Setting Up Monitoring Thresholds

Threshold is an optimal value set by you for a device or a group. Cisco Prime LMS compares this threshold rule with the polled data. If the threshold rule is violated consecutively, for the number of times specified, LMS generates an alert.

You can also configure LMS to send alert notifications as an e-mail, a trap or a syslog.

This section explains how to set up the monitoring thresholds and contains:

- Managing Fault Thresholds
- Setting Up Performance Thresholds
- TrendWatch Setup

Managing Fault Thresholds

You can manage thresholds for:

- All devices managed by LMS Monitoring
- LMS System Defined Groups
- Customizable Fault Groups (for devices)
- System Defined Fault groups, for example Access Port Groups, Interface Groups and Trunk Port Groups and their own sub groups.

This section describes how to configure and manage thresholds for device groups and contains the following topics:

- Viewing Thresholds
- Previewing Thresholds
- Editing Thresholds
- Restoring Factory Settings for Thresholds
- Threshold Categories for Devices, Interfaces, and Ports
- Threshold Definitions
- Threshold Parameter Values and Events
Managing Fault Thresholds

Note

In this release, LMS Fault management functionality supports generic devices such as unknown devices and non-Cisco devices. The device group selector in the Fault Threshold Management page displays Unknown Device Type group and Non Cisco Devices group.

Viewing Thresholds

You can view the thresholds that are associated with device groups, trunk port groups, access port groups, and interface groups.

Since there may be many ports and interfaces, you can use a link in the Threshold Parameter Summary to launch a separate page with all of the ports and interface members of the group. You can also save a comma separated value (CSV) version of the port or interface summary.

Step 1

Select either one of the following from the menu:

- Monitor > Threshold Settings > Fault > Threshold Settings
- Monitor > Fault Settings > Setup > Threshold Settings

Step 2

Select any device group from the group selector.
Chapter 2  Setting Up Monitoring Thresholds

Managing Fault Thresholds

Step 3  
Click the View button.

The Thresholds Summary tabular display opens in a separate window and displays the following:

<table>
<thead>
<tr>
<th>Summary</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heading</td>
<td></td>
</tr>
<tr>
<td>Device Name</td>
<td>IP address or DNS name of the device (device group summaries only).</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (device group summaries only).</td>
</tr>
<tr>
<td>Threshold Parameters</td>
<td></td>
</tr>
<tr>
<td>Category Name</td>
<td>Threshold category.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether threshold analysis is enabled (true) or disabled (false).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Threshold name.</td>
</tr>
<tr>
<td>Metric</td>
<td>Unit of measurement for parameter value:</td>
</tr>
<tr>
<td>%—percent.</td>
<td></td>
</tr>
<tr>
<td>count—number of occurrences.</td>
<td></td>
</tr>
<tr>
<td>sec—number of seconds.</td>
<td></td>
</tr>
<tr>
<td>C—centigrade.</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Factory setting for the parameter.</td>
</tr>
<tr>
<td>Current</td>
<td>Current value for the parameter.</td>
</tr>
<tr>
<td>Overriding Group</td>
<td>Group from which threshold parameter values are applied. (This is the highest priority group to which the element belongs.)</td>
</tr>
</tbody>
</table>

Step 4  
After viewing the threshold parameters, close the tabular display window.

You can export the data from tabular displays or print the tabular displays. See Reports Management with Cisco Prime LAN Management Solution 4.2 for more details.

For additional information, see the following topic:
- Viewing the Overriding Group—Examples

Previewing Thresholds

When you preview thresholds parameters, you can see the edited threshold parameters before you apply the changes.

Note  
Preview is only supported for Device Type Groups.

Step 1  
Select either one of the following from the menu:
- Monitor > Threshold Settings > Fault > Threshold Settings
or
- Monitor > Fault Settings > Setup > Threshold Settings

Step 2  
Select any device type group from the group selector.
Step 3  Click the Preview button.

The Thresholds Summary tabular display opens in a separate window and displays the following

<table>
<thead>
<tr>
<th>Summary</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>IP address or DNS name of the device (device group summaries only).</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (device group summaries only).</td>
</tr>
<tr>
<td>Category Name</td>
<td>Threshold category.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether threshold analysis is enabled (true) or disabled (false).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Threshold name.</td>
</tr>
<tr>
<td>Metric</td>
<td>Unit of measurement for parameter value:</td>
</tr>
<tr>
<td></td>
<td>• %—percent.</td>
</tr>
<tr>
<td></td>
<td>• count—number of occurrences.</td>
</tr>
<tr>
<td></td>
<td>• sec—number of seconds.</td>
</tr>
<tr>
<td></td>
<td>• C—centigrade.</td>
</tr>
<tr>
<td>Default</td>
<td>Factory setting for the parameter.</td>
</tr>
<tr>
<td>Current</td>
<td>Current value for the parameter.</td>
</tr>
<tr>
<td>Overriding Group</td>
<td>Group from which threshold parameter values are applied. (This is the highest priority group to which the element belongs.)</td>
</tr>
</tbody>
</table>

Step 4  After previewing the threshold parameters, close the tabular display window.

The Threshold Parameter Summary report displays the edited parameters for the selected device group. You can see the preview of the edited parameters based on the grouping of the devices in the selected device group.

Preview Threshold Parameter — Examples

The following example helps you to understand the preview of the displayed edited threshold parameters:

Let us consider the devices D1, D2, D3, and D4 belonging to the following four groups:
- Routers: D1 and D2
- Switches and Hubs: D2 and D3
- Customizable Group1: D1 and D3
- Customizable Group 2: D2 and D4

Let the Overriding Group order of the groups be:
- Customizable Group1
- Routers
- Switches and Hubs
- Customizable Group 2
Let the Relative voltage threshold parameter of the Environment Settings category for the groups be:

- Routers: 20
- Switches and Hubs: 30
- Customizable Group1: 40
- Customizable Group 2: 50

To edit the Relative voltage threshold parameter of a device group and to see the preview, do the following:

### Step 1
Select Routers which contains D1 and D2.

### Step 2
Edit the Relative voltage threshold parameter by changing it to 80.

### Step 3
Click the Preview button to see the edited parameters.

The Threshold Parameter Summary report for Routers (D1 and D2) is displayed.

The edited Relative voltage threshold parameter value 80 will be displayed only against the device D2. Although D2 belongs to the groups Routers, Switches and Hubs, and Customizable Group 2, Routers is the overriding group among them. Since D2 belongs to the overriding group Routers, the edited parameter 80 is displayed against D2.

D1 belongs to the groups Routers and Customizable Group1 where Customizable Group1 is the overriding group. So instead of the edited value 80, the value 40, which belongs to Customizable Group1 will be displayed against D1.

For more information on Overriding Groups, see Viewing the Overriding Group—Examples. To change the priority of the Device groups, see Setting Priorities.

Although the thresholds are saved in the database, they are not yet applied to the IP fabric. See Applying Polling and Threshold Changes.

**Editing Thresholds**

When you edit thresholds, you edit values that are associated with groups, not with individual devices, ports, or interfaces. For ports and interfaces, you can activate or deactivate an entire group of threshold settings (for example, if you want to disable Reachability Settings for an entire interface group).

### Step 1
Select either one of the following from the menu:

- Monitor > Threshold Settings > Fault > Threshold Settings
- Monitor > Fault Settings > Setup > Threshold Settings

### Step 2
Select a data source.

The available data sources are:

- Device
- Device Groups
- Port Groups
**Step 3**  
Select a group for which you can set or edit thresholds.

**Step 4**  
Click Edit.

The Managing Thresholds: Edit page appears, displaying the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the device group selected.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device function (not applicable to port or interface groups)</td>
</tr>
<tr>
<td>Threshold Category</td>
<td>Only those categories that are applicable to the members in the group are displayed.</td>
</tr>
<tr>
<td>Parameter</td>
<td>The parameters for the currently selected object and threshold category are displayed, including:</td>
</tr>
<tr>
<td></td>
<td>• Current value for each threshold</td>
</tr>
<tr>
<td></td>
<td>• An entry field for a new value.</td>
</tr>
<tr>
<td></td>
<td>• Default check boxes that allow you to reset factory settings for all thresholds or for selected thresholds.</td>
</tr>
</tbody>
</table>

**Step 5**  
Edit the thresholds by selecting the threshold category and changing the thresholds appropriately:

- To reset factory settings for all thresholds in the category, select the Default check box in the table heading.
- To set values for individual thresholds for a group, enter data for each threshold.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Value</td>
<td>Enter a new value. This is optional.</td>
</tr>
<tr>
<td>Default</td>
<td>If you entered a new value, do not select Default check box.</td>
</tr>
<tr>
<td></td>
<td>To reset thresholds to the factory settings, select this check box.</td>
</tr>
<tr>
<td></td>
<td>The Default check box in the table heading can override this setting.</td>
</tr>
</tbody>
</table>

- To activate or deactivete an entire group of threshold settings for interface and port groups select the Customize Settings button. For example, this can be Interface and Port Flapping settings for interface or port groups, or Reachability settings for device groups.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional Settings</td>
<td>Threshold settings groups that are not currently enabled.</td>
</tr>
<tr>
<td>Active Settings</td>
<td>Threshold settings groups that are currently enabled.</td>
</tr>
</tbody>
</table>

Use the Add or Remove button to select the settings group you want to enable or disable.

- To activate or deactivate all threshold settings, activate or deactivate the Disable All Threshold Settings for this Group check box.
Step 6  Save the thresholds by doing either one of the following:

- Click **Save** to save the thresholds and display the Thresholds: Edit page again.
- Click **OK** to save the thresholds and close the Thresholds: Edit page.

Step 7  Click **Preview** to see the edited threshold parameters before applying the changes.

Step 8  Apply the changes so that the changes come into effect. See **Applying Polling and Threshold Changes**.

