FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine

Release 2.5

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine

CONTENTS

CHAPTER 1 **FAQs and Troubleshooting** 1-1

General FAQs and Troubleshooting 1-1

Faults FAQs and Troubleshooting 1-11

Devices FAQs and Troubleshooting 1-13

Configuration FAQs and Troubleshooting 1-19

Firmware FAQs and Troubleshooting 1-24

Reports FAQs and Troubleshooting 1-32

Radio Manager FAQs and Troubleshooting 1-36

Administration FAQs and Troubleshooting 1-43

CHAPTER 2 **Fault Descriptions** 2-1

Access Point Faults 2-2

WLSE Fault 2-20

AAA Server Faults 2-20

Switch Faults 2-25

Router Fault 2-28

INDEX

FAQs and Troubleshooting

This FAQ and troubleshooting guide consists of the following sections:

- General Questions—See General FAQs and Troubleshooting, page 1-1
- Faults—Faults FAQs and Troubleshooting, page 1-11
- Devices—Devices FAQs and Troubleshooting, page 1-13
- Configuration—Configuration FAQs and Troubleshooting, page 1-19
- Firmware—Firmware FAQs and Troubleshooting, page 1-24
- Reports—Reports FAQs and Troubleshooting, page 1-32
- Radio Manager —Radio Manager FAQs and Troubleshooting, page 1-36
- Administration—Administration FAQs and Troubleshooting, page 1-43

General FAQs and Troubleshooting

- General FAQs, page 1-1
- General Troubleshooting, page 1-3

General 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 SSH be disabled?, page 1-2
- Can I run a job to convert a number of access points from non-IOS to IOS?
- What are the requirements for WLSE usernames and passwords?

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 SSH be disabled?

A. It cannot be disabled on the WLSE itself, but you can use the firewall command to deny all SSH connections. For example, the following CLI command will cause the WLSE to reject all incoming SSH connections on the Ethernet 0 interface but allows connections through other protocols and other ports:

```
firewall ethernet0 private firewall ethernet0 private ssh
```

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 2.5*.

Q. What are the requirements for WLSE usernames and passwords?

A. Usernames can be up to 32 characters long, and you can use the alphanumeric characters and other characters as described in the Naming Guidelines appendix of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. Passwords are from 5 to 8 characters long, and you can use the alphanumeric characters plus the underscore (_). Both usernames and passwords are case sensitive.

General Troubleshooting

This section provides the following troubleshooting information:

- After the WLSE reboots, the login screen appears, followed by an Internal Server Error message.
- 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.
- Cannot recover after incorrect setup program entry.
- Cannot log into the system.
- Cannot log in as a system administrator.
- After the WLSE starts up, the setup login prompt appears. Use the setup program. 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.

Symptom After the WLSE reboots, the login screen appears, followed by an Internal Server Error message.

Possible Cause The servlet engine in the WLSE is starting up.

Recommended Action Wait for 20 to 30 seconds, then log in again.

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.

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

1. 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.
2. Do you know the password for any system user accounts?

   If no, see Cannot log in as a system administrator., page 1-5.

   If yes, continue to the next step.
3. If you are certain you entered a valid username and password, contact Cisco's Technical Assistance Center for assistance.

Symptom Cannot log in as a system administrator.

Possible Cause All administrator passwords have been lost.

Recommended Action Perform the following procedure:

1. Connect a console to the WLSE's console port.

   For the WLSE 1105, use the serial port on the front panel; do not use the serial port on the back panel as a console port.

   For the WLSE 1130, the serial/console port is on the back panel.
2. Power the system off, then power it back on. The following prompt appears:

   ```
   LILO boot:
   ```
3. Press the Tab key. The following prompt appears:

   ```
   boot:
   ```
4. Enter the following command. This puts the WLSE in maintenance image mode.

   ```
   CiscoBreR
   [root@CiscoMaintImage/]#
   ```

5. Enter the following command. This erases the WLSE's configuration, returns the WLSE to factory defaults, and reloads the WLSE.

```
[root@CiscoMaintImage/]# erase config
```

Symptom After the WLSE starts up, the setup login prompt appears. Use the setup program. 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

1. 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.

2. 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.

3. Use the **show interfaces** command to determine if the Ethernet 0 interface is disabled or misconfigured.

   For more information on the **show interfaces** command, see the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

   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.

4. 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.

5. 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

1. Make sure that the system can connect to the network. Attempt to connect the system using a Web browser.

   If you cannot connect, continue.

