Using the HP Web Browser Interface

Contents

Overview ................................................................. 4-2
General Features ......................................................... 4-3
Starting an HP Web Browser Interface Session with the Switch . . 4-4
  Using a Standalone Web Browser in a PC or UNIX Workstation . . 4-4
  Using HP TopTools for Hubs & Switches ......................... 4-5
Tasks for Your First HP Web Browser Interface Session .......... 4-7
  Viewing the “First Time Install” Window ......................... 4-7
  Creating Usernames and Passwords in the Browser Interface ...... 4-8
  Online Help for the HP Web Browser Interface ................... 4-11
Support/Mgmt URLs Feature ........................................... 4-12
  Support URL .......................................................... 4-13
  Help and the Management Server URL ............................. 4-13
Status Reporting Features ............................................. 4-15
  The Overview Window ............................................... 4-15
  The Port Utilization and Status Displays ........................ 4-16
  The Alert Log ........................................................ 4-19
  The Status Bar ....................................................... 4-22
  Setting Fault Detection Policy .................................... 4-23
Overview

The HP web browser interface built into the switch lets you easily access the switch from a browser-based PC on your network. This lets you do the following:

- Optimize your network uptime by using the Alert Log and other diagnostic tools
- Make configuration changes to the switch
- Maintain security by configuring usernames and passwords

This chapter covers the following:

- General features (page 4-3).
- Starting a web browser interface session (page 4-4)
- Tasks for your first web browser interface session (page 4-7):
  - Creating usernames and passwords in the web browser interface (page 4-8)
  - Selecting the fault detection configuration for the Alert Log operation (page 4-23)
  - Getting access to online help for the web browser interface (page 4-11)
- Description of the web browser interface:
  - Overview window and tabs (page 4-15)
  - Port Utilization and Status displays (page 4-16)
  - Alert Log and Alert types (page 4-19)
  - Setting the Fault Detection Policy (page 4-23)

Note

If you want security beyond that achieved with user names and passwords, you can disable access to the web browser interface. This is done by either executing `no web-management` at the Command Prompt or changing the `Web Agent Enabled` parameter setting to `No` (page 6-4).
General Features

The Series 5300XL switch include these web browser interface features:

Switch Configuration:
- Ports
- VLANs and Primary VLAN
- Fault detection
- Port monitoring (mirroring)
- System information
- Enable/Disable Multicast Filtering (IGMP) and Spanning Tree
- IP
- Support and management URLs

Switch Security: Passwords

Switch Diagnostics:
- Ping/Link Test
- Device reset
- Configuration report

Switch status
- Port utilization
- Port counters
- Port status
- Alert log

Switch system information listing
Starting an HP Web Browser Interface Session with the Switch

You can start a web browser session in the following ways:

■ Using a standalone web browser on a network connection from a PC or UNIX workstation:
  • Directly connected to your network
  • Connected through remote access to your network
■ Using a management station running HP TopTools for Hubs & Switches on your network

Using a Standalone Web Browser in a PC or UNIX Workstation

This procedure assumes that you have a supported web browser installed on your PC or workstation, and that an IP address has been configured on the switch. (For more on assigning an IP address, refer to “IP Configuration” on page 7-3.)

1. Make sure the Java\textsuperscript{TM} applets are enabled for your browser. If they are not, use the options menu in your browser to do the following:
   • In Netscape, enable the \textbf{Java} and \textbf{JavaScript} options.
   • In Microsoft Internet Explorer, enable the \textbf{Java Permissions}.

Refer to your selected browser’s online Help for specific information on enabling the Java applets.
2. Type the IP address (or DNS name) of the switch in the browser Location or Address field and press [Enter]. (It is not necessary to include http://.)

   switch4108  [Enter]  (example of a DNS-type name)

   10.11.12.195  [Enter]  (example of an IP address)

If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, switch4108) that you can type in the Location or Address field instead of the IP address. Using DNS names typically improves browser performance. See your network administrator for any name associated with the switch.

Using HP TopTools for Hubs & Switches

HP TopTools for Hubs & Switches is designed for installation on a network management workstation. For this reason, the HP TopTools system requirements are different from the system requirements for accessing the switch's web browser interface from a non-management PC or workstation. For HP TopTools requirements, refer to the information provided with HP TopTools for Hubs & Switches.

