



Troubleshooting

This section provides suggestions for troubleshooting the Wireless LAN Solution Engine components. If the suggestions do not resolve the error, check the release notes for a possible work around, or contact the Cisco TAC or your customer support.

This section includes troubleshooting suggestions for the following:

- [Faults, page 8-2](#)
- [Configure, page 8-3](#)
- [Firmware, page 8-8](#)
- [Reports, page 8-9](#)
- [Administration, page 8-11](#)

Faults

Table 8-1 Troubleshooting Hints for Faults

Feature	Symptom	Probable Cause	Possible Solution
Faults > Display Faults	The Display Fault view is blank.	There are no faults to report based on the filtering criteria you entered.	Not applicable.
	The Description column in the Display Faults table shows, "SNMP query received authentication error response."	The user created for community strings does not have Admin, Ident, Firmware, and SNMP privileges.	Make sure the SNMP community string set on the WLSE (Administration > Discover > Device Credentials.) is the same as the string set on the access point (Setup > Security > User Information.).
	The Description column in the Display Faults table shows, "Authentication failed. Please check LEAP credentials."	The server is reachable but the credentials are incorrect.	Make sure that the credentials are set correctly by selecting Administration > Discover > LEAP, RADIUS, or EAP-MD5 Server.
Faults > Notification Settings	Email fails to arrive at destination.	The SMTP server is not configured properly.	Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

Configure

Table 8-2 Troubleshooting Hints for Configure

Feature	Symptom	Probable Cause	Possible Solution
Configure > Templates	The access point is inaccessible through the HTTP port set through template configuration job.	The HTTP port setting does not take effect until the access point is cold restarted.	Cold restart the access point.
	Template configuration job fails every time.	The access point is not set up properly.	Make sure the WLSE is configured as a TFTP server for the access point. For additional information, see Set Up Devices, page 6-12 .
Configure > Jobs	The Undo function does not work.	Your job includes custom values.	None.
		Your job includes routing table configurations (only for versions prior to 11.23T).	
		Your job for undoing a user shows as successful but the user is not removed from the access point.	The Undo function only works for new users that are added to the access point. If a user is being added in place of an existing user on the access point, the existing user will remain after the Undo job.

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
		<p>Your job includes the following Security options, which are not supported by the Undo function:</p> <ul style="list-style-type: none"> • Local Admin Authentication under the Local Admin Access • Encryption Key Values under Local AP/Client Security • Shared Secret under Server-Based Security. • Shared Secret under Accounting. 	
		Your job includes the FTP username and password.	
		You are trying to Undo a job that has already been undone.	
		Your job is HTTP-based but you have not set up the HTTP credentials.	Add HTTP credentials using Administration >Discover >Device Credentials >HTTP User/Password
		You are trying to Undo a job that contains Custom values, which are not supported by the Undo function.	None.

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	An HTTP job does not run or fails.	The credentials are not set properly.	Make sure the credentials on the WLSE are the same as the credentials on the access point or bridge using Administration > Discover > Device Credentials .
			Make sure the credentials on the access point or bridge have firmware rights.
	The TFTP server is not set up correctly.	The TFTP setting on the access point should point to the WLSE as its TFTP server. This can be done by applying a template configuration, containing TFTP server settings, through an SNMP job (only 11.08T and higher)	
	The device is not responding to HTTP jobs.	HTTP browsing is disabled on the AP because of this job run.	At the access point console, turn on non-console browsing, or schedule an SNMP job for the device if its version is 11.08T or higher.
An SNMP job does not run or fails.	The community string is not set properly.		Make sure the SNMP community string set on the WLSE is the same as the string set on the access point or bridge using Administration > Discover > Device Credentials .
			Make sure the SNMP community string on the access point or bridge has firmware rights.

