configuration problems. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Evaluate Configuration Validator**.

Table 5: Evaluate Configuration Validator Settings

Option	Usage Guidelines
Enter Information	

Option	Usage Guidelines
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	Check this check box to compare the web authentication configuration.
Profiler Configuration	Check this check box to compare the Profiler configuration.
Trustsec	Check this check box if you want to compare Trustsec configuration.
802.1X	Check this check box if you want to compare the 802.1X configuration, and choose one of the available options.

Posture Troubleshooting Settings

The following table describes the fields on the Posture troubleshooting page, which you use to find and resolve posture problems on the network. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Posture Troubleshooting**.

Table 6: Posture Troubleshooting Settings

Option	Usage Guidelines
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
Posture Status	Select the authentication status to filter on:
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. The RADIUS authentication records that are created during this time range are used.

Option	Usage Guidelines
Start Date-Time:	(Available only when 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:	(Available only when 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 Settings

The following table describes the fields on the **tcpdump** utility page, which you use to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **TCP Dump**.

Table 7: TCP Dump Settings

Option	Usage Guidelines
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. **Note** Inline Posture Nodes are not supported.

Option	Usage Guidelines
Network Interface	Choose the network interface to monitor from the drop-down list. **Note** You must configure all network interface cards (NICs) with an IPv4 or IPv6 address so that they are displayed in the Cisco ISE Admin portal.
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.

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.

SXP-IP Mappings

The following table describes the fields on the SXP-IP mappings page, which you use to compare mappings between a device and its peers. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Trustsec Tools** > **SXP-IP Mappings**.

Peer SXP Devices

Table 8: Peer SXP Devices for SXP-IP Mappings

Option	Usage Guidelines
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.

Option	Usage Guidelines
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.
Protocol	• Choose the protocol. **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.

IP User SGT

The following table describes the fields on the IP User SGT page, which you use to compare IP-SGT values on a device with an ISE assigned SGT. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **TrustSec Tools** > **IP User SGT**.

Table 9: IP User SGT

Option	Usage Guidelines
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.

Device SGT Settings

The following table describes the fields on the Device SGT page, which you use to compare the device SGT with the most recently assigned value. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Trustsec Tools** > **Device SGT**.

Table 10: Device SGT Settings

Option	Usage Guidelines
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. **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.

Option	Usage Guidelines
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.

Progress Details Settings

The following table describes the fields on the Progress Details page, which is displayed when you click the **User Input Required** button in any of the diagnostic tools. This page displays detailed troubleshooting information. The navigation path for this page is: **Operations** > **Troubleshoot** > **Diagnostic Tools** > **Any Diagnostic Tool**.

Table 11: Progress Details Settings

Option	Usage Guidelines
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. **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	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.

Option	Usage Guidelines
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

The following table describes the fields on the results summary page, which is displayed as a result when you use any diagnostic tool.

Table 12: RADIUS Authentication Troubleshooting Results Summary

Option	Usage Guidelines
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. Any configuration errors are indicated by red text.