



FAQs and Troubleshooting

This chapter consists of the following sections:

- [Hardware Troubleshooting, page 7-1](#)
- [Software Troubleshooting and FAQs, page 7-8](#)

For the most up to date FAQs and troubleshooting information, see the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.0* on Cisco.com.

Hardware Troubleshooting

This section provides the following troubleshooting information:

- [Cannot recover after incorrect setup program entry.](#)
- [Cannot log into the system.](#)
- [The WLSE cannot connect to the network.](#)
- [Cannot connect to the WLSE using a Web browser.](#)
- [The system time or date is incorrect.](#)
- [The system cannot boot from the hard drive during a reboot.](#)
- [Cannot connect to system with Telnet or Telnet interaction is slow.](#)

Symptom Cannot recover after incorrect setup program entry.

Possible Cause You entered incorrect text during the initial setup and want to fix the entry.

Recommended Action Exit setup by pressing **Ctrl-c**. Then run **erase config** to remove the incorrect installation information and rerun the setup program. If you use the erase config command to erase the previous WLSE configuration, and run the setup program again, you will be required to get a new certificate. Use the **mkcert** command or Administration > Appliance > Security > SSL (HTTPS).

Symptom Cannot log into the system.

Possible Cause You did not run the setup program to create an initial system configuration or you lost all the user account passwords.

Recommended Action

- a. Did you run the setup program after booting the system for the first time?
If no, run the setup program.
If yes, continue to the next step.
- b. Do you know the password for any system user accounts?
If no, reconfigure the system to create a new user account.
If yes, continue to the next step.
- c. If you are certain you entered a valid username and password, contact Cisco's Technical Assistance Center for assistance.

Symptom The WLSE cannot connect to the network.

Possible Cause

- The network cable is not connected to the Ethernet 0 port.
- The Ethernet 0 interface is disabled or misconfigured.
- The system is configured correctly, but the network is down or misconfigured.
- DNS is misconfigured. Ping commands will result in a 50-70% failure rate in Pings from the WLSE (Web interface and CLI).

Recommended Action

- a. Verify that the network cable is connected to the Ethernet 0 port and the Ethernet indicator is lit.
 - If the network cable is not connected, connect it.
 - If the network cable is connected but the Ethernet indicator is not lit, these are the probable causes:

The network cable is faulty.

The network cable is the wrong type (for example, a cross-over type, rather than the required straight-through type).

The port on the default gateway to which the system connects is down.

- If the network cable is connected and the Ethernet indicator is on but the system cannot connect to the network, continue to the next step.

- b. Use the **ping** command to perform the following tests:

- Try to ping a well-known host on the network. A DNS server is a good target host.

If the ping command gets a response, the system is connected to the network. If the system cannot connect to a particular host, the problem is either with the network configuration or that host. Contact your network administrator for assistance.

If the ping command does not get a response, continue.

- Attempt to connect to another host on the same subnet as the system.
If the ping command can connect to a host on the same subnet, but cannot connect to a host on a different subnet, the default gateway is probably down.
If the ping command cannot connect to any hosts, continue to the next step.
- c. Use the **show interfaces** command to determine if the Ethernet 0 interface is disabled or misconfigured.
If the Ethernet 0 interface is disabled, enable it. If it is misconfigured, configure it correctly. For more information, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*.
If the interface is enabled and correctly configured, continue to the next step.
- d. Contact your network administrator to verify that there are no conditions on the network that prevent the system from connecting to the network.
If conditions prevent the system from connecting to the network, have your network administrator correct them.
- e. If no conditions are preventing the system from connecting to the network, contact Cisco's Technical Assistance Center.

Symptom Cannot connect to the WLSE using a Web browser.

Possible Cause

- The system cannot connect to the network.
- HTTP or HTTPS is not enabled
- If connecting via HTTP, the IP address was not appended with **:1741**.
- The client system is not configured.

Recommended Action

- a. Make sure that the system can connect to the network. Attempt to connect the system using a Web browser.
If you cannot connect, continue.

- b. If you are attempting to connect via HTTP, verify that the IP address is appended with **:1741**.
- c. If you are attempting to connect via HTTP, verify that HTTP is enabled. If you are attempting to connect via HTTPS, verify that HTTPS is enabled. For more information, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*.
- d. Verify that the browser is configured correctly, and attempt to connect to the WLSE. For more information, see these *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*. If you cannot connect, continue to step 5.
- e. At the system console, or through Telnet, verify that the Web Server and tomcat are running by entering the following:

```
# services status
```

```
If they are running, go to step 7. If they are not running  
continue to step 6.
```

- f. Stop the system services by entering the following:

```
# services stop
```
- g. Restart the system services by entering the following:

```
# services start
```
- h. Try to connect the system using a Web browser.
If you cannot connect, continue to the next step.
- i. Reboot the system by entering the **reload** command.
- j. If you still cannot connect to the system using a Web browser, contact Cisco's Technical Assistance Center for assistance.