2. If you are attempting to connect via HTTP, verify that the IP address is appended with **:1741**.
3. 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*.
4. 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.
5. 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.
   ```

6. Stop the system services by entering the following:

   ```
   # services stop
   ```

7. Restart the system services by entering the following:

   ```
   # services start
   ```

8. Try to connect the system using a Web browser.

   If you cannot connect, continue to the next step.

9. Reboot the system by entering the **reload** command.

For more information on the **reload** command, see the CLI appendix in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

10. 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.

For information about maintaining the system time and date, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

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 *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

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.

1. 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 **telnetenable** CLI command. For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help

   To enable or disable Telnet on individual ports, use the **firewall** CLI command. For more information on this command, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help

2. 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.

3. 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.

4. 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 2. The command returns the IP address of the host.

5. 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.

6. 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.

7. 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.

Faults FAQs and Troubleshooting

- Faults FAQs, page 1-11
- Faults Troubleshooting, page 1-12

Faults FAQs

- 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. Does acknowledging a fault clear it?

A. No, it only removes it from the Active list. For a description of fault states, see the information on understanding fault states in the online help.

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 the online help.

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.

Faults 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.

Devices FAQs and Troubleshooting

- Devices FAQs, page 1-13
- Devices Troubleshooting, page 1-15

Devices FAQs

- Why is hostname (device name), 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?
- What are the extra inventories listed in the Run Now folder?
- What are the results of adding or removing an interface from an access point?
- Can the WLSE discover access points that are connected to non-Cisco switches?

Q. Why is hostname (device name), sysContact, and sysLocation information not updated in the WLSE after I change these parameters on the access point?

A. The hostname (device name), 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.

Q. What are the extra inventories listed in the Run Now folder?

A. The radio management module runs periodic immediate inventories.

Q. What are the results of adding or removing an interface from an access point?

A. If you physically remove an interface (for example, removing 11b from a dual-interface AP 1200), the WLSE will automatically detect the change during the next inventory cycle. If you physically *add* an interface, you must delete the device and rediscover it. Otherwise, the inventory data might be invalid.

Q. Can the WLSE discover access points that are connected to non-Cisco switches?

A. The APs cannot be discovered through CDP, but you can import the APs from a file or enter them all as seeds in the WLSE UI.

Devices 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.
- Devices are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed.
- Access points are placed in Misconfigured Devices group even though they have been configured with the correct ISO views.
- The SNMP Query Authorization Exception is recorded in the discovery log.
- Frequent client inventories are causing too much network traffic or degrading WLSE performance.
- Inventory is taking longer than expected and a message about no logs available appears in the inventory log.
- When entering device Telnet or SSH credentials on the WLSE, authentication fails if the & character appears in a name or password.

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 Devices are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed.

Possible Cause IOS devices are not configured correctly with an ISO view. Also, see the following Symptom: Access points are placed in Misconfigured Devices group even though they have been configured with the correct ISO views., page 1-18.

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 (Devices > 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, 2.5* 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 Devices > Discover > Run Inventory > 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 Devices > 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 Devices > Discover > Run Inventory > Run Now. For more information on discovery, see the online help discovery section or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

Symptom Access points are placed in Misconfigured Devices group even though they have been configured with the correct ISO views.

Possible Cause Unknown.

Recommended Action Delete the access points from the WLSE and run a new discovery on them.

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 2.5*.

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 Devices > Discover > Inventory > Polling 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 (Devices > Discover > Inventory > Run Inventory).

Symptom Inventory is taking longer than expected and a message about no logs available 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 When entering device Telnet or SSH credentials on the WLSE, authentication fails if the & character appears in a name or password.

Possible Cause The WLSE ignores the & character and all characters that follow it.

Recommended Action Do not use & in Telnet/SSH credentials that must be entered on the WLSE.

Configuration FAQs and Troubleshooting

- Configuration FAQs, page 1-19
- Configuration Troubleshooting, page 1-22

Configuration 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?
- Can I give a configuration job a name that is used for a firmware or radio management job?

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 Devices > Discover > Inventory > Polling > 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?

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.

For additional information, or for information about configuring a router as a DHCP server, see the online help.

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.

Q. Can I give a configuration job a name that is used for a firmware or radio management job?

A. No. Job names cannot be duplicated.

Configuration Troubleshooting

- HTTP configuration jobs are picking up the wrong template.
- An IOS template job failed.
- Configuration jobs fail because the Telnet/SSH credentials are not valid, even though credentials have been entered on the WLSE.

Symptom HTTP configuration jobs are picking up the wrong template.

Possible Cause If the access point's FTP setting is the same as the DHCP server, then HTTP config job picks up the wrong template from wrong WLSE server.

Recommended Action None. This is how the access point functions and there is no workaround.

Symptom An IOS template job failed.

Possible Cause The template has the hostname configured instead of the IP address, and the DNS name resolution is not configured correctly on the access point.

