



IPSWITCH

Network Monitoring with SNMP

This document describes how SNMP is used in WhatsUp Gold v11 and provides examples on how to configure performance, active, and passive monitors.

Introduction

SNMP (Simple Network Management Protocol) enables WhatsUp Gold to monitor and manage network performance, report and troubleshoot network problems, and better prepare for future network growth. It is a flexible technology that can be used across operating systems and device types.

For example, the SNMP agent on a router can provide information about the device's network configuration and operations, such as the device's network interfaces, routing tables and network traffic statistics. The Management Information Base (MIB) is like a two-way interpreter for WhatsUp Gold. The MIB lets an SNMP agent, such as WhatsUp Gold, know what Object Identifier (OID) or SNMP objects the remote device understands and provides a structure for the SNMP agent to communicate with the device. The OID is displayed as a series of numbers separated by dots that represent where on the MIB Tree the object is located. The target device, such as a router, already understands the commands that it supports and how it will respond (or interpret) to commands it receives.

The structure, or rules, of the MIB is defined in SMI (Structure of Management Information) files also called MIB files. WhatsUp Gold supports SMI v1 and v2.

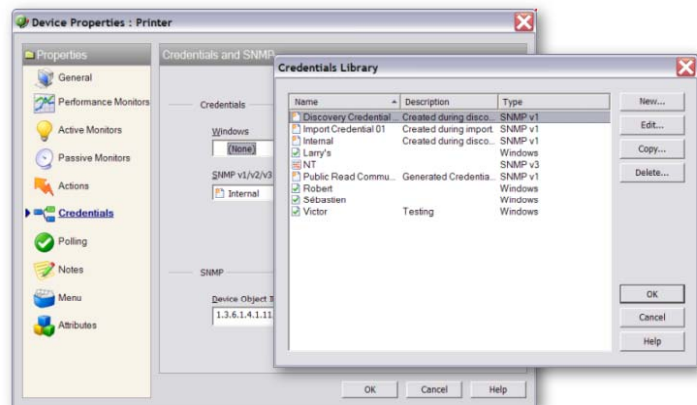
How WhatsUp Gold Uses SNMP

In WhatsUp Gold, there are three types of SNMP Monitors that you can assign to a device: Passive Monitors, Active Monitors, and Performance Monitors. The differences between these monitors come in the way they gather and report data.

- **Active.** Active Monitors query network services installed on a device then wait on the response.
- **Performance.** These monitors gather data about specific properties on a device that is then presented visibly in performance graphs.
- **Passive.** These monitors 'listen' for specific types of information sent from a device.

These monitors are stored in their respective library, and are associated to individual devices through device properties.

To read data on an SNMP device, WhatsUp Gold must have permissions to access the device. When configuring the monitors for devices, you must provide the proper SNMP credential (a read community string for SNMPv1 or SNMPv2, or a SNMPv3 user) for the devices being monitored. SNMP credentials are configured in the Credentials Library and selected for a device in the Credentials section of Device Properties. If you do not supply the proper SNMP credentials for a device, WhatsUp Gold cannot gather statistics or use the specified monitor for the device. If you do not supply the proper SNMP read community string (or SNMP credential), WhatsUp Gold cannot gather statistics or use



the specified monitor for that device. **Note:** SNMP Passive Monitors (traps) do not require credentials.

Using SNMP in Device Discovery

During device discovery, you can scan your network with SNMP SmartScan. Use the SNMP read community strings (separated by commas) entered on the SNMP SmartScan Settings dialog to get a list of devices from an SNMP device that supports the IP MIB (such as an enabled router).

After the devices are found, the devices are checked for information about the network and whether they respond to any of the community strings that were entered during the discovery. WhatsUp Gold does this by asking for the SYSOBJECTID (1.3.6.1.2.1.1.2). If the device answers, we know that it is SNMP enabled. Also, if the device does respond to the request for the SYSOBJECTID, WhatsUp Gold takes additional steps to check if any of the SNMP-based Active or Performance monitors, selected during the Discovery dialog, respond to any of the community strings. When the discovery occurs, as long as one credential finds at least one device, the credential is added to the Credentials Library. The devices that are SNMP enabled are identified, scanned for active and performance monitors, their OIDs are recorded, and a Credential entry is added for the device.

Note: When WhatsUp Gold is installed, a default SNMPv1 credential named Public Read Community is created by default.

