Troubleshooting ACS with the Monitoring and Report Viewer

This chapter describes the diagnostic and troubleshooting tools that the Monitoring and Report Viewer provides for the Cisco Secure Access Control System.

This chapter contains the following sections:

Available Diagnostic and Troubleshooting Tools

The Monitoring and Report Viewer provides the following:

Connectivity Tests

When you have authentication problems, you can perform a connectivity test to check for connectivity issues. You can enter the hostname or the IP address of the network device that you are trying to connect with and execute the following commands from the web interface: **ping**, **traceroute**, and **nslookup**.

The Monitoring and Report Viewer displays the output of these commands. See Performing Connectivity Tests, page 14-3 for detailed instructions on how to perform the connectivity tests.

ACS Support Bundle

You can use the ACS support bundle to prepare diagnostic information for TAC to troubleshoot problems with ACS.

Support bundles typically contain the ACS database, log files, core files, and Monitoring and Report Viewer support files. You can exclude certain files from the support bundle, per ACS node. You can download the support bundle to your local computer. The browser (depending on its configuration) displays the progress of the download and prompts you to save the support bundle to an appropriate location.

- If the ACS server is a primary instance, the support bundle includes an export of the ACS configuration.
- If the ACS server is a secondary instance, the ACS database is not included.
- If the ACS server is a log collector, the support bundle includes an export of the monitoring and report configuration and collected AAA audit and diagnostic logs.
- If the ACS server is not the log collector, the monitoring and reporting configuration is not included in the support bundle. See Downloading ACS Support Bundles for Diagnostic Information, page 14-4 for detailed instructions on how to download ACS support bundles.

Expert Troubleshooter

Expert Troubleshooter is an easy-to-use, web-based troubleshooting utility that helps you diagnose and troubleshoot problems in ACS deployments. It reduces the time that you take to diagnose the problem and provides you detailed instructions on how to resolve the problem.

You can use Expert Troubleshooter to diagnose and troubleshoot passed and failed authentications. For example, if a user is unable to gain access to the network, you can use the Expert Troubleshooter to diagnose the cause of this problem.

Expert Troubleshooter provides you the option to run **show** commands on any network device from the ACS web interface. The output of the **show** command is returned to you in precisely the same manner as the output appears on a console.

You can use Expert Troubleshooter to evaluate the configuration of any network device to see if there are any discrepancies that cause the problem. ACS 5.8 supports evaluating communication with network devices over IPv6 along with IPv4.

In addition, Expert Troubleshooter provides you four diagnostic tools for troubleshooting Security Group Access device-related problems.

The Expert Troubleshooter identifies the cause of the problem and lists an appropriate course of action that you can take to resolve the problem. See Working with Expert Troubleshooter, page 14-5 for more information on the various tools that Expert Troubleshooter offers.

Table 14-1 describes the diagnostic tools that ACS 5.8 offers:

Table 14-1 Expert Troubleshooter - Diagnostic Tools

Diagnostic Tool	Description
RADIUS Authentication Troubleshooting	Troubleshoots a RADIUS authentication. See Troubleshooting RADIUS Authentications, page 14-6 for more information.
Execute Network Device Command	Executes any **show** command on a network device. See Executing the Show Command on a Network Device, page 14-9 for more information.
Evaluate Configuration Validator	Evaluates the configuration of a network device. See Evaluating the Configuration of a Network Device, page 14-10 for more information.

Table 14-1 Expert Troubleshooter - Diagnostic Tools (continued)

Diagnostic Tool	Description
Trust Sec Tools	
Egress (SGACL) Policy	Compares the Egress Policy (SGACL) between a network device and ACS. See Comparing SGACL Policy Between a Network Device and ACS, page 14-11 for more information.
SXP-IP Mappings	Compares SXP mappings between a device and peers. See Comparing the SXP-IP Mappings Between a Device and its Peers, page 14-12 for more information.
IP User SGT	Compares IP-SGTs on a device with ACS authentication-assigned User-IP-SGT records. See Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records, page 14-14 for more information.
Device SGT	Compares device SGT with ACS-assigned SGT. See Comparing Device SGT with ACS-Assigned Device SGT, page 14-15 for more information.

Performing Connectivity Tests

You can test your connectivity to a network device with the device's hostname or IP address. For example, you can verify your connection to an identity store by performing a connectivity test. In ACS 5.8, you can also test the connectivity of remote machines.

To test connectivity between your ACS and a device's hostname or IP address:

Step 1 Select **Monitoring and Reports > Troubleshooting > Connectivity Tests**.

The Connectivity Tests page appears.

Step 2 Click the IPv4 or IPv6 radio button to select the appropriate IP address type.

Step 3 Modify the fields in the Connectivity Tests page as described in Table 14-2.