Symptom The system time or date is incorrect.

Possible Cause

- NTP is misconfigured.
- The system clock is set incorrectly.

Recommended Action Make sure NTP is configured correctly and that the system clock is set correctly.

Symptom The system cannot boot from the hard drive during a reboot.

Possible Cause

- The disk has a physical error.
- The disk image is corrupted.

Recommended Action If the WLSE cannot boot from the hard drive, the hard drive needs to be reimaged. Use the Recovery CD to reimage your WLSE. For more information, see the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine*.

Symptom Cannot connect to system with Telnet or Telnet interaction is slow.

Possible Cause

- Telnet is disabled or configured incorrectly.
- The WLSE cannot recognize host names.

If you are not using name recognition, slow or non-existent telnet interaction is an expected problem.



Note Telnet is disabled by default. SSH is enabled by default.

Recommended Action :

If the problem is not the network, perform the following steps. Connect to the console port if you cannot Telnet to the WLSE.

- a. Check the Telnet settings to be sure Telnet is enabled and configured correctly. For more information, see the following

To check the Telnet settings, or to enable or disable Telnet on specific domains or IP addresses, use the **telnet** CLI command.

To enable or disable Telnet on individual ports, use the **firewall** CLI command.

- b. If you have specified hosts using the **telnetenable** CLI command, make sure the host from which you are attempting to Telnet is on the list.
- c. If you are using a DNS server, perform the following step:

Configure the system to use a functioning DNS server by entering:

```
# ip name-server ip-address
```

where *ip-address* is the IP address of the DNS server.

If you are using the **import** CLI command, proceed to the next step.

- d. Verify that the system can get DNS services from the network by entering the following command:

```
# nslookup dns-name {hostname | ip-address}
```

where *dns-name* is the DNS name of a host on the network that is registered in DNS and *hostname* and *ip-address* is the same IP address specified in **b**. The command returns the IP address of the host.

- e. If the system cannot resolve DNS names to IP addresses, the DNS server it is using is not working properly.

Resolve the network DNS problem, then continue.

- f. If you are using the **import** CLI command to resolve host names, verify that the WLSE can resolve host names by entering the following command:

```
ping hostname
```

where *hostname* is a host name that has been mapped to an IP address, or imported in a host file, using the **import** command.

- g. If the system can resolve DNS names to IP addresses but you still cannot connect to the system using Telnet, or Telnet interaction with the system is extremely slow, contact Cisco's Technical Assistance Center.

Software Troubleshooting and FAQs

This section provides the following frequently asked questions and troubleshooting information:

- General Questions—See [General FAQs and Troubleshooting, page 7-8](#)
- Faults Tab—[Faults FAQs and Troubleshooting, page 7-10](#)
- Configuration Tab—[Configuration FAQs and Troubleshooting, page 7-13](#)
- Firmware Tab—[Firmware FAQs and Troubleshooting, page 7-17](#)
- Reports Tab—[Reports FAQs and Troubleshooting, page 7-24](#)
- Administration Tab—[Administration FAQs and Troubleshooting, page 7-28](#)

General FAQs and Troubleshooting

- [FAQs, page 7-8](#)
- [Troubleshooting, page 7-9](#)

FAQs

- [Can several users be logged on and managing the same access point at once?](#)
 - [What ports and protocols does the WLSE use?](#)
 - [Can I use a different HTTP port to manage the access point?](#)
 - [Is Telnet enabled or disabled by default on the WLSE?](#)
 - [Can I run a job to convert a number of access points from non-IOS to IOS?](#)
- Q.** Can several users be logged on and managing the same access point at once?
- A.** Yes, several users can view data and reports on the same access point. More than one user can create configuration and firmware update jobs for the same access point and these will be run in the order they are scheduled. Configuration templates may be modified by more than one user at the same time and the last write will overwrite the others.

- Q.** What ports and protocols does the WLSE use?
- A.** For discovery and fault monitoring, the WLSE primarily uses SNMP (UDP port 161). For applying configuration changes, the WLSE uses SNMP, HTTP (TCP port 80 or as configured), and TFTP (UDP port 69).
- Q.** Can I use a different HTTP port to manage the access point?
- A.** Yes, the HTTP port can be changed on the access point. The change will be reflected in WLSE after the next inventory cycle, or if you choose to run inventory now for the devices on which HTTP port was changed. This is assuming the inventory is done by SNMP and not HTTP.
- Q.** Is Telnet enabled or disabled by default on the WLSE?
- A.** Telnet is disabled by default for security reasons. SSH is enabled by default.
- Q.** Can I run a job to convert a number of access points from non-IOS to IOS?
- A.** Yes, you can run a firmware job, using a special IOS upgrade image that is available on Cisco.com. For more information, see the firmware upgrade information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Troubleshooting

This section provides the following troubleshooting information:

- [A search for an access point using APs Based on Client IP, displays the following message, “search yielded no results.”](#)
- [When I try to access an access point web page through the WLSE, the following error message appears: Action Cancelled.](#)

Symptom A search for an access point using APs Based on Client IP, displays the following message, “search yielded no results.”

