



Fault Monitoring

The Faults tab displays information to help you monitor your devices. All the device information shown under this tab is polled from the devices in your network.

Following are the subtabs under Faults:



Note

Some of the subtabs may not be visible to some users.

- **Display Faults**—See [Viewing Fault Information](#), page 2-1
- **Manage Fault Settings**—See [Managing Fault Settings](#), page 2-18
- **Manage Network-Wide Settings**—See [Managing Network-Wide Settings](#), page 2-49
- **Notification Settings**—See [Notification Settings](#), page 2-51

Viewing Fault Information



Note

For an explanation of the faults, see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

The topics covered in this section are:

- [Understanding Fault and Security Policy Monitoring, page 2-2](#)
- [Displaying Faults, page 2-6](#)
- [Clearing Summary Table Faults, page 2-9](#)
- [Acknowledging Faults, page 2-10](#)
- [Viewing Fault Details, page 2-10](#)

Related Topics

- [Specifying Fault Thresholds, page 2-37.](#)
- [Specifying Security Policies, page 2-25.](#)

Understanding Fault and Security Policy Monitoring

The fault monitoring feature interrogates managed devices for specific data, compares these data against thresholds, and declares faults when the thresholds have been crossed. You can configure the WLSE to generate a notification as an SNMP trap and/or a syslog message after a fault has been declared. The data interrogated by the fault monitoring feature includes security configuration parameters (security policy monitoring) and SNMP parameters used for performance related faults.



Note

The WLSE does not receive SNMP traps and should not be considered a full featured fault management tool for wireless access points. You can use the notification feature, however, to integrate the WLSE into more advanced fault management applications (see [Setting Trap Notification, page 2-51](#)).

The following topics are included in this section:

- [How Are Faults Generated?, page 2-3](#)
- [Understanding Fault States, page 2-3](#)
- [Understanding Security Policy Monitoring Faults, page 2-4](#)
- [Understanding Threshold-Related Faults, page 2-4](#)

How Are Faults Generated?

The WLSE declares a fault condition for a managed device when an abnormal condition is detected. An abnormal condition for a managed device occurs when a system component is not configured or functioning properly, or when processed data related to system components exceed performance [thresholds](#).

Related Topics

- [Understanding Fault States, page 2-3](#)

Understanding Fault States

Faults can be in any of the following states:

- **Active**—This is a state in which at least one of the conditions contributing to the fault is broken.

For example, the CPU utilization threshold has three states: OK, Degraded and Overloaded. In this case, OK is the ‘best’ state and Overloaded and Degraded are ‘broken’ states. Similarly, a port threshold might have an Up and a Down state, where Up is the ‘best’ state and Down is the ‘broken’ state.

- **Acknowledged**—This is a state in which you have selected an Active fault from the Fault Summary, and acknowledged it. The fault is removed from the Active list, but the conditions contributing to the fault still exist.

Faults can be acknowledged from the Summary Page. See [Acknowledging Faults, page 2-10](#)

- **Cleared**—This is a state in which all the conditions contributing to the fault no longer exist or when the administrator selects a fault and clears it.

Faults generated by polling are automatically cleared based on polled data. When the fault has not been generated by polling, or when polling has been disabled, the fault can be manually cleared from the following places:

- Summary Page—See [Clearing Summary Table Faults, page 2-9](#).
- Fault Details Window—See [Viewing Fault Details, page 2-10](#).
- Thresholds and Policies—See [Viewing Current Faults, page 2-47](#)

Related Topics

- [Managing Fault Settings, page 2-18](#)
- [Understanding Fault and Security Policy Monitoring, page 2-2](#)

Understanding Security Policy Monitoring Faults

Many WLAN security vulnerabilities can be mitigated by correctly configuring the WLAN. You can use the WLSE to validate a critical set of configuration parameters and generate faults if improper configurations are detected.

The WLSE uses SNMP to periodically interrogate the configuration parameters of managed devices. If the configuration parameter is not correctly configured, a fault is generated. For example, you can use the WLSE to periodically verify that Publicly Secure Packet Forwarding (PSPF) is configured and enforced on wireless devices. If the WLSE determines that PSPF has been turned off on a wireless device, it will generate a fault for the security misconfiguration.

After you have established security policies in your network, you can use this feature to validate that the security policies are enforced on managed access points.

Related Topics

- [Specifying Security Policies, page 2-25](#)
- [Understanding Fault and Security Policy Monitoring, page 2-2](#)

Understanding Threshold-Related Faults

The WLSE compares data retrieved from managed devices against thresholds and can generate faults when the thresholds are exceeded. You can configure the priority of the fault condition and the threshold conditions for the fault (see [Specifying Fault Thresholds, page 2-37](#)).

Each WLSE fault is described by a finite state machine (FSM). A WLSE fault is described by either a two-state FSM or a three-state FSM. In each fault FSM, state transitions occur when polled and processed data exceed a configured threshold. These thresholds are defined by two parameters—a configured state transition condition and a number of polling intervals.