This procedure assumes that:

- You have installed the recommended web browser on a PC or workstation that serves as your network management station.
- The networked device you want to access has been assigned an IP address and (optionally) a DNS name and has been discovered by HP TopTools for Hubs & Switches. (For more on assigning an IP address, refer to “IP Configuration” on page 7-3.)

To establish a web browser session with HP TopTools running, do the following on the network management station:

1. Make sure the Java™ applets are enabled for your web browser. If they are not, refer to the web browser online Help for specific information on enabling the Java applets.

2. Do one of the following tasks:
   - On the HP TopTools Maps view, double-click on the symbol for the networking device that you want to access.
   - In HP TopTools, in the Topology Information dialog box, in the device list, double-click on the entry for the device you want to access (IP address or DNS name).
Using the HP Web Browser Interface  
Starting an HP Web Browser Interface Session with the Switch  

3. The web browser interface automatically starts with the Status Overview window displayed for the selected device, as shown in figure 4-1.

**Note**
If the Registration window appears, click on the **Status** tab.

---

**Figure 4-1. Example of Status Overview Screen**
Tasks for Your First HP Web Browser Interface Session

The first time you access the web browser interface, there are three tasks that you should perform:

- Review the “First Time Install” window
- Set Manager and Operator passwords
- Set access to the web browser interface online help

Viewing the “First Time Install” Window

When you access the switch’s web browser interface for the first time, the Alert log contains a “First Time Install” alert, as shown in figure 4-2. This gives you information about first time installations, and provides an immediate opportunity to set passwords for security and to specify a Fault Detection policy, which determines the types of messages that will be displayed in the Alert Log.

Double click on First Time Install in the Alert log (figure 4-1 on page 4-6). The web browser interface then displays the “First Time Install” window, below.

![First Time Install Window](image)

**Figure 4-2. First-Time Install Window**
This window is the launching point for the basic configuration you need to perform to set web browser interface passwords to maintain security and Fault Detection policy, which determines the types of messages that will be displayed in the Alert Log.

To set web browser interface passwords, click on secure access to the device to display the Device Passwords screen, and then go to the next page. (You can also access the password screen by clicking on the Security tab.)

To set Fault Detection policy, click on select the fault detection configuration in the second bullet in the window and go to the section, “Setting Fault Detection Policy” on page 4-23. (You can also access the password screen by clicking on the Configuration tab, and then [Fault Detection] button.)

Creating Usernames and Passwords in the Browser Interface

You may want to create both a username and password to create access security for your switch. There are two levels of access to the interface that can be controlled by setting user names and passwords:

- **Operator.** An Operator-level user name and password allows read-only access to most of the web browser interface, but prevents access to the Security window.

- **Manager.** A Manager-level user name and password allows full read/write access to the web browser interface.
To set the passwords:

1. Access the Device Passwords screen by one of the following methods:
   - If the Alert Log includes a “First Time Install” event entry, double click on this event, then, in the resulting display, click on the secure access to the device link.
   - Select the Security tab.

2. Click in the appropriate box in the Device Passwords window and enter user names and passwords. You will be required to repeat the password strings in the confirmation boxes.

   Both the user names and passwords can be up to 16 printable ASCII characters.

3. Click on [Apply Changes] to activate the user names and passwords.
Passwords you assign in the web browser interface will overwrite previous passwords assigned in either the web browser interface, the Command Prompt, or the switch console. That is, the most recently assigned passwords are the switch’s passwords, regardless of which interface was used to assign the string.

Using the Passwords

Figure 4-4. Example of the Password Window in the Web Browser Interface

The manager and operator passwords are used to control access to all switch interfaces. Once set, you will be prompted to supply the password every time you try to access the switch through any of its interfaces. The password you enter determines the capability you have during that session:

- Entering the manager password gives you full read/write capabilities
- Entering the operator password gives you read and limited write capabilities.

Using the User Names

If you also set user names in the web browser interface screen, you must supply the correct user name for web browser interface access. If a user name has not been set, then leave the User Name field in the password window blank.

