



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 2-7](#)
- **Notification Settings**—See [Notification Settings, page 2-20](#)

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 2-15](#) to set threshold levels.)

A fault can also occur when a system policy is violated. (See [Notification Settings, page 2-20](#) to set policies.)

Displayed fault information is retained by default for 30 days. To change the default, see [Managing System Parameters, page 6-73](#).



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	From the list, select the severity from P1, which is the highest severity level to P5, which is the lowest severity level, to display: <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.

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

Field	Description
State	From the list, select a states to display: <ul style="list-style-type: none">• All—Faults in all states are displayed.• Active—Faults are active (current) and have not been acknowledged.• Acknowledged—Faults that are active and have been acknowledged.• Cleared—Faults that have been cleared (no longer in an Active or Acknowledged 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 Using the Device Center, page 5-1 .
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 5-1 .
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 2-5 .
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 1-5 . Click to see fault details. See Viewing Fault Details, page 2-5 .

- Step 4** 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.
- Step 5** To acknowledge (change the state from Active to Acknowledged):
- A single fault, select it, then click **Acknowledge**.
 - All faults, click **Select All**, then click **Acknowledge**.
- Step 6** To unacknowledge (change the state from Acknowledged to Active):
- A single fault, select it, then click **Unacknowledged**.
 - All faults, click **Select All**, then click **Unacknowledged**.
-

Related Topics

- [Managing Profiles, page 2-7](#)
- [Notification Settings, page 2-20](#)

Viewing Fault Details

The following tables are displayed in the Fault Details window.

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.

Fault details for

Table 2-3 *Fault Details Table*

Column	Description
IP	The device IP address.
Name	The device hostname.

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

Column	Description
Family	The device family.
Product	The product name.
Type	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. 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.
ifIndex	A unique number that identifies the interface.

Conditions**Table 2-4** *Conditions Table*

Column	Description
Name	The fault condition.
State	The state of the device.
Severity	The fault severity level.
Description	A description of the fault.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Time Display, page 1-5 .

Fault History**Table 2-5** *Fault History Table*

Column	Description
State	The state of the device.
Severity	The fault severity level.
Description	A description of the fault.
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 1-5 .
By	Displays the username of the person who changed the fault state. If the fault state has not been 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 2-8](#)
- [Copying a Profile, page 2-8](#)
- [Renaming a Profile, page 2-9](#)
- [Editing a Profile, page 2-9](#)
- [Deleting a Profile, page 2-10](#)

- [Assigning a Profile to a Device](#), page 2-10
- [Viewing Devices](#), page 2-11

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 2-9.)

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 2-9](#).)

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 2-12](#).
-

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 2-12](#)
- **Thresholds**—See [Specifying Fault Thresholds, page 2-15](#)

Specifying Security Policies

This option allows you to activate or deactivate a set of pre-defined 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 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—Go to [Step 2](#)
 - Firmware Version—Go to [Step 5](#)
 - Broadcast SSID Disabled—Go to [Step 8](#)
 - WEP Enabled—Go to [Step 8](#)
 - LEAP Enabled—Go to [Step 8](#)

- WEP Key Length—Go to [Step 10](#)
- HTTP Disabled—Go to [Step 8](#)
- Telnet Disabled—Go to [Step 8](#)
- PSPF Enabled—Go to [Step 8](#)
- User Manager Enforced—Go to [Step 8](#)
- HTTP Authentication—Go to [Step 8](#)

Step 2 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.

Step 3 Click **Add** to add the SSID to the list, then go to [Step 11](#).

Step 4 To remove an SSID from the list, select it, click **Remove**, then go to [Step 11](#).

Step 5 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 6 Click **Add** to add the firmware version to the list, then go to [Step 11](#).

Step 7 To remove a firmware version from the list, select it, click **Remove**, then go to [Step 11](#).

Step 8 Complete the following:

Field	Description
Verify	Select if you want to verify one of the following: <ul style="list-style-type: none"> • Broadcast SSID is disabled • WEP is enabled • LEAP is enabled • HTTP is disabled • Telnet is disabled • PSPF is enabled • User Manager Capabilities are enforced • HTTP authentication
Polling Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 9 Go to [Step 11](#).

Step 10 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 11 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

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.

**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 2-15.
- **Switch**—See [Setting Switch Fault Thresholds](#), page 2-17.
- **Router**—See [Setting Router Fault Thresholds](#), page 2-19.
- **LEAP**—See [Setting Server Response Time](#), page 2-19.
- **Radius**—See [Setting Server Response Time](#), page 2-19.
- **EAP-MD5**—See [Setting Server Response Time](#), page 2-19.

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**.

Procedure

Step 1 Select any of the following to set values for:

- SNMP Reachable—Go to [Step 2](#).
- RF Port Status—Go to [Step 2](#).
- RF Port Utilization—Go to [Step 4](#).
- RF Port Packet Errors—Go to [Step 4](#).
- RF Port WEP Errors—Go to [Step 4](#).
- RF Port FCS Errors—Go to [Step 4](#).
- Ethernet Port Status—Go to [Step 2](#).

- Ethernet Port Utilization—Go to [Step 4](#).
- Ethernet Port Packet Errors—Go to [Step 4](#).
- Associated Clients—Go to [Step 4](#).
- SSID Mismatch Rate—Go to [Step 4](#).
- Association Rate—Go to [Step 4](#).

Step 2 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 3 Continue to [Step 5](#).

Step 4 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.

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

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**.

Procedure

- Step 1** Select any of the following to set values for:
- SNMP Reachable—Go to [Step 2](#).
 - CPU Utilization—Go to [Step 4](#).
 - Memory Utilization—Go to [Step 4](#).
 - Port Status—Go to [Step 2](#).
 - Port Utilization—Go to [Step 4](#).
 - Module Status—[Step 2](#).

Step 2 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 3 Go to step [Step 5](#).

Step 4 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 5 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

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.

Setting Server Response Time

Using this option, you can set up a threshold for LEAP, RADIUS, and EAP-MD5 server response time. 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	
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.

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 2-15](#)
- [Notification Settings, page 2-20](#)

Setting Trap Notification

This option allows you to enable the WLSE 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.

The MIB that defines the trap and the varbinds can be found at the following URL: <ftp://ftp.cisco.com/pub/mibs/v2/CISCO-DEVICE-EXCEPTION-REPORTING-MIB.mib>

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.
- Step 3** Complete the following:

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

Related Topics

- [Setting Syslog Notification, page 2-22](#)
- [Emailing Faults, page 2-23](#)

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.

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.

Related Topics

- [Setting Trap Notification, page 2-21](#)
- [Emailing Faults, page 2-23](#)

Emailing Faults

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.

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

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

```
FaultId 19
DeviceId 106
DeviceIp 172.20.29.118
DeviceName sj-W-10-AP-118
MOId {MOID[c=1013,d=106,i=379]}
AlarmState Active
Description SSID policy violation
Severity P1
```

- An example of the same message sent in an XML format will appear as follows:

```
<Msg><FaultId>19</FaultId><DeviceId>106</DeviceId><DeviceIP>172.
20.29.118</DeviceIP><DeviceName>sj-W-10-AP-118<DeviceName><MOId>
{MOID[c=1013,d=106,i=379]}</MOId><AlarmState>Active</AlarmState>
<Description>SSID policy violation
</Description><Severity>P1</Severity></Msg>
```

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.

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.

Related Topics

- [Setting Trap Notification, page 2-21](#)
- [Setting Syslog Notification, page 2-22](#)

