



## 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 [Displaying Faults, page 2-1](#)
- **Manage Profiles**—See [Managing Profiles, page 2-10](#)
- **Notification Settings**—See [Notification Settings, page 2-37](#)

## Displaying Faults

This window displays device fault information. A fault is an abnormal condition that occurs when a system component exceeds a performance [threshold](#) or is not functioning properly. See [Specifying Fault Thresholds, page 2-27](#) to set threshold levels.

A fault can also occur when a system policy is violated. See [Notification Settings, page 2-37](#) to set policies.

Displayed fault information is retained by default for 30 days. To change the default, see [Managing System Parameters, page 6-107](#).

Using this option you can view faults. You can also:

- Clear Faults—See [Clearing Summary Table Faults, page 2-5](#)
- Acknowledge the Faults—See [Acknowledging Faults, page 2-5](#)


**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.
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"> <li>• P1—Severity P1 faults.</li> <li>• P1-P2—Severity P1 and P2 faults.</li> <li>• P1-P3—Severity P1 through P3 faults.</li> <li>• P1-P4—Severity P1 through P4 faults.</li> <li>• P1-P5—Severity P1 through P5 faults.</li> <li>• All—Severity P1 through P5 faults, and faults that have been cleared.</li> </ul>

**Table 2-1** *Display Faults Filter Bar (continued)*

Field	Description
State	From the list, select a state to display. See <a href="#">Understanding Fault States, page 2-6</a> for a description of each state.
Name/IP	Enter a complete or partial device name or IP address.

**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 <a href="#">Using the Device Center, page 5-2</a> .
Hostname	The device for which the fault is reported. Click to see various reports about the device. For information on the reports, see <a href="#">Using the Device Center, page 5-2</a> .
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.

**Table 2-2** *Display Faults Table (continued)*

Column	Description
Description	<p>A description of the fault.</p> <p>Click to see fault details. See <a href="#">Viewing Fault Details, page 2-7</a>.</p> <p>For information on specific faults, see <a href="#">FAQs, page 7-10</a>.</p>
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	<p>Indicates the time, based on the client browser, that the state of the device last changed. See <a href="#">Time Display, page 1-6</a>.</p> <p>Click to see fault details. See <a href="#">Viewing Fault Details, page 2-7</a>.</p>

- 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

When you 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**.



---

**Note**

It may be a few seconds before the faults clear.

---

### Related Topics

[Understanding Fault States, page 2-6](#)

## 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 2-6](#)

## 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 2-5](#)

- **Cleared**—This is a state in which all the conditions contributing to the fault are in their best state.

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 2-5](#).
- Fault Details Window—See [Viewing Fault Details, page 2-7](#).
- Thresholds and Policies—See [Viewing Current Faults, page 2-35](#)

---

### Related Topics

- [Managing Profiles, page 2-10](#)
- [Notification Settings, page 2-37](#)

## Viewing Fault Details

When you click the link in the Description or Timestamp fields in the Fault Summary Table, 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.

**Table 2-3** *Fault Details Table (continued)*

Column	Description
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><b>Note</b> 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><b>Note</b> 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	<p>The state of the device.</p> <p>See <a href="#">Understanding Fault States</a> for a description of the states.</p>
Severity	The fault severity level.
Description	<p>A description of the fault.</p> <p>For information on specific faults, see <a href="#">FAQs, page 7-10</a>.</p>

Table 2-4 Conditions Table (continued)

Column	Description
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed.  See <a href="#">Time Display, page 1-6</a> .
Clear	Click <b>Clear</b> , then refresh your browser window to view the updated fault display.  <b>Note</b> 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 <a href="#">Understanding Fault States</a> for a description of the states.
Severity	The fault severity level.
Description	A description of the fault.  For information on specific faults, see <a href="#">FAQs, page 7-10</a> .
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 <a href="#">Time Display, page 1-6</a> .
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 Profiles

Every device managed by the WLSE has a profile assigned to it. A profile is made up of threshold values and policy settings.