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The job failed.	There are multiple reasons a job may have failed.	Make sure all the bootstrapping steps have been performed correctly on the access point. Check the jobvm.log by selecting Administration > Appliance > Status > View Log File to further identify and report the problem.
		When applying a configuration template on a job with multiple devices, if the job fails on even one of the devices, the job is categorized as Failed.	Check if the Job Run Detail > Job Run Log to identify exactly which job(s) failed.
	The job is unverified.	If after applying a configuration template on a device, the device reboots, the job will be categorized as Unverified.	Check the access point to verify whether the job has completed and the new template has been applied.
	The job failed and the Job Run Detail > Job Run Log indicates a timeout while reaching the device.	The configuration template you applied has caused the device to either reboot or made it inaccessible.	Make sure the configuration you apply will not cause the device to become inaccessible. For example, do not set up access lists that block all traffic to the Ethernet port. If the device is inaccessible, it might have rebooted after the configuration template was applied. Refer to the template screens to see if any variable is set with an R indicating a possible reboot if the setting is applied.

Table 8-2 Troubleshooting Hints for Configure (continued)

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The job is reported as failed, but the configuration was applied successfully to the devices.	The SNMP timeout to the device is too short.	Select Administration > Discover > Device Credentials > SNMP Communities and increase the SNMP timeout.
	The job completed with errors.	This error can be seen in jobs where pre- or post-configuration backups before or after applying the new configuration fail, but the new configuration is applied successfully.	Check if “Completed with errors” appears in the Job Run Detail > Job Run Log to identify this problem.
	There is a time discrepancy in scheduled jobs.	The time is not set correctly on the WLSE.	<ol style="list-style-type: none"> 1. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows: <ol style="list-style-type: none"> a. Enter services stop to stop services. a. Enter the clock command to reset the time. a. Enter services start to restart the services. 2. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.

Firmware

Table 8-3 Troubleshooting Hints for Firmware

Feature	Symptom	Probable Cause	Possible Solution
Firmware > Jobs	There is a time discrepancy in scheduled jobs.	The time was not set correctly on the WLSE.	<ol style="list-style-type: none"> Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows: <ol style="list-style-type: none"> Enter services stop to stop services. Enter the clock command to reset the time. Enter services start to restart the services. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.
	Firmware is not updated on all the devices included the job.	There were warnings during the job but Ignore Warnings was not set. A firmware job runs even though there are warnings, but the job fails for the devices that had warnings.	Select Ignore Warnings in Firmware > Jobs > Create Job before running the job. See Finishing the Job, page 4-14 .
	Email about job completion fails to arrive at destination.	The SMTP server is not specified.	Configure the mail route by selecting Administration > Appliance > Configure Mailroute . See Specifying an SMTP Mail Server, page 6-71 .

Table 8-3 Troubleshooting Hints for Firmware

Feature	Symptom	Probable Cause	Possible Solution
Firmware > Jobs (continued)	An SNMP job fails	The read community string does not have sufficient permissions.	To allow SNMP reads, the access point must have a user with at least SNMP and FIRMWARE permissions, and the read community defined on the WLSE must be equivalent to a user on the access point with SNMP and FIRMWARE permissions. For more information, see Set Up Devices, page 6-12 and Specify Community Strings, page 6-7 .

Reports

Table 8-4 Troubleshooting Hints for Reports

Feature	Symptom	Probable Cause	Possible Solution
Reports	After running a job, the updated data does not appear in a report.	A full polling cycle has not completed and the new data has not been entered in the database.	Verify that the polling cycle has completed as follows: <ol style="list-style-type: none"> 1. Select Administration > Appliance > Status > View Log File. 2. Click jobvm.log. 3. Scroll through the log to find the message: “Finished Inventory” for your particular job.

Table 8-4 Troubleshooting Hints for Reports (continued)

Feature	Symptom	Probable Cause	Possible Solution
Reports > Scheduled Email Jobs	Email fails to arrive at its destination.	The SMTP server is not configured properly.	Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute .
	There is a time discrepancy in the scheduled email jobs.	The time is not set correctly on the WLSE.	<ol style="list-style-type: none"> 1. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows: <ol style="list-style-type: none"> a. Enter services stop to stop services. a. Enter the clock command to reset the time. a. Enter services start to restart the services. 2. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.
Reports > Wireless Clients	The access point data in the Historical Associations report is not accurate.	The wireless client was associated with an access point managed by the WLSE, but it subsequently associated with an access point that was added to the network, but not yet managed by the WLSE.	Verify that the associated access points are in the managed devices folder by selecting Administration > Discover > Managed Devices > Manage/Unmanage .