Recommended Action Use the IP address or configure the DNS name correctly on the access point.

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 Devices > 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 1-30.

Firmware FAQs and Troubleshooting

- Firmware FAQs, page 1-24
- Firmware Troubleshooting, page 1-26

Firmware FAQs

- How can firmware images be imported?
- Are firmware jobs run by using both HTTP and SNMP?
- What kinds of job logs are available?
- How many devices can I have in one firmware job?
- Can I give a firmware job a name that is used for a configuration or radio management 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 AP 350, 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. 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.

Q. Can I give a firmware job a name that is used for a configuration or radio management job?

A. No. Job names cannot be duplicated.

Firmware Troubleshooting

- There is a time discrepancy in a job.
- 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.
- A conversion job fails because the firmware installation does not start.
- When downloading firmware from Cisco.com, an error message about cryptography permissions appears.
- When downloading firmware from Cisco.com, an error message about connectivity failure appears.
- Firmware and configuration jobs fail because the Telnet/SSH credentials are not valid.
- After conversion to IOS, the native VLAN information is not correct.

Symptom There is a time discrepancy in a job.

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.

For more information on setting the time, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

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 displayed when the job was saved. Jobs for devices with warnings do not run; the job runs only for devices that do not have any warnings.

Recommended Action Solve the problems indicated in the warning messages 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.

For more information on updating firmware, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

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 The "not verified" status may not mean that the job has failed. The WLSE may time out before confirming whether the upgrade succeeded. To make sure, you can run an on-demand inventory on the devices in question to find out whether the firmware upgrade was installed. For more information, see the Inventory online help, or select Devices > DISCOVER > Inventory > Run Inventory Now.

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

Caution Do not take the following action 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 2.5*.

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 take the following action 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, 2.5*.

Recommended Action

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 A conversion job fails because the firmware installation does not start.

Possible Cause The AP may not have enough free memory. A minimum of 4 MB (DRAM) of free space is required for the conversion to succeed.

Recommended Action To check the free space available, use the CLI command :vxdiag_memshow. You can temporarily remove the 11a radio to free up space. For more information, see the access point documentation on Cisco.com.

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 When downloading firmware from Cisco.com, an error message about connectivity failure appears.

Possible Cause DNS is not configured on the WLSE.

Recommended Action Configure DNS on the WLSE and make sure the WLSE can resolve the cisco.com domain name. For information about configuring DNS, see the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5* or the *Installation and Configuration Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

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 Devices > 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 User Name and User Password fields empty)

`enable prompt #`	Not supported. Configure the device accordingly.

Symptom After conversion to IOS, the native VLAN information is not correct.

Possible Cause If VLANs are configured on non-IOS devices and none of them is configured as native, the conversion process automatically makes one VLAN native. This may not be the correct native VLAN. If more than one device is included in the conversion job, a different VLAN may become native in some APs.

Recommended Action Access the AP(s) via Telnet or the console and change the native VLAN to the desired one.

Reports FAQs and Troubleshooting

- Reports FAQ, page 1-32
- Reports Troubleshooting, page 1-32

Reports 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 Devices > Discover > Inventory > Polling). The data shown in reports is as current as the time the data was collected from the devices.

Reports 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 Devices > Discover > Inventory > Polling.

⚠ **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 and dot11mib fault is displayed., page 1-16 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 Devices > Discover > Inventory > Polling 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 Devices > 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.

Radio Manager FAQs and Troubleshooting

- Radio Manager FAQs
- Radio Manager Troubleshooting

Radio Manager FAQs

Configuration

- For each AP to report radio information back to WLSE, does each AP need to be configured as a WDS AP?
- If so, do I need a separate username and password for each? If not, how many WDS APs would I need?
- Do I need a separate Infrastructure SSID for the APs that are configured as WDS?Why don’t I see the building or floor node in the device tree in the Assisted Site Survey Wizard?

Assisted Site Survey Wizard

- Why don't I see the device that I am looking for in the Assisted Site Survey device tree?
- When I select devices in the Assisted Site Survey Wizard, why are some shown in red?
- When I’m using the Assisted Site Survey Wizard, why is the Next button disabled after I complete step one?
- In the Assisted Site Survey Wizard, why is Use Old Radio Scan Data disabled?

- In the Assisted Site Survey Wizard, what does None mean in the Last Scan Time field?
- In the Assisted Site Survey Wizard, why is the Next button disabled on the radio scan step?
- Why did my radio scan job fail in the Assisted Site Survey Wizard?
- When I'm using the Assisted Site Survey Wizard, the radio scan progress advances very slowly. How long does it radio scan normally take?
- Can I skip client walkabout in the Assisted Site Survey Wizard even though the number of data shown is zero?
- In the client walkabout step in the Assisted Site Survey Wizard, what is the Recall button for?
- What is the difference between the Number of Location Data and Number of New Location Data fields?
- In the Constraints and Goals step in the Assisted Site Survey Wizard, how do I select multiple channels in the channel list?
- How long should the Constraints and Goals calculation step take in the Assisted Site Survey Wizard?
- Where can I see the result of the Constraints and Goals calculation in the Assisted Site Survey Wizard?
- If I don't like result of the Constraints and Goals calculation in the Assisted Site Survey Wizard, what can I do?
- When I apply the configuration in the Assisted Site Survey Wizard, where do I see the results?
- In the last step of the Assisted Site Survey Wizard, why is the Next button disabled?

Miscellaneous

- Can I give a radio management job a name that is used for a firmware or configuration management job?

Configuration

Q. For each AP to report radio information back to WLSE, does each AP need to be configured as a WDS AP?