Possible Cause The device you are searching for is an IOS device. This type of search only works for non-IOS devices.

Recommended Action None.

Symptom When I try to access an access point web page through the WLSE, the following error message appears: Action Cancelled.

Possible Cause The SNMP user on the access point does not have enough rights.

Recommended Action Log in to the access point web interface, select Setup > Security > User Information, and make sure that the user corresponding to the SNMP community (which is set up in the WLSE under Discovery > Device Credentials) has been granted rights for the following: firmware, admin, and snmp.

Faults FAQs and Troubleshooting

- [FAQs, page 7-10](#)
- [Troubleshooting, page 7-13](#)

FAQs

- [What causes the fault: Dot11mib view is not enabled on some access points?](#)
- [What causes the fault: LEAP Disabled?](#)
- [What causes the fault: Authentication failed. Please check LEAP credentials?](#)
- [What causes the fault: SSID Policy Violation?](#)
- [What causes the fault on non-IOS devices: SNMP query received authentication error response?](#)
- [What causes the fault: Duplicate IP was found during discovery?](#)
- [Does acknowledging a fault clear it?](#)
- [What traps are sent from the WLSE?](#)
- [What trap types are forwarded by the WLSE?](#)
- [Does a MIB or trap definition file exist for the WLSE?](#)
- [What information is emailed in a fault notification?](#)

- Q.** What causes the fault: Dot11mib view is not enabled on some access points?
- A.** The device is not configured properly for management by the WLSE; the ISO view has not been created. See [Devices are placed in Misconfigured Devices group after discovery.](#), page 7-31.
- Q.** What causes the fault: LEAP Disabled?
- A.** This can be caused if you have enabled this policy and you are using a non-Cisco client with EAP.
- Q.** What causes the fault: Authentication failed. Please check LEAP credentials?
- A.** 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.
- Q.** What causes the fault: SSID Policy Violation?
- A.** The fault can occur under two conditions:
- When the SSID listed under Faults > Manage Profiles > Security Policies > SSID does not match the SSID on the access point. If you configured different SSIDs among managed access points, you need to enter all of the SSIDs, or this fault will be generated for access points whose SSIDs are not listed.
 - When the SSID policy for an IOS access point is enabled, but the guest mode is disabled, the access point sends an SSID made up of all zeros and equivalent to the length of the first configured SSID. This causes an SSID policy violation. To work around this problem, enable the access point's guest SSID.
- Q.** What causes the fault on non-IOS devices: SNMP query received authentication error response?
- A.** The SNMP authorization error occurs when the AP the user created for community strings does not have Write, SNMP, Firmware and Admin 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).

- Q.** What causes the fault: Duplicate IP was found during discovery?
- A.** A devices is discovered by the WLSE with an IP address that is already in use.
You can either:
- Assign a new IP address to the device.
 - If you have substituted a device for the device with the same IP, and want to continue to use that IP, then delete the original device, and run discovery again.
- Q.** Does acknowledging a fault clear it?
- A.** No, it only removes it from the Active list. For a description of fault states, see [Understanding Fault States, page 2-6](#).
- Q.** What traps are sent from the WLSE?
- A.** Traps are sent based on fault policy and threshold settings on the WLSE. The WLSE only sends out v2c traps, so make sure your trap listener is configured to accept v2c traps.
- Solaris 2.8- based NetView 7.1 receives and displays the SNMP v2c fault notification traps from WLSE, but Windows-based NetView 7.1 supports only v1 traps and cannot receive and display any v2c traps from the WLSE.
- Q.** What trap types are forwarded by the WLSE?
- A.** No traps are forwarded from other devices.
- Q.** What information is emailed in a fault notification?
- A.** For a description see [Email Notification Message Format, page 2-43](#).
- Q.** Does a MIB or trap definition file exist for the WLSE?
- A.** Yes, from the Cisco.com download site, download MIB CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my and load it into the trap receiver.

Troubleshooting

- [The Display Fault view is blank.](#)
- [Email fails to arrive at its destination.](#)
- [No VLAN fault information is displayed for IOS access points.](#)

Symptom The Display Fault view is blank.

Possible Cause There are no faults to report based on the filtering criteria you entered.

Recommended Action Not applicable.

Symptom Email fails to arrive at its destination.

Possible Cause The SMTP server is not configured properly.