The Threshold Parameter Summary report displays the edited parameters for the selected device group. You can see the preview of the edited parameters based on the grouping of the devices in the selected device group. For more information, see the **Preview Threshold Parameter — Examples** given in the Previewing Thresholds section.

### Restoring Factory Settings for Thresholds

You can use this procedure to reset all thresholds for a device group, and you can reset all categories of thresholds to use factory settings.

**Before You Begin**

To review factory settings for thresholds before you apply them, view the thresholds for the device group. See **Viewing Thresholds**. Current values are displayed along with the factory settings.

**Step 1**

Select either one of the following from the menu:

- **Monitor > Threshold Settings > Fault > Threshold Settings**
- **Monitor > Fault Settings > Setup > Threshold Settings**

Step 2  Select a device group for which you can set thresholds.

Step 3  Click the Factory Setting button.

A confirmation dialog box appears.

Step 4  Click **Yes**.

**Note**  The settings are stored in the database, but not yet applied to the IP fabric. See **Applying Polling and Threshold Changes**.

For additional information, see the following topics:

- **Viewing Thresholds**
- **Previewing Thresholds**
- **Threshold Definitions**
- **Threshold Parameter Values and Events**
Threshold Categories for Devices, Interfaces, and Ports

Table 2-1 lists the threshold categories for each device group. For the parameters that you can set for each threshold category, see Threshold Definitions, or Threshold Parameter Values and Events.

Table 2-1  Threshold categories for devices, interfaces, and ports

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS System Defined Groups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Broadband Cable</td>
<td>Controlled by LMS Group</td>
<td>• Reachability</td>
</tr>
<tr>
<td>• Cisco Interfaces and Modules</td>
<td>Administration</td>
<td>• Processor and Memory</td>
</tr>
<tr>
<td>• Content Networking</td>
<td></td>
<td>• Environment</td>
</tr>
<tr>
<td>• DSL &amp; LREs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Non Cisco Devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Optical Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Routers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security and VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Server Fabric Switches</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Storage Networking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Switches and Hubs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Universal Gateways and Access Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unknown Device Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Voice and Telephony</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Wireless</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Network Management</td>
<td></td>
<td>• Reachability</td>
</tr>
<tr>
<td>• Non Cisco Devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Unknown Device Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-1  Threshold categories for devices, interfaces, and ports

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Defined Fault Groups—Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000” Type contains “ETHER” or “CSMADC”</td>
<td>Generic interface/port performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Backup interface support</td>
</tr>
<tr>
<td>10 GB Ethernet</td>
<td>MaxSpeed = “10000000000” Type contains “ETHER” or “CSMADC”</td>
<td>Dial-On-Demand interface support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interface/port flapping</td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMADC”</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td></td>
</tr>
<tr>
<td>Token Ring</td>
<td>Type contains “TOKEN”</td>
<td></td>
</tr>
<tr>
<td>ISDN physical interface</td>
<td>InterfaceCode contains “ISDNPHYSICAL”</td>
<td></td>
</tr>
<tr>
<td>ISDN B channel</td>
<td>InterfaceCode contains “ISDNBCHANNEL”</td>
<td></td>
</tr>
<tr>
<td>ISDN D channel</td>
<td>InterfaceCode contains “ISDNDCONNECT”</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>Type contains “Serial” or “FrameRelay”</td>
<td></td>
</tr>
<tr>
<td>FDDI</td>
<td>Type contains “FDDI”</td>
<td></td>
</tr>
<tr>
<td>Backup(^1)</td>
<td>Type contains “ISDN”</td>
<td></td>
</tr>
<tr>
<td>Dial-On-Demand(^1)</td>
<td>Type contains “PPP” or “SLIP”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
Threshold Definitions

When you manage thresholds, you must select a device group and a threshold category. Threshold categories contain groups of parameters or thresholds that apply to that category. For the threshold parameters that you can set for each category, see Table 2-2.

For more information on Threshold Definitions, see:

- Backup Interface Support
- Dial-On-Demand Interface Support
- Environment
- Generic Interface/Port Performance
- Interface/Port Flapping
- Processor and Memory
- Reachability

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Rule</th>
<th>Threshold Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Defined Fault Groups—Access Port</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000” Type contains “ETHER” or “CSMACD”</td>
<td>Generic interface/port performance Interference/port flapping</td>
</tr>
<tr>
<td>10 GB Ethernet</td>
<td>MaxSpeed = “10000000000” Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>System Defined Fault Groups—Trunk Ports</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GB Ethernet</td>
<td>MaxSpeed = “1000000000” Type contains “ETHER” or “CSMACD”</td>
<td>Generic interface/port performance Interference/port flapping</td>
</tr>
<tr>
<td>10 GB Ethernet</td>
<td>MaxSpeed = “10000000000” Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>10/100MB Ethernet</td>
<td>Type contains “ETHER” or “CSMACD”</td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>Type contains “ATM”</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

1. Dial-On-Demand and Backup interface settings are related. If one interface type is set to active, and you change the other interface type from optional to active, the first interface type will be changed from active to optional.

For additional information, see Threshold Parameter Values and Events.
Backup Interface Support

The Backup Interface Support threshold configures an interface as a backup. When an interface is identified as a backup:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Maximum Uptime

The maximum length of time, in seconds, that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Dial-On-Demand Interface Support

The Dial-On-Demand Interface Support threshold identifies an interface as dial-on-demand. In this case:

- The InterfaceOperationallyDown event is not generated if the interface is down.
- The ExceededMaximumUptime event is generated if the interface stays up too long.

Maximum Uptime

The maximum length of time that the interface may be up before the ExceededMaximumUptime event is generated. If the value of this parameter is 0, the ExceededMaximumUptime event is disabled.

Environment

The Environment threshold controls the monitoring of the system environment.

Relative Temperature Threshold

Indicates how close the current temperature value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown temperature is 50° C and the Relative temperature threshold is 10%, the OutofRange event occurs if the temperature exceeds 45° C.

Relative Voltage Threshold

Indicates how close the current voltage value can be to the value that triggers an emergency shutdown, expressed as a percentage of the emergency shutdown value. For example, if the shutdown value is +30V and the Relative voltage threshold is 10%, the OutofRange event occurs if the voltage exceeds +27V.

Generic Interface/Port Performance

The Generic Interface/Port Performance thresholds configure the monitoring of a non-Ethernet network adapter’s performance characteristics. The categories include basic parameters—such as utilization, errors, broadcast, and packet drops—common to all media types.

Broadcast Threshold

The upper threshold for broadcast traffic, expressed as a percentage of the total bandwidth.
Collision Threshold

The upper threshold for collisions, expressed as a percentage of the total number of output packets. This threshold applies only to Ethernet settings for ports, trunks, and interfaces.

Discard Threshold

The upper threshold for dropped packets, expressed as a percentage of the total number of packets.

Error Threshold

The upper threshold for packet errors, expressed as a percentage of the total number of packets. LMS generates the HighErrorRate event when both the Error threshold and Error traffic threshold are reached or exceeded.

Error Traffic Threshold

The upper threshold for packet rate, expressed as a percentage of the total bandwidth. LMS generates the HighErrorRate event when both the Error threshold and Error traffic threshold are reached or exceeded. The value for Error traffic threshold can include up to two decimal places.

Queue Drop Threshold

The acceptable percentage of packets dropped because of full queues, expressed as a percentage of the total number of packets.

Utilization Threshold

The upper threshold for link utilization, expressed as a percentage of the total bandwidth.

LMS uses the DuplexMode special variable to specify duplexity (UNSPECIFIED, by default), and DuplexSource to track the duplexity setting source (NONE by default).

LMS uses the following algorithm to determine duplexity:

1. LMS checks the portDuplexity MIB attribute in the CISCO-STACK-MIB, and:
   - If the value is set to either half duplex or full duplex, LMS uses that setting for DuplexMode and sets DuplexSource to ENTERPRISE_MIB.
   - If the device is not a Cisco stack switch, the portDuplexity attribute is not present, or the portDuplexity attribute is present but its value is auto/disagree, LMS proceeds to Step 2.

2. LMS checks the dot3StatsDuplexStatus MIB attribute in the ETHERLIKE-MIB, and:
   - If the value is set to either half duplex or full duplex, LMS uses that setting for DuplexMode and sets DuplexSource to ETHERLIKE_MIB.
   - If the dot3StatsDuplexStatus attribute is not present, or it is present but its value is unknown, LMS proceeds to Step 3.
3. LMS checks the cdpCacheDuplex MIB attribute in the CISCO-CDP-MIB, and:
   - If the value is set to either half duplex or full duplex, LMS uses that setting for DuplexMode (for both local and remote ports), and sets DuplexSource to NEIGHBOR_MIB.
   - If the value is unknown, LMS proceeds to Step 4.

4. If LMS cannot correctly determine the duplex mode (because it was not set manually nor was it set in the MIB), LMS will set DuplexSource to ASSUMED and do the following:
   - If the interface is a 10-MB Ethernet interface, LMS will assume the setting is half duplex. (LMS considers an interface to be 10-MB Ethernet when its Type=“*ETHER*” and its MaxSpeed=1000000.)
   - For all other interfaces, LMS will assume the setting is full duplex.

Interface/Port Flapping

The Interface/Port Flapping thresholds control the analysis of network adapters (ports and interfaces) that are continually going up and down, or flapping.

Flapping analysis monitors SNMP link down traps to identify a flapping network adapter. LMS reports flapping as a fault condition. For more information, How LMS Troubleshooting Calculates Repeated Restarts and Flapping.

Link Trap Threshold

The number of SNMP link down traps that must be received within the Link trap window for LMS to consider the interface or port flapping. A value of 0 disables flapping analysis.