A. No, each AP does not need to be enabled as a WDS AP. Rather, each AP participating in the Radio Monitoring should have a subset of the WDS configuration which includes only the WLCCP username and password.

Q. If so, do I need a separate username and password for each? If not, how many WDS APs would I need?

A. No, you do not need a separate username and password for each. Each WDS AP (either 1100 or 1200) supports up to 30 APs.

Q. Do I need a separate Infrastructure SSID for the APs that are configured as WDS?

A. No, the infrastructure SSID configuration does not need to be altered.

Assisted Site Survey Wizard

Q. Why don’t I see the building or floor node in the device tree in the Assisted Site Survey Wizard?

A. Expand the building node to see all floors that belong to the building. If you expand the building node and the floors still do not appear, close the Wizard and make sure the building and floor exist in the Location Manager navigation tree. If the building or floor does not exist in the Location Manager navigation tree, you first need to create them and then restart the Assisted Site Survey Wizard. See the topic Adding Building Information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*.

Q. Why don't I see the device that I am looking for in the Assisted Site Survey device tree?

A. Expand the building and floor nodes to see all devices that belong to a building or floor. If the device still does not appear, close the Assisted Site Survey Wizard and make sure the device appears in the Location Manager navigation tree. If the device does not appear in the Location Manager navigation tree, select **Tools > Find Device** to locate it. If you find the device, move it to the desired location. See the topic Adding Devices to the Floor Map in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*. If the device does not appear in Location Manager, it might not have been discovered by the system. See the topic Managing

Device Discovery in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, 2.5*. After adding the device and specifying its location, restart the Assisted Site Survey Wizard.

Q. When I select devices in the Assisted Site Survey Wizard, why are some shown in red?

A. The devices might be red if:

- The devices are not in the Managed state. Select Devices > Discover > Manage/Unmanage to verify that the devices are Managed.
- The devices are not in infrastructure mode. Go to the AP configuration for the individual device and verify that it is in "Infrastructure Mode" with the proper WDS assigned.

Q. When I'm using the Assisted Site Survey Wizard, why is the **Next** button disabled after I complete step one?

A. You have not selected any acceptable devices that are required for the next step. If any of the selected devices are shown in red, you need to deselect them before you can go to the next step.

Q. In the Assisted Site Survey Wizard, why is **Use Old Radio Scan Data** disabled?

A. You might not have previously run radio scan for the selected devices. You must start a new radio scan.

Q. In the Assisted Site Survey Wizard, what does *None* mean in the Last Scan Time field?

A. The selected device was not included in a previous radio scan.

Q. In the Assisted Site Survey Wizard, why is the **Next** button disabled on the radio scan step?

A. You need to run radio scan by clicking **Start**. When the radio scan is complete, you will be able to click **Next**.

Q. Why did my radio scan job fail in the Assisted Site Survey Wizard?

A. Look at the log window to find out exact failure cause. If radio scan failed:

- Make sure the devices have the correct setup for WDS. Also verify that WDS is authenticated to WLSE and that WDS has an IP address pointing to WLSE.
- Make sure the devices have the correct SNMP read/write community strings that match the WLSE setting.

Q. When I'm using the Assisted Site Survey Wizard, the radio scan progress advances very slowly. How long does it radio scan normally take?

A. Radio scan normally takes about 5 to 10 minutes to complete. If you suspect the program has stalled, check its status by selecting Radio Manager > AP Radio Scan and viewing the progress of the job.

Q. Can I skip client walkabout in the Assisted Site Survey Wizard even though the number of data shown is zero?

A. Yes, you can skip client walkabout. However, performing a client walkabout will generate better parameters for your wireless network.

Q. In the client walkabout step in the Assisted Site Survey Wizard, what is the **Recall** button for?

A. You can click **Recall** to display a list of the last five client MAC addresses that were used for the previous client walkabout. To retrieve a previously used MAC address, click **Recall** and select a MAC address from the list.

Q. What is the difference between the **Number of Location Data** and **Number of New Location Data** fields?

A. Number of Location Data is the total number of data found by client walkabout for the current session plus any previous sessions. Number of New Location Data is the total number of data found by client walkabout for the current session only. The numbers in these two fields can increase at the same time during a client walkabout.

Q. In the Constraints and Goals step in the Assisted Site Survey Wizard, how do I select multiple channels in the channel list?

A. For Windows users, control-click on the channels to add them to the selection. The selected channels are highlighted.

Q. How long should the Constraints and Goals calculation step take in the Assisted Site Survey Wizard?

A. It varies depending on the amount of radio scan and client walkabout data. The more data you have, the longer it will take to calculate.

Q. Where can I see the result of the Constraints and Goals calculation in the Assisted Site Survey Wizard?

A. If the calculation was successful, you can click **Next** to view the result.

Q. If I don't like result of the Constraints and Goals calculation in the Assisted Site Survey Wizard, what can I do?

A. Go back and specify different constraints and goals, and then recalculate the constraints and goals.

Q. When I apply the configuration in the Assisted Site Survey Wizard, where do I see the results?

A. Check Location Manager to view the configuration changes. You might need to refresh the Location Manager window by selecting View > Refresh Data. In rare cases, the wizard might have failed to apply the configuration. In that case, check your SNMP settings, particularly the WRITE community string, for the devices.

Q. In the last step of the Assisted Site Survey Wizard, why is the **Next** button disabled?

A. This is the last step in Assisted Site Survey Wizard. You can close the Wizard unless you want to repeat any previous steps.

Miscellaneous

Q. Can I give a radio management job a name that is used for a firmware or configuration management job?

A. No. Job names cannot be duplicated.

Radio Manager Troubleshooting

- WDS has been set up on the AP and WLSE, but WDS isn't authenticating with WLSE.
- My clients are not being authenticated through WDS.
- After completing the Assisted Site Survey, Location Manager did not update to include the applied configurations.

Symptom WDS has been set up on the AP and WLSE, but WDS isn't authenticating with WLSE.

The “Not Authenticated” you see in response to the "show wlccp wnm status” command means that the WDS component has not authenticated the WLSE. There are two possible causes:

Possible Cause The device credentials in the WLSE are not correct. The user name and password should match the user names and passwords entered on the WDS AP and the AAA server.

Recommended Action To correct the credentials:

1. Select **Devices** > **Discover** > **Device Credentials** > **WLCCP Credentials**.
2. Change the **Radius User Name** and **Radius Password** fields to match the user names and passwords entered on the WDS AP and the AAA server.