Two-State Finite State Machines

The RF Port Status for managed wireless bridges and/or access points is an example of a two-state fault FSM:

- The clear state for the RF port status FSM corresponds to when the RF port status is administratively and operationally up.
- The fault state for the RF port status FSM corresponds to when the RF port status is administratively up but operationally down.

Therefore, when the WLSE polls a managed wireless bridge or access point and determines that its RF port is administratively up but operationally down, and this condition has existed for the configured number of polling intervals, the WLSE will generate a fault for the device, indicating that RF port status is down. If during subsequent polling, the WLSE determines the RF port status is both administratively and operationally up for the required number of polling intervals, the WLSE will clear the RF port status down fault for the device.

Three-State Finite State Machines

The RF port utilization for managed wireless bridges and access points is an example of the three-state fault FSM. RF port utilization is measured as a percent of available bandwidth on the wireless device's RF port. For this example, we will make the following assumptions:

- The threshold for the degraded state for RF port utilization is fifty percent utilization for three polling cycles.
- The threshold for the overloaded state is eighty percent utilization for three polling cycles.
- The RF port utilization for each managed device is considered in the OK state when the utilization is below fifty percent for any two consecutive polling cycles.

Using these threshold values, the WLSE will generate faults for:

- The degraded state if the RF port utilization is between fifty and eighty percent for three consecutive polling intervals.
- The overloaded state if the RF port utilization moves above 80% for three consecutive polling intervals.

In both cases, if subsequent polling indicates the RF port utilization has moved below fifty percent for two consecutive polling cycles, the fault condition will clear.

Related Topics

- [Understanding Fault and Security Policy Monitoring, page 2-2](#)

Displaying Faults

**Note**

For an explanation of the faults, see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

This window displays device fault information.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults > Display Faults**. The Fault window appears.

Step 2 Use the Filter: bar to display the faults you want to view:

Table 2-1 *Display Faults Filter Bar*

Field	Description
Devices	From the list, select the device type whose fault summary you want to display.

Table 2-1 Display Faults Filter Bar (continued)

Field	Description
Severity	<p>From the list, select the severity from P1, which is the highest severity level to P5, which is the lowest severity level, to display:</p> <ul style="list-style-type: none"> • P1—Severity P1 faults. • P1-P2—Severity P1 and P2 faults. • P1-P3—Severity P1 through P3 faults. • P1-P4—Severity P1 through P4 faults. • P1-P5—Severity P1 through P5 faults. • All—Severity P1 through P5 faults, and faults that have been cleared.
State	<p>From the list, select a state to display.</p> <p>See Understanding Fault States, page 2-3 for a description of each state.</p>
Name/IP	<p>Enter a complete or partial device name or IP address.</p>
Refresh (Sec)	<p>Enter the number of seconds (30 seconds or higher) to indicate how often you want the screen to refresh.</p> <p>The default is 60 seconds. You cannot enter a value under 30 seconds.</p>

Step 3 Click **Apply**. The following table appears:



Note If no data is displayed in the table, there are no faults for your filtering selection to report.

Table 2-2 Display Faults Table

Column	Description
IP Address	The device IP address. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 6-2 .
Hostname	The device for which the fault is reported. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 6-2 .
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 2-10 . Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-8 . Click to see fault details. See Viewing Fault Details, page 2-10 .

- To sort table data, click on the column heading you want to use to sort the data:
 - A triangle indicates ascending order.
 - An upside-down triangle indicates descending order.
 - No triangle indicates that the data is not sorted.
-

Clearing Summary Table Faults

There are two ways in which you can clear faults:

- Select **Faults > Display Faults**. The Summary Table appears with the faults that meet the filtering criteria you selected.
 - To clear an individual fault, select it, then click **Clear**.
 - To clear more than one fault, select them, then click **Clear**.
 - To clear all the faults, click **Select All**, then click **Clear**.
- Click the Description or Timestamp fields in the Summary Table for a particular fault, and the Fault Details page appears. Click the Clear button in the Conditions table.



Note

It may be a few seconds before the faults clear.

Related Topics

- [Viewing Fault Details, page 2-10](#)
- [Understanding Fault States, page 2-3](#)

Acknowledging Faults

When you select **Faults > Display Faults** the Summary Table appears with the faults that meet the filtering criteria you selected.

- To acknowledge an individual fault, select it, then click **Acknowledge**.
- To acknowledge more than one fault, select them, then click **Acknowledge**.
- To acknowledge all the faults, click **Select All**, then click **Acknowledge**.

Related Topics

[Understanding Fault States, page 2-3](#)

Viewing Fault Details

There are two types of fault detail windows:

- [Device Fault Details, page 2-10](#)—Displays details about the device, its fault conditions and history.
- [Rogue Access Point Details, page 2-14](#)—Displays details about the unknown access point, beacon and location information, switch port tracing, reporting access points, and fault history.



Note

For an explanation of the faults, see the Fault Description Table in the *FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5* on Cisco.com.

Device Fault Details

When you click the link in the Description or Timestamp fields in the Fault Summary Table for an device, the following tables are displayed in the Fault Details window:

- [Fault details for](#)
- [Conditions](#)
- [Fault History](#)

**Note**

You can clear one or more faults from the Conditions table by selecting them, then clicking **Clear**. It may be a few seconds before the faults clear.