Link Trap Window

The amount of time used to monitor flapping analysis of a port or interface. If the number of link down traps meets or exceeds the Link trap threshold during this window of time, the interface or port is considered to be flapping.

Processor and Memory

The Processor and Memory thresholds control the performance monitoring of a system's processor and its associated memory elements.

Backplane Utilization Threshold

The upper threshold for a backplane utilization of a switch, expressed as a percentage of the total backplane bandwidth.

Free Memory Threshold

The lower threshold for the acceptable amount of free memory, as measured by the ratio of free memory to the total memory.

Memory Buffer Miss Threshold

The upper threshold for the number of buffer misses, expressed as a percentage of the total number of buffer requests.
Memory Buffer Utilization Threshold

The upper threshold for the number of buffers used, expressed as a percentage of the total number of buffers.

Memory Fragmentation Threshold

The lower threshold for memory fragmentation. The fragmentation value is the ratio of the largest number of contiguous unallocated bytes to the total amount of free memory. For example, a value of 5 indicates that the largest free buffer must be at least 5% of the free memory.

Processor Utilization Threshold

The upper threshold for processor utilization, expressed as a percentage of the total capacity of the processor.

Reachability

The Reachability thresholds configure the reachability parameters for network adapters (ports and interfaces). They also control the analysis of systems that repeatedly restart, triggering Repeated Restarts and Flapping events. The following parameters are included in the Reachability Settings threshold category.

Restart Trap Threshold

The number of SNMP cold or warm start traps that must be received within the amount of time set by the Restart trap window parameter for LMS to consider a system to be performing excessive restarts. A value of 0 disables restart analysis. For more information, see How LMS Troubleshooting Calculates Repeated Restarts and Flapping

Note

If you want cold and warm start traps to generate events to be displayed immediately in the Alerts and Activities display, set the value of Restart trap threshold to 1.

Restart Trap Window

The amount of time used to monitor repeated restarts of a system. If the number of start traps meets or exceeds the Restart trap threshold during this window of time, the system is considered to be performing excessive restarts.

The minimum value is 30 seconds, and the maximum value is 3600 seconds.
## Threshold Parameter Values and Events

Table 2-2 lists threshold categories, the threshold parameters in each category, minimum, maximum, and default values for the threshold parameters, and the events that LMS generates when values pass the threshold.

### Note
Most thresholds are upper thresholds, representing the highest acceptable value. Lower thresholds are the exception and are footnoted as such.

<table>
<thead>
<tr>
<th>Threshold Category</th>
<th>Applicable Threshold Parameters (with unit of measure)</th>
<th>Values</th>
<th>Events Generated after Value Passes Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Min</td>
<td>Max</td>
</tr>
<tr>
<td>Backup Interface Support</td>
<td>Maximum uptime (seconds)</td>
<td>0</td>
<td>86400</td>
</tr>
<tr>
<td>Dial-on-Demand</td>
<td>Maximum uptime (seconds)</td>
<td>0</td>
<td>86400</td>
</tr>
<tr>
<td>Environment</td>
<td>Relative temperature threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Relative voltage threshold (%)</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Generic Interface/Port Performance</td>
<td>Broadcast threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Collision threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Discard threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Error threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Error traffic threshold (%)</td>
<td>0.00</td>
<td>100.00</td>
</tr>
<tr>
<td></td>
<td>Queue drop threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Utilization threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>Interface/Port Flapping</td>
<td>Link trap threshold (count)</td>
<td>0</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>Link trap window (seconds)</td>
<td>30</td>
<td>3600</td>
</tr>
<tr>
<td>Processor and Memory</td>
<td>Backplane utilization threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Free memory threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Memory buffer miss threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Memory buffer utilization threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Memory fragmentation threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Processor utilization threshold (%)</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>Reachability</td>
<td>Restart trap threshold (count)</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Restart trap window (seconds)</td>
<td>30</td>
<td>3600</td>
</tr>
</tbody>
</table>

1. Lower threshold—event is generated when the parameter value is lower than the value you set for it.

### Note
The Utilization threshold is 65% for 10MB-100MB Ethernet sub-group of Trunk Port Groups.
For additional information, see the following topics:

- Threshold Categories for Devices, Interfaces, and Ports
- Threshold Definitions

## Setting Up Performance Thresholds

This section explains how to configure and manage thresholds for a MIB variable. It contains:

- Creating a Threshold
- Editing a Threshold
- Deleting a Threshold
- Filtering Thresholds
- Viewing Threshold Configuration Details

Threshold rule can be set for only one MIB variable at a time and you can set many thresholds for each MIB variable. You can set threshold rules for all the MIB variables on a device selected for polling.

Cisco Prime LMS compares this threshold rule with the polled data. If the threshold rule is violated for a consecutive number of times, LMS generates an alert. This condition is called threshold violation.

Cisco Prime LMS allows you to use user-defined external commands or scripts. These external commands or scripts are run whenever there is a threshold violation. Cisco Prime LMS does not track the results generated from the user-defined external commands or scripts.

You can also configure LMS to send alert notifications as an e-mail, a trap or a syslog.

From the Threshold Setup page, you can create a threshold for a MIB variable, modify the threshold set for a MIB variable and delete the threshold.

To access the Threshold Setup page, select **Monitor > Threshold Settings > Performance** from the menu. The List of Thresholds dialog box appears.

Table 2-3 describes the fields and buttons in the List of Thresholds dialog box.

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold Name</td>
<td>Configured threshold. For example, CPU Threshold.</td>
</tr>
<tr>
<td></td>
<td>Click on the Name hyperlink to view the details of the threshold created.</td>
</tr>
<tr>
<td>No. of Devices</td>
<td>Number of devices associated with the threshold.</td>
</tr>
<tr>
<td>Variable</td>
<td>MIB variable associated with the threshold. For example, cpmCPUTotal5minRev</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition applied for monitoring threshold violation. For example, &gt;=</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the threshold value.</td>
</tr>
<tr>
<td>Violation Count</td>
<td>Configured violation count. An alert is triggered if the specified violation count matches with the actual number of violations.</td>
</tr>
</tbody>
</table>
Table 2-3  List of Thresholds Fields and Buttons (continued)

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Severity level of the threshold violation. For example, Critical, Medium, Low. Severity is a user preference set based on the threshold requirement.</td>
</tr>
<tr>
<td>Script</td>
<td>Displays the user-defined external command or script.</td>
</tr>
<tr>
<td>E-Mail ID</td>
<td>E-mail address to which alert notifications are sent when threshold violation occurs. You can enter multiple e-mail addresses separated by commas or semicolons.</td>
</tr>
<tr>
<td>Create (button)</td>
<td>Creates threshold for MIB variable. See Creating a Threshold.</td>
</tr>
<tr>
<td>Edit (button)</td>
<td>Modifies an existing threshold. See Editing a Threshold.</td>
</tr>
<tr>
<td>Delete (button)</td>
<td>Deletes an existing threshold. See Deleting a Threshold.</td>
</tr>
</tbody>
</table>
| Filter              | Select the filter criteria and enter the data. Use one of the following filter criteria and click Show:  
  - Threshold Name  
  - Variable Name  
  - Severity  
  - Violation Count  
  See Filtering Thresholds. |

You can perform the following tasks from the List of Thresholds dialog box:

- Creating a Threshold
- Editing a Threshold
- Deleting a Threshold
- Filtering Thresholds
- Viewing Threshold Configuration Details
Creating a Threshold

You can set and monitor the optimal value for a MIB variable by defining threshold rules. This is done by selecting a template, choosing an appropriate MIB variable, selecting MIB variable instances and applying a threshold criteria. You can configure the threshold criteria based on your requirement.

To create a threshold:

**Step 1**
Select Monitor > Threshold Settings > Performance from the menu.
The List of Thresholds dialog box appears.

**Step 2**
Click Create.
The Threshold Configuration dialog box appears.

Table 2-4 describes the fields in the Threshold Configuration dialog box.

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threshold Details</strong></td>
<td></td>
</tr>
<tr>
<td>Threshold Name</td>
<td>Enter a descriptive name for the threshold. The name must be unique. The name can contain a mix of alphabets, numerals, and some special characters (such as - _ . # @ $).</td>
</tr>
<tr>
<td>Template Name</td>
<td>Displays a list of System-defined and User-defined templates as a drop-down list. Select a template name from the drop-down list. For example, CPU Utilization.</td>
</tr>
</tbody>
</table>
| Variable Name | Displays a list of MIB variables polled using the template as a drop-down list. Select a MIB variable from the drop-down list. For example, cpmCPUTotal5min. For Device Availability and Interface Availability, only the following MIB variables are listed:  
- sysUpTime (for Device Availability)  
- ifOperStatus (for Interface Availability) |
| **Threshold Criteria** | |
| Condition | Displays a list of conditions (such as >=, <=, >, <, ==, !=). Select a condition for applying the threshold. The condition is applied to the value entered in the Value field. To set thresholds for device availability and interface availability, the condition must be specified as equals (==). |
Table 2-4  Threshold Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Enter the threshold value. This value acts as a benchmark to monitor the MIB variable. You will be notified if the polled data violates the condition set (such as $\geq$, $\leq$, $&gt;$, $&lt;$, $==$, $!=$) for the threshold value. If you have selected Device Availability template or Interface Availability template, then the following values are displayed in the Value drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• Device Availability</td>
</tr>
<tr>
<td></td>
<td>• Sys Down</td>
</tr>
<tr>
<td></td>
<td>• Sys Up</td>
</tr>
<tr>
<td></td>
<td>• Interface Availability</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
</tbody>
</table>
Setting Up Performance Thresholds

No. of Violations Enter a value to indicate the number of violations allowed before generating alerts. This can also be a fractional value.
Based on the value entered, an alert is triggered if the threshold value is violated for consecutive polling cycles.
If the threshold value is not violated during any one polling cycle, the No. of Violations count is reset to zero.
The following example shows you what happens when the threshold violation alert is triggered and the value is reset.
Set the following Threshold Criteria to monitor the CPU Utilization:
- Condition: >=
- Value: 70%
- No. of Violations: 3

Case 1:
Assume that these are the CPU Utilization values:
- During first polling cycle — 72%
- During second polling cycle — 75%
- During third polling cycle — 74%
In this case, the threshold value is violated consecutively for three polling cycles. Hence, an alert is triggered when the threshold value is violated on the third polling cycle.

