



FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, 1.3

This FAQ and troubleshooting guide consists of the following sections:

- [Hardware Troubleshooting, page 1](#)
- [Software Troubleshooting and FAQs, page 5](#)

Hardware Troubleshooting

This section provides the following troubleshooting information:

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

Cannot recover after incorrect installation entry.

Probable Cause:

You entered incorrect text during the installation setup and want to fix the entry.

Possible Solution:

Exit the installation 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.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Cannot log into the system.**Probable Cause:**

- You did not run the setup program to create an initial system configuration.
- You lost all the user account passwords.

Possible Solution:

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, reconfigure the system to create a new user account.
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.

The WLSE cannot connect to the network.**Probable 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).

Possible Solution:

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:
 - a. 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.
 - b. 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 *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. 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 *Hardware Installation and Configuration Guide for the CiscoWorks 1105 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.

Cannot connect to the WLSE using a Web browser.

Probable 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.

Possible Solution:

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 *Hardware Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.
4. Verify that the browser is configured correctly, and attempt to connect to the WLSE. For more information, see these *Hardware Installation and Configuration Guide for the CiscoWorks 1105 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
```

- Restart the system services by entering the following:

```
# services start
```

- Try to connect the system using a Web browser.

If you cannot connect, continue to step 9.

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

For more information on the **reload** command, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

- If you still cannot connect to the system using a Web browser, contact Cisco's Technical Assistance Center for assistance.

The system time or date is incorrect.

Probable Cause:

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

Possible Solution:

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 1105 Wireless LAN Solution Engine*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

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

Probable Cause:

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

Possible Solution:

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 *Hardware Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

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

Probable Cause:

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



Note If you are not using name recognition, slow or non-existent telnet interaction is an expected problem. For more information, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Possible Solution:

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 **telnet** CLI command.
For more information on this command, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. 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 1105 Wireless LAN Solution Engine*. 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 steps
 - a. 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 step 4..
 - b. 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.
 - c. 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.
4. 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.
5. If the system can resolve DNS names to IP addresses but you still cannot connect to the system using Telnet, or Telnet interaction with the system is extremely slow, contact Cisco's Technical Assistance Center.

Software Troubleshooting and FAQs

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

- General Questions—See [General FAQs and Troubleshooting, page 6](#)
- Faults Tab—[Faults FAQs and Troubleshooting, page 7](#)
- Configuration Tab—[Configuration FAQs and Troubleshooting, page 9](#)
- Firmware Tab—[Firmware FAQs and Troubleshooting, page 12](#)
- Reports Tab—[Reports FAQs and Troubleshooting, page 14](#)
- Administration Tab—[Administration FAQs and Troubleshooting, page 16](#)

General FAQs and Troubleshooting

- [FAQs, page 6](#)
- [Troubleshooting, page 6](#)

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?](#)

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.

Troubleshooting

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

Probable Cause:

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

Possible Solution:

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

Faults FAQs and Troubleshooting

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

FAQs

- [Does acknowledging a fault clear it?](#)
- [What causes the fault “LEAP Disabled”?](#)
- [What causes the fault “Authentication failed. Please check LEAP credentials”?](#)
- [What causes the fault “SNMP query received authentication error response”?](#)
- [What traps are sent from the WLSE?](#)
- [What trap types are actually forwarded?](#)
- [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.

Q. What causes the fault “LEAP Disabled”?

A. LEAP is considered enabled only when following conditions are set in the access point (on the Radio Data Encryption (WEP) page):

- Network-EAP is selected.
- If Open authentication type is selected, then Require EAP must also be selected.
- If Shared authentication type is selected, then Require EAP option must also be selected.

The LEAP Disabled fault is generated if above criteria is not met. The following are possible scenarios that can produce the Leap Disabled fault:

- You selected Open authentication type and Require EAP. This will cause the fault because Network-EAP is not selected.
- You selected Network-EAP and Share authentication type. This will cause the fault because Required EAP under Share is not selected.

If you only selected Network-EAP, the fault will not be generated.

Q. What causes the fault “Authentication failed. Please check LEAP credentials”?

A. The server is reachable but the credentials are incorrect.

Q. What causes the fault “SNMP query received authentication error response”?

- A. The SNMP authorization error occurs when the AP the user created for community strings does not have Write, SNMP, Firmware and Admin privileges.
- Make sure the SNMP community string set on the WLSE (Administration > Discover > Device Credentials.) is the same as the string set on the access point (Setup > Security > User Information).
- Make sure that the credentials are set correctly by selecting Administration > Discover > LEAP, RADIUS, or EAP-MD5 Server.