When adding a single device, click the **Advanced** button on the Add New Device dialog to enter the SNMP read string for the device you are adding. If correct, the OID is recorded in device properties for that device, and an SNMP credential is created for the string used.

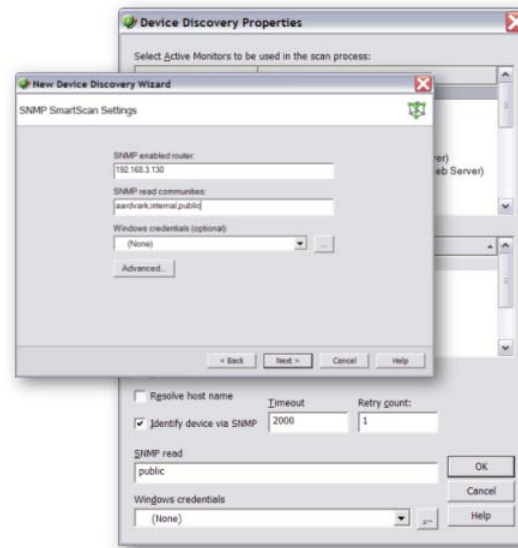
Supported Versions of SNMP

WhatsUp Gold supports SNMPv1, SNMPv2c, and SNMPv3. SNMPv1 and v2c are very similar in the way the application communicates with a device.

SNMPv3 reports the same data as v2, but uses a different authentication scheme. Instead of community strings, v3 devices require a username and password to poll to the device. In addition, users can be configured on the v3 device to have the data packets encrypted before they are sent to a device requesting the SNMP information.

Creating SNMP Monitors

The following sections provide further details on creating SNMP monitors in WhatsUp Gold. Each monitor type is described, and real-world scenarios and solutions are used to give you ideas on how to use SNMP Monitors on your network.



Adding MIB to WhatsUp Gold

In some cases, you may want to add MIB files to the WhatsUp Gold system to make it easier to find specific OIDs within the MIB file. If you are reporting and alerting on non-enterprise OIDs, you may be able to use the MIB files already installed with the application.

To add the MIB file to the application, copy the file to the `<install directory>\WhatsUp\Data\Mibs` folder in your installation directory. After the MIB is in that directory, you must restart the WhatsUp Gold application to see the MIB in the MIB Browser.

Note: If you are using the WhatsUp Gold web interface, you need to restart the web service after adding a MIB. Also, to use polling, you need to restart the WhatsUp Gold engine service after adding a MIB.

Where to get MIBs

If you do not have the MIB files you need for your devices, contact the device manufacturer, or search their website. If you still cannot find the proper file, there are several online resources that you can try.

Ipswitch http://www.ipswitch.com/products/whatsup/index.asp?t=mib_library

Cisco <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

mibDepot <http://www.mibdepot.com/index.shtml>

Standard MIBs are published as RFCs (Request for Comments) and can be downloaded from the official RFC repository at: <http://www.ietf.org/rfc>

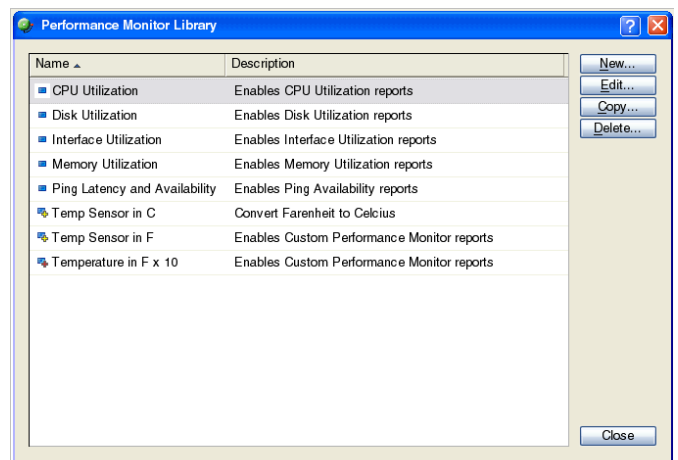
Using SNMP Performance Monitors

WhatsUp Gold is installed with four default performance monitors that use SNMP to monitor specific types of performance data on your network devices:

- CPU Utilization
- Disk Utilization
- Interface/Bandwidth Utilization
- Memory Utilization

These monitors represent the majority of performance issues encountered in the day-to-day operation of networked devices. If you need to monitor other values reported on the device, you must create a custom performance monitor for that device.

The following example shows why you might need to create a custom performance monitor, and how to create the monitor for the device.