Fault details for**Table 2-3** *Fault Details Table*

Column	Description
IP	The device IP address.
Name	The device hostname.
Family	The device family.
Product	The product name.
Type	<p>The device or the device sub-entity (which could include a logical entity, such as software or a service) in which the fault is found.</p> <p>Note If the Type is a sub-entity, additional columns appear with keys and values to help identify the precise sub-entity. These additional keys and values are MIB variables.</p>
ifIndex	<p>A unique number that identifies the interface.</p> <p>Note This value only displays when you are viewing fault details for ports.</p>

Conditions

Table 2-4 Conditions Table

Column	Description
Name	The fault condition.
State	The state of the device. See Understanding Fault States for a description of the states.
Severity	The fault severity level.
Description	A description of the fault. Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-8 .
Clear	Click Clear , then refresh your browser window to view the updated fault display. Note It may be a few seconds before the fault clears.

Fault History

Table 2-5 *Fault History Table*

Column	Description
State	The state of the device. See Understanding Fault States for a description of the states.
Severity	The fault severity level.
Description	A description of the fault. Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
Change	A description of the state change.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display , page 1-8.
By	Displays the username of the person who changed the fault state. If the fault state has not been cleared or acknowledged, nothing is displayed in this column.

Rogue Access Point Details

When you click the link in the Description or Timestamp fields in the Fault Summary Table for an unknown access point, the following tables are displayed in the Rogue Access Point Details window:

- [Rogue Access Point Details](#)
- [Beacon Information](#)
- [Location Estimation](#)
- [Switch Port Tracing](#)
- [Reporting APs](#)
- [Fault History](#)

Rogue Access Point Details

A rogue access point is an AP that has not been identified as Friendly. By default, all unknown radios are classified as Rogue until you change them to Friendly.

A Friendly access point is an AP that you know exists, for example, a neighboring network's AP, but that you are not going to modify in any way.

Table 2-6 *Rogue Access Point Details Table*

Column	Description
BSSID	Basic Service Set (BSS) identifier.
State	The state of the device.
Vendor	The name of the vendor that manufactured this AP.
Change To Friendly AP	Click Change To Friendly AP , then refresh your browser window to view the updated fault display. Note It may be a few seconds before the classification is changed.
Delete	Click Delete , then refresh your browser window to view the updated fault display. Note It may be a few seconds before the rogue AP is deleted.

Beacon Information**Table 2-7 Beacon Information Table**

Column	Description
SSID	Service set identifier used by client devices to associate with an access point.
Beacon Interval	The beacon interval on which the rogue AP is transmitting.
Channel	The channel on which the rogue AP is transmitting.
Data Rates	The data rates on which the rogue AP is transmitting.

Location Estimation**Table 2-8 Location Estimation Table**

Column	Description
Location	The estimated location of the rogue AP.
Timestamp	Indicates the time, based on the client browser, the rogue was detected. See Time Display, page 1-8 .
View in Location Manager	Click View in Location Manager to display a graphical view of the approximate location of the rogue AP. For more information about how the Location Manager locates an unknown radio, see Finding Unknown Radios, page 7-52 .

Switch Port Tracing

Table 2-9 Switch Port Tracing Table

Column	Description
Switch IP	The IP address of the switch to which the rogue AP is connected.
Switch Port	The port of the switch to which the rogue AP is connected.
Traced MAC Address	The MAC address of the rogue AP.
Timestamp	Indicates the time, based on the client browser, the rogue AP switch port was detected. See Time Display, page 1-8 .
Re-Trace	Click Re-Trace to locate the switch port again. This is useful if the rogue AP was moved and connected to a different port.

Reporting APs

Table 2-10 Reporting APs Table

Column	Description
Reporting AP IP Address	The IP address of the AP that has located the rogue AP.
Reporting AP BSSID	The basic service set (BSS) identifier that contains the AP that has located the rogue AP.
RSSI	Received signal strength indicator of the reporting AP. This value is used to estimate the location of the rogue AP relative to the reporting AP.
Reporting AP Location	The physical location of the AP that has located the rogue AP.

Fault History

The following table contains a history of the faults raised against this rogue AP.

Table 2-11 *Fault History Table*

Column	Description
State	The state of the device. See Understanding Fault States for a description of the states.
Severity	The fault severity level.
Description	A description of the fault. Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
Change	A description of the state change.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-8 .
By	Displays the username of the person who changed the fault state. If the fault state has not been cleared or acknowledged, nothing is displayed in this column.

Managing Fault Settings

Every device managed by the WLSE has a fault setting (also called a fault policy profile) assigned to it. Fault settings include threshold values and security policies.

If you have not assigned a specific setting to a device, it uses the system Default setting. Default settings can be edited, but cannot be deleted.