- 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.
- Q. What trap types are actually forwarded?
- A. No traps are forwarded from other devices.
- Q. What information is emailed in a fault notification?
- A. The notification message sent by WLSE has the following attributes:
- FaultId—Unique identifier for the fault
 - DeviceId—Unique identifier used by WLSE for the device with the fault
 - DeviceIp—IP address of the device with the fault
 - DeviceName—Name of the device with the fault
 - MOId—Identifier used by WLSE for the subcomponent of the device with the fault
 - AlarmState—State of the Alarm (Active or Cleared)
 - Description—Text describing the last update to the fault
 - Severity—Severity of the fault
- Q. Does a MIB or trap definition file exist for the WLSE?
- A. Yes, from the Cisco.com download site, download MIB CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my and load it into the trap receiver.

Troubleshooting

- [A user is still receiving emails for faults even though they have been removed from fault notification list.](#)
- [A profile named with a back slash\(\\) as the final character renders the Manage Profiles window unusable.](#)
- [The Display Fault view is blank.](#)
- [Email fails to arrive at its destination.](#)

A user is still receiving emails for faults even though they have been removed from fault notification list.

Probable Cause:

The changes have not been implemented correctly.

Possible Solution:

Restart the ExcepReporter process under Administration > Appliance > Diagnostic > Processes.

A profile named with a back slash(\) as the final character renders the Manage Profiles window unusable.

Probable Cause:

A back slash at the end of the name is not supported.

Possible Solution:

Reinitialize the database, but note that this action erases all information contained within the database.

The Display Fault view is blank.

Probable Cause:

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

Possible Solution:

Not applicable.

Email fails to arrive at its destination.

Probable Cause:

The SMTP server is not configured properly.

Possible Solution:

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

Configuration FAQs and Troubleshooting

- [FAQs, page 9](#)
- [Troubleshooting, page 11](#)

FAQs

- [Can you undo a configuration update?](#)
- [How long is the configuration job history kept in the WLSE?](#)
- [How are configuration files transferred to access points?](#)
- [Do jobs use HTTP or SNMP to initiate a configuration upload?](#)
- [Is it necessary to validate a job?](#)
- [What kinds of job logs are available?](#)
- [What is startup configuration?](#)
- [If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?](#)
- [What is auto configuration?](#)

Q. Can you undo a configuration update?

A. Yes, but only for successful jobs and device versions 11.21 for AP350/AP340 and 11.54T for AP1200.

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, refer to the online help.

Q. How long is the configuration job history kept in the WLSE?

A. The default time is 30 days. You can change this by navigating to Administration > System Parameters > Job History Truncation Interval. Also, by default, for the recurring jobs, the last 30 runs are maintained in the database.

Q. How are configuration files transferred to access points?

A. Even though access points support both TFTP and FTP, the WLSE uses only TFTP to upload and download configuration files.

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.



Note NOTE: Make sure the user ID is a numeric value and not a textual value.

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

Q. Is it necessary to validate a job?

A. We recommend that you always validate a job before saving it. This will help in locating any possible problems before applying the job.

Q. What kinds of job logs are available?

A. There are two kinds of job logs: Job run log and the jobvm log.

- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
- The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting Administration > Appliance > View Log File, then clicking **jobvm.log**.

Q. What is startup configuration?

- A. Startup configuration is used right after a device (access point) reboots. It requires DHCP server to be properly set up to allow the access point to pick its startup configuration from WLSE. For this to work, you must set up the following:
- a. Option 066 on the DHCP server as the IP address of WLSE
 - b. Option 067 on the DHCP server as the boot file name you entered while saving the startup template.

Q. What is auto configuration?

- A. Auto configuration is used after the device has been discovered and inventory has been collected for it. This template can be applied based on criteria you define while saving your auto-configuration template.

Q. If I make changes to the startup template, will those modifications be automatically uploaded to the access points that already had that startup template applied?

- A. No. If you make modifications to the startup template, you will have to reapply the template.

Troubleshooting

- [An error message indicates that the device version to which I am assigning a template is not supported.](#)
- [The access point is not accessible through the HTTP port set with template configuration job.](#)

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

Probable Cause:

The device version was released after your WLSE was released.

Possible Solution:

Deselect **Enable Version Checking** in Configuration > Template Creation > Finish.

The access point is not accessible through the HTTP port set with template configuration job.

Probable Cause:

The HTTP port setting does not take effect until the access point is cold restarted.

Possible Solution:

Cold restart the access point.

Firmware FAQs and Troubleshooting

- [FAQs, page 12](#)
- [Troubleshooting, page 13](#)

FAQs

- [Can firmware images be imported?](#)
- [Are firmware jobs run on both HTTP and SNMP?](#)
- [What kinds of job logs are available?](#)
- [Is it necessary to validate a firmware job?](#)

Q. 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 enters the version string and the device type for the image attributes. For imports from the desktop, you must make sure that the version and the device type strings are correctly entered in the image attributes. For example, for an AP350, image version 12.00T, the image string must be entered as 12.00T; not 12.0 or 12.00 or 12.0T.

Q. Are firmware jobs run on both HTTP and SNMP?

A. Yes. Firmware jobs run on both HTTP and SNMP mechanisms.

- The HTTP mechanism 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.

- 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 AP) must match those entered on the WLSE SNMP device credentials screen.
 - There is no need to change TFTP server settings for the SNMP mechanism, although you can use the SNMP mechanism to change the TFTP server settings on the AP to be used in the HTTP mechanism. Enter valid credentials in the Security > Local Admin Access template screen.