Recommended Action Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

Symptom No VLAN fault information is displayed for IOS access points.

Possible Cause WEP keys have not been configured in each VLAN. When the WEP keys are configured in the IOS access points, VLAN information is accessible by SNMP.

Recommended Action Configure the WEP keys for the corresponding VLAN.

Configuration FAQs and Troubleshooting

- [FAQs, page 7-14](#)
- [Troubleshooting, page 7-17](#)

FAQs

- If I create a configuration template that includes WEP key settings how can I verify that they were set on the access point (the access point does not show WEP key settings on its web interface)?
 - Can you undo a configuration update?
 - How long is the configuration job history kept in the WLSE?
 - Do jobs use HTTP or SNMP to initiate a configuration upload?
 - Is it necessary to validate a job?
 - What kinds of job logs are available?
 - What is startup configuration?
 - If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?
 - What is auto configuration?
- Q.** If I create a configuration template that includes WEP key settings how can I verify that they were set on the access point (the access point does not show WEP key settings on its web interface)?
- A.** For security reasons, the access point does not show or send WEP key information. One of the ways to verify the update is to look at the WEP Key length. The only way to verify the contents of the WEP key is to try associating a client that uses that WEP key.
- Q.** Can you undo a configuration update?
- A.** Yes, but only for successful jobs and device versions 11.23T and above for the 340 and 350 access points and bridges, and versions 11.56 and above for AP1200. The Undo feature cannot be used for IOS devices.
- To undo a job, view the Job Run Details table under Configuration > Jobs, select the job you want to undo, and click Undo. For more specific information, see the online help.

- Q.** How long is the configuration job history kept in the WLSE?
- A.** The default time is 30 days. You can change this by navigating to Administration > System > System Parameters > Job History Truncation Interval. Also, by default, for the recurring jobs, the last 30 runs are maintained in the database.
- Q.** Do jobs use HTTP or SNMP to initiate a configuration upload?
- A.** WLSE Configuration jobs can use either HTTP or SNMP as the mechanism to initiate a configuration template upload to an access point.
- The HTTP mechanism is valid for all supported device versions. The following setup parameters must be in place for HTTP mechanism to function properly:
 - HTTP credentials for the device (with admin and firmware privileges on the access point) must match those entered on the WLSE HTTP device credentials screen.
 - TFTP server settings on the access point (Setup > FTP), must refer to the WLSE's IP address.



Note Both username and password in the device credentials are case sensitive.

- The SNMP mechanism is valid for versions 11.08T and higher. The following setup parameters must be in place for SNMP to function properly:
 - SNMP credentials for the device (with admin and firmware privileges on the access point) must match those entered on the WLSE SNMP device credentials screen.
 - There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the Security > Local Admin Access template screen.

The SNMP job mechanism can be used to update TFTP settings, which are needed by HTTP-based jobs. This setting is available under Service > FTP in the configuration templates screens.

- Q.** Is it necessary to validate a job?
- A.** We recommend that you always validate a job before saving it. This will help in locating any possible problems before applying the job.
- Q.** What kinds of job logs are available?
- A.** There are two kinds of job logs: Job run log and the jobvm log.
- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
 - The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting **Administration > Appliance > View Log File**, then clicking **jobvm.log**.
- Q.** What is startup configuration?
- A.** Startup configuration is used right after a device (access point) reboots. It requires DHCP server to be properly set up to allow the access point to pick its startup configuration from WLSE. For this to work, you must set up the following:
- a. Enter the <IP address of the WLSE> in the **Boot Server Host Name** field (option number 066) on the DHCP server.
 - b. Enter <startup file name> in the **BootfileName** field (option number 067) on the DHCP server.
- Q.** What is auto configuration?
- A.** Auto configuration is used after the device has been discovered and inventory has been collected for it. This template can be applied based on criteria you define while saving your auto-configuration template.
- Q.** If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?
- A.** No. If you make modifications to the startup template, you will have to reapply the template.

Troubleshooting

- [An error message indicates that the device version to which I am assigning a template is not supported.](#)
- [Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.](#)

Symptom An error message indicates that the device version to which I am assigning a template is not supported.

Possible Cause The device version was not supported at the time the WLSE was released.

Recommended Action Deselect **Enable Version Checking** in Configuration > Template Creation > Finish to assign the template to the device anyway. Or, import the updated list of devices to the WLSE, select Administration > System > New Version Support.

Symptom Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.

Possible Cause The credentials entered on the WLSE do not exactly match the data entered in Administration > Discovery > Device Credentials > Telnet/SSH User/Password.

Recommended Action Make sure that the Telnet/SSH credentials data entered on the WLSE show the correct device login response. Match the device login sequence with the credential fields, as shown in [Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.](#), page 7-23.