The topics covered in this section are:

- [Understanding Fault Settings, page 2-18](#)
- [Creating a Setting, page 2-19](#)
- [Copying a Setting, page 2-20](#)
- [Renaming a Setting, page 2-21](#)
- [Editing a Setting, page 2-22](#)
- [Deleting a Setting, page 2-22](#)
- [Viewing a Summary, page 2-23](#)
- [Assigning a Setting to a Device, page 2-23](#)

Understanding Fault Settings

A fault policy profile (or fault setting) is a set of security policy settings and fault thresholds that is assigned to one or more managed devices. Multiple profiles can be created for devices, but a managed device can only be assigned one profile at a time. If a device is not explicitly assigned a profile, it will be assigned the default profile.

Fault policy profiles allows you to engineer security policies and fault polling to the needs of their network(s). You can create a profile to customize:

- Thresholds and security configurations that generate fault events
- Fault priority
- Polling interval frequency

For example, Site A is connected via high-speed LAN connections, and remote Sites B and C are connected via slow WAN links. It might be appropriate to configure a fault policy profile for each site, where many of the parameters are checked more frequently for Site A than for Sites B and C.

Here is another example. Suppose access points in Site A with IP addresses 10.1.5.5 and 10.1.5.6 are intended to provide public network access, but the other Site A access points are for private use. In this case, there are different security misconfiguration policies appropriate for the public access points than for the private access points. This means that the fault policy profile for the public access points will check for different SSIDs than the profile for the private access points:

- The public profile may check that PSPF is enforced on the access points, which is usually not appropriate for private networks where all clients are trusted.
- The private profile may confirm that EAP is enforced on the private access points, but the public profile will probably not check for EAP enforcement.

Related Topics

- [Specifying Security Policies, page 2-25](#)
- [Specifying Fault Thresholds, page 2-37](#)

Creating a Setting

Use this option to create a setting.



Note

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
 - Step 2** Enter a unique name. See [Naming Guidelines, page A-1](#) for details.
 - Step 3** Click **Create New**. The new name appears in the Existing Fault Settings list and the The Editing Profile window appears. See [Editing a Setting, page 2-22](#).



Note The new setting is a copy of the Default setting.

Related Topics

[Understanding Fault Settings, page 2-18](#)

Copying a Setting

Use this option to copy an existing setting to use as a base for a new setting.



Note Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
 - Step 2** Select the setting you want to copy from the Existing Fault Settings box, then click **Create Copy**. A dialog box appears asking you to enter a name for the copy.
 - Step 3** Enter a unique name. See [Naming Guidelines, page A-1](#) for details.
 - Step 4** Click **OK**. The new name appears in the Existing Fault Settings list.
 - Step 5** Select the name, then click **Edit**. The Editing Profile window appears. See [Editing a Setting, page 2-22](#).
-

Related Topics

[Understanding Fault Settings, page 2-18](#)

Renaming a Setting

Use this option to rename a setting.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
 - Step 2** Select the profile you want to rename from the Existing Fault Settings box, then click **Rename**. A dialog box appears asking you to enter a new name.
 - Step 3** Enter a unique name. See [Naming Guidelines, page A-1](#) for details.
 - Step 4** Click **OK**. The new name appears in the Existing Fault Settings list.
-

Related Topics

[Understanding Fault Settings, page 2-18](#)

Editing a Setting

Use this option to edit a setting.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the setting you want to edit from the Existing Fault Settings box, then click **Edit**. The Editing Settings window appears.
- Step 3** Select the policies and thresholds in the left pane that you want to assign to the setting. For a description, see [Setting Security Policies and Thresholds, page 2-24](#).
-

Related Topics

[Understanding Fault Settings, page 2-18](#)

Deleting a Setting

Use this option to delete a setting.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the profile you want to delete from the Existing Fault Settings box, then click **Delete**. A window appears asking if you want to delete the setting.



Note Any devices that were assigned the deleted setting will be automatically assigned the Default setting.

Step 3 Click **OK** to delete it.

Viewing a Summary

Use this option to view a summary of the current selections for a particular fault setting.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**. The Fault Settings dialog box appears.
- Step 2** Select the setting you want to view from the Existing Fault Settings box, then click **View Summary**. A window displays the current fault settings.
- Step 3** Click **OK** to close the window.
-

Assigning a Setting to a Device

Use this option to assign a setting to a single device or a group of devices. Devices can only have one setting assigned to them at a time.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Faults > Manage Fault Settings**
- Step 2** Assign a setting to devices either of the following ways:
- From the Editing Settings window, click **Assign Devices**.
 - From the Fault Settings window, select a setting from the **Existing Fault Settings** list, then click **Assign Devices**.
- Step 3** If you want to search for devices, use the dialog box in the left pane above the device selector. For information on how to search or use the device selector, see [Using the Device Selector and Search, page 1-9](#).
- Step 4** If you know which device you want, use the device selector to select the devices. They are added to the list of Available Devices.
- Step 5** From the list of Available Devices, select the device to which you want to apply the profile and click >>. The devices are moved to the Selected Devices list.
- Step 6** Click **Continue**. A confirmation dialog box appears for the device assignment.
- Step 7** Click **OK** to accept the device assignment or **Cancel** to cancel the device assignment.
-

Related Topics

[Understanding Fault Settings, page 2-18](#)

Setting Security Policies and Thresholds

When you create or edit a setting, you can also assign security policy settings and fault thresholds. The following choices appear in the left pane of the Editing Settings window:

- Security Policies—See [Specifying Security Policies, page 2-25](#)
- Thresholds—See [Specifying Fault Thresholds, page 2-37](#)

Specifying Security Policies

This option allows you to activate or deactivate a set of predefined policies for access points. The policies you set in this window will determine how some of the faults are displayed in the **Faults > Display Faults** subtab.