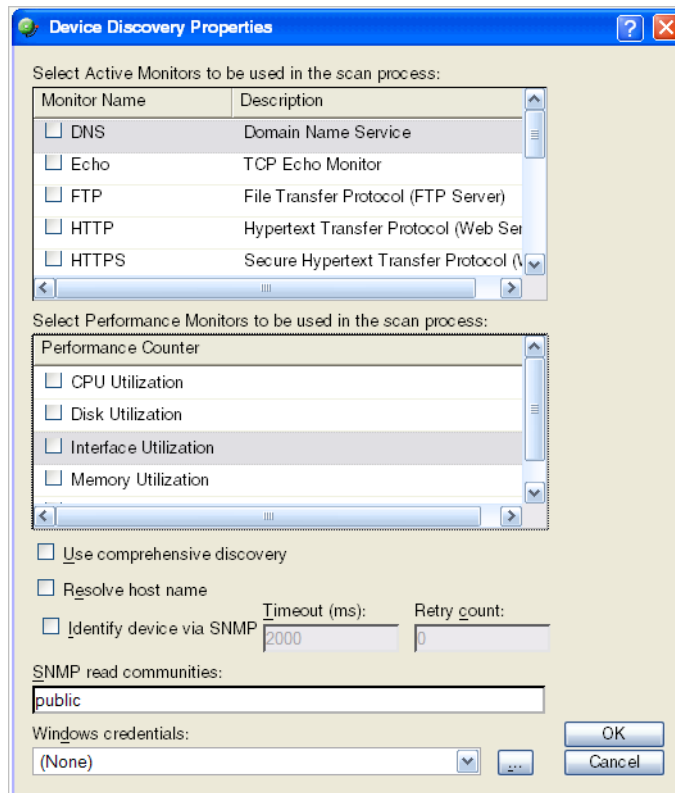
Performance Monitor Library

Example

It is important to keep your server room at a constant temperature. If the temperature is too low or too high, some of your hardware could be damaged, or the room could be uncomfortable for those who must work in the room on a regular basis. The thermostat on the cooling unit is set at 65 degrees Fahrenheit. Recently, more devices have been added to the room, and you are not sure the cooling unit can keep up with the additional heat sources.

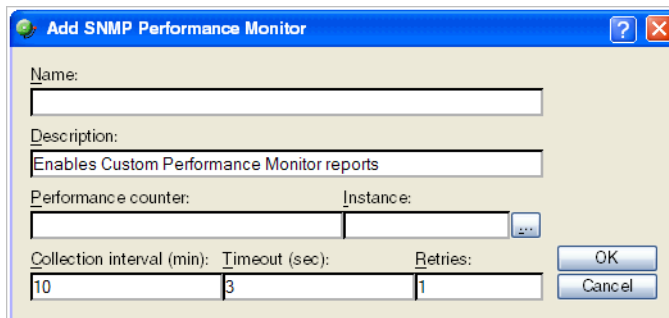
You install a SNMP enabled temperature sensor in the server room, and want to configure WhatsUp Gold to monitor and chart the temperature readings on the sensor. Following are the steps to configure this type of monitor:

1. Right-click on the map you want to add the temperature sensor to.
2. From the right-mouse menu, select **New Device**. The Add New Device dialog opens.
3. Enter the temperature sensor's IP address, then click **Advanced**. The Device Discovery Properties dialog opens.



4. Clear any selected Active Monitors and Performance Counter monitors except for the Ping active monitor.

5. Check the **Identify device via SNMP** and **Resolve host name** options, then click **OK**.
6. Enter the read community string in the **SNMP read** box. In this case, the string is *public*.
7. Click **OK**. The Add New Device dialog opens.
8. Click **OK**. WhatsUp Gold scans the IP address using the SNMP community string to identify the device. When the scan is complete, Device Properties for that device appears.
9. Click **Performance Monitors**. The Device Properties Performance Monitors dialog opens.
10. Click **New**. The Select Performance Monitor dialog opens.
11. In the **What type of monitor would you like to create?** list, select **SNMP Performance Monitor**, then click **OK**. The Add SNMP Performance Counter dialog opens.