Case 2:
Assume that these are the CPU Utilization values:
- During first polling cycle — 72%
- During second polling cycle — 75%
- During third polling cycle — 68%
In this case, the threshold value is not violated consecutively for three polling cycles. Hence, the No. of Violation count is reset to zero.

Severity Select any of the following applicable severities from the drop-down list:
- Critical
- Medium
- Low
Severity is a user preference set based on the threshold requirement.

Table 2-4 Threshold Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| No. of Violations| Enter a value to indicate the number of violations allowed before generating alerts. This can also be a fractional value. Based on the value entered, an alert is triggered if the threshold value is violated for consecutive polling cycles. If the threshold value is not violated during any one polling cycle, the No. of Violations count is reset to zero. The following example shows you what happens when the threshold violation alert is triggered and the value is reset. Set the following Threshold Criteria to monitor the CPU Utilization: • Condition: >= • Value: 70% • No. of Violations: 3 Case 1: Assume that these are the CPU Utilization values: • During first polling cycle — 72% • During second polling cycle — 75% • During third polling cycle — 74% In this case, the threshold value is violated consecutively for three polling cycles. Hence, an alert is triggered when the threshold value is violated on the third polling cycle. Case 2: Assume that these are the CPU Utilization values: • During first polling cycle — 72% • During second polling cycle — 75% • During third polling cycle — 68% In this case, the threshold value is not violated consecutively for three polling cycles. Hence, the No. of Violation count is reset to zero. Severity Select any of the following applicable severities from the drop-down list: • Critical • Medium • Low Severity is a user preference set based on the threshold requirement.
### Setting Up Performance Thresholds

#### Execute Script
Select the Execute Script check box. Use the Browse button to select a user-defined external command or script. This external command or script is executed when threshold violation occurs. You are allowed to select user-defined external command or a script only from the following directory paths:
- In Windows, `${NMSROOT}\hum\thresholdscript`
- In Solaris or Soft Appliance, `${NMSROOT}/hum/thresholdscript`

$NMSROOT$ is the default LMS installation directory.

#### Notification Details

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send E-Mail to</td>
<td>Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: <a href="mailto:user@domain.com">user@domain.com</a>. You can enter multiple e-mail addresses, separated by commas or semicolons.</td>
</tr>
<tr>
<td>Send Trap to</td>
<td>Check the check box to send Traps to the Trap Receiver Group when a threshold violation occurs. Select the Trap Receiver Group from the drop-down list. LMS uses CISCO-EPM-NOTIFICATION-MIB trap message format to generate SNMP traps when an alert occurs. For more information, see Notification MIB. This field is optional.</td>
</tr>
<tr>
<td>Send Syslog to</td>
<td>Check this check box to send Syslog information to Syslog Receiver Group when a threshold violation occurs. Select the Syslog Receiver Group from the drop-down list. This field is optional.</td>
</tr>
</tbody>
</table>
| Severity             | Select any of the following applicable severities for the Syslog information, from the drop down list:  
  - Emergency: Signifies that the system is unusable.  
  - Alert: Signifies that an action must be taken immediately.  
  - Critical: Signifies that the condition is critical.  
  - Error: Signifies an error condition.  
  - Warning: Signifies warning conditions.  
  - Notice: Signifies that there is a normal but important condition.  
  - Informational: Signifies information messages.  
  - Debug: Signifies debug-level messages. |

#### Select Instances or Groups

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Selector</td>
<td>Select one or more instances from the Instances listed in the tree. You can do basic and advanced search of instances in the Instance selector.</td>
</tr>
<tr>
<td>Port Group Selector</td>
<td>Select the desired port groups from the group selector. To set threshold for a port group, a poller should be created with the port group.</td>
</tr>
</tbody>
</table>

### Table 2-4 Threshold Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
</table>
Table 2-4  Threshold Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Group Selector</td>
<td>Select the desired device groups from the group selector.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To set threshold for a device group, a poller should be created with the device group.</td>
</tr>
<tr>
<td>Instance Selector</td>
<td></td>
</tr>
<tr>
<td>Search Input</td>
<td>Enter your search expression in this field. You can enter the instance name. You can enter only instance name and not device name for the search input.</td>
</tr>
<tr>
<td>All</td>
<td>Click <strong>All</strong> to view all the device instances for the selected MIB variable. Check the check boxes to select the instances.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays all your Simple or Advanced search results and you can select all instances, clear all instances, or select a few instances from the list.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the instances that you have selected in the All or Search Results tab or through a combination of both. You can also use this tab to deselect the instances you have already selected.</td>
</tr>
<tr>
<td>Create (button)</td>
<td>Creates the threshold and resets the fields in the Threshold Configuration dialog box to add a new threshold.</td>
</tr>
<tr>
<td>Cancel (button)</td>
<td>Cancels the creation of threshold.</td>
</tr>
</tbody>
</table>

Step 3  Go to the Threshold Details pane.
Step 4  Enter a descriptive name for the Threshold. For example, CPU Threshold.
Step 5  Select a template from the drop-down list.
        The drop-down list shows a list of all the System-defined and User-defined templates.
        If you have selected Port Groups, only the interface-related templates will be displayed.
Step 6  Select a MIB variable from the drop-down list.
        The drop-down list shows a list of MIB variables polled using the selected template. For example, cpmCPUTotal5minRev.
        The selected MIB variable displays all the polled device instances in the Instance Selector pane.
Step 7  Select one of the following radio buttons:
        • Instance Selector
        • Port Group Selector
        • Device Group Selector
        If you have selected Instance Selector, select the required instances from the instance tree.
        If you have selected Port Group Selector, select the required port groups.
        If you have selected Device Group Selector, select the required device groups.
Step 8  Go to the Threshold Criteria pane.
Step 9  Select a condition from the drop-down list.
        The condition is set based on the threshold value entered in the Value field.
To know the device availability and interface availability, you must select the condition as equals (==).

**Step 10** Enter the threshold value in the Value field.

If you have selected the template name as Device Availability or Interface Availability, then the following values are displayed in the Value drop-down list:

- For Device Availability
  - Sys Down
  - Sys Up
- For Interface Availability
  - Down
  - Up

**Step 11** Enter a value in the No. of Violations field.

This value indicates the number of violations permitted during consecutive polling cycles. Based on the value entered, an alert is triggered if the threshold value is violated for consecutive polling cycles.

If the threshold value is not violated during any one polling cycle, the No. of Violations count is reset to zero.

**Step 12** Select a severity from the Severity drop-down list. For example, Critical, Medium or Low.

**Step 13** Click Browse.

The Server Side File Browser dialog box appears, prompting you to locate the external command or script from the directory path where LMS is installed.

You are allowed to select an external command or script only from the following directory paths:

- In Windows, $NMSROOT\hum\thresholdscript
- In Solaris or Soft Appliance, $NMSROOT/thresholdscript

$NMSROOT is the default LMS Installation directory. If you try to access any other directory path, an appropriate error message is displayed.

Table 2-5 describes the fields in the Server Side File Browser dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Displays the directory path to locate the external command or script.</td>
</tr>
<tr>
<td>Directory Content</td>
<td>Displays the files and folders within the directory path.</td>
</tr>
</tbody>
</table>

**Step 14** Locate the external command or script and click OK.

The script should be of an extension .bat for Windows and .sh for Solaris or Soft Appliance, and should have proper executable permissions.

LMS executes the script when threshold violation occurs.

The following environmental variables are passed to the script:

- **Threshold Name**—Name of the threshold set for a MIB variable. Environmental variable key passed to the script: `ThresholdName`.
- **Device Name**—Name of the device for which the threshold violation occurred. Environmental variable key passed to the script: `DeviceName`. 

• MIB Variable Name—Name of the MIB variable which violated the threshold.
  Environmental variable key passed to the script: MibVarName.
• Instance Name—Name of the device instance for which the threshold violation occurred.
  For example, CPU of Switching Processor. Environmental variable key passed to the script: InstanceName.
• Configured Value—Value set for monitoring threshold violation.
  Environmental variable key passed to the script: ConfiguredValue.
• Breach Value—Actual value of threshold violation.
  Environmental variable key passed to the script: BreachValue.
• Number of Violations—Number of consecutive threshold violations occurred.
  Environmental variable key passed to the script: NoOfOccurrences.
• Severity—Severity of the threshold such as Critical, Medium, Low.
  Environmental variable key passed to the script: Severity.
• Date and Time—Date and time at which the threshold violation occurred.
  Environmental variable key passed to the script: TimeOfOccurance.

LMS does not track the results generated from the user-defined external command or script.

Step 15  Select the Notify Me check box and enter the e-mail address in the E-mail ID field to receive E-mail notifications of threshold violation.

  The E-mail address must be in the format: user@domain.com.

  The E-mail ID field supports multiple e-mail addresses, separated by commas or semicolons.

Step 16  Select the Send Trap check box to send Trap information when any threshold violation has occurred.

Step 17  Select the Trap Receiver Group from the drop-down list.

Step 18  Select the Send Syslog check box to send Syslog information to Syslog Receiver Group when any threshold violation has occurred.

Step 19  Select the Syslog Receiver Group from the drop-down list.

Step 20  Click Create to add the threshold.

  A message appears, confirming that threshold is added successfully.

Step 21  Click OK.