Possible Cause The WDS AP has not been managed in the WLSE.

Recommended Action To manage the WDS AP:

1. Select **Devices** > **Discover** > **Managed/Unmanaged**.
2. Look in the **New** folder for your WDS AP.
3. Select it, then select **Manage**. The process will take 1-2 minutes.

After the WLSE is authenticated by the WDS, the WDS reports its member APs to the WLSE, so they are “discovered” by the WLSE. After these member APs have been discovered, you will need to manage them as well.

Symptom My clients are not being authenticated through WDS.

Possible Cause You have not created a server group on the WDS APs for client authentication.

Recommended Action To create a server group on the WDS APs for client authentication, you can use the AP CLI, the AP web interface, or the WLSE configuration templates. For more information, see the device setup information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.7*.

Symptom After completing the Assisted Site Survey, Location Manager did not update to include the applied configurations.

Possible Cause You did not refresh the Location Manager window.

Recommended Action In the Location Manager window, select View > Refresh Data.

Administration FAQs and Troubleshooting

- Administration FAQs, page 1-43
- Administration Troubleshooting, page 1-44

Administration FAQs

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.

Administration Troubleshooting

This section contains the following troubleshooting information:

- Users cannot log in after failure of the alternative authentication source.
- Some users are not listed under User Admin > Manage Users.
- 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.
- 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.

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 on recovering from the loss of all admin passwords in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

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 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 r*emote 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 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 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 2.5*.

Fault Descriptions

This section provides the following information on the faults displayed in **Faults > Display Faults**. The following information is provided:

- Fault—The fault as it appears in the Display Faults table.
- Explanation—An explanation as to why the fault occurred.
- Related Setting—The threshold or policy you assigned to devices under **Faults > Manage Fault Settings**, when applicable.
- Recommended Action—An action that can be taken to clear the displayed fault.

Fault tables are provided for each device type:

- Access Point Faults, page 2-2
- WLSE Fault, page 2-20
- AAA Server Faults, page 2-20
- Switch Faults, page 2-25
- Router Fault, page 2-28

Access Point Faults

Table 2-1 Access Point Faults

Fault Description	Type	Explanation	Related Setting	Recommended Action
AP is in a Degraded state *number* associated clients	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: AP is in OK state.	Manage Fault Settings > Thresholds > Access Point > Associated Clients	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
AP is in an Overloaded state *number* associated clients	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: AP is in OK state.	Manage Fault Settings > Thresholds > Access Point > Associated Clients	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
AP is not registered with any WDS	IOS	The managed IOS access point is not registered with any WDS. For Radio Manager functionality to work, all IOS access points must register with a WDS. If an access point is not registered, it will be excluded from all the Radio Manager procedures, which will provide incorrect results.	Manage Fault Settings > Access Point > Thresholds > Registration Error	Verify that the WLCCP credentials for wireless domain services (WDS) are configured correctly. For more information, see the managing devices information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.
Broadcast Key Rotation is disabled	Non-IOS and IOS	The broadcast key rotation has been disabled. When this fault is cleared, the following message displays: Broadcast Key Rotation is enabled.	Manage Fault Settings > Security Policies > Key Rotation per VLAN	Log in to the access point and enable the broadcast key rotation interval.
Broadcast SSID is disabled	Non-IOS and IOS	Broadcast SSID has been disabled. When this fault is cleared, the following message displays: Broadcast SSID is enabled	Manage Fault Settings > Security Policies > Broadcast SSID Disabled	Log in to the access point and enable SSID for broadcast mode.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Client association rate is Degraded *number* per minute	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Client association rate is OK.	Manage Fault Settings > Thresholds > Access Point > Association Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Client association rate is Overloaded *number* per minute	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Client association rate is OK.	Manage Fault Settings > Thresholds > Access Point > Association Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Client authentication error rate is Degraded *number* per minute	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Client association error rate is OK.	Manage Fault Settings > Thresholds > Access Point > Authentication Error Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Client authentication error rate is Overloaded *number* per minute	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Client association error rate is OK.	Manage Fault Settings > Thresholds > Access Point > Authentication Error Rate	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Device state is rogue access point	IOS	The WLSE detected a rogue access point. (This is an access point that is not being managed and is unknown to the WLSE.)	Manage Network-Wide Settings > Rogue AP Detection	Use Location Manager (select Radio Manager > Location Manager) to locate the rogue access point.
Device was not reachable via SNMP	Non-IOS and IOS	The SNMP Agent could be down. When this fault is cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Thresholds > Access Point > SNMP Reachable	Make sure SNMP is enabled on the device and that the agent is not down. Take a MIB walk of the device to make sure sysup time is returning 0, which indicates Device is reachable.
		The SNMP community string in the access point has been changed, and then a discovery job is run.	Not applicable.	Change the SNMP community string on the WLSE to match the new community string on the access point, then run discovery again.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Duplicate IP is found	Non-IOS and IOS	WLSE discovery detects a second device with the same IP address in the network. When this fault is cleared, the following message displays: Duplicate IP is valid.	There is no setting associated with this fault.	Do one of the following: • 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.
		When changing the MAC address of the FastEthernet interface to the MAC address of a radio interface, the WLSE might detect the access point as a duplicate device. This is because during discovery, the uniqueness of the device is based on its FastEthernet MAC address.		Delete the device, and run discovery again.
EAP is disabled	Non-IOS and IOS	The EAP has been disabled. When this fault is cleared, the following message displays: EAP is enabled	Manage Fault Settings > Security Policies > EAP Enforced	Log in to the access point and enable the Network EAP and Open authentication.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