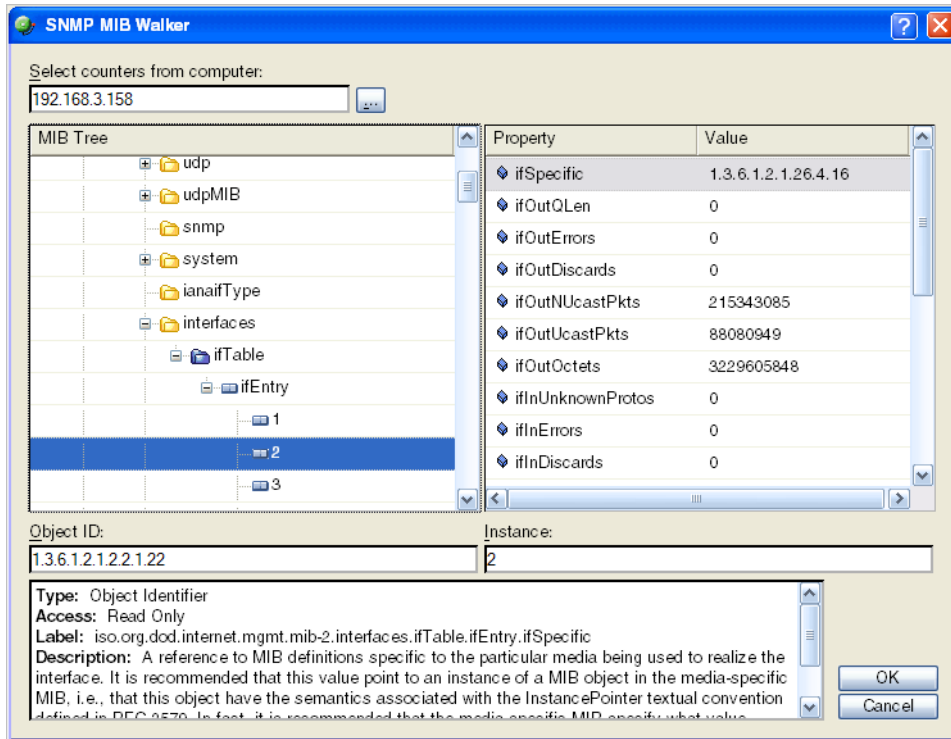


12. Enter Temperature Sensor in F in the **Name** box.
13. Click the browse (...) button. The SNMP MIB Walker dialog opens.

Note: Make sure that the manufacturer's MIB for the temperature sensor has been added to the <install directory>\WhatsUp\Data\Mibs folder in the installation directory.

Note: After adding a new MIB, you need to restart the WhatsUp Gold web interface or console application and restart the web service. Also, to use polling, you need to restart the WhatsUp Gold engine service after adding a MIB.

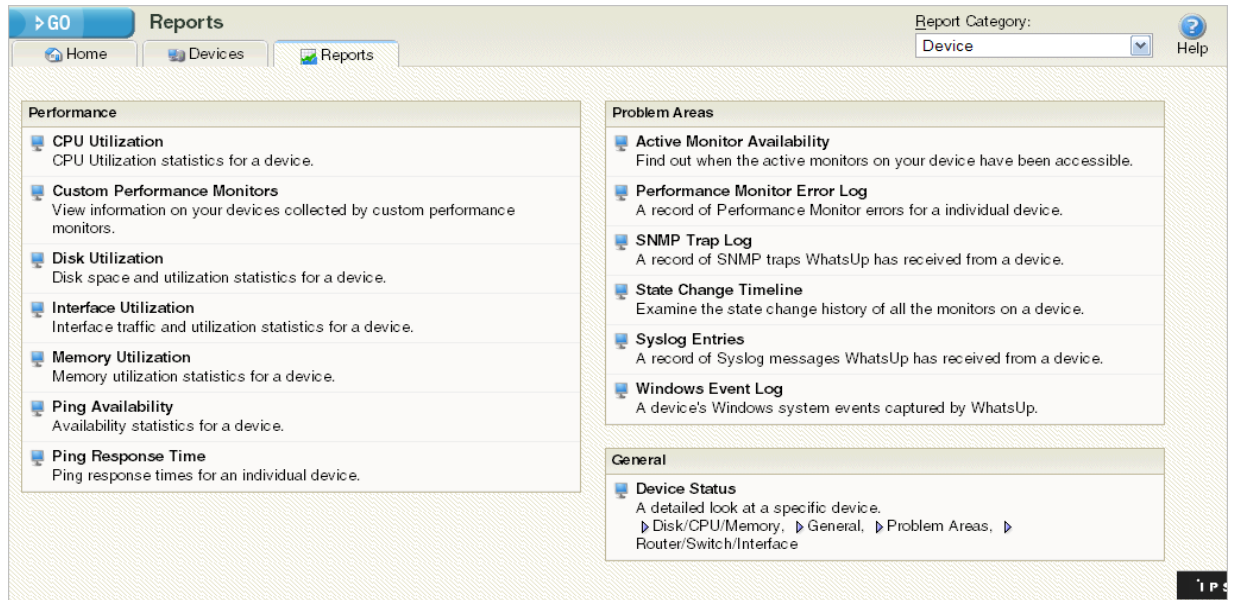
- Browse to the specific performance counter in the MIB. See the device documentation for more information about the MIB options. The **Object ID (OID)** box automatically enters the OID you selected from the MIB Tree.