Firmware FAQs and Troubleshooting

- [FAQs, page 7-18](#)
- [Troubleshooting, page 7-20](#)

FAQs

- How can firmware images be imported?
- Are firmware jobs run by using both HTTP and SNMP?
- What kinds of job logs are available?
- Is it necessary to validate a firmware job?
- How many devices can I have in one firmware job?

Q. How can firmware images be imported?

A. Firmware images can be imported to WLSE from the desktop as well as Cisco.com. While importing any image from Cisco.com, the WLSE reads the version string and the device type for the image attributes. For imports from the desktop, you must make sure that the version and the device type strings are correctly entered in the image attributes. For example, for an AP350, image version 12.00T, the image string must be entered as 12.00T; not 12.0 or 12.00 or 12.0T.

Q. Are firmware jobs run by using both HTTP and SNMP?

A. Yes. Firmware jobs use both HTTP and SNMP protocols.

- HTTP is valid for all supported device versions. The following setup parameters must be in place for HTTP to function properly:
 - HTTP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE HTTP device credentials screen.
 - TFTP server settings on the access point must reference the WLSE's IP address.



Note

Both username and password in the device credentials are case sensitive.

- SNMP is valid for versions 11.08T and higher. The following setup parameters must be in place for SNMP to function properly:
 - SNMP credentials for the device (with admin and firmware privileges on the AP) must match those entered on the WLSE SNMP device credentials screen.
 - There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the Security > Local Admin Access template screen.



Note NOTE: Make sure to provide a numeric value in the user ID field (template screen).

- Q.** What kinds of job logs are available?
- A.** There are two kinds of job logs: Job run log and the jobvm log.
- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
 - The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting Administration > Appliance > View Log File, then clicking **jobvm.log**.
- Q.** Is it necessary to validate a firmware job?
- A.** We recommend that you always validate a job before saving it to make sure that you do not overlook any possible errors or warnings.
- Validation produces Warnings and Errors. Errors are never ignored but Warnings can be ignored if Ignore Warnings is checked. If the user wants to upload an image that the WLSE does not recognize, select Ignore Warnings to circumvent the version checking engine of WLSE and apply the new image.

- Q.** How many devices can I have in one firmware job?
- A.** There is no limit, although it is recommended that you work with device groups and set up jobs accordingly (for example, by location or building). While a job is running, the WLSE allocates resources for updating 20 devices in parallel. At any given time, 20 devices will be upgrading and the remainder will be waiting for resources to become available.

Troubleshooting

- There is a time discrepancy in scheduled jobs.
- Email about job completion fails to arrive at destination.
- Firmware is not updated on all the devices included in a job.
- An SNMP job fails..
- A firmware job ends with status “not verified.”
- Firmware jobs over slow links do not succeed.
- When downloading firmware from Cisco.com, an error message about cryptography permissions appears.
- Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.

Symptom There is a time discrepancy in scheduled jobs.

Possible Cause The time was not set correctly on the WLSE.

Recommended Action

- a. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows:
 - Enter **services stop** to stop services.
 - Enter the **clock** command to reset the time.
 - Enter **services start** to restart the services.
- b. Set the time in local browser time, select Administration > Appliance > Time/NTP/Name.

Symptom Email about job completion fails to arrive at destination.

Possible Cause The SMTP server is not specified.

Recommended Action Configure the mail route by selecting Administration > Appliance > Configure Mailroute.

Symptom Firmware is not updated on all the devices included in a job.

Possible Cause There were warnings during the job run and Ignore Warnings was not selected when creating the job. Jobs for devices with warnings do not run; the job runs only for devices that do not have any warnings (if Ignore Warnings is not selected).

Recommended Action

- Select Ignore Warnings in the Finish step of Firmware > Jobs > Create Job before running the job.

Possible Cause If two firmware jobs were scheduled closely together, the second job contained some of the same devices as the first job. Those devices could not be updated because the first job was already running.

Recommended Action It is recommended that firmware jobs be run on groups of devices. Each group should be exclusive; that is, no device should be a member of more than one group.

Symptom An SNMP job fails.

Possible Cause The read community string does not have sufficient permissions.

Recommended Action The access point must have a user with at least SNMP, FIRMWARE, and ADMIN permissions for read-only access.

Access points with software releases prior to 12.01(T) must have a user with SNMP, FIRMWARE, ADMIN, and IDENT permissions for read-only access.

Symptom A firmware job ends with status “not verified.”



Note A status of “not verified” does not always mean that the job has failed. The WLSE may have timed out before verifying whether the job succeeded.

Possible Cause The device may be taking a long time to reboot.



Caution

Do not use the following procedure for firmware jobs that you are running to convert non-IOS access points to IOS. See the special conversion instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Recommended Action Increase the value of the Device Reboot Wait Timeout parameter by accessing the WLSE through the following URL:

`http://your_wlse:1741/debug/jobprops.jsp`

where *your_wlse* is the name of the WLSE.