Table 14-2 Connectivity Tests

Option	Description
Hostname or IP Address	Enter the hostname or IP address of a connection you want to test. Click **Clear** to clear the hostname or IP address that you have entered.
ping	Click to see the **ping** command output, where you can view the packets sent and received, packet loss (if any) and the time for the test to complete.
traceroute	Click to see the **traceroute** command output, where you can view the intermediary IP addresses (hops) between your ACS and the tested hostname or IP address, and the time for each hop to complete.
nslookup	Click to see the **nslookup** command output, where you can see the server and IP address of your tested domain name server hostname or IP address.

Step 4 Click **ping**, **traceroute**, or **nslookup**, depending upon your test.

The output of the **ping**, **traceroute**, or **nslookup** command appears.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Downloading ACS Support Bundles for Diagnostic Information

To create and download an ACS support bundle:

Step 1 Select **Monitoring and Reports > Troubleshooting > ACS Support Bundle**.

The ACS Support Bundle page appears with the fields described in Table 14-3:

Table 14-3 ACS Support Bundle Page

Option	Description
Server	Name of an ACS node instance. Click to display the Download Parameters for the Server page, to create and download an ACS support bundle for the ACS node instance.
IP Address	*Display only.* Indicates the IP address of an associated ACS node.
Node Designation	*Display only.* Indicates the primary or secondary instance of an associated ACS node.

Step 2 Choose a server and click **Get Support Bundle.**

The Download Parameters for the Server page appears. You can create and download an ACS support bundle for the associated ACS node instance.

Note ACS 5.8 allows you to download the support bundle to an IPv6 URL-specified destination.

Step 3 Select the download options you want to incorporate in your ACS support.tar.gz file.

Downloading a support bundle can be slow if the size of the file is extremely large. For faster downloads, do not include core files and View support files in the support bundle.

The options are:

- Encrypt Support Bundle—Check this box to encrypt the support bundle. Specify the decrypting password in **Passphrase** and confirm the password in **Confirm Passphrase**.
- Include full configuration database—Check this box to have the whole database included in the support bundle. If this option in not checked, only a subset of the database is included in the support bundle. Click **Include sensitive information** or **Exclude sensitive information** to include or exclude sensitive information in the logs.

  Sensitive information consists of passwords in the encrypted format, ACS configuration data, and so on.
- Include debug logs—Check this check box to include debug logs, then click **All**, or click **Recent** and enter a value from 1 to 999 in the file(s) field to specify which debug logs to include.
- Include local logs—Check this check box to include local logs, then click **All**, or click **Recent** and enter a value from 1 to 999 in the file(s) field to specify which debug logs to include.

- Include core files—Check this check box to include core files, then click **All** or click **Include files from the last** and enter a value from 1 to 365 in the day(s) field.
- Include monitoring and reporting logs—Check this check box to include monitoring and reporting logs, then click **All** or click **Include files from the last** and enter a value from 1 to 365 in the day(s) field.

  Specify which monitoring and reporting logs to include:

  - AAA Audit
  - AAA Diagnostics
  - System Diagnostics
  - AAA Accounting
  - Administrative and Operational Audit
- Include system logs—Check the check box to include system logs, then click **All** or **Recent** and enter a value from 1 to 999 in the file(s) field.

  You can enter a description in the Description field, if you need.

Step 4 Click:

- **Download** to download the support bundle with the options you specified. The support bundle is created and downloaded.
- **Restore Defaults** to clear the changes you made and return to the default settings.

Note ACS does not pick up the core files while creating or downloading the support bundle for the associated ACS node instance by default. If you want to include the core files in the support bundle, you can check the **Include core files** check box. You can check the **Encrypt Support Bundle** check box to encrypt the support bundle in ACS. It will ensure that the core files are encrypted and included in the supported bundle.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Working with Expert Troubleshooter

The following sections describe how to use the Expert Troubleshooter diagnostic tools:

- Troubleshooting RADIUS Authentications, page 14-6
- Executing the Show Command on a Network Device, page 14-9
- Evaluating the Configuration of a Network Device, page 14-10
- Comparing SGACL Policy Between a Network Device and ACS, page 14-11
- Comparing the SXP-IP Mappings Between a Device and its Peers, page 14-12

- Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records, page 14-14
- Comparing Device SGT with ACS-Assigned Device SGT, page 14-15

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Troubleshooting RADIUS Authentications

Use the RADIUS Authentication diagnostic tool to troubleshoot issues with RADIUS authentications. To do this, you must:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

The Expert Troubleshooter page appears.

Step 2 Select RADIUS Authentication Troubleshooting from the list of troubleshooting tools.

The RADIUS Authentication Troubleshooter page appears.

Step 3 Modify the fields as shown in Table 14-4 to filter the RADIUS authentications that you want to troubleshoot.