EAP per SSID is disabled	Non-IOS and IOS	EAP per SSID has been disabled on the access point. When this fault is cleared, the following message displays: EAP per SSID is enabled	Manage Fault Settings > Security Policies > EAP Per SSID Enforced	Log in to the access point and enable the Network EAP and Open authentication per SSID.
Ethernet bandwidth utilization is Degraded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Ethernet bandwidth utilization is OK.	Manage Fault Settings > Thresholds > Access Point > Ethernet Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Ethernet bandwidth utilization is Overloaded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Ethernet bandwidth utilization is OK.	Manage Fault Settings > Thresholds > Access Point > Ethernet Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Firmware version policy violation (*version number*)	Non-IOS and IOS	The wrong version number for policy checking has been entered. When this fault is cleared, the following message displays: Firmware version is valid.	Manage Fault Settings > Security Policies > Firmware Version	Make sure that the firmware version that is entered in the policy setting matches the firmware version on the access point.
		The access point is running an unauthorized firmware version. When this fault is cleared, the following message displays: Firmware version is valid.		Make sure that you have entered authorized versions in the policy setting. Update the firmware on the access point to an authorized version.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
HotStandBy is active	Non-IOS and IOS	The access point that is configured for hot standby has become active. The following conditions could cause the hot standby access point to become active: the primary access point is down, the Ethernet port is down, or the Radio port is down. When this fault is cleared, the following message displays: HotStandBy is disabled.	Manage Fault Settings > Security Policies > HotStandBy Status	For non-IOS access points: 1. Check the primary access point, the Ethernet port, or the Radio port to see why the hot standby access point has been activated. 2. Correct the condition. For example, if the Radio Port on the formerly active access point was in a disabled state, then enable it using the access point GUI. 3. Launch the GUI for access point that is currently in Active Takeover mode. 4. Select the Hot Standby section and click **Start Hot Standby mode** to reconfigure the access point to Hot Standby mode.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
				For IOS access points: 1. Check the primary access point, the Ethernet port, or the Radio port to see why the hot standby access point has been activated. 2. Correct the condition. For example, if the Radio Port on the formerly active access point was in a disabled state, then enable it using the access point GUI. 3. Launch the GUI for access point that is currently in Active Takeover mode. 4. Select Hot Standby, click **Disabled** , then click **Apply**. 5. Click **Enabled**, then enter the Radio MAC address of Monitored Radio Port, leave the Polling interval and Timeout for Each Polling fields blank,. 6. Click **Apply** to reconfigure the access point to Hot Standby mode.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
HTTP access is enabled	Non-IOS	HTTP has been enabled on the access point. When this fault is cleared, the following message displays: HTTP access is disabled.	Manage Fault Settings > Security Policies > HTTP Disabled	Log in to the access point and disable HTTP access.
HTTP access without login is enabled	Non-IOS	The allowBrowseWithoutLogin setting on the access point is set. When this fault is cleared, the following message displays: HTTP access without login is disabled.	Manage Fault Settings > Security Policies > HTTP Authentication	Log in to the access point and disable the allowBrowseWithoutLogin setting.
Non 802.11 interference detected	IOS	The WLSE detected a non-802.11 interference.	Manage Network-Wide Settings > Interference Detection	Use AP Radio Scan (select Radio Manager > AP Radio Scan) to locate the rogue access point.
Packet Error is in Degraded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault is cleared, the following message displays: Packet Error is in OK state.	Manage Fault Settings > Thresholds > Access Point > RF Port Packet Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Packet Error is in is in Overloaded state (*error rate %*)	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault is cleared, the following message displays: Packet Error is in OK state.	Manage Fault Settings > Thresholds > Access Point > RF Port Packet Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Port is administratively set to down	Non-IOS and IOS	The port has been set to Down by the administrator. When this fault is cleared, the following message displays: Port is up	This fault is not generated based on a threshold or policy violation.	There is no action necessary; the port has been deliberately shut down.
Port is down	Non-IOS and IOS	The port is operationally down. When this fault is cleared, the following message displays: Port is up	This fault is not generated based on a threshold or policy violation.	Check the device to determine why the port is down. If you have added or removed an interface from an access point, the WLSE might generate an erronous fault. S ee What are the results of adding or removing an interface from an access point?, page 1-14.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
PSPF is disabled	Non-IOS	The PSPF port has been disabled. PSPF (Publicly Secure Packet Forwarding) is a feature that prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network. When the fault is cleared, the following message displays: The PSPF is enabled.	Manage Fault Settings > Security Policies > PSPF Enabled	Log in to the access point and enable the PSPF setting.
Retry Count rate is Degraded *number* per minute	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: Retry Count rate is OK	Manage Fault Settings > Thresholds > Access Point > Max Retry Counts	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Retry Count rate is Overloaded *number* per minute	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: Retry Count rate is OK	Manage Fault Settings > Thresholds > Access Point > Max Retry Counts	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
RF bandwidth utilization is Degraded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When the fault is cleared, the following message displays: RF bandwidth utilization is OK	Manage Fault Settings > Thresholds > Access Point > RF Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
RF bandwidth utilization is Overloaded (*utilization %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When the fault is cleared, the following message displays: RF bandwidth utilization is OK	Manage Fault Settings > Thresholds > Access Point > RF Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
SNMP query received authorization error response	Non-IOS	The access point's user community strings do not have Admin, Ident, Firmware, SNMP privileges. The WLSE might not be able to access some SNMP information from the access point that requires these privileges. When the fault is cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Thresholds > Access Point > SNMP Reachable	Make sure the SNMP community string set on the WLSE (Devices > Discover > Device Credentials > SNMP Communities) is the same as the string set on the access point (Setup > Security > User Information).

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