**Note**

Security Policies are disabled by default unless otherwise noted.

You can also view the current faults for each setting. See [Viewing Current Faults, page 2-47](#).

**Note**

Your login determines whether you can use this option.

Procedure

Step 1

In the left pane, select the policy you want to apply to the setting:

- SSID—See [Setting the SSID Policy, page 2-26](#).
- Firmware Version (IOS)—See [Setting the Firmware Version Policy, page 2-27](#).
- Firmware Version (Non-IOS)—See [Setting the Firmware Version Policy, page 2-27](#).
- Broadcast SSID Disabled—See [Setting the Broadcast SSID Disabled Policy, page 2-28](#).
- Key Rotation per VLAN—See [Setting Key Rotation Disabled per VLAN Policy, page 2-28](#).
- WEP Encryption per VLAN—See [Setting WEP Encryption per VLAN Policy, page 2-29](#).
- WEP Enforced—See [Setting the WEP Enforced Policy, page 2-30](#).
- EAP Enforced—See [Setting the EAP Enforced Policy, page 2-31](#).
- EAP Per SSID Enforced—See [Setting EAP Per SSID Enforced Policy, page 2-32](#).
- WEP Key Length—See [Setting WEP Key Length Policy, page 2-33](#).
- HotStandBy Status—See [Setting the HotStandBy Status Policy, page 2-33](#).

- HTTP Disabled (Non-IOS)—See [Setting the HTTP Disabled \(Non-IOS\) Policy, page 2-34](#).
- Telnet Disabled (Non-IOS)—See [Setting the Telnet Disabled \(Non-IOS\) Policy, page 2-35](#).
- PSPF Enabled (Non-IOS)—See [Setting the PSPF Enabled \(Non-IOS\) Policy, page 2-35](#).
- User Manager Enforced (Non-IOS)—See [Setting the User Manager Enforced \(Non-IOS\) Policy, page 2-36](#).
- HTTP Authentication (Non-IOS)—See [Setting the HTTP Authentication \(Non-IOS\) Policy, page 2-37](#).

Related Topics

[Understanding Security Policy Monitoring Faults, page 2-4](#)

Setting the SSID Policy

Procedure

Step 1 To activate the policy, do the following:

Field	Description
Verify	Select if you want to verify that SSID is enabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Enter SSID	Enter the unique identifier used by client devices to associate with the access point. Any alphanumeric character up to 32 characters long. This is for the primary SSID.

Step 2 Click **Add** to add the SSID to the list.

Step 3 To remove an SSID from the list, select it, click **Remove**.

- Step 4** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 5** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 6** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the Firmware Version Policy

Procedure

- Step 1** To activate the policy, do the following:

Field	Description
Verify	Select if you want to verify that firmware version is enabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Firmware Version	Enter the firmware version.

- Step 2** Click **Add** to add the firmware version to the list.
- Step 3** To remove a firmware version from the list, select it, click **Remove**.
- Step 4** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 5** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 6** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the Broadcast SSID Disabled Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting Key Rotation Disabled per VLAN Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select if you want to verify that key rotation is disabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Field	Description
Available Vlans	Lists all the VLAN ID numbers that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting WEP Encryption per VLAN Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select if you want to verify that key rotation is disabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
WEP Key Length	Select to indicate the bit length.

Field	Description
Available Vlans	Lists all the VLAN ID number that are available. To apply the policy to one of the available VLANs, select it, then click >> to move it to the Selected VLANs list.
Selected Vlans	Lists the VLAN identification numbers to which this policy is applied. To remove a VLAN ID from the list, select it, then click << to move it to the Available VLANs list.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the WEP Enforced Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify Broadcast SSID is disabled
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the EAP Enforced Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting EAP Per SSID Enforced Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select if you want to verify that key rotation is disabled.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
Available SSID	Lists the SSIDs that are available. To move an SSID to the Selected SSID list, select it, then click >>.
Selected SSID	Lists the SSIDs to which this policy is applied. To remove an SSID from the Selected list, select it, then click <<.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting WEP Key Length Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select if you want to verify the WEP key length.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
WEP Key Length	Select to indicate the bit length.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the HotStandBy Status Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the HTTP Disabled (Non-IOS) Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the Telnet Disabled (Non-IOS) Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Setting the PSPF Enabled (Non-IOS) Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the User Manager Enforced (Non-IOS) Policy

Procedure

- Step 1** Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting the HTTP Authentication (Non-IOS) Policy

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to verify.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-47](#) for details.

Specifying Fault Thresholds

This option allows you to set polling and [exception](#) threshold values collected from the devices you are monitoring.

The threshold values you set in this window will determine how the faults are displayed in the **Faults > Display Faults** subtab.

You can also view the current faults for each of these thresholds. See [Viewing Current Faults, page 2-47](#).