Table 14-4 RADIUS Authentication Troubleshooter Page

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 14-4 RADIUS Authentication Troubleshooter Page (continued)

Option	Description
Time Range	Define a time range from the Time Range drop-down list box. The Monitoring and Report Viewer fetches the RADIUS authentication records that are created during this time range. The available options are: • 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 the Monitoring and Report Viewer to fetch at a time from the Fetch Number of Records drop-down list. The available options are 10, 20, 50, 100, 200, and 500.
Active Directory Domain Name	Enter the Active Directory domain name. The AD records are fetched only when the AD details are provided.
Active Directory Domain Admin Name	Enter the Active Directory domain administrator name. The AD records are fetched only when the AD details are provided.
Active Directory Domain Admin Password	Enter the Active Directory domain administrator password. The AD records are fetched only when the AD details are provided.

Step 4 Click **Search** to display the RADIUS authentications that match your search criteria.

The Search Result table is populated with the results of your search. The following fields appear in the table: Time, Status, Username, MAC Address, Audit Session ID, Network Device IP, Failure Reason, and Access Service.

Step 5 Choose the RADIUS authentication record from this table that you want to troubleshoot, and click **Troubleshoot**.

The Expert Troubleshooter begins to troubleshoot your RADIUS authentication. The Monitoring and Report Viewer prompts you for additional input, if required.

For example, if the Expert Troubleshooter must connect to a network device, it prompts you for connection parameters and login credentials.

Note If the RADIUS authentication was done against AD, then ACS asks for AD credentials before it begins the troubleshooting process. You have to enter the AD credentials each time you access these reports.

Step 6 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 7 Click **Submit**.

The Progress Details page appears. This page provides a summary and might prompt you for additional input, if required. If the Monitoring and Report Viewer requires additional input, you must click the **Click User Input Required** button. A dialog box appears.

Step 8 Modify the fields in the dialog box as described in Table 14-5 and click **Submit**.

Table 14-5 Progress Details Page - User Input Dialog Box

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 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)	
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.

Step 9 Click **Done** to return to the Expert Troubleshooter.

The Progress Details page refreshes periodically to display the tasks that are performed as troubleshooting progresses. After the troubleshooting is complete, the Show Results Summary button appears.

Step 10 Click **Show Results Summary**.

The Results Summary page appears with the information described in Table 14-6.

Table 14-6 Results Summary Page

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. Any configuration errors are indicated by red text.

Step 11 Click **Done** to return to the Expert Troubleshooter.

The Monitoring and Report Viewer provides you the diagnosis, steps to resolve the problem, and troubleshooting summary to help you resolve the problem.

Note You can launch the RADIUS authentication troubleshooter from the RADIUS authentication report pages as well. You must drill down to the details page of a particular RADIUS authentication to launch this diagnostic tool.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Executing the Show Command on a Network Device

The Execute Network Device Command diagnostic tool allows you to run any **show** command on a network device from the ACS web interface. The result of the **show** command is precisely what you would see on a console and can be used to identify problems in the device configuration. To run a **show** command on any network device:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select **Execute Network Device Command** from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in Table 14-7.

Table 14-7 Execute Show Command on a Network Device

Option	Description
Enter Information	
Network Device IP	Enter the IPv4 or IPv6 address of the network device on which you want to run the **show** command.
Command	Enter the **show** command that you want to run.

Step 3 Click **Run** to run the **show** command on the specified network device.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 5 Click **Submit** to run the show command on the network device and view the output.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Evaluating the Configuration of a Network Device

You can use this diagnostic tool to evaluate the configuration of a network device and identify any missing or incorrect configuration. The Expert Troubleshooter compares the configuration on the device with the standard configuration. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Click Evaluate Configuration Validator from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in Table 14-8.

Table 14-8 Evaluate Configuration Validator

Option	Description
Enter Information	
Network Device IP	Enter the IPv4 or IPv6 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	Checked by default.
RADIUS	Checked by default.
Device Discovery	Checked by default.
Logging	Checked by default.

Table 14-8 Evaluate Configuration Validator

Option	Description
Web Authentication	Check this check box if you want to compare the web authentication configuration.
Profiler Configuration	Check this check box if you want 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)

Step 3 Click **Run**.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in Table 14-5.

The Troubleshooting Progress Details page appears. The Expert Troubleshooter retrieves the CLI response from the network device. A new window appears and prompts you to select the interfaces for which you want to analyze the interface configuration.

Step 5 Check the check boxes the interfaces that you want to analyze, and click **Submit** to evaluate the configuration of the interfaces.

The Progress Details page appears with a summary.

Step 6 Click **Show Results Summary** to view the troubleshooting summary.