Increase the value of the Device Reboot Wait Timeout parameter and run the job again.



Note Do not make this value extremely high. It is advisable to keep this value to something slightly higher than the actual reboot time of the slowest access point.

Symptom Firmware jobs over slow links do not succeed.

Possible Cause The access points being upgraded are connected to the WLSE over a slow link (less than 1.544 Mbps) and the job is timing out.



Caution

Do not use the following procedure for firmware jobs that you are running to convert non-IOS access points to IOS. See the special conversion instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Recommended Action

Increase the job operation timeout as follows:

- a. Access the WLSE through the following URL:
`http://your_wlse:1741/debug/jobprops.jsp`
- b. Increase the value of the Per device job operation timeout parameter. For example, for a 56kbps link, the recommended value is 2400 seconds (40 minutes). On a 128kbps link, the recommended value is 1200 seconds (20 minutes).

Symptom When downloading firmware from Cisco.com, an error message about cryptography permissions appears.

Possible Cause The first time you attempt to download firmware, the WLSE displays this message: `Error while selecting or displaying image details. Please log into cisco.com and make sure your username has acknowledged cryptography permissions for downloading IOS images.`

Recommended Action Log into Cisco.com and acknowledge the cryptography permissions. After you have acknowledged these permissions, you can import IOS images to the WLSE.

Symptom Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.

Possible Cause The credentials entered on the WLSE do not exactly match the data entered in Administration > Discovery > Device Credentials > Telnet/SSH User/Password.

Recommended Action Make sure that the Telnet/SSH credentials data entered on the WLSE show the correct device login response. Match the device login sequence with the credential fields as follows.

Device Login Sequence	Telnet Credential Fields Required
Username: Password: prompt > enable Password: enable prompt #	User Name User Password Enable Password
Password: prompt > enable Password: enable prompt #	User Password Enable Password (leave the User Name field empty)
prompt > enable Password: enable prompt #	Enable Password (leave the User Name and User Password fields empty)
enable prompt #	Not supported. Please configure the device accordingly.

Reports FAQs and Troubleshooting

- [FAQ, page 7-24](#)
- [Troubleshooting, page 7-24](#)

FAQ

- Q.** Are any of the reports real-time reports?
- A.** The reports are not real time. They are based on data that is collected periodically. The frequency with which the data is collected is user configurable (see Administration > System Parameters). The data shown in reports is as current as the time the data was collected from the devices.

Troubleshooting

- [The Top N Busiest Clients report and the Client Statistics report display 0 \(zero\) values.](#)
- [Some report fields are blank.](#)

- The client association data in the Group Client Association report differs from the data shown in the Current Client Associations report.
- The access point data in the Historical Associations report is not accurate.
- The Summary and/or Detailed report for access points is empty.
- The group report for a user-defined group contains no data.
- After running a job, the updated data does not appear in a report.
- Email fails to arrive at its destination.
- There is a time discrepancy in the scheduled email jobs.
- No VLAN information is displayed for IOS access points.

Symptom The Top N Busiest Clients report and the Client Statistics report display 0 (zero) values.

Possible Cause Wireless client polling frequency is set to 51 minutes by default. The counters could reset between two polling cycles which would cause zero values when the reports are run.

Recommended Action Increase the polling frequency by selecting Administration > System > System Parameters.



Caution

Increasing the polling frequency could have an effect on performance.

Symptom Some report fields are blank.

Possible Cause The device is not configured properly for management by the WLSE; the ISO view has not been created.

Recommended Action See [Devices are placed in Misconfigured Devices group after discovery.](#), page 7-31 for information about how to correct the problem.

Symptom The client association data in the Group Client Association report differs from the data shown in the Current Client Associations report.

Possible Cause The data for the Group Client Association report is collected using performance attributes polling and the data shown in the Current Client Association report uses wireless client polling.

Whichever report has a higher polling frequency will contain the most up to date data. Select Administration > System > System Parameters to view polling frequency.

Recommended Action None.

Symptom The access point data in the Historical Associations report is not accurate.

Possible Cause The wireless client was associated with an access point managed by the WLSE, but subsequently associated with an access point that was added to the network, but not yet managed by the WLSE.

Recommended Action Verify that the associated access points are in the managed devices folder by selecting Administration > Discover > Managed Devices > Manage/Unmanage.

Symptom The Summary and/or Detailed report for access points is empty.

Possible Cause The SNMP user may not have the correct rights assigned.

Recommended Action

- a. Open a browser window to the access point, and select Setup > Security > User Information.
- b. 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.
- c. If not, click on the user and assign all these rights.

Symptom The group report for a user-defined group contains no data.

Possible Cause Reports cannot be displayed for a user-defined group that contains another group.