Note

Your login determines whether you can use this option.

Threshold choices include the following options:

- **Access Point**—See [Setting Access Point Fault Thresholds](#), page 2-38.
- **Switch**—See [Setting Switch Fault Thresholds](#), page 2-41.
- **Router**—See [Setting Router Fault Thresholds](#), page 2-43.
- **LEAP**—See [Setting Server Response Time](#), page 2-44.
- **PEAP**—See [Setting Server Response Time](#), page 2-44.
- **RADIUS**—See [Setting Server Response Time](#), page 2-44.
- **EAP-MD5**—See [Setting Server Response Time](#), page 2-44.
- **WLSE**—See [Setting WLSE Dot11 MIB View](#), page 2-46.
- **WDS**—See [Setting WDS Thresholds](#), page 2-46.

Related Topics

[Understanding Threshold-Related Faults](#), page 2-4

Setting Access Point Fault Thresholds

Using this option, you can set up thresholds for access point faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.



Note

The following thresholds are enabled by default: SNMP Reachable, RF Port Status and Ethernet Port Status.

- See [Setting Up or Down Status](#), page 2-39 to set the fault thresholds for the following access point faults:
 - SNMP Reachable
 - RF Port Status
 - Ethernet Port Status
 - Registration Error

- See [Setting Overloaded, Degraded, and OK Status, page 2-40](#) to set the fault thresholds for the following access point faults:
 - RF Port Utilization
 - RF Port Packet Errors
 - RF Port WEP Errors
 - Ethernet Port Utilization
 - Ethernet Port Packet Errors
 - Max Retry Count
 - Associated Clients
 - Association Rate
 - Authentication Error Rate

Setting Up or Down Status

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Overloaded, Degraded, and OK Status

Procedure

- Step 1** Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.
-

Setting Switch Fault Thresholds

Using this option, you can set up thresholds for switch faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.



Note

The following thresholds are enabled by default: SNMP Reachable and Port Status.

- See [Setting Up or Down Status, page 2-42](#) to set the fault thresholds for the following switch faults:
 - SNMP Reachable
 - Port Status
 - Module Status
- See [Setting Overloaded, Degraded, and OK Status, page 2-43](#) to set the fault thresholds for the following:
 - CPU Utilization
 - Memory Utilization
 - Port Utilization

Setting Up or Down Status

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Overloaded, Degraded, and OK Status

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Router Fault Thresholds

Using this option, you can set up the router's SNMP reachable threshold. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting Server Response Time

Using this option, you can set up a threshold for LEAP, PEAP, RADIUS, and EAP-MD5 server response time. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.



Note This threshold is enabled by default.

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Settings	
Unavailable	From the list, select the severity level and the number of polling cycles before the status is Unavailable.
Authentication Failure	From the list, select the severity level and the number of polling cycles before the status indicates an Authentication Failure.
Overloaded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the response time, and the number of polling cycles before the status is OK.

- Step 2** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
- Step 3** Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).
- Step 4** Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting WLSE Dot11 MIB View

Using this option, you can set up a threshold for the dot11 MIB view. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.



Note

This threshold is enabled by default.

For information on the dot11 MIB view fault, see [Faults FAQs, page 10-12](#).

Procedure

Step 1 Complete the following:

Field	Description
Verify	Select to enable a threshold for this component.
Poll Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this threshold.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Setting WDS Thresholds

Using this option, you can set the following thresholds for the access point providing wireless domain services (WDS) on the wireless LAN:

- Authentication Failures
- WLSE-WDS Link Status

When a threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

**Note**

These thresholds are enabled by default.

You can set the following WDS thresholds:

- Authentication Failures
- WLSE-WDS Link Status

Procedure

Step 1 Complete the following:

Field	Description
Enable	Select to enable a threshold for this component.
Settings	
Down	From the list, select the severity level before the status is Down.
Up	The fault is cleared and the status is Up.

Step 2 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Step 3 Click **Assign Devices** to assign this setting to a device or group of devices. For information on assigning devices, see [Assigning a Setting to a Device, page 2-23](#).

Step 4 Click **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-47](#) for details.

Viewing Current Faults

When you click the link at the bottom of any policy or threshold, a window appears that allows you to view all the faults associated with it.

Using this window, you can view the faults and clear them.

Procedure

- Step 1** To view the faults associated with each threshold or policy, click the **View current faults for this setting** link at the bottom of the screen.

The following table appears:

Field	Description
IP Address	The device IP address. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 6-2 .
Hostname	The device for which the fault is reported. Click to see various reports about the device. For information on the reports, see Using the Device Center, page 6-2 .
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 2-10 . Note For an explanation of the faults, see the Fault Description Table in the <i>FAQ and Troubleshooting Guide for the Wireless LAN Solution Engine, Release 2.5</i> on Cisco.com.
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-8 . Click to see fault details. See Viewing Fault Details, page 2-10 .

- To clear an individual fault, select it, then click **Clear**.
- To clear more than one fault, select them, then click **Clear**.
- To clear all the faults, click **Select All**, then click **Clear**.



Note It may be a few seconds before the faults clear.