Note that the Command Prompt and switch console interfaces use only the password, and do not prompt you for the User Name.
Using the HP Web Browser Interface

Tasks for Your First HP Web Browser Interface Session

If You Lose a Password

If you lose the passwords, you can clear them by pressing the Clear button on the front of the switch. *This action deletes all password and user name protection from all of the switch’s interfaces.*

*The Clear button is provided for your convenience, but its presence means that if you are concerned with the security of the switch configuration and operation, you should make sure the switch is installed in a secure location, such as a locked wiring closet.*

Online Help for the HP Web Browser Interface

Online Help is available for the web browser interface. You can use it by clicking on the question mark button in the upper right corner of any of the web browser interface screens.

![The Help Button](image)

*Figure 4-5. The Help Button*

Context-sensitive help is provided for the screen you are on.

**Note**

If you do not have HP TopTools for Hubs and Switches installed on your network and do not have an active connection to the World Wide Web, then Online help for the web browser interface will not be available.

For more on Help access and operation, refer to “Help and the Management Server URL” on page 4-13.
Support/Mgmt URLs Feature

The Support/Mgmt URLs window enables you to change the World Wide Web Universal Resource Locator (URL) for two functions:

- **Support URL** – a support information site for your switch
- **Management Server URL** – the site for online help for the web browser interface, and, if set up, the URL of a network management station running HP TopTools for Hubs & Switches.

3. Enter URLs for:
   - the support information source you want the switch to access when you click on the web browser interface Support tab – the default is HP's ProCurve network products World Wide Web home page
   - the URL of the network Management server or other source of the online help files for this web browser interface. (The default accesses Help on HP's World Wide Web site.)

4. Click on Apply Changes

![Figure 4-6. The Default Support/Mgmt URLs Window]
Support URL

This is the site that the switch accesses when you click on the Support tab on the web browser interface. The default URL is:

http://www.hp.com/go/procurve

which is the World Wide Web site for Hewlett-Packard's networking products.

Click on the [Support] button on that page and you can get to support information regarding your switch, including white papers, operating system (OS) updates, and more.

You could instead enter the URL for a local site that you use for entering reports about network performance, or whatever other function you would like to be able to easily access by clicking on the [Support] tab.

Help and the Management Server URL

This field specifies which of the following two locations the switch will use to find online Help for the web browser interface:

- The URL of online Help provided by HP on the world wide web
- The URL of a network management station running HP TopTools for Hubs & Switches

Providing Online Help. The Help files are automatically available if you install HP TopTools for Hubs & Switches on your network or if you already have Internet access to the World Wide Web. (The Help files are included with HP TopTools for Hubs & Switches, and are also automatically available from HP via the World Wide Web.)

Retrieval of the Help files is controlled by automatic entries to the Management Server URL field on the Configuration / Support/Mgmt URLs screen, shown in figure 4-6. The switch is shipped with the URL set to retrieve online Help from the HP World Wide Web site. However, if HP TopTools for Hubs & Switches is installed on a management station on your network and discovers the switch, the Management Server URL is automatically changed to retrieve the Help from your TopTools management station.

If Online Help Fails To Operate. Do one of the following:

- If HP TopTools for Hubs & Switches is installed and running on your network, enter the IP address or DNS name of the network management station in the Management Server URL field shown in figure 4-7 on page 4-14.
If you have World Wide Web access from your PC or workstation, and do not have HP TopTools installed on your network, enter the following URL in the Management Server URL field shown in figure 4-7 on page 4-14:

http://www.hp.com/rnd/device_help

Figure 4-7. How To Access Web Browser Interface Online Help

**Policy Management and Configuration.** HP Top Tools for Hubs & Switches can perform network-wide policy management and configuration of your switch. The Management Server URL field identifies the management station that is performing that function. For more information, refer to the documentation provided on the HP TopTools for Hubs & Switches CD shipped with the switch.
Status Reporting Features

Browser elements covered in this section include:
- The Overview window (below)
- Port utilization and status (page 4-16)
- The Alert log (page 4-19)
- The Status bar (page 4-22)

The Overview Window

The Overview Window is the home screen for any entry into the web browser interface. The following figure identifies the various parts of the screen.