The Results Summary page appears with the information described in Table 14-6. The missing configurations appear in red.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing SGACL Policy Between a Network Device and ACS

For Security Group Access-enabled devices, ACS assigns an SGACL for every source SGT-destination SGT pair based on the Egress policy matrix that you configure in ACS. The Egress policy diagnostic tool does the following:

1. Connects to the device whose IP address you provide and obtains the ACLs for each source SGT— destination SGT pair.
2. Checks the Egress policy that is configured in ACS and obtains the ACLs for each source SGT— destination SGT pair.

3. Compares the SGACL policy obtained from the network device with the SGACL policy obtained from ACS.
4. Displays the source SGT —destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.

To compare the SGACL policy between a network device and ACS:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select **Egress (SGACL) Policy** from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and shows the Network Device IP field.

Step 3 Enter the IP address of the Security Group Access device whose SGACL policy you want to compare with ACS.

Step 4 Click **Run** to compare the SGACL policy between ACS and the network device.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 5 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 6 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 7 Click **Show Results Summary** to view the diagnosis and resolution steps.

The Results Summary page appears with the information described in Table 14-6.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing the SXP-IP Mappings Between a Device and its Peers

Security Group Access devices communicate with their peers and learn their SGT values. The Security Exchange Protocol-IP (SXP)-IP Mappings diagnostic tool connects to the device whose IP address you provide and lists the peer devices' IP addresses and SGT values.

You must select one or more of the device's peers. This tool connects to each of the peers that you select and obtains their SGT values to verify that these values are the same as the values that it learned earlier.

Use this diagnostic tool to compare the SXP-IP mappings between a device and its peers. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select **SXP-IP Mappings** from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and shows the Network Device IP field.

Step 3 Enter the IP address of the network device.

Step 4 Click **SXP-IP Mappings** from the list of troubleshooting tools.

The Expert Troubleshooter page refreshes and shows the following field:

Network Device IP—Enter the IP address of the network device.

Step 5 Click **Run**.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 6 Click the **User Input Required** button and modify the fields as described in Table 14-5.

The Troubleshooting Progress Details page appears. The Expert Troubleshooter retrieves SGA SXP connections from the network device and again prompts you to select the peer SXP devices.

Step 7 Click the **User Input Required** button.

A new window appears with the fields as described in Table 14-9.

Table 14-9 Peer SXP Devices

Option	Description
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.
VRF	VRF instance of the peer device.
Peer SXP Mode	SXP mode of the peer device; for example, whether it is a speaker or a listener.
Self SXP Mode	SXP mode of the network device; for example, whether it is a speaker or a listener.
Connection State	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. 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 from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 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.

Step 8 Check the check box of the peer SXP devices for which you want to compare the SXP mappings and enter the Common Connection Parameters as described in Table 14-9.

Step 9 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 10 Click **Show Results Summary** to view the diagnosis and resolution steps.

The Results Summary page appears with the information described in Table 14-6.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records

For Security Group Access-enabled devices, ACS assigns each user an SGT value through RADIUS authentication. The IP User SGT diagnostic tool connects to the network device whose IP address you provide and does the following:

1. Obtains a list of all IP-SGT assignments on the network device.
2. Checks the RADIUS authentication and accounting records for each IP-SGT pair to find out the IP-SGT-User value that ACS has assigned to it most recently.
3. Displays the IP-SGT pairs in a tabular format and identifies whether the SGT values most recently assigned by ACS and those on the device are the same or different.

Use this diagnostic tool to compare the IP-SGT values on a device with ACS-assigned SGT. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Click **IP User SGT** from the list of troubleshooting tools.

The Expert Troubleshooter page refreshes and lists the fields described in Table 14-10.

Table 14-10 IP User SGT

Option	Description
Enter Information	
Network Device IP	Enter the IPv4 or IPv6 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.

Step 3 Click **Run**.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 5 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 6 Click **Show Results Summary** to view the diagnosis and resolution steps.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing Device SGT with ACS-Assigned Device SGT

For Security Group Access-enabled devices, ACS assigns each network device an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device whose IP address you provide and does the following:

1. Obtains the network device's SGT value.
2. Checks the RADIUS authentication records to determine the SGT value that ACS had assigned to it most recently.
3. Displays the Device-SGT pairs in a tabular format and identifies whether the SGT values are the same or different.

Use this diagnostic tool to compare the device SGT with ACS-assigned device SGT. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

The Expert Troubleshooter page appears.

Step 2 Click **Device SGT** from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in Table 14-11.

Table 14-11 Device SGT

Option	Description
Enter Information	
Network Device IPs (comma-separated list)	Enter the network device IPv4 or IPv6 addresses (for the device whose SGT you want to compare with the SGT of an ACS-assigned device), separated by commas.
Common Connection Parameters	
Use Common Connection Parameters	Check 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 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.

Step 3 Click **Run**.

The Progress Details page appears with a summary.

Step 4 Click **Show Results Summary** to view the results of device SGT comparison.

The Results Summary page appears with the diagnosis, resolution, and troubleshooting summary.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2