Managing Network-Wide Settings

Using this option, you can set the following network-wide policies:

- Rogue AP Detection—See [Setting Rogue AP Detection, page 2-49](#)
- Interference Detection—See [Setting Interference Detection, page 2-50](#)

Setting Rogue AP Detection

Use this option to enable rogue access point detection and to assign a severity level to the fault. When this condition is met, a fault is generated and can be viewed under **Faults > Display Faults**.

Procedure

- Step 1** Select **Faults > Manage Network-Wide Settings > Rogue AP Detection**.
- Step 2** Complete the following:

Field	Description
Enable	Select to enable the setting.
Setting	From the list, select the severity level to assign the fault when a rogue access point is detected.

- Step 3** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
-

Setting Interference Detection

Use this option to set the threshold condition for interference detection. When the condition is met, a fault is generated and can be viewed under **Faults > Display Faults**.

Procedure

- Step 1** Select **Faults > Manage Network-Wide Settings > Interference Detection**.
- Step 2** Complete the following:

Field	Description
Enable	Select to enable the setting.
Settings	
Degraded	From the list, select the severity level, the interference level, the percentage, and the time interval before the status is Degraded.
OK	From the list, select the interference level, the percentage and the time interval before the status is OK.

- Step 3** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
-

Notification Settings

When a fault is detected, the WLSE can send automated notifications in the form of SNMP traps, syslog messages, and email alerts. You can specify multiple recipients for each notification type, and choose to deliver the message using either a plain text or XML format.

This section has the following options:

- [Setting Trap Notification](#)
- [Setting Syslog Notification](#)
- [Emailing Faults](#)

**Note**

Your login determines whether you can use this option.

Related Topics

- [Viewing Fault Information, page 2-1](#)
- [Specifying Fault Thresholds, page 2-37](#)

Setting Trap Notification

This option allows you to enable the WSLE to send north-bound exception notification to one or more SNMP trap receivers. The exception notification contains information such as device name and IP, fault number, timestamp, exception severity, and a message describing the problem.

**Note**

The WLSE supports only SNMP v2c traps. Solaris 2.8-based NetView 7.1 receives and displays the SNMP v2c fault notification traps from WLSE. Windows-based NetView 7.1 supports only v1 traps and cannot receive and display any v2c traps from the WLSE.

The following MIB defines the trap and the varbinds:
CISCO-DEVICE-EXCEPTION-REPORTING-MIB.my. It can be downloaded from the Cisco.com download site and loaded into the trap receiver.

Before You Begin

Make sure your SNMP trap receiver's trap receiving daemon is set to the correct port. The default port is set to 162.

Procedure

- Step 1** Select **Faults > Notification Settings**. The Fault Notification Settings dialog box appears.
- Step 2** Select the message format for the notification: Plain Text or XML. See [Trap Notification Message Format, page 2-53](#) for an example.
- Step 3** Complete the following:

Field	Description
Trap	Select to enable trap notification.
Host	Enter the hostname/IP of the SNMP trap receiver to which you want to send SNMP trap notification.
Port	Enter the port number if different from the default of 162.
Community	Enter the community string.

- Step 4** If you want a different host to receive trap notification, click **Add Row**. There is no limit to the number you can enter.
- To a row, click **Delete**, next to the row you want to remove.
- Step 5** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Trap Notification Message Format

You have the option of sending the trap notification as plain text or in an XML format.

- An example of a trap notification message using plain text will appear as follows:

```
Mon Jun 02 18:17:56 2003 192.168.98.44 A tcpConnectionClose trap
received from enterprise cisco with 7 arguments: tslineSesType=48;
tcpConnState=1; loctcpConnElapsed=10.10.10.31;
loctcpConnInBytes=OK; loctcpConnOutBytes=8583602;
cderExcepData = FaultId 48
DeviceId 1784
DeviceIP 10.10.10.31
DeviceName 10.10.10.31
MO RF Port awc0
Change Cleared by user admin
ChangeSeverity OK
StateChange SSID is OK
AlarmState Cleared
OverallSeverity OK
```

- An example of a trap notification message using XML will appear as follows:

```
cderExcepTableIndex = 48
cderExcepId = 1
cderExcepHostAddressType = 1
cderExcepHostAddress = 10.10.10.31
cderExcepPriorityDescription = OK
cderExcepTime = Jun 02 17:47:48 2003
cderExcepData =
<Msg><FaultId>48</FaultId><DeviceId>1784</DeviceId><DeviceIP>10.
10.10.31</DeviceIP><DeviceName>10.10.10.31</DeviceName><MO>RF
Port awc0</MO><Change>Cleared by user
admin</Change><ChangeSeverity>OK</ChangeSeverity><StateChange>SS
ID is
OK</StateChange><AlarmState>Cleared</AlarmState><OverallSeverity
>OK</OverallSeverity></Msg>
cderExcepReportedBy = FaultNotifier@samuraiwhat.cisco.com
```

Setting Syslog Notification

This option allows you to send syslog messages to selected syslog servers. The messages contain information such as device name and IP, fault number, date and time, exception severity, and a message about what is wrong.