Figure 4-8. The Overview Window
The Port Utilization and Status Displays

The Port Utilization and Status displays show an overview of the status of the switch and the amount of network activity on each port. The following figure shows a sample reading of the Port Utilization and Port Status.

![Port Utilization and Status Displays](image)

**Figure 4-9. The Graphs Area**

**Port Utilization**

The Port Utilization bar graphs show the network traffic on the port with a breakdown of the packet types that have been detected (unicast packets, non-unicast packets, and error packets). The Legend identifies traffic types and their associated colors on the bar graph:

- **% Unicast Rx & All Tx**: This is all unicast traffic received and all transmitted traffic of any type. This indicator (a blue color on many systems) can signify either transmitted or received traffic.

- **% Non-Unicast Pkts Rx**: All multicast and broadcast traffic received by the port. This indicator (a gold color on many systems) enables you to know “at-a-glance” the source of any non-unicast traffic that is causing high utilization of the switch. For example, if one port is receiving heavy broadcast or multicast traffic, all ports will become highly utilized. By color-coding the received broadcast and multicast utilization, the bar graph quickly and easily identifies the offending port. This makes it faster and easier to discover the exact source of the heavy traffic because you don’t have to examine port counter data from several ports.

- **% Error Pkts Rx**: All error packets received by the port. (This indicator is a reddish color on many systems.) Although errors received on a port are not propagated to the rest of the network, a consistently high number of errors on a specific port may indicate a problem on the device or network segment connected to the indicated port.
- **Maximum Activity Indicator**: As the bars in the graph area change height to reflect the level of network activity on the corresponding port, they leave an outline to identify the maximum activity level that has been observed on the port.

**Utilization Guideline.** A network utilization of 40% is considered the maximum that a typical Ethernet-type network can experience before encountering performance difficulties. If you observe utilization that is consistently higher than 40% on any port, click on the Port Counters button to get a detailed set of counters for the port.

**To change the amount of bandwidth the Port Utilization bar graph shows.** Click on the bandwidth display control button in the upper left corner of the graph. (The button shows the current scale setting, such as 40%.) In the resulting menu, select the bandwidth scale you want the graph to show (3%, 10%, 25%, 40%, 75%, or 100%), as shown in figure 4-10.

Note that when viewing activity on a gigabit port, you may want to select a lower value (such as 3% or 10%). This is because the bandwidth utilization of current network applications on gigabit links is typically minimal, and may not appear on the graph if the scale is set to show high bandwidth utilization.

![Figure 4-10. Changing the Graph Area Scale](image)

**To display values for each graph bar.** Hold the mouse cursor over any of the bars in the graph, and a pop-up display is activated showing the port identification and numerical values for each of the sections of the bar, as shown in figure 4-11 (next).

![Figure 4-11. Display of Numerical Values for the Bar](image)
Port Status

The Port Status indicators show a symbol for each port that indicates the general status of the port. There are four possible statuses:

- **Port Connected** – the port is enabled and is properly connected to an active network device.

- **Port Not Connected** – the port is enabled but is not connected to an active network device. A cable may not be connected to the port, or the device at the other end may be powered off or inoperable, or the cable or connected device could be faulty.

- **Port Disabled** – the port has been configured as disabled through the web browser interface, the switch console, or SNMP network management.

- **Port Fault-Disabled** – a fault condition has occurred on the port that has caused it to be auto-disabled. Note that the Port Fault-Disabled symbol will be displayed in the legend only if one or more of the ports is in that status. See appendix B, “Monitoring and Analyzing Switch Operation” for more information.

Figure 4-12. The Port Status Indicators and Legend
The Alert Log

The web browser interface Alert Log, shown in the lower half of the screen, shows a list of network occurrences, or alerts, that were detected by the switch. Typical alerts are **Broadcast Storm**, indicating an excessive number of broadcasts received on a port, and **Problem Cable**, indicating a faulty cable. A full list of alerts is shown in the table on page 4-20.