SSID policy violation *SSID assigned to the access point*	Non-IOS and IOS	The SSID entered in the WLSE is different from the SSID assigned to the access point. When the fault is cleared, the following message displays: SSID is valid.	Manage Fault Settings > Security Policies > SSID	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.
		The access point is configured with an unauthorized SSID.		Make sure that you have entered authorized SSIDs in the SSID policy. Change the SSID on the access point to an authorized SSID.
	IOS	The SSID policy for an IOS access point is enabled, but the "guest mode" is disabled. This causes the access point to send an SSID made up of all zeros and equivalent to the length of the first configured SSID.	Manage Fault Settings > Security Policies > SSID	Enable the access point's guest mode.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
Telnet access is enabled	Non-IOS	Telnet has been enabled on the access point. When this fault has been cleared, the following message displays: Telnet access is disabled	Manage Fault Settings > Security Policies > Telnet Disabled	Log in to the access point and disable the Telnet access setting.
User capabilities are not enforced	Non-IOS	The enableUserMgr setting is not set on the access point. When this fault has been cleared, the following message displays: User capabilities are enforced.	Manage Fault Settings > Security Policies > User Manager Enforced	Log in to the access point and enable the User Mgr setting.
Vlan WEP key length policy violation	Non-IOS and IOS	The WEP key length per VLAN setting has been violated. When this fault has been cleared, the following message displays: Vlan WEP key length is ok.	Manage Fault Settings > Security Policies > WEP Encryption per Vlan	Make sure the WEP key length selected in the policy setting matches the access point settings.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
WDS appears down.	IOS	The WLSE failed to receive "keep active" messages from the WDS. This happens when the WDS is down or when the network is down.	Manage Fault Settings > Thresholds > WDS > WLSE-WDS Link Status	Check the network connectivity, the WDS status, and the WLSE and WDS credentials.
WEP Error is in Degraded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: WEP Error is in OK state	Manage Fault Settings > Thresholds > Access Point > RF Port WEP Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
WEP Error is in Overloaded state (*error rate %)*	Non-IOS and IOS	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: WEP Error is in OK state	Manage Fault Settings > Thresholds > Access Point > RF Port WEP Errors	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
WEP is disabled	Non-IOS and IOS	WEP has been disabled. When this fault has been cleared, the following message displays: WEP is enabled.	Manage Fault Settings > Security Policies > WEP Enforced	Log in to the access point and enable WEP.

Table 2-1 Access Point Faults (continued)

Fault Description	Type	Explanation	Related Setting	Recommended Action
WEP key length policy violation	Non-IOS and IOS	The WEP key length setting has been violated. When this fault has been cleared, the following message displays: WEP key length is OK.	Manage Fault Settings > Security Policies > WEP Key Length	Check the WEP key settings on the access point to make sure they match the WLSE settings.
WNM failed to authenticate with WDS.	IOS	Authentication required to open a WLCCP channel between the WLSE and the WDS failed.	Manage Fault Settings > Thresholds > WDS > Authentication Failures	Verify that the WLSE credentials used to authenticate with the WDS are correct. For more information, see the managing devices information in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.5*.

WLSE Fault

Table 2-2 WLSE Fault

Fault Description	Explanation	Related Setting	Recommended Action
Dot11mib view is not enabled on some Access Points. Please consult online help for details	The device is not configured with the iso (dot11 mib) view, and cannot be managed effectively by the WLSE. This can cause some WLSE report information to be missing and some WLSE faults may not be generated. When this fault has been cleared, the following message displays: No Dot11mib view misconfigurations detected.	Manage Fault Settings > Thresholds > WLSE > Dot11mib view enabled	Configure the devices and the WLSE as described in Devices are placed in Misconfigured Devices group after discovery and dot11mib fault is displayed., page 1-16.

AAA Server Faults

Table 2-3 Server Faults

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
Authentication failed. Please check EAP-MD5, LEAP, PEAP, or RADIUS credentials	EAP-MD5	The server is reachable but the credentials are incorrect. When this fault has been cleared, the following message displays: Authentication succeeded	Manage Fault Settings > Thresholds > EAP-MD5 /LEAP/ PEAP/RADIUS> Response Time	Make sure that the credentials are set correctly by selecting Devices > Discover > AAA Server.

Table 2-3 Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
EAP-MD5 server is not available	EAP-MD5	The EAP-MD5 server is not available. When this fault has been cleared, the following message displays: EAP-MD5 server is available	Manage Fault Settings > Thresholds > Leap > Response Time	Check the server configuration.
EAP-MD5 server is Degraded	EAP-MD5	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: EAP-MD5 server is OK	Manage Fault Settings > Thresholds > EAP-MD5 > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
EAP-MD5 server is Overloaded	EAP-MD5	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: EAP-MD5 server is OK	Manage Fault Settings > Thresholds > EAP-MD5 > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-3 Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
LEAP server is not available	LEAP	The LEAP server is not available. This can be caused if you have enabled this policy and you are using a non-Cisco client with EAP. When this fault has been cleared, the following message displays: LEAP server is available	Manage Fault Settings > Thresholds > Leap > Response Time	Check the server configuration.
LEAP server is Degraded	LEAP	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: LEAP server is OK.	Manage Fault Settings > Thresholds > Leap > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
LEAP server is Overloaded	LEAP	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: LEAP server is OK.	Manage Fault Settings > Thresholds > Leap > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-3 Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
PEAP server is not available	PEAP	The PEAP server is not available. When this fault has been cleared, the following message displays: PEAP server is available	Manage Fault Settings > Thresholds > Peap > Response Time	Check the server configuration.
PEAP server is Degraded	PEAP	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: PEAP server is OK.	Manage Fault Settings > Thresholds > Peap > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
PEAP server is Overloaded	PEAP	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: PEAP server is OK	Manage Fault Settings > Thresholds > Peap > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Radius server is not available	PEAP	The RADIUS server is not available. When this fault has been cleared, the following message displays: Radius server is available	Manage Fault Settings > Thresholds > Radius > Response Time	Check your server configuration.

Table 2-3 Server Faults (continued)

Fault Description	Server Type	Explanation	Related Setting	Recommended Action
Radius server is Degraded	PEAP	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: Radius server is OK.	Manage Fault Settings > Thresholds > Radius > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Radius server is Overloaded	PEAP	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: Radius server is OK.	Manage Fault Settings > Thresholds > Radius > Response Time	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Switch Faults