  The Threshold Configuration dialog box appears, allowing you to create more thresholds.

  Or

  Click Cancel to cancel the threshold creation process.

  The created threshold is listed in the List of Thresholds dialog box.
## Editing a Threshold

You can modify the threshold criteria of an existing threshold using the Edit button. You can only make changes to the threshold criteria and the selection of instances. You cannot make changes to the threshold details (Threshold Name, Template Name, Variable Name).

You can edit only one threshold at a time. If you select multiple thresholds using the check box, the Edit button is disabled.

To edit a threshold:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select <strong>Monitor &gt; Threshold Settings &gt; Performance</strong> from the menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The List of Thresholds dialog box appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the threshold by checking the corresponding check box.</td>
</tr>
<tr>
<td></td>
<td>If you select multiple thresholds, the Edit button is disabled.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td>The Threshold Configuration dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>See <a href="#creating-a-threshold">Creating a Threshold</a> for the description of the fields that appear in the Threshold Configuration dialog box.</td>
</tr>
<tr>
<td></td>
<td>You cannot select a different data source while editing thresholds. However, you can modify the same data source.</td>
</tr>
<tr>
<td></td>
<td>For example, if you have selected Instance Selector while creating thresholds, you can add or delete instances. You cannot select other data sources from Device Group Selector or Port Group Selector.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Make the necessary changes to the Select Instances and Threshold Criteria panes.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Update</strong>.</td>
</tr>
<tr>
<td></td>
<td>A message appears, confirming that the threshold is updated successfully.</td>
</tr>
<tr>
<td></td>
<td>The updated threshold is listed in the List of Thresholds dialog box.</td>
</tr>
</tbody>
</table>

## Deleting a Threshold

LMS allows you to delete thresholds using the Delete button. You are allowed to delete only one threshold at a time.

Before a threshold is deleted, you are prompted to confirm the deletion because you cannot restore a threshold that you have deleted from the database.

To delete a threshold:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select <strong>Monitor &gt; Threshold Settings &gt; Performance</strong> from the menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The List of Thresholds dialog box appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the threshold by checking the corresponding check box.</td>
</tr>
</tbody>
</table>
Step 3  Click **Delete**.

A message appears, prompting you to confirm the deletion.

Step 4  Click **OK** to delete the threshold or **Cancel** to cancel the operation.

If you choose to click **OK**, a message appears that the threshold is deleted successfully.

The List of Thresholds dialog box appears.

---

**Filtering Thresholds**

This section describes how you can use the filter option to display the threshold information based on a specific criteria.

To filter threshold information:

**Step 1**  Select **Monitor > Threshold Settings > Performance** from the menu.

The List of Thresholds dialog box appears.

**Step 2**  Select a criteria for filtering from the drop-down list.

**Step 3**  Enter the data to be filtered in the text field.

**Table 2-10** describes the methods you can follow to filter the data.

**Step 4**  Click **Show**.

The List of Thresholds dialog box appears, displaying the threshold information based on the filter criteria.

**Table 2-10** describes the criteria available to filter.

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
</table>
| Threshold Name      | Select **Threshold Name** and enter the data. You can use any of the following methods to filter by entering:  
|                     | • Complete threshold name  
|                     | • Any three consecutive characters of the threshold name  
|                     | • Any wildcard characters of the threshold name (such as *a, a*, *a*)  |
| Variable Name       | Select **Variable Name** and enter the data. You can use any of the following methods to filter by entering:  
|                     | • Complete MIB variable name  
|                     | • Any three consecutive characters of the MIB variable name  |
| Severity            | Select **Severity** and enter the severity as Critical, Medium, or Low.    |
| Violation Count     | Select **Violation Count** and enter the violation count numeric value.   |
Viewing Threshold Configuration Details

You can view the threshold configuration details listed for each device, in a tabular format.

To view a threshold configuration:

**Step 1**
Select **Monitor > Threshold Settings > Performance** from the menu.

The List of Thresholds dialog box appears.

**Step 2**
Click on the threshold name link.

The Threshold View page appears, displaying the threshold configuration details.

Table 2-7 describes the fields in the Threshold View page.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td>Displays the list of instances selected for the device.</td>
</tr>
<tr>
<td>Go to Device</td>
<td>Select a device name from the drop-down list. The threshold configuration details for the selected device is displayed.</td>
</tr>
<tr>
<td>Export</td>
<td>Click the Export icon to export threshold configuration details to a file of CSV or PDF format.</td>
</tr>
<tr>
<td>Print</td>
<td>View the threshold configuration details in a printer-friendly format.</td>
</tr>
</tbody>
</table>

TrendWatch Setup

This section explains how to configure and manage a TrendWatch for a MIB variable.

This section also explains:
- Creating a TrendWatch
- Editing a TrendWatch
- Deleting a TrendWatch
- Deactivating a TrendWatch
- Activating a TrendWatch
- Copying a TrendWatch
- Filtering TrendWatch

The TrendWatch feature ensures that the capacity, performance, and utilization of critical resource remains within the defined service level.

You can configure TrendWatch through LMS, by setting up rules for each MIB-variable or thresholds for a specific time period. TrendWatch will be scheduled (Immediate, Once, Daily, Weekly, and Monthly) as a job. You can configure it to send alert notifications through e-mail, trap or Syslog.
TrendWatch allows you to continuously monitor a value over time, sampling the value at periodic intervals to view the trends. You can watch variable trends in days, weeks, months and years. You can identify trends that develop over time and take appropriate actions.

TrendWatch does not monitor real-time data. It is calculated on past or historical data.

You can create TrendWatch reports either for thresholds that are changed or for devices from the Report Management page. For Threshold-based TrendWatches, all the instances selected in the threshold, apply to a particular TrendWatch.

The TrendWatch rule can be set for only one MIB variable at a time and you can set many TrendWatches for each MIB variable. You can set TrendWatch rules for all MIB variables on a device that is selected for polling.

LMS compares the TrendWatch rule with the polled data. If the TrendWatch rule is violated, LMS generates an alert. This condition is called TrendWatch violation.

You can create a TrendWatch for a MIB variable, based on a template or on a threshold. The TrendWatch Setup page allows you to create, modify, or delete a TrendWatch.

To access the TrendWatch Setup page, select Monitor > Threshold Settings > TrendWatch. The List of TrendWatches page appears.
Table 2-8 describes the fields and buttons in the List of TrendWatches page.

### Table 2-8  List of TrendWatch Fields and Buttons

<table>
<thead>
<tr>
<th>Field / Button Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrendWatch Name</td>
<td>Displays the TrendWatch name. For example, CPU TrendWatch. Click on the Name hyperlink to view the details of the TrendWatch created.</td>
</tr>
<tr>
<td>No. of Devices</td>
<td>Number of devices associated with the TrendWatch.</td>
</tr>
</tbody>
</table>
| Status              | Status of a TrendWatch. The following TrendWatch status is displayed:  
  • Active—LMS is currently querying for device instances.  
  • Inactive—LMS has stopped querying for device instances. |
| Variable            | MIB variable associated with the TrendWatch. For example, cpmCPUTotal5minRev |
| Severity            | Severity level of the TrendWatch violation. For example, Critical, Medium, Low  
  Severity is a user preference set based on the TrendWatch requirement. |
| E-Mail ID           | E-mail address to which alert notifications are sent when TrendWatch violation occurs. |
| Create (button)     | Creates a TrendWatch. See Creating a TrendWatch. |
| Edit (button)       | Modifies an existing TrendWatch. See Editing a TrendWatch. |
| Delete (button)     | Deletes an existing TrendWatch. See Deleting a TrendWatch. |
| Activate (button)   | Activates an inactive TrendWatch to monitor device instances. See Activating a TrendWatch. |
| De-activate (button)| Stops a TrendWatch from monitoring device instances. See Deactivating a TrendWatch. |
| Copy (button)       | Creates a TrendWatch from an existing TrendWatch. See Copying a TrendWatch. |
| Filter              | Select the filter criteria and enter the data. Use one of the following filter criteria and click Show:  
  • TrendWatch Name  
  • Variable Name  
  • Severity  
  See Filtering TrendWatch. |
| Show (button)       | Shows the TrendWatches based on filter criteria |
You can perform the following tasks from the List of TrendWatches page:

- Creating a TrendWatch
- Editing a TrendWatch
- Deleting a TrendWatch
- Deactivating a TrendWatch
- Activating a TrendWatch
- Copying a TrendWatch
- Filtering TrendWatch

## Creating a TrendWatch

You can configure a TrendWatch for a MIB variable by defining rules, so that you can monitor the trend for a given period of time and keep the values within the defined service level.

You can configure the TrendWatch criteria based on your requirement. You can create TrendWatches based on:

- Templates
- Thresholds

This section contains:

- Creating a TrendWatch Based on Templates
- Creating a TrendWatch Based on Threshold

## Creating a TrendWatch Based on Templates

You can create TrendWatch rules on a MIB variable to monitor the devices for TrendWatches. Some examples of TrendWatch rules are:

- When the average weekly CPU or interface utilization goes up or down relative to previous week by \( n\% \).
- When the device or interface availability over a period is less than \( n\% \).
- When the average utilization of the interface is above \( n\% \).
- When the availability was used down for \( N \) minutes, more than \( X \) times in a week/month/quarter
- When the minimum value is less than \( N \) for \( X \) times over a period of \( Y \) weeks
- When \( n \) percentage of times the utilization is greater than \( x \) percentage.
To create a TrendWatch based on template:

**Step 1**  
Select **Monitor > Threshold Settings > TrendWatch** from the menu.  
The List of TrendWatches page appears.

**Step 2**  
Click **Create**.  
The TrendWatch Configuration dialog box appears.

*Table 2-9* describes the fields in the TrendWatch Configuration dialog box.