Recommended Action Display individual reports for the sub-groups or devices within the user-defined group.

Symptom After running a job, the updated data does not appear in a report.

Possible Cause A full polling cycle has not completed and the new data has not been entered in the database.

Recommended Action Verify that the polling cycle has completed as follows:

- a. Select Administration > Appliance > Status > View Log File.
- b. Click **jobvm.log**.
- c. Scroll through the log to find the message: “Finished Inventory” for your particular job.

Symptom Email fails to arrive at its destination.

Possible Cause The SMTP server is not configured properly.

Recommended Action Configure the SMTP server by selecting Administration > Appliance > Configure Mailroute.

Symptom There is a time discrepancy in the scheduled email jobs.

Possible Cause The time is not set correctly on the WLSE.

Recommended Action

- a. Reset the WLSE time to Universal Coordinated Time (UTC) using CLI commands as follows:
Enter **services stop** to stop services.
Enter the **clock** command to reset the time.
Enter **services start** to restart the services.
- b. Set the time in local browser time, select **Administration > Appliance > Time/NTP/Name**.

Symptom No VLAN information is displayed for IOS access points.

Possible Cause WEP keys have not been configured in each VLAN. When the WEP keys are configured in the IOS access points, VLAN information is accessible by SNMP.

Recommended Action Configure the WEP keys for the corresponding VLAN.

Administration FAQs and Troubleshooting

- [FAQs, page 7-28](#)
- [Troubleshooting, page 7-29](#)

FAQs

- [How can I verify the status of the database?](#)
- [Why is sysContact and sysLocation information not updated in the WLSE after I change these parameters on the access point?](#)
- [What is an invalid CDP seed?](#)
- [Can I discover devices if CDP is disabled?](#)

- Q.** How can I verify the status of the database?
- A.** You can verify that the WLSE database is running by using the **show process** CLI command. If the command output includes the db2sync process, the database is running.
- Q.** Why is sysContact and sysLocation information not updated in the WLSE after I change these parameters on the access point?
- A.** The sysContact and sysLocation parameters are updated during discovery, not during inventory. Make sure you schedule a periodic discovery under Administration > Discover > Scheduled Discovery.
- Q.** What is an invalid CDP seed?
- A.** An invalid seed is a device that does not run Cisco Discovery Protocol (CDP), such as a PC or workstation). Such a device does not function as a seed because it does not allow the WLSE to traverse the network and find other devices. In the discovery run log, invalid seeds are shown as SNMP unreachable.
- Q.** Can I discover devices if CDP is disabled?
- A.** If CDP is disabled on network devices, you can still discover access points by entering the IP addresses of all of them on the WLSE as seed values. However, the WLSE cannot discover switches directly attached to such access points, and switch-related reports will be empty.

Troubleshooting

This section contains the following troubleshooting information:

- [Devices were discovered but are not displayed in the GUI; for example, in Reports.](#)
- [There is a time discrepancy in the scheduled discovery jobs.](#)
- [Users cannot log in after failure of the alternative authentication source.](#)
- [Some users are not listed under User Admin > Manage Users.](#)
- [Devices are placed in Misconfigured Devices group after discovery..](#)

- When using Internet Explorer 6.0 to install a new image on a WLSE from a repository located on a Windows XP machine, the progress bar does not appear in the Install Software Updates window. This problem also occurs when you use Internet Explorer 6.0 and a Windows XP system as a client to install a new image on a WLSE.
- The SNMP Query Authorization Exception is recorded in the discovery log.
- Cannot back up the WLSE configuration to a Windows 2000 or Windows XP Server.
- Cannot log in with a username and password created in the CLI.
- Frequent client inventories are causing too much network traffic or degrading WLSE performance.

Symptom Devices were discovered but are not displayed in the GUI; for example, in Reports.

Possible Cause The devices have not been moved to the Managed state.

Recommended Action Select Administration > Discover > Managed Devices. Move the devices from New or Unmanaged to Managed.

Intermediate switches with no access points directly connected to them are shown to be discovered in the Administration > Tasks History > Discovery logs but will not show up in Administration > Discover > Managed Devices > Manage/Unmanage.

Symptom There is a time discrepancy in the scheduled discovery jobs.

Possible Cause The local or system time is not set correctly on the WLSE.

Recommended Action

- a. Reset the WLSE system time (UTC) using CLI commands as follows:
 - Enter **services stop** to stop services.
 - Enter the **clock** command to reset the time.
 - Enter **services start** to restart the services.
- b. Set the local browser time. Select Administration > Appliance > Time/NTP/Name.

Symptom Users cannot log in after failure of the alternative authentication source.

Possible Cause The WLSE falls back to the Local authentication module.