Table 2-4 Switch Faults

Fault Description	Explanation	Related Setting	Recommended Action
CPU utilization is Degraded *(utilization %)*	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: CPU utilization is Ok.	Manage Fault Settings > Thresholds > Switch > CPU Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
CPU utilization is Overloaded (*utilization %)*	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: CPU utilization is Ok.	Manage Fault Settings > Thresholds > Switch > CPU Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Device was not reachable via SNMP	The SNMP Agent on the switch is down. When this fault has been cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Thresholds > Switch > SNMP Reachable	Make sure that the switch SNMP agent is active.
Module is down	The module is down. When this fault has been cleared, the following message displays: Module is up.	Manage Fault Settings > Thresholds > Switch > Module Status	Check the module in the switch and correct the problem.

Table 2-4 Switch Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Port could not agree with other end on duplex mode	The port could not agree with the far end on port duplex, and is in disagree(3) mode. When this fault has been cleared, the following message displays: Port duplex state is OK.	This fault is not generated based on a threshold or policy violation.	Make sure the duplex mode on both ends match.
Switch memory utilization is Degraded (*utilization %)*	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: Switch memory utilization is Ok.	Manage Fault Settings > Thresholds > Switch > Memory Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Switch memory utilization is Overloaded (*utilization %)*	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: Switch memory utilization is Ok.	Manage Fault Settings > Thresholds > Switch > Memory Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Table 2-4 Switch Faults (continued)

Fault Description	Explanation	Related Setting	Recommended Action
Switch Port bandwidth utilization is Degraded (*utilization %*)	The fault threshold set for the degraded state has been exceeded. When this fault has been cleared, the following message displays: Switch port bandwidth utilization is Ok.	Manage Fault Settings > Thresholds > Switch > Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.
Switch Port bandwidth utilization is Overloaded (*utilization %*)	The fault threshold set for the overloaded state has been exceeded. When this fault has been cleared, the following message displays: Switch port bandwidth utilization is Ok.	Manage Fault Settings > Thresholds > Switch > Port Utilization	Verify that the fault threshold is set correctly. If the threshold is set correctly, review your network to determine the action necessary to clear the fault condition.

Router Fault

Table 2-5 Router Fault

Fault Description	Explanation	Related Setting	Recommended Action
Device was not reachable via SNMP	The SNMP Agent on the switch is down. When this fault has been cleared, the following message displays: Device was reachable via SNMP.	Manage Fault Settings > Thresholds > Router > SNMP Reachable	Make sure that the router SNMP agent is active.

INDEX

A

AAA server

fault descriptions 2-20

access point

accessing through WLSE, troubleshooting 1-4

AP web page, accessing 1-4

fault descriptions 2-2

interface

adding, results of 1-14

removing, results of 1-14

reports, VLAN information in 1-36

Administration tab

FAQs 1-43

troubleshooting 1-44

B

backing up and restoring WLSE configuration

Windows 2000 or XP server 1-45

booting, WLSE 1-4, 1-9

browser

cannot connect to WLSE 1-7

IE, installing software updates 1-45

C

CDP

discovery without using 1-14

seed, invalid 1-14

client

inventory, troubleshooting 1-18

reports 1-33

configuration

auto-configuration 1-22

FAQs 1-19

IOS template job failures 1-23

job history, retention of 1-20

protocols used for jobs 1-20

startup template, changes to 1-22

Telnet/SSH credentials not valid 1-23

troubleshooting 1-22

updates, undoing 1-20

WEP key settings 1-20

credentials, Telnet/SSH 1-19

D

database

checking database status 1-43

date and time
  incorrect 1-9
device credentials, Telnet/SSH 1-19
device name, updates to 1-14
Devices tab
  FAQs 1-13
  troubleshooting 1-15
discovery
  devices discovered, but not displayed 1-15
  Misconfigured Devices group 1-16
  seed devices 1-14
  SNMP Authorization Exception in discovery log 1-18
  time discrepancy in jobs 1-15
  troubleshooting 1-15
  without CDP 1-14
dot11 mib fault
  description of 2-20
  troubleshooting 1-16

F

FAQs
  Administration 1-43
  configuration 1-19
  devices 1-13
  faults 1-11
  firmware 1-24
  general 1-1
  radio manager 1-36
  reports 1-32
faults
  AAA server fault descriptions 2-20
  access point fault descriptions 2-2
  acknowledging 1-12
  clearing 1-12
  descriptions of 2-1
  email of 1-13
  FAQs 1-11
  MIB file 1-12
  no display 1-12
  router fault description 2-28
  switch fault descriptions 2-25
  troubleshooting 1-12
firmware
  connectivity failure 1-30
  cryptography permissions, message about 1-30
  email fails to arrive 1-27
  FAQs 1-24
  job logs 1-25
  job not verified 1-28
  number of devices in jobs 1-25
  slow links 1-29
  SNMP job fails 1-28
  some devices not updated 1-27
  Telnet/SSH credentials not valid 1-30
  time discrepancy in jobs 1-26
  troubleshooting 1-24

G

groups
  Misconfigured Devices group 1-16

I

inventory
  effects on traffic and performance 1-18
  extra inventories 1-14
  FAQs 1-14
  length of time required 1-18

L

logging in
  cannot log in 1-5
  cannot log in as system administrator 1-5
  failure of authentication source 1-44
  password created in CLI 1-45

M

Misconfigured Devices system group
  moving devices from 1-16

N

network
  connection failure 1-6

P

passwords, loss of 1-5
performance
  problems caused by frequent client inventory 1-18
protocols
  SSH, disabling 1-2
  Telnet, enabling 1-2
  used for configuration jobs 1-20

R

radio manager
  Assisted Site Survey
    client walkabout, skipping 1-40
    configuration, not updated 1-43
    configuration, results of 1-41
    Constraints and Goals, calculations of 1-41
    devices in red 1-39
    device tree 1-38
    job, failure of 1-39
    Last Scan Time Field 1-39
    Location Data fields 1-40
    missing building or floor nodes 1-38
    multiple channels, selecting 1-40
    Next button disabled 1-39, 1-41

radio scan slow 1-40

Recall button 1-40

Use Old Radio Scan Data disabled 1-39

FAQs 1-36

inventories run by 1-14

troubleshooting 1-42

reports

blank fields in 1-33

client reports, 0 values in 1-33

FAQs 1-32

not real-time 1-32

troubleshooting 1-32

VLAN information missing 1-36

routers, fault message for 2-28

S

search, for devices

no results yielded 1-4

security

authentication (WLSE)

failure of authentication source 1-44

troubleshooting 1-44

seed

invalid 1-14

setup program

incorrect entry 1-4

network connection fails 1-6

software, on WLSE

updates

Internet Explorer, problems using 1-45

SSH

disabling 1-2

switches, fault descriptions 2-25

sysContact information, updates to 1-14

sysLocation information

updates to 1-14

T

Telnet

& not accepted in credentials 1-19

connecting to WLSE 1-10

enabling 1-2

time

incorrect 1-9

traps

definition file 1-12

not forwarded 1-12

type of 1-12

troubleshooting

administration 1-44

configuration 1-22

devices 1-15

faults 1-12

firmware 1-26

radio manager 1-42

reports 1-32

U

users
- authentication failure 1-44
- not listed in UI 1-44
- password created in CLI not accepted 1-45
- simultaneous access to access points 1-2

V

VLANs
- in reports 1-36