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

Q. What kinds of job logs are available?

A. There are two kinds of job logs: Job run log and the jobvm log.

- The job run log is where events are logged for a particular job's run. This log can be used to check what went wrong with the job and make any required corrections. The job run log can be viewed by selecting a particular job from the job list, then clicking **Job Run Detail**. From the window that pops up, select a particular run for the job, then click **Job Run Log**.
- The jobvm.log is a global log for all types of jobs. It is used mainly for development troubleshooting. The jobvm.log can be viewed by selecting Administration > Appliance > View Log File, then clicking **jobvm.log**.

Q. Is it necessary to validate a firmware job?

A. We recommend that you always validate a job before saving it to make sure that you do not overlook any possible errors or warnings.

Validation produces Warnings and Errors. Errors are never ignored but Warnings can be ignored if Ignore Warnings is checked. If the user wants to upload an image that the WLSE does not recognize, select Ignore Warnings to circumvent the version checking engine of WLSE and apply the new image.

Troubleshooting

- [There is a time discrepancy in scheduled jobs.](#)
- [Firmware is not updated on all the devices included in the job.](#)
- [Email about job completion fails to arrive at destination.](#)
- [An SNMP job fails.](#)
- [The firmware job verification was not completed.](#)

There is a time discrepancy in scheduled jobs.

Probable Cause:

The time was not set correctly on the WLSE.

Possible Solution:

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

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

Probable Cause:

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

Possible Solution:

Select Ignore Warnings in Firmware > Jobs > Create Job before running the job.

See the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

Email about job completion fails to arrive at destination.

Probable Cause:

The SMTP server is not specified.

Possible Solution:

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

See the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

An SNMP job fails

Probable Cause:

The read community string does not have sufficient permissions.

Possible Solution:

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.

For more information, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*. You can access a PDF version of this guide by clicking **View PDF** in the WLSE's online help.

The firmware job verification was not completed.

Probable Cause:

The device may be taking a long time to reboot.

Possible Solution:

Increase the Device reboot wait timeout to a higher value.



Note Do not make this value extremely high as it could result in slowing firmware jobs. It is always advisable to keep this value slightly higher than the actual reboot time of the worst access point.

Reports FAQs and Troubleshooting

- [FAQ, page 14](#)
- [Troubleshooting, page 15](#)

FAQ

Q. Are any of the reports real-time reports?

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

Troubleshooting

- [The 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.](#)

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

Probable Cause:

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

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

Possible Solution:

None.

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

Probable 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.

Possible Solution:

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

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

Probable Cause:

The SNMP user may not have the correct rights assigned.

Possible Solution:

- 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.

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

Probable Cause:

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

Possible Solution:

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

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

Probable Cause:

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

Possible Solution:

Verify that the polling cycle has completed as follows:

1. Select Administration > Appliance > Status > View Log File.
2. Click **jobvm.log**.
3. Scroll through the log to find the message: "Finished Inventory" for your particular job.

Email fails to arrive at its destination.

Probable Cause:

The SMTP server is not configured properly.

Possible Solution:

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

There is a time discrepancy in the scheduled email jobs.

Probable Cause:

The time is not set correctly on the WLSE.

Possible Solution:

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

Administration FAQs and Troubleshooting

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

FAQs

- Q. Can you 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.

Troubleshooting

- [The Version field is blank in the Device Details screen under Administration > Managed Devices > Manage/Unmanage > Managed.](#)
- [Devices were discovered but are not displayed in the GUI; for example, in Reports.](#)
- [There is a time discrepancy in the scheduled discovery jobs.](#)
- [Users cannot log in after failure of the alternative authentication source.](#)
- [Some users are not listed under User Admin > Manage Users.](#)

The Version field is blank in the Device Details screen under Administration > Managed Devices > Manage/Unmanage > Managed.

Probable Cause:

The device information has not been updated.

Possible Solution:

Run Inventory Now on the device. If that does not work, then Run Discovery Now on the device.

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

Probable Cause:

The devices have not been moved to the Managed state.

Possible Solution:

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.

There is a time discrepancy in the scheduled discovery jobs.

Probable Cause:

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

Possible Solution:

1. Reset the WLSE system time (UTC) using CLI commands as follows:
 - a. Enter **services stop** to stop services.
 - b. Enter the **clock** command to reset the time.
 - c. Enter **services start** to restart the services.

2. Set the local browser time. Select Administration > Appliance > Time/NTP/Name.

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

Probable Cause:

The WLSE falls back to the Local authentication module.

Possible Solutions:

- Users can log in using their local passwords.
- The system administrator can log in using the admin log in.
- All users with CLI access can log in using the CLI.
- If you still cannot log in, follow the procedure in the Recovering from Loss of All Administrator Passwords section in the *Hardware Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

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

Probable Cause:

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

Possible Solution:

None.