



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](#)
- **Specify Fault Thresholds**—See [Specifying Fault Thresholds, page 2-7](#)
- **Specify Policies**—See [Specifying Policies, page 2-13](#)
- **Fault Forwarding**—See [Forwarding Faults, page 2-15](#)

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 2-7](#) to set threshold levels.)

A fault can also occur when a system policy is violated. (See [Specifying Policies, page 2-13](#) to set policies.)

Displayed fault information is retained by default for 30 days. To change the default, see [Managing System Parameters, page 6-59](#).

**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 states to display:</p> <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).

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	<p>The device IP address.</p> <p>Click to see the device's summary report. For:</p> <ul style="list-style-type: none"> • Access Points— see Displaying an AP Summary Report, page 5-11. • Switches— see Displaying a Switch Summary Report, page 5-17. • Routers— see Displaying a Router Summary Report, page 5-19.
Hostname	<p>The device for which the fault is reported.</p> <p>Click to see the device's summary report. For:</p> <ul style="list-style-type: none"> • Access Points— see Displaying an AP Summary Report, page 5-11. • Switches— see Displaying a Switch Summary Report, page 5-17. • Routers— see Displaying a Router Summary Report, page 5-19.
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	A description of the fault. Click to see fault details. See Viewing Fault Details, page 2-6 .
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 Date and Time Display on the WLSE, page 1-2 . Click to see fault details. See Viewing Fault Details, page 2-6 .

- 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, check 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, check it, then click **Unacknowledged**.
 - All faults, click **Select All**, then click **Unacknowledged**.

Related Topics

- [Specifying Fault Thresholds, page 2-7](#)
- [Specifying Policies, page 2-13](#)
- [Forwarding Faults, page 2-15](#)

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

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>

Conditions

Column	Description
Name	The fault condition.
State	The state of the device.
Severity	The fault severity level.

Column	Description
Description	A description of the fault.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Date and Time Display on the WLSE, page 1-2 .

Fault History

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 Date and Time Display on the WLSE, page 1-2 .
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.

Specifying Fault Thresholds

This window 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.

The Specify Fault Threshold window has the following options:

- **Access Point**—See [Setting Access Point Fault Thresholds, page 2-8](#).
- **Switch**—See [Setting Switch Fault Thresholds, page 2-10](#).
- **LEAP**—See [Setting LEAP Server Response Time, page 2-12](#).

Related Topics

- [Displaying Faults, page 2-1](#)
- [Specifying Policies, page 2-13](#)
- [Forwarding Faults, page 2-15](#)

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 **Faults > Specify Fault Thresholds**. The Fault threshold window appears.
- Step 2** Select **Access Point** in the left pane and the menu expands.
- Step 3** Select any of the following to set values for:
- SNMP Reachable—Go to [Step 4](#).
 - RF port status—Go to [Step 4](#).
 - RF port utilization—Go to [Step 6](#).
 - RF port packet errors—Go to [Step 6](#).
 - RF port WEP errors—Go to [Step 6](#).
 - RF port FCS errors—Go to [Step 6](#).
 - Ethernet port status—Go to [Step 4](#).

- Ethernet port utilization—Go to [Step 6](#).
- Ethernet port packet errors—Go to [Step 6](#).

Step 4 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling 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 5 Continue to [Step 7](#).

Step 6 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling 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 7 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 **Faults > Specify Fault Threshold**. The Fault threshold window appears.
- Step 2** Select **Switch** in the left pane and the menu expands.
- Step 3** Select any of the following to set values for:
- SNMP Reachable—Go to [Step 4](#).
 - CPU utilization—Go to [Step 6](#).
 - Memory utilization—Go to [Step 6](#).
 - Port Status—Go to [Step 4](#).
 - Port Utilization—Go to [Step 6](#).
 - Module Status—[Step 4](#).
- Step 4** Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling 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 5 Go to step [Step 7](#).

Step 6 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling 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 7 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Setting LEAP Server Response Time

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

Procedure

-
- Step 1** Select **Faults > Specify Fault Threshold**. The LEAP Server:Response Time threshold window appears.
- Step 2** Select **LEAP** in the left pane and the menu expands.
- Step 3** Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling 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 4** Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.
-

Specifying Policies

This window 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** Select **Faults > Specify Policies**. The Access Point window appears.
- Step 2** In the left pane, select the variable for which you want to set a policy.
- SSID—Go to [Step 3](#)
 - Broadcast SSID Disabled—Go to [Step 6](#)
 - WEP Enabled—Go to [Step 6](#)
 - LEAP Enabled—Go to [Step 6](#)
 - WEP Key Length—Go to [Step 8](#)
 - HTTP Disabled—Go to [Step 6](#)
 - Telnet Disabled—Go to [Step 6](#)
 - User Manager Enforced—Go to [Step 6](#)
 - HTTP Authentication—Go to [Step 6](#)
- Step 3** To activate the policy, do the following:

Field	Description
Verify	Check if you want to verify that SSID is enabled.
Polling Interval	From the list, select the polling interval.

Field	Description
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 4 Click **Add** to add the SSID to the list, then go to [Step 9](#).

Step 5 To remove an SSID from the list, select it, click **Remove**, then go to [Step 9](#).

Step 6 Complete the following:

Field	Description
Verify	Check 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 • 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 7 Go to [Step 9](#).

Step 8 Complete the following:

Field	Description
Verify	Check if you want to verify the WEP key length.
Polling 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 9 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Related Topics

- [Displaying Faults, page 2-1](#)
- [Specifying Fault Thresholds, page 2-7](#)
- [Forwarding Faults, page 2-15](#)

Forwarding Faults

This window allows you to set SNMP traps to enable north-bound exception notification to specified hosts, issue syslog messages to selected syslog servers, and send exception notification email to selected users.

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 2-7](#)
- [Specifying Policies, page 2-13](#)

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.

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 > Fault Forwarding**. The Fault Forwarding dialog box appears.

Step 2 Complete the following:

Field	Description
Trap	Check 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 3 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 4** 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 2-17](#)
- [Emailing Faults, page 2-18](#)

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 > Fault Forwarding**. The Fault Forwarding dialog box appears.
- Step 2** Complete the following:

Field	Description
Syslog	Check 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 3** 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 2-16](#)
- [Emailing Faults, page 2-18](#)

Emailing Faults

The emailed exception notification contains information such as device name and IP, fault number, exception severity, and a message about what is wrong

Procedure

- Step 1** Select **Faults > Fault Forwarding**. The Fault Forwarding dialog box appears.
- Step 2** Complete the following:

Field	Description
Email	Check 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 these uses to receive.

- Step 3** 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 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 2-16](#)
- [Setting Syslog Notification, page 2-17](#)