Recommended Action

- 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.
- If you still cannot log in, follow the procedure in the Recovering from Loss of All Administrator Passwords section in the *Configuration and Installation Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Symptom Some users are not listed under User Admin > Manage Users.

Possible Cause Only the creator of a user can view that user's name in the list. The admin user, however, can view all users.

Recommended Action None.

Symptom Devices are placed in Misconfigured Devices group after discovery.

Possible Cause IOS devices are not configured correctly with an ISO view. The dot11mib fault appears for these devices.

Recommended Action Perform the following tasks on the devices and the WLSE. Either configure the devices individually or create a configuration template with the relevant custom values and create a job for the devices.

- To configure devices individually:
 - a. Use Telnet or SSH to log in to the device, then enter enable mode.
 - b. In global configuration mode, enter the following commands in sequence:

```
# snmp-server view iso iso included
```

```
# snmp-server community community_string view iso RO
```

where *community_string* is the device's read-only community string. This is the same string that should exist in the WLSE's SNMP credentials screen (Administration > Discover > Device Credentials > SNMP Communities). If it is not entered there, see the following instructions for entering device credentials in the WLSE.

- c. Exit from the global configuration mode, and enter the following command:

```
# write memory
```

- To configure devices by using a template:
 - a. Use the procedures in the configuration template instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0* to create a template.
 - b. Enter the following custom values in the template:

```
snmp-server view iso iso included
```

```
snmp-server community community_string view iso RO
```

- c. Run a configuration job on the devices in the Misconfigured Devices group:
 - Select the template created in the previous step.
 - Either select the Misconfigured Devices group or the devices in the group.
 - Schedule the job to run at the desired time.
- d. After the configuration job finishes successfully, the dot11 mib fault will be cleared after the next discovery cycle. You can run a manual discovery immediately after the configuration job finishes; select Administration > Discover > DISCOVER > Run Now.

- Perform the following steps on the WLSE:
 - a. If the device's ISO community string has not been entered on the WLSE, select Administration > Discover > Device Credentials > SNMP Communities. Then, enter the same community strings that you configured on the devices in the previous procedure.

Otherwise, the devices will be placed back in the Misconfigured Devices group after the next discovery cycle.
 - b. Rediscover the devices by using them as seed devices in an immediate discovery. Select Administration > Discover > DISCOVER > Run Discovery Now. For more information on discovery, see the online help discovery section or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Symptom When using Internet Explorer 6.0 to install a new image on a WLSE from a repository located on a Windows XP machine, the progress bar does not appear in the Install Software Updates window. This problem also occurs when you use Internet Explorer 6.0 and a Windows XP system as a client to install a new image on a WLSE.

Possible Cause The Internet Explorer 6.0 browser on Windows XP does not come with the Java plug-in installed.

Recommended Action Before using a Windows XP machine as a *remote repository* to update WLSE software, perform the following on the repository:

- a. Install the JRE version 1.3.1_08 or later browser plug-in.
- b. In the browser, select Tools > Internet Options > Privacy. Lower the slider all the way down to achieve the **Accept All Cookies** setting.

Before using a Windows XP machine as a *client* to update WLSE software, install the JRE 1.3.1_08 or later browser plug-in on the client machine.

You can download the plug-in from third-party sources such as Sun Microsystems or IBM.

Symptom The SNMP Query Authorization Exception is recorded in the discovery log.

Possible Cause The community string on the access point does not have admin and firmware rights.

Recommended Action In the configuration template or on the access point, assign the missing rights to the community string. For more information, see the information on setting up devices in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Symptom Cannot back up the WLSE configuration to a Windows 2000 or Windows XP Server.

Possible Cause The backup directory is not writable.

Recommended Action Set the directory to UNIX mode and make it write-enabled. For more information, see the backup and restore instructions in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.0*.

Symptom Cannot log in with a username and password created in the CLI.

Possible Cause The password is too long.

Recommended Action Reset the password by using the CLI **username** command, or log in by using the first 8 characters of the password. Passwords should be from 5 to 8 characters long.

Symptom Inventory is taking longer than expected and the following message appears in the inventory log:

```
No logs available. Waiting for resources to start job.
```

Possible Cause If there are also SNMP timeouts on the network, inventory jobs will take much longer. Other jobs may be using all of the available resources. Also, the next scheduled inventory will not run until the current inventory finishes.

Recommended Action None.

Symptom Frequent client inventories are causing too much network traffic or degrading WLSE performance.

Possible Cause Running frequent client inventories when managing large numbers of access points (1,000 or more) generates a great deal of traffic and may degrade WLSE performance.

Recommended Action Increasing the Wireless Client Poll Interval in Administration > System > System Parameters will reduce the polling frequency. If you need more frequent client polling for a subset of your access points, use the Scheduled Inventory feature instead (Administration > Discover > Inventory > Scheduled Inventory).