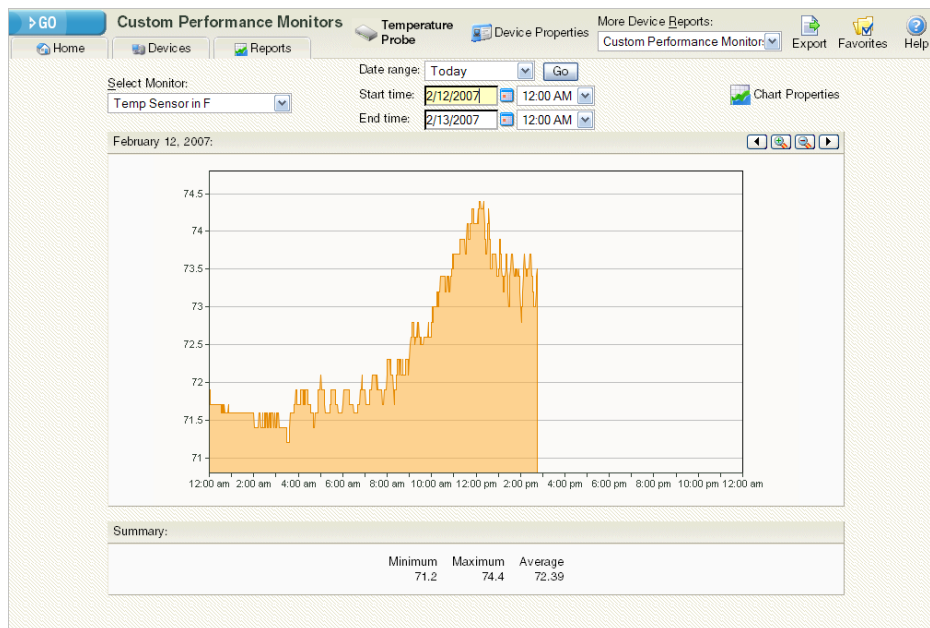
- Select a Property from the **Property** list on the right side. The **Instance** box displays the Instance value based on the Property you select.
- Click **OK**. The Add SNMP Performance Monitor dialog opens.
- In the **Collection Interval (min)** box, enter 5 to have WhatsUp Gold collect the data on the device every five minutes.
- Enter a value for the **Timeout (sec)** and **Retries**, then click **OK**. The Device Properties Performance Monitors dialog opens. Click **OK**.
- Click **Close** to add the monitor and begin collecting data.

It will take several polls to produce enough data to see informative data on the graph. After you have enough data, you can view the performance reports:

1. In the Device View or Map View, right-click the device you for which you created the monitor, then select **Device Reports**. The Report View opens to the Device Reports list.



2. Click the **Custom Performance Monitors** report. This report shows the data collected on the device since the monitor was activated. The report graphs all of the temperature readings gathered at the specified interval. You can change the date and time of the displayed data to show more detail on the graph. Below the graph, the summary bar shows the maximum, minimum, and average value for the time period selected.

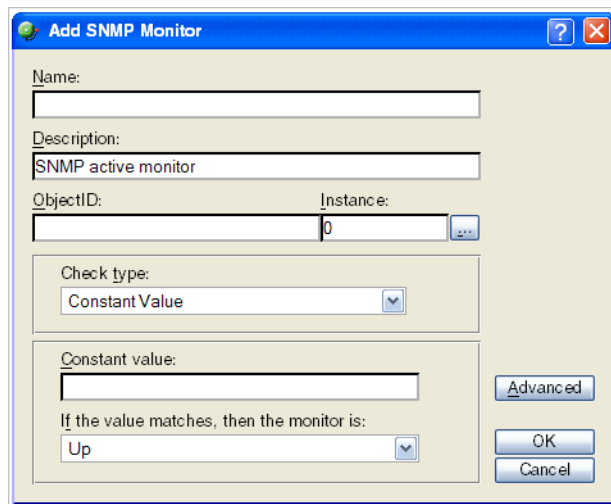


Using an SNMP Active Monitor

Now that you have several days of performance data for your device, you notice that you had occasional spikes in the data that you cannot account for. You can't tell if a door was left open, a device was turned on, or if there is something else that would explain this type of spike. You decide that you want to be notified when one of the spikes occurs, but only if the spike is, in your opinion, too high.