<table>
<thead>
<tr>
<th>Status</th>
<th>Alert</th>
<th>Date/Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Excessive CRC/alignment errors</td>
<td>16-Sep-99 7:58:44 AM</td>
<td>Excessive CRC/Alignment errors on port: 8.</td>
</tr>
<tr>
<td>-</td>
<td>Firsttime installation</td>
<td>13-Sep-99 3:36:29 PM</td>
<td>Important installation information for your switch</td>
</tr>
</tbody>
</table>

**Figure 4-13. Example of the Alert Log**

Each alert has the following fields of information:

- **Status** – The level of severity of the event generated. Severity levels can be Information, Normal, Warning, and Critical. If the alert is new (has not yet been acknowledged), the New symbol is also in the Status column.
- **Alert** – The specific event identification.
- **Date/Time** – The date and time the event was received by the web browser interface. This value is shown in the format: *DD-MM-YY HH:MM:SS AM/PM*, for example, *16-Sep-99 7:58:44 AM*.
- **Description** – A short narrative statement that describes the event. For example, **Excessive CRC/Alignment errors on port: 8**.

**Sorting the Alert Log Entries**

The alerts are sorted, by default, by the Date/Time field with the most recent alert listed at the top of the list. The second most recent alert is displayed below the top alert and so on. If alerts occurred at the same time, the simultaneous alerts are sorted by order in which they appear in the MIB.

The alert field that is being used to sort the alert log is indicated by which column heading is in bold. You can sort by any of the other columns by clicking on the column heading. The Alert and Description columns are sorted alphabetically, while the Status column is sorted by severity type, with more critical severity indicators appearing above less critical indicators.
Alert Types

The following table lists the types of alerts that can be generated.

Table 4-1. Alert Strings and Descriptions

<table>
<thead>
<tr>
<th>Alert String</th>
<th>Alert Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Time Install</td>
<td>Important installation information for your switch.</td>
</tr>
<tr>
<td>Too many undersized/giant packets</td>
<td>A device connected to this port is transmitting packets shorter than 64 bytes or longer than 1518 bytes (longer than 1522 bytes if tagged), with valid CRCs (unlike runts, which have invalid CRCs).</td>
</tr>
<tr>
<td>Excessive jabbering</td>
<td>A device connected to this port is incessantly transmitting packets (&quot;jabbering&quot;), detected as oversized packets with CRC errors.</td>
</tr>
<tr>
<td>Excessive CRC/alignment errors</td>
<td>A high percentage of data errors has been detected on this port. Possible causes include:</td>
</tr>
<tr>
<td></td>
<td>• Faulty cabling or invalid topology.</td>
</tr>
<tr>
<td></td>
<td>• Duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other)</td>
</tr>
<tr>
<td></td>
<td>• A malfunctioning NIC, NIC driver, or transceiver</td>
</tr>
<tr>
<td>Excessive late collisions</td>
<td>Late collisions (collisions detected after transmitting 64 bytes) have been detected on this port. Possible causes include:</td>
</tr>
<tr>
<td></td>
<td>• An overextended LAN topology</td>
</tr>
<tr>
<td></td>
<td>• Duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other)</td>
</tr>
<tr>
<td></td>
<td>• A misconfigured or faulty device connected to the port</td>
</tr>
<tr>
<td>High collision or drop rate</td>
<td>A large number of collisions or packet drops have occurred on the port. Possible causes include:</td>
</tr>
<tr>
<td></td>
<td>• A extremely high level of traffic on the port</td>
</tr>
<tr>
<td></td>
<td>• Duplex mismatch</td>
</tr>
<tr>
<td></td>
<td>• A misconfigured or malfunctioning NIC or transceiver on a device connected to this port</td>
</tr>
<tr>
<td></td>
<td>• A topology loop in the network</td>
</tr>
<tr>
<td>Excessive broadcasts</td>
<td>An extremely high percentage of broadcasts was received on this port. This degrades the performance of all devices connected to the port. Possible causes include:</td>
</tr>
<tr>
<td></td>
<td>• A network topology loop—this is the usual cause</td>
</tr>
<tr>
<td></td>
<td>• A malfunctioning device, NIC, NIC driver, or software package</td>
</tr>
<tr>
<td>Loss of Link</td>
<td>Lost connection to one or multiple devices on the port.</td>
</tr>
</tbody>
</table>

Note When troubleshooting the sources of alerts, it may be helpful to check the switch’s Port Status and Port Counter windows and the Event Log in the console interface.
Viewing Detail Views of Alert Log Entries

By double clicking on Alert Entries, the web browser interface displays a Detail View or separate window detailing information about the events. The Detail View contains a description of the problem and a possible solution. It also provides four management buttons:

- **Acknowledge Event** – removes the New symbol from the log entry
- **Delete Event** – removes the alert from the Alert Log
- **Cancel Button** – closes the detail view with no change to the status of the alert and returns you to the Overview screen.