If you have not assigned a specific profile to a device it has the system Default profile. The default profile can be edited, but it cannot be deleted.

The topics covered in this section are:

- [Creating a Profile, page 2-11](#)
- [Copying a Profile, page 2-11](#)
- [Renaming a Profile, page 2-12](#)
- [Editing a Profile, page 2-12](#)
- [Deleting a Profile, page 2-13](#)
- [Assigning a Profile to a Device, page 2-14](#)
- [Viewing Devices, page 2-15](#)

## Creating a Profile

Use this option to create a profile.



Note

---

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1 Select **Faults > Manage Profiles**. The Profiles 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 Profiles list.



Note

---

The new profile is a copy of the Default profile.

---

- Step 4 Select the name, then click **Edit**. The Editing Profile window appears. See [Editing a Profile, page 2-12](#).
- 

## Copying a Profile

Use this option to copy a profile that you can use as a base for another profile.



Note

---

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1 Select **Faults > Manage Profiles**. The Profiles dialog box appears.
- Step 2 Select the profile you want to copy from the Existing Profiles 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 Profiles list.
- Step 5 Select the name, then click **Edit**. The Editing Profile window appears. See [Editing a Profile, page 2-12](#).
- 

## Renaming a Profile

Use this option to rename a profile.



Note

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1 Select **Faults > Manage Profiles**. The Profiles dialog box appears.
- Step 2 Select the profile you want to rename from the Existing Profiles 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 Profiles list.
- 

## Editing a Profile

Use this option to edit a profile.



Note

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1 Select **Faults > Manage Profiles**. The Profiles dialog box appears.
  - Step 2 Select the policy you want to edit from the Existing Policies box, then click **Edit**. The Editing Profile window appears.
  - Step 3 Select the policies and thresholds in the left pane that you want to assign to the profile. For a description, see [Profile Choices, page 2-15](#).
- 

## Deleting a Profile

Use this option to delete a profile.



### Note

Your login determines whether you can use this option.

---

### Procedure

---

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



### Note

Any devices that were assigned this deleted profile will be assigned the Default profile.

---

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

## Assigning a Profile to a Device

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

**Note**

---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Faults > Manage Profiles**. The Profiles dialog box appears.
  - Step 2** Select the profile you want to assign to the devices from the Existing Profiles box, then click **Assign to Devices**. The Assigning Profiles window appears.
  - Step 3** If you want to search for devices, use the dialog box in the left pane above the device selector:
    - a. From the list, select the method you want to use to search for the device: by name or by IP address.
    - b. Enter the IP address or name, or use an asterisk (\*) as a wildcard to denote numbers and letters, then click **Go**. The requested device appears in the Search Results folder.
  - 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.
-

## Viewing Devices

Use this option to view the devices that have been assigned to a profile.



Note

---

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Faults > Manage Profiles**. The Profiles dialog box appears.
- Step 2** Select a profile from Existing Profiles box, then click **View Devices**. A window appears listing the devices that are assigned to that profile.
- 

## Profile Choices

When you create or edit a profile, the following choices appear in the left pane of the Editing Profile window:

- **Security Policies**—See [Specifying Security Policies, page 2-15](#)
- **Thresholds**—See [Specifying Fault Thresholds, page 2-27](#)

## 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 policy. See [Viewing Current Faults, page 2-35](#).



Note

---

Your login determines whether you can use this option.