Before You Begin

Make sure your syslog server is turned on to be able to receive messages from the Wireless LAN Solution Engine. Also make sure that the receiving process is configured to receive messages from remote hosts (for example, start syslogd with -r option on some UNIX versions).

Procedure

-
- Step 1** Select **Faults > Notification Settings**. The Fault Notification Settings dialog box appears.
- Step 2** Select the message format for the notification: Plain Text or XML. See [Syslog Notification Message Format, page 2-55](#) for an example.
- Step 3** Complete the following:

Field	Description
Syslog	Select to send syslog messages to designated syslog servers.
Enter Syslog host names	Enter the hostname/IP for the syslog servers. Names must be separated by a space, a comma, a semicolon, or a new line.

- Step 4** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.
-

Syslog Notification Message Format

You have the option of sending the fault notification as plain text or in an XML format.

- An example of a syslog fault notification message using plain text will appear as follows:

```
<189> Jun 03 01:26:59 samuraiwhat FaultNotifier:%FLT-6-MSG:FaultId
48\nDeviceId 1784\nDeviceIP 10.10.10.31\nDeviceName
10.10.10.31\nMO RF Port awc0\nChange Cleared by user
admin\nChangeSeverity OK\nStateChange SSID is OK\nAlarmState
Cleared\nOverallSeverity OK
```

- An example of a syslog fault notification message using XML will appear as follows:

```
<189> Jun 03 00:57:15 samuraiwhat
FaultNotifier:%FLT-6-MSG:<Msg><FaultId>48</FaultId><DeviceId>1784<
/DeviceId><DeviceIP>10.10.10.31</DeviceIP><DeviceName>10.10.10.31<
/DeviceName><MO>RF Port awc0</MO><Change>Cleared by user
admin</Change><ChangeSeverity>OK</ChangeSeverity><StateChange>SSID
is
OK</StateChange><AlarmState>Cleared</AlarmState><OverallSeverity>O
K</OverallSeverity></Msg>
```

Emailing Faults

E-mail recipients can be configured to receive fault notifications based on fault priority.

Before You Begin

Configure the mailroute so that the WLSE knows where to send the e-mails. Enter the mail server hostname or IP address by selecting **Administration > Appliance > Configure Mailroute**.

Procedure

-
- Step 1** Select **Faults > Notification Settings**. The Fault Notification Settings dialog box appears.
- Step 2** Select the message format for the notification: Plain Text or XML. See [Email Notification Message Format, page 2-56](#).

Step 3 Complete the following:

Field	Description
Email	Select to enable email notification of exception information.
Enter email addresses	Enter the email addresses of users you want to receive exception notification. Addresses must be separated by a space, a comma, a semicolon, or a new line.
Priority	From the list, select the priority of the exceptions you want to email.



Tip If email notification is not working, you might need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

Step 4 If you want a different group of users to receive different priority level exceptions, click **Add Row** to add another set of email addresses. There is no limit to the number of email addresses you can enter.

To delete a row, click **Delete**, next to the row you want to remove.

Step 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Email Notification Message Format

The emailed exception notification contains the following information:

Attribute	Description
FaultId	A unique identifier for the fault.
DeviceId	A unique identifier used by the WLSE for the device with the fault.

Attribute	Description
DeviceIp	The IP address of the device with the fault.
DeviceName	The name of the device with the fault.
MOId	The identifier used by the WLSE for the subcomponent of the device with the fault.
AlarmState	The state of the Alarm (Active or Cleared).
Description	A description of the last updated to the fault.
Severity	The severity of the fault.
	Note OK indicates a cleared (fixed) fault.

You have the option of sending the fault notification as plain text or in an XML format.

- An example of an email notification message using plain text will appear as follows:

```
Subject:10.10.10.31[10.10.10.31] OK notification. FaultId 48. RF
Port awc0 SSID is OK. Cleared by user admin
From:FaultNotifier@samuraiwhat.cisco.com
Date:Tue, 3 Jun 2003 01:26:59 GMT
To:user@cisco.com
FaultId 48
DeviceId 1784
DeviceIP 10.10.10.31
DeviceName 10.10.10.31
MO RF Port awc0
Change Cleared by user admin
ChangeSeverity OK
StateChange SSID is OK
AlarmState Cleared
OverallSeverity OK
```

- An example of an email notification message using XML will appear as follows:

```
Subject:10.10.10.31[10.10.10.31] P1 notification. FaultId 48. RF
Port awc0 SSID is ViolatingPolicy. SSID policy violation tracyp
From:FaultNotifier@samuraiwhat.cisco.com
Date:Tue, 3 Jun 2003 00:57:55 GMT
To:user@cisco.com
<Msg><FaultId>48</FaultId><DeviceId>1784</DeviceId><DeviceIP>10.10
.10.31</DeviceIP><DeviceName>10.10.10.31</DeviceName><MO>RF Port
awc0</MO><Change>Cleared by user
admin</Change><ChangeSeverity>OK</ChangeSeverity><StateChange>SSID
is
OK</StateChange><AlarmState>Cleared</AlarmState><OverallSeverity>O
K</OverallSeverity></Msg>
```