A sample Detail View describing an Excessive CRC/Alignment Error alert is shown here.

---

**Excessive CRC/Alignment Errors on port A8**

**Description:**
A high percentage of data errors was detected on port A8.

**Possible causes:**
The possible causes include faulty cabling or topology, half/full duplex mismatch, a misconfigured NIC, or a malfunctioning NIC, NIC driver, or transceiver.

**Actions:**
1. If port A8 is 100Base-T, make sure the cable connectors, punch-down blocks, and patch panels connecting to that port are Category 5 or better. Verify the correctness of the installation using a Category 5 test device.
2. Check the directly-connected device for mismatches in half/full duplex operation (half duplex on the switch and full duplex on the connected device, or the reverse).
3. Update the NIC driver software.
4. Verify that the network topology conforms to IEEE 802.3 standards.
5. Replace or relocate the cable. Also check the wiring closet components, transceivers, and NICs for proper operation.

---

**Figure 4-14. Example of Alert Log Detail View**
The Status Bar

The Status Bar is displayed in the upper left corner of the web browser interface screen. Figure 4-15 shows an expanded view of the status bar.

The Status Bar consists of four objects:

- **Status Indicator**. Indicates, by icon, the severity of the most critical alert in the current display of the Alert Log. This indicator can be one of three shapes and colors as shown in the following table.

<table>
<thead>
<tr>
<th>Color</th>
<th>Switch Status</th>
<th>Status Indicator Shape</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Normal Activity; “First time installation” information available in the Alert log.</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Green</td>
<td>Normal Activity</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Yellow</td>
<td>Warning</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Red</td>
<td>Critical</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

- **System Name**. The name you have configured for the switch by using Identity screen, `system name` command, or the switch console **System Information** screen.

- **Most Critical Alert Description**. A brief description of the earliest, unacknowledged alert with the current highest severity in the Alert Log, appearing in the right portion of the Status Bar. In instances where multiple critical alerts have the same severity level, only the earliest unacknowledged alert is deployed in the Status bar.
Setting Fault Detection Policy

One of the powerful features in the web browser interface is the Fault Detection facility. For your switch, this feature controls the types of alerts reported to the Alert Log based on their level of severity.

Set this policy in the Fault Detection window (figure 4-16).

**Figure 4-16. The Fault Detection Window**

The Fault Detection screen contains a list box for setting fault detection and response policy. You set the sensitivity level at which a network problem should generate an alert and send it to the Alert Log.

To provide the most information on network problems in the Alert Log, the recommended sensitivity level for Log Network Problems is **High Sensitivity**. The Fault Detection settings are:
■ **High Sensitivity.** This policy directs the switch to send all alerts to the Alert Log. This setting is most effective on networks that have none or few problems.

■ **Medium Sensitivity.** This policy directs the switch to send alerts related to network problems to the Alert Log. If you want to be notified of problems which cause a noticeable slowdown on the network, use this setting.

■ **Low Sensitivity.** This policy directs the switch to send only the most severe alerts to the Alert Log. This policy is most effective on a network that normally has a lot of problems and you want to be informed of only the most severe ones.

■ **Never.** Disables the Alert Log and transmission of alerts (traps) to the management server (in cases where a network management tool such as HP TopTools for Hubs & Switches is in use). Use this option when you don't want to use the Alert Log.

The Fault Detection Window also contains three Change Control Buttons:

■ **Apply Changes.** This button stores the settings you have selected for all future sessions with the web browser interface until you decide to change them.

■ **Clear Changes.** This button removes your settings and returns the settings for the list box to the level it was at in the last saved detection-setting session.

■ **Reset to Default Settings.** This button reverts the policy setting to Medium Sensitivity for Log Network Problems.