Table 8-4 Troubleshooting Hints for Reports (continued)

Feature	Symptom	Probable Cause	Possible Solution
Reports > Current > Summary Reports > Current > Detailed	The report for access points is empty.	The SNMP user may not have the correct rights assigned.	Open a browser window to the access point, and select Setup > Security > User Information . Make sure that the user corresponding to the SNMP community (which is set up in WLSE in Discovery > Device Credentials) has been granted rights for the following: Ident, firmware, admin, snmp, and write. If not, click on the user and assign all these rights.
Reports > Current	The report is empty for a group report on a user-defined group.	Reports cannot be displayed for a user-defined group that contains another group.	Display individual reports for the sub-groups or devices within the user-defined group.

Administration

The following table lists troubleshooting hints for **Administration > Discover**.

Table 8-5 Troubleshooting Hints for the Discover Subtab

Feature	Symptom	Probable Cause	Possible Solution
Administration > Discover > Managed Devices	Devices were discovered but are not displayed in the GUI; for example, in Reports.	The devices have not been moved to the Managed state.	Select Administration > Discover > Managed Devices . Move the devices from New or Unmanaged to Managed. See Manage Devices, page 6-3 .

Table 8-5 Troubleshooting Hints for the Discover Subtab (continued)

Feature	Symptom	Probable Cause	Possible Solution
Administration > Discover > DISCOVER	There is a time discrepancy in the scheduled discovery jobs.	The local or system time is not set correctly on the WLSE.	<ol style="list-style-type: none"> 1. Reset the WLSE system time (UTC) using CLI commands as follows: <ol style="list-style-type: none"> a. Enter services stop to stop services. a. Enter the clock command to reset the time. a. Enter services start to restart the services. 2. Set the local browser time. Select Administration > Appliance > Time/NTP/Name.

Table 8-5 Troubleshooting Hints for the Discover Subtab (continued)

Feature	Symptom	Probable Cause	Possible Solution
Administration > Discover > DISCOVER	Devices are not discovered.	The device is not specified as a seed or the CDP distance is not high enough to reach the device.	Specify the device as a seed or increase the CDP distance so that devices are discovered in Administration > Discover > Schedule Discovery or Run Discovery Now . See Managing Device Discovery, page 6-10 .
		CDP is not enabled on the device.	Enable CDP on the device; see Set Up Devices, page 6-12 . If you are not using CDP, you can import devices from a file or from CiscoWorks2000; see Importing Devices, page 6-28 .
		The device is a switch that does not have an access point attached to it.	Switches are not discovered unless they have an access point attached to them. Discovery can proceed beyond the switch, but the switch itself is not discovered. Make sure a properly configured access point is attached to the switch. See Set Up Devices, page 6-12 .
		SNMP is not enabled on the device or SNMP community strings are not entered on the WLSE.	SNMP must be enabled on the device and credentials must be entered on the WLSE. See Set Up Devices, page 6-12 or Specifying Device Credentials, page 6-6 .
		SNMP timeouts or retries are set too low.	Reset the timeouts and retries. See Specifying Device Credentials, page 6-6 .
		The device is down.	None.
		The device is not supported.	None. See the Supported Devices table for supported devices and software versions.

The following table lists troubleshooting hints for **Administration > Appliance**.

Table 8-6 Troubleshooting Hints for the Appliance Subtab

Feature	Symptom	Probable Cause	Possible Solution
Administration > Appliance > Security > Authentication Modules	Users cannot log in after failure of the alternative authentication source.	The WLSE falls back to the Local authentication module.	Users can log in using their local passwords.
			The system administrator can log in using the admin log in.
			All users with CLI access can log in using the CLI.

The following table lists troubleshooting hints for **Administration > User Admin**.

Table 8-7 Troubleshooting Hints for the User Admin Subtab

Feature	Symptom	Probable Cause	Possible Solution
Administration > User Admin > Manage Users	Some users are not listed.	Only the creator of a user can view that user's name in the list. The admin user, however, can view all users.	None. For more information, see Managing Users, page 6-77 .