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TrendWatch Details</strong></td>
<td></td>
</tr>
<tr>
<td>TrendWatch Name</td>
<td>Enter a descriptive name for the TrendWatch. The name must be unique. It should not be the same as any existing report name. The name can contain a mix of alphabets, numerals, and some special characters (such as - _ . ).</td>
</tr>
<tr>
<td>Based on</td>
<td>Select either <strong>Template</strong> or <strong>Threshold</strong> to configure TrendWatch depending on your requirement. Based on your selection either a list of templates or thresholds configured is listed. The Template Name, Variable Name, and TrendWatch Conditions will be disabled if you select the Threshold-based TrendWatch. The condition, value and instances will be obtained from the threshold definition.</td>
</tr>
<tr>
<td>Template Name</td>
<td>Displays a list of System-defined and User-defined templates that are being polled by the historic pollers, as a drop-down list. Select a template name from the drop-down list. For example, CPU Utilization. This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch. If you have selected Port Group selector, the interface related templates will be listed.</td>
</tr>
</tbody>
</table>
| Variable Name | Displays a list of MIB variables being polled using the template, as a drop-down list. Select a MIB variable from the drop-down list. For example, `cpmCPU/Total5min`. For Device Availability and Interface Availability, only the following MIB variables are listed:  
- sysUpTime (for Device Availability)  
- ifOperStatus (for Interface Availability)  
This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch. |
### TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Severity</strong></td>
<td>Select any of the following applicable severities from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>- Critical</td>
</tr>
<tr>
<td></td>
<td>- Medium</td>
</tr>
<tr>
<td></td>
<td>- Low</td>
</tr>
<tr>
<td></td>
<td>Severity is set based on your TrendWatch requirement.</td>
</tr>
<tr>
<td></td>
<td>If you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch, then the Threshold severity will be listed in the drop-down list.</td>
</tr>
</tbody>
</table>

### Select Instances or Groups

<table>
<thead>
<tr>
<th>Instance Selector</th>
<th>Select one or more instances from the Instances listed in the tree.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can do basic and advanced search of devices in the Instance selector.</td>
</tr>
<tr>
<td>Port Group Selector</td>
<td>Select the desired port groups from the group selector.</td>
</tr>
<tr>
<td>Device Group Selector</td>
<td>Select the desired device groups from the group selector.</td>
</tr>
</tbody>
</table>

### Instance Selector

<table>
<thead>
<tr>
<th>Search Input</th>
<th>Enter your search expression in this field.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can enter only instance name and not device name for the search input.</td>
</tr>
<tr>
<td>All</td>
<td>Click <strong>All</strong> to view all the device instances for the selected MIB variable. Check the check boxes to select the instances.</td>
</tr>
<tr>
<td>Search Results</td>
<td>Displays all your Simple or Advanced search results. You can select all instances, clear all instances, or select a few instances from this list.</td>
</tr>
<tr>
<td></td>
<td>Advanced search is applicable only if you select to create TrendWatch based on templates.</td>
</tr>
<tr>
<td>Selection</td>
<td>Lists all the instances that you have selected in the All or Search Results tab or a combination of both. You can also use the instance tree to</td>
</tr>
<tr>
<td></td>
<td>deselect the instances you have already selected. The Select Instance tree will list only the devices being polled for the MIB variable selected</td>
</tr>
<tr>
<td></td>
<td>in the Variable Name drop-down list.</td>
</tr>
<tr>
<td></td>
<td>This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch.</td>
</tr>
<tr>
<td>Condition</td>
<td>Displays a list of conditions (such as &gt;=, &lt;=, &gt;, &lt;, ==, !=, Relatively Up, Relatively Down). Select a condition for applying the TrendWatch.</td>
</tr>
<tr>
<td></td>
<td>The default is None.</td>
</tr>
<tr>
<td></td>
<td>The condition is applied to the value entered in the Value field.</td>
</tr>
<tr>
<td></td>
<td>This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch.</td>
</tr>
</tbody>
</table>
Value

Enter the TrendWatch value. This value acts as a benchmark to monitor the MIB variable. You will be notified if the polled data violates the condition set (such as $\geq$, $\leq$, $>$, $<$, $==$, $!=$, Relatively Up, Relatively Down)) for the TrendWatch value.

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.

### Table 2-9 TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
<td>Enter the TrendWatch value. This value acts as a benchmark to monitor the MIB variable. You will be notified if the polled data violates the condition set (such as $\geq$, $\leq$, $&gt;$, $&lt;$, $==$, $!=$, Relatively Up, Relatively Down)) for the TrendWatch value. This field is disabled if you have selected <strong>Threshold</strong> to configure Threshold based TrendWatch.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>TrendWatch Conditions</strong></th>
<th>Displays a list of Group By types (such as Hourly, Daily, Weekly, Monthly and Quarterly) to perform TrendWatch. Select any one of the following Group By types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group By</strong></td>
<td>None—Displayed by default. Hourly—Monitors the MIB variable based on the condition on an hourly basis. Daily—Monitors the MIB variable based on the condition on a daily basis. Weekly—Monitors the MIB variable based on the condition on a weekly basis. Monthly—Monitors the MIB variable based on the condition on a monthly basis. Quarterly—Monitors the MIB variable based on the condition on a quarterly basis. Yearly—Monitors the MIB variable based on the condition on a yearly basis.</td>
</tr>
</tbody>
</table>

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.
### TrendWatch Setup

**Aggregate**
Displays a list of values (such as Min, Max, Avg, Std Deviation). Select a value to evaluate the variable for a condition.

Select any one of the following Aggregate types:
- None—Displayed by default.
- Average—Average of polled value. For example, average value per hour.
- Minimum—Minimum of polled value. For example, minimum value per hour.
- Maximum—Maximum of polled value. For example, maximum value per hour.
- Std Deviation—Standard deviation of polled value. For example, standard deviation of the values per hour.

If you have selected Device Availability template or Interface Availability template, then only Average will be listed in the drop-down list and it will be selected by default.

This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch.

**Trend**

**Occurred**
Specify how many times the TrendWatch violation has occurred.

Enter a value in the text field, select either At least, Exactly, or Almost from the drop-down list, and select a time frame of your trend watch.

Select the time frame as **Times** or **Percentage of Times** from the drop-down list.

**Last**
Click the Last radio button to monitor whether the trend has occurred in the last *n* days or weeks, or months, or years.

Enter a value in the text field and select a time frame for the TrendWatch.

- Days—Specify the trend occurrence date interval
- Weeks—Specify the trend occurrence Week interval
- Months—Specify the trend occurrence Month interval
- Years—Specify the trend occurrence Years interval

For example, 5 Days, 2 Weeks, 3 Months, 1 Year

This field is disabled if you have selected the **From** radio button.

**From**
Click the From radio button to generate whether the trend has occurred in the specified date and time.

Specify the start date and time that the TrendWatch condition has occurred.

Select the date by clicking it in the Calendar icon; select the time from the drop-down list.

The From date must be earlier than the current date.

### Table 2-9 TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| Aggregate      | Displays a list of values (such as Min, Max, Avg, Std Deviation). Select a value to evaluate the variable for a condition. Select any one of the following Aggregate types:  
- None—Displayed by default.  
- Average—Average of polled value. For example, average value per hour.  
- Minimum—Minimum of polled value. For example, minimum value per hour.  
- Maximum—Maximum of polled value. For example, maximum value per hour.  
- Std Deviation—Standard deviation of polled value. For example, standard deviation of the values per hour.  
If you have selected Device Availability template or Interface Availability template, then only Average will be listed in the drop-down list and it will be selected by default. This field is disabled if you have selected **Threshold** to configure Threshold based TrendWatch. |
| Occurred       | Specify how many times the TrendWatch violation has occurred. Enter a value in the text field, select either At least, Exactly, or Almost from the drop-down list, and select a time frame of your trend watch. Select the time frame as **Times** or **Percentage of Times** from the drop-down list. |
| Last           | Click the Last radio button to monitor whether the trend has occurred in the last *n* days or weeks, or months, or years. Enter a value in the text field and select a time frame for the TrendWatch.  
- Days—Specify the trend occurrence date interval  
- Weeks—Specify the trend occurrence Week interval  
- Months—Specify the trend occurrence Month interval  
- Years—Specify the trend occurrence Years interval  
For example, 5 Days, 2 Weeks, 3 Months, 1 Year  
This field is disabled if you have selected the **From** radio button. |
| From           | Click the From radio button to generate whether the trend has occurred in the specified date and time. Specify the start date and time that the TrendWatch condition has occurred. Select the date by clicking it in the Calendar icon; select the time from the drop-down list. The From date must be earlier than the current date. |
### Table 2-9  TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>Specify the end date and time that the TrendWatch condition has occurred. Select the date by clicking it in the Calendar icon; select the time from the drop-down list. The To date must be later than the From date and earlier than the current date.</td>
</tr>
<tr>
<td>Show Rule</td>
<td>Click <strong>Show Rule</strong> to view the created TrendWatch rule. The created TrendWatch rule is displayed in the message box.</td>
</tr>
</tbody>
</table>

**Notification Details**

<table>
<thead>
<tr>
<th>Send Email to</th>
<th>Check this check box for notification through e-mail. The e-mail will contain all the TrendWatch job details. In case of any violations, violation details will be added to the TrendWatch details. Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: <code>user@domain.com</code> You can enter multiple e-mail addresses, separated by commas or semicolons. This field is optional.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach Report</td>
<td>Check this check box to attach a CSV report to the e-mail. By default, a CSV file is sent as an attachment to the e-mail ID specified. If you check Add Full Report check box, instead of CSV, a PDF format of the report will be sent as an attachment to the specified e-mail id. You need to enable the E-mail Attachment check box and specify the Maximum Attachment size in the System Preferences dialog box (<strong>Admin &gt; System &gt; System Preferences</strong>) to send the report as an E-mail. If the file size exceeds the Maximum Attachment size, the URL link of the report is sent as an e-mail. You can click the URL link to view the report.</td>
</tr>
<tr>
<td>Send Trap to</td>
<td>Check this check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list. LMS uses CISCO-EPM-NOTIFICATION-MIB trap message format to generate SNMP traps when an alert occurs. For more information, see <strong>Notification MIB</strong>. This field is optional.</td>
</tr>
<tr>
<td>Send Syslog to</td>
<td>Check this check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list. This field is optional.</td>
</tr>
</tbody>
</table>
### TrendWatch Setup

#### Severity
Select any of the following applicable severities for the Syslog information, from the drop down list:
- **Emergency**: Signifies that the system is unusable.
- **Alert**: Signifies that an action must be taken immediately.
- **Critical**: Signifies that the condition is critical.
- **Error**: Signifies an error condition.
- **Warning**: Signifies warning conditions.
- **Notice**: Signifies that there is a normal but important condition.
- **Informational**: Signifies information messages.
- **Debug**: Signifies debug-level messages.