---

## Procedure

---

- Step 1** In the left pane, select the variable for which you want to set a policy.
- SSID—See [Setting the SSID Policy, page 2-17](#).
  - Firmware Version (IOS)—See [Setting the Firmware Version Policy, page 2-18](#).
  - Firmware Version (Non-IOS)—See [Setting the Firmware Version Policy, page 2-18](#).
  - Broadcast SSID Disabled—See [Setting the Broadcast SSID Disabled Policy, page 2-18](#).
  - Key Rotation per VLAN—See [Setting Key Rotation Disabled per VLAN Policy, page 2-19](#).
  - WEP Encryption per VLAN—See [Setting WEP Encryption per VLAN Policy, page 2-20](#).
  - WEP Enforced—See [Setting the WEP Enforced Policy, page 2-21](#).
  - EAP Enforced—See [Setting the EAP Enforced Policy, page 2-21](#).
  - EAP Per SSID Enforced—See [Setting EAP Per SSID Enforced Policy, page 2-22](#).
  - WEP Key Length—See [Setting WEP Key Length Policy, page 2-23](#).
  - HotStandBy Status—See [Setting the Hot StandBy Status Policy, page 2-23](#).
  - HTTP Disabled (Non-IOS)—See [Setting the HTTP Disabled \(Non-IOS\) Policy, page 2-24](#).
  - Telnet Disabled (Non-IOS)—See [Setting the Telnet Disabled \(Non-IOS\) Policy, page 2-24](#).
  - PSPF Enabled (Non-IOS)—See [Setting the PSPF Enabled \(Non-IOS\) Policy, page 2-25](#).
  - User Manager Enforced (Non-IOS)—See [Setting the User Manager Enforced \(Non-IOS\) Policy, page 2-26](#).
  - HTTP Authentication (Non-IOS)—See [Setting the HTTP Authentication \(Non-IOS\) Policy, page 2-26](#).
-

## 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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.
Enter 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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.
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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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.
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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) for details.

## Setting the Hot StandBy 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) for details.
- 

### Setting the Telnet Disabled (Non-IOS) Policy

#### Procedure

---

- Step 1** Complete the following:

Field	Description
Verify	Select to verify.

Field	Description
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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this policy. See [Viewing Current Faults, page 2-35](#) 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 2-35](#).



### 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 2-27](#).
- **Switch**—See [Setting Switch Fault Thresholds, page 2-30](#).
- **Router**—See [Setting Router Fault Thresholds, page 2-32](#).
- **LEAP**—See [Setting Server Response Time, page 2-33](#).
- **PEAP**—See [Setting Server Response Time, page 2-33](#).
- **RADIUS**—See [Setting Server Response Time, page 2-33](#).
- **EAP-MD5**—See [Setting Server Response Time, page 2-33](#).
- **WLSE**—See [Setting WLSE Dot11 MIB View, page 2-34](#).

## 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 2-29](#) to set the fault thresholds for the following access point faults:
  - SNMP Reachable
  - RF Port Status
  - Ethernet Port Status
- See [Setting Overloaded, Degraded, and OK Status, page 2-29](#) 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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-35](#) 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.

Field	Description
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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-35](#) 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 2-31](#) to set the fault thresholds for the following switch faults:
  - SNMP Reachable
  - Port Status
  - Module Status

- See [Setting Overloaded, Degraded, and OK Status, page 2-32](#) 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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-35](#) 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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults](#), page 2-35 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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-35](#) 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 [FAQs, page 7-10](#).

### 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 **View current faults for this setting** to see the faults associated with this threshold. See [Viewing Current Faults, page 2-35](#) 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 <a href="#">Using the Device Center, page 5-2</a> .
Hostname	The device for which the fault is reported.  Click to see various reports about the device. For information on the reports, see <a href="#">Using the Device Center, page 5-2</a> .
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 <a href="#">Viewing Fault Details, page 2-7</a> .  For information on specific faults, see <a href="#">FAQs, page 7-10</a> .
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 <a href="#">Time Display, page 1-6</a> .  Click to see fault details. See <a href="#">Viewing Fault Details, page 2-7</a> .

- 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.

---

## Notification Settings

The WLSE has the capability to send traps, syslog messages, and emails when a fault is detected.

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

- [Displaying Faults, page 2-1](#)
- [Specifying Fault Thresholds, page 2-27](#)

## 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 2-39](#) 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 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.
- 

## 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 2-41](#) 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

### 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 2-43](#).
- 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 may 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.
- 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.
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. <b>Note</b> 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 tracyv
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>
```