#### Schedule Details

<table>
<thead>
<tr>
<th>Schedule Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Immediate</strong></td>
<td>TrendWatch is run immediately.</td>
</tr>
<tr>
<td><strong>Once</strong></td>
<td>TrendWatch is run only once for the set date and time.</td>
</tr>
<tr>
<td><strong>Daily</strong></td>
<td>TrendWatch is run daily at the scheduled time.</td>
</tr>
<tr>
<td><strong>Weekly</strong></td>
<td>TrendWatch is run weekly for the set date and time.</td>
</tr>
<tr>
<td><strong>Monthly</strong></td>
<td>TrendWatch is run monthly for the set date and time.</td>
</tr>
</tbody>
</table>

#### Start At
 Specify the date and time that the TrendWatch is scheduled for. The time should be later than the current time. This field is disabled if you have selected **Immediate** as the Schedule Type.

#### Report Information

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Publish Path</td>
<td>Browse and select the path to publish your report.</td>
</tr>
</tbody>
</table>
### TrendWatch Setup

#### Step 3
Go to the TrendWatch Details pane and enter a descriptive name for the TrendWatch. For example, CPU Threshold.

#### Step 4
Select **Template** from the Based On radio button to configure TrendWatch based on the template.

#### Step 5
Select a template from the Template Name drop-down list. The drop-down list shows all the System-defined and User-defined templates.

#### Step 6
Select a MIB variable from the Variable Name drop-down list. The drop-down list shows all the MIB variables associated with that template. For example, `cpmCPUPTotal5minRev`.

Based on the selected MIB variable, all the polled device instances are listed in the Select Instances pane.

#### Step 7
Select a severity from the Severity drop-down list. For example, Critical, Medium or Low.

#### Step 8
Select one of the following radio buttons:
- Instance Selector
- Port Group Selector
- Device Group Selector

If you have selected Instance Selector, select the required instances from the instance tree.

If you have selected Port Group Selector, select the required port groups.

If you have selected Device Group Selector, select the required device groups.

---

### Table 2-9  TrendWatch Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field / Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Full Report</td>
<td>Use the Add Full Report check box to create a PDF format of the report for all devices. If you check this check box along with Attach Report check box, a PDF format of the report will be sent as an attachment to the specified e-mail ID. If the file size exceeds the Maximum Attachment size, then a CSV file will only be sent as an attachment along with the URL link of the HTML report. You can download the PDF format of the report using the export option provided in the HTML report. The PDF format of the report takes longer time to generate as it includes the report for all the polled devices. Inventory &gt; Device Administration &gt; Add as Managed Devices. Scheduling PDF reports with large number of data on a daily basis results high CPU and memory usage. We recommend you to schedule PDF reports with less number of data at optimal time intervals.</td>
</tr>
<tr>
<td>Create (button)</td>
<td>Creates the TrendWatch and resets the fields in the TrendWatch Configuration dialog box to add a new TrendWatch.</td>
</tr>
<tr>
<td>Cancel (button)</td>
<td>Cancels the creation of TrendWatch.</td>
</tr>
</tbody>
</table>
Step 9  Go to the TrendWatch Conditions pane.
Here you can define the TrendWatch condition.
For example you can find out whether the TrendWatch violation occurrence for the CPU Utilization, has a daily average that is greater than 50% and it occurs at least 10% of times. This means, if the device is polled for 100 times and there are 10 violation, it is 10% of times

Step 10  Select Group By Value from the Group By drop-down list.
For example Hourly, Daily, Monthly, Quarterly, and Yearly.
The condition is set based on the TrendWatch value entered in the Value field.

Step 11  Select the Aggregate value from the Aggregate drop-down list.
If you have selected the template name as Device Availability or Interface Availability, then only Average will be listed in the drop down list and it will be selected by default.

Step 12  Select a condition from the Condition drop-down list.
The condition is set based on the TrendWatch value entered in the Value field.
For example, the hourly average of CPU Utilization is relatively up by 50%. This means that if the value for the current hourly average is 75% and the value for the last hourly average was 50%, then the hourly average of CPU Utilization has gone relatively up by 50%.

Step 13  Enter the TrendWatch value in the Value field.

Step 14  Go to the Trend pane and select At least, Exactly, or Atmost from the drop-down list.

Step 15  Enter the value in the text box and select the number of times or the percentage of times that the trend has occurred, from the drop-down list.

Step 16  Select Times or Percentage of Times from the drop-down list.
For example assume that you have configured a TrendWatch rule for last one day on an hourly basis. If the difference between two hours is greater than or equal to the set value then the trendwatch violation has occurred.

Step 17  Either:
  a. Select the Last radio button and enter the number in the text box,
  b. Select Days, Weeks, Months or Years from the drop-down list.
Or
  a. Select the From radio button and enter the date from the calendar
  b. Select the time from the drop-down list.
  c. Enter the To date from the calendar
  d. Select the time from the drop-down list.
For example, assume that you have configured a TrendWatch rule for an instance with the trend that occurs for at least five times in the past two weeks. If these criteria is not met, a TrendWatch violation has occurred and is stored in the database.

Step 18  Click Show Rule to view the created TrendWatch rule.
Step 19 Go to the Notification Details pane.
- Check the check box to send notification through e-mail. Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: user@domain.com. You can enter multiple e-mail addresses, separated by commas or semicolons.
- Check the Attach report check box to attach the report as a CSV file. This CSV file is sent to the e-mail address specified in the e-mail field.
- Check the check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list.
- Check the check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list.

Step 20 Go to the Schedule Details pane and select the Schedule type from the drop-down list.

Step 21 Specify the date and time the job is scheduled at. This field is disabled if you have selected Immediate as the Schedule Type.

Step 22 Go to Report Information pane and specify the path to publish the reports.

Step 23 Check the Add Full Report check box to create a PDF format of the report for all devices.

Step 24 Click Create to add the TrendWatch.
A message appears, confirming that TrendWatch is added successfully.

Step 25 Click OK.
The TrendWatch Configuration dialog box appears, allowing you to create more TrendWatches.
Or
Click Cancel to cancel the TrendWatch creation process.
The created TrendWatch is listed in the List of TrendWatches page.

Step 26 Click on the Name hyperlink to view the details of the TrendWatch created.

Creating a TrendWatch Based on Threshold

You can create TrendWatch rules on a threshold to monitor the devices for TrendWatches. An example of TrendWatch rules in this scenario is:
If the absolute value for CPU utilization is greater than $n\%$, for $x$ times in a week/month/year.

To create a TrendWatch based on threshold:

Step 1 Select Monitor > Threshold Settings > TrendWatch from the menu.
The List of TrendWatches page appears.

Step 2 Click Create.
The TrendWatch Configuration dialog box appears.
Table 2-9 describes the fields in the TrendWatch Configuration dialog box.

Step 3 Go to the TrendWatch Details pane and enter a descriptive name for the TrendWatch.
For example, CPU threshold.

Step 4 Select Threshold from the Based on Radio button to configure TrendWatch based on threshold.
Step 5 Go to the Select Thresholds pane and select the required threshold from the instance tree.

Step 6 Go to the Trend pane and select At least, Exactly or Atmost from the drop-down list.

Step 7 Enter a value in the text box.

Step 8 Select Times from the drop-down list.

This will be the only option available because you have selected Threshold to configure Threshold based TrendWatch.

Step 9 Either:

a. Select the Last radio button and enter the number in the text box,

b. Select Days, Weeks, Months or Years from the drop-down list.

Or

a. Select the From radio button and enter the date from the calendar.

b. Select the time from the drop-down list.

c. Enter the To date from the calendar.

d. Select the time from the drop-down list.

For example, assume that you have configured a TrendWatch rule for an instance with the trend that occurs for at least two times in the past one day. If this criteria is not met, a TrendWatch violation has occurred and is stored in the database.

Step 10 Click Show Rule to view the created TrendWatch rule.

Step 11 Go to the Notification Details pane.

- Check the check box to send alert notification through e-mail. Enter the e-mail address to which LMS sends alert messages. The e-mail address must be in the format: user@domain.com. You can enter multiple e-mail addresses, separated by commas or semicolons.

- Check the Attach report check box to attach the report as a CSV file. This CSV file is sent to the e-mail address specified in the e-mail field.

- Check the check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list.

- Check the check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list. Select the severity for the Syslog information from the Severity drop-down list.

Step 12 Go to the Schedule Details pane and select the Schedule type from the drop-down list.

Step 13 Specify the date and time the job is scheduled at.

Step 14 Go to Report Information pane and specify the path to publish the reports.

Step 15 Check the Add Full Report check box to create a PDF format of the report for all devices.

Step 16 Click Create to add the TrendWatch.

A message appears, confirming that TrendWatch is added successfully.
Step 17 Click OK. The TrendWatch Configuration dialog box appears, allowing you to create more TrendWatches. Or Click Cancel to cancel the TrendWatch creation process. The created TrendWatch is listed in the List of TrendWatches page.

Step 18 Click on any TrendWatch name link. The TrendWatch view appears, displaying the TrendWatch rule details.

Editing a TrendWatch

You can modify the TrendWatch criteria of an existing TrendWatch using the Edit button. You can only make changes to the Notification details, Schedule details and the selection of Thresholds for threshold based TrendWatch.

You cannot make changes to the TrendWatch details (TrendWatch Name, Template Name, Variable Name).

You can edit only one TrendWatch at a time. If you select multiple TrendWatches using the check box, the Edit button is disabled.

To edit a TrendWatch:

Step 1 Select Monitor > Threshold Settings > TrendWatch from the menu. The List of TrendWatches page appears.

Step 2 Select the TrendWatch by checking the corresponding check box. If you select multiple TrendWatches the Edit button is disabled.

Step 3 Click Edit. The TrendWatch Configuration dialog box appears. See Table 2-9 for the description of the fields that appear in the Template-based TrendWatch dialog box. You cannot select a different data source while editing trendwatch. However, you can modify the same data source.

For example, if you have selected Instance Selector while creating trendwatches, you can add or delete instances. You cannot select other data sources from Device Group Selector or Port Group Selector.

Step 4 Make the necessary changes to the Select Instances, Notification details and Schedule Details panes.

Note In the Schedule details pane, the Daily, Weekly and Monthly options are available for periodic reports.

Step 5 Click Update. A message appears, confirming that the TrendWatch is updated successfully. The updated TrendWatch is listed in the List of TrendWatches page.
Deleting a TrendWatch

LMS allows you to delete TrendWatches using the Delete button. Before a TrendWatch is deleted, you are prompted to confirm the deletion because you cannot restore a TrendWatch that you have deleted from the database.

Deleting a TrendWatch will delete the associated report and all its instances.

You can select multiple TrendWatches and delete them together.

To delete a TrendWatch:

---

**Step 1** Select Monitor > Threshold Settings > TrendWatch from the menu.

The List of TrendWatches page appears.

**Step 2** Select the TrendWatch by checking the corresponding check box.

**Step 3** Click Delete.

A message appears, prompting you to confirm the deletion.

**Step 4** Click OK to delete the TrendWatch or Cancel to cancel the operation.

If you choose to click OK, a message appears stating that the TrendWatch is deleted successfully.

Deactivating a TrendWatch

If you do not want the TrendWatch to monitor a (the polled) MIB variable, you can deactivate it using the De-activate button on the List of TrendWatches page.

For example, if there is an outage, you may not want notification e-mails for a particular period of time. In such instances you may choose to de-activate TrendWatches.

You can select multiple TrendWatches and deactivate them together.

To deactivate a TrendWatch:

---

**Step 1** Select Monitor > Threshold Settings > TrendWatch from the menu.

The List of TrendWatches page appears.

**Step 2** Select the TrendWatch to be deactivated by checking the check box.

**Step 3** Click De-activate.

A message appears, prompting you to confirm the deactivation.

**Step 4** Click OK to deactivate the TrendWatch.

Or

Click Cancel to cancel the operation.

If you click OK, a message appears that the TrendWatch is changed to an inactive state.

The List of TrendWatches page appears, displaying the status of the TrendWatch as Inactive.
Activating a TrendWatch

If you want an inactive TrendWatch to start monitoring a device for MIB variables, you can activate it using the Activate button on the List of TrendWatches page. You can select multiple TrendWatches and activate them together.

To activate a TrendWatch:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Monitor &gt; Threshold Settings &gt; TrendWatch</strong> from the menu. The List of TrendWatches page appears.</td>
</tr>
<tr>
<td>2</td>
<td>Select the TrendWatch to be activated by checking the appropriate check box.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Activate</strong>. A message appears, prompting you to confirm the activation.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>OK</strong> to activate the TrendWatch. Or Click <strong>Cancel</strong> to cancel the operation. If you click <strong>OK</strong>, a message appears that the TrendWatch is changed to an active state. The List of TrendWatches page appears, displaying the status of the TrendWatch as <strong>Active</strong>. If you activate a TrendWatch, the monitoring starts based on the schedule.</td>
</tr>
</tbody>
</table>

**Note**
If you have selected multiple trendWatches with a combination of Active and In-active trendwatches, then Activate and De-activate buttons will be disabled.

Copying a TrendWatch

You can create a copy of an existing TrendWatch by selecting a TrendWatch name and clicking the Copy option. For example, if you want to copy the same set of conditions for different set of devices or instances, you may choose to copy a TrendWatch.

To copy a TrendWatch:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select <strong>Monitor &gt; Threshold Settings &gt; TrendWatch</strong> from the menu. The List of TrendWatches page appears.</td>
</tr>
<tr>
<td>2</td>
<td>Check the check box corresponding to the TrendWatch name in the list.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Copy</strong>. The TrendWatch configuration dialog box appears, displaying the settings in the existing TrendWatch. <strong>Table 2-9</strong> describes the fields in the TrendWatch Configuration dialog box.</td>
</tr>
</tbody>
</table>
Step 4  Go to the TrendWatch Details pane and enter a descriptive name for the TrendWatch. For example, CPU Threshold.

The Template Name, Variable Name, Severity and TrendWatch conditions will be disabled when you configure a TrendWatch based on the threshold.

Step 5  Select a MIB variable from the Variable Name drop-down list.

The drop-down list shows a list of MIB variables polled using the selected template. For example, `cpmCPUTotal5minRev`.

The selected MIB variable displays all the polled device instances in the Select Instances pane.

Step 6  Modify the data source, if required.

Note  You cannot select a different data source while copying Trendwatch. However, you can modify the same data source. For example, if you have selected Instance Selector while creating Trendwatches, you can add or delete instances. You cannot select other data sources from Device Group Selector or Port Group Selector.

Step 7  Select a severity from the Severity drop-down list. For example, Critical, Medium or Low.

Step 8  Go to the TrendWatch Conditions pane and select the Group By value from the Group By drop-down list. For example Hourly, Daily, Monthly, Quarterly, and Yearly.

The condition is set, based on the TrendWatch value entered in the Value field.

Step 9  Select the Aggregate value from the Aggregate drop-down list.

Step 10  Select a condition from the Condition drop-down list.

The condition is set based on the TrendWatch value that you have entered in the Value field.

Step 11  Enter the TrendWatch value in the Value field.

Step 12  Go to the Trend pane, and enter the time period in the text field.

Step 13  Select Times or Percentage of Times from the drop-down list.

For example, assume that you have configured a TrendWatch rule for last one day on hourly basis. If the difference between two hours is greater than or equal to the set value then the TrendWatch rule is violated and will be stored in the database.

Step 14  Click Show Rule to view the created TrendWatch rule.

Step 15  Go to the Notification Details pane.

- Check the check box for alert notification through e-mail. Enter the e-mail address to which LMS sends alert messages.
- Check the Add Report check box to attach a PDF report with the e-mail notification.
- Check the check box to send Traps to the Trap Receiver Group when any TrendWatch violation has occurred. Select the Trap Receiver Group from the drop-down list.
- Check the check box to send Syslog information to Syslog Receiver Group when any TrendWatch violation has occurred. Select the Syslog Receiver Group from the drop-down list.

Step 16  Go to the Schedule Details pane and select the Schedule type from the drop-down list.

Step 17  Specify the date and time the job is scheduled at.

Step 18  Go to Report Information pane and specify the path to publish the reports.
Step 19 Check the Add Full Report check box to create a PDF format of the report for all devices.

Step 20 Click Create to add the TrendWatch.

A message appears, confirming that TrendWatch is added successfully.

Step 21 Click OK.

The TrendWatch Configuration dialog box appears, allowing you to create more TrendWatches.

Or

Click Cancel to cancel the TrendWatch creation process.

The created TrendWatch is listed in the List of TrendWatches page.

---

**Filtering TrendWatch**

This section describes how you can use the Filter option to display the TrendWatch information based on a specific criteria.

To filter TrendWatch information:

Step 1 Select **Monitor > Threshold Settings > TrendWatch** from the menu.

The List of TrendWatches page appears.

Step 2 Select a criteria for filtering from the drop-down list.

Step 3 Enter the data to be filtered in the text field.

*Table 2-10* describes the methods you can follow to filter the data.

Step 4 Click Show.

The List of TrendWatches page appears, displaying the TrendWatch information based on the filter criteria.
Table 2-10 describes the criteria available to filter.

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrendWatch Name</td>
<td>Select <strong>TrendWatch Name</strong> and enter the data. You can use any of the following filter methods by entering:</td>
</tr>
<tr>
<td></td>
<td>• Complete TrendWatch name</td>
</tr>
<tr>
<td></td>
<td>• Any three consecutive characters of the TrendWatch name</td>
</tr>
<tr>
<td></td>
<td>• Any wildcard characters of the TrendWatch name (such as <em>a, a</em>, <em>a</em>)</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Select <strong>Variable Name</strong> and enter the data. You can use any of the following methods to filter by entering:</td>
</tr>
<tr>
<td></td>
<td>• Complete MIB variable name</td>
</tr>
<tr>
<td></td>
<td>• Any three consecutive characters of the MIB variable name</td>
</tr>
<tr>
<td></td>
<td>• Any wildcard characters of the MIB variable name (such as <em>a, a</em>, <em>a</em>)</td>
</tr>
<tr>
<td>Severity</td>
<td>Select <strong>Severity</strong> and choose the severity as Critical, Medium, or Low.</td>
</tr>
<tr>
<td>Violation Count</td>
<td>Select <strong>Violation Count</strong> and enter the violation count in numeric value.</td>
</tr>
</tbody>
</table>