To do this, you can create an active monitor that watches the returned value and makes sure that the value falls in an acceptable range. To create this monitor:

1. In the web interface click **Go > Configure > Active Monitor Library**. The Active Monitor Library dialog opens.
2. Click **New**. The Select Active Monitor Type dialog opens.
3. In the **What type of Active Monitor would you like to create?** list, select **SNMP Monitor**, then click **OK**. The Add SNMP Monitor dialog opens.



4. In the **Name** box, enter `Temperature Range`.
5. Click the browse (...) button. The MIB Browser dialog opens.
6. In the **Select counters from computer** box, enter the IP address of the device for which you're setting up the Active Monitor.
7. In the **SNMP v1/v2/v3 credentials** list, select the **public** credentials from the list, then click **OK**. The SNMP MIB Walker dialog opens.
8. Browse to the specific performance counter in the MIB. Select the same Object ID and Instance that you used in the Performance Monitor options, then click **OK**. The Add SNMP dialog opens.
9. In the **Check type** list, select **Range of Values**.
10. The temperature sensor reports the temperature 60°F as 600. Therefore, enter 600 in the **Low value** box as the lowest temperature that should be in the server room.
11. Enter 700 in the **High value** box, since anything over 70°F is considered too high for the server room, then click **OK**. The Active Monitor Library dialog opens.

12. Click **Close**.
13. Return to the Device View or Map View, select the device you are creating an Active Monitor for, right-click and select **Device Properties**. The Device Properties dialog opens.
14. Click **Active Monitors**. The Device Properties Active Monitors dialog opens.
15. Click **Add**. The Select Active Monitor Type dialog opens.
16. In the **What type of Active Monitor would you like to add to this device?** list, select **Temperature Range**, then click **Next**. The Set Polling Properties dialog opens.
17. Make sure the **Enable Polling for this Active Monitor** is selected, then click **Next**. The Setup Actions for Monitor State Changes dialog opens.
18. Select the type of action you want to use for the monitor. Select an Action Policy that you have configured through the Action Policy Library, or select **Apply individual actions** to build a list of actions that you select from the Action Library. See the Help for more information on the action options.
19. Click **Finish** to begin using this active monitor on the device.

Now that the monitor is configured, you are alerted when the temperature reported by the sensor falls outside of the acceptable temperature range.

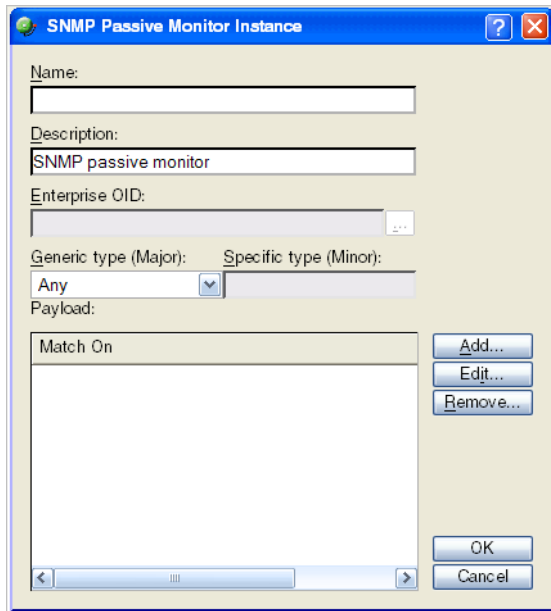
An SNMP Passive Monitor

Many people depend on a particular network printer to publish business-critical reports. When the printer is down, the print queue grows quite large before anyone notices that their reports are not printing. This causes unacceptable printing delays. You have been tasked with monitoring this printer to make sure the toner is at an acceptable level, and that there are no errors keeping the printer from functioning properly.

To do this monitoring, you decide to create an SNMP Passive Monitor that listens for a critical error message or a message that says the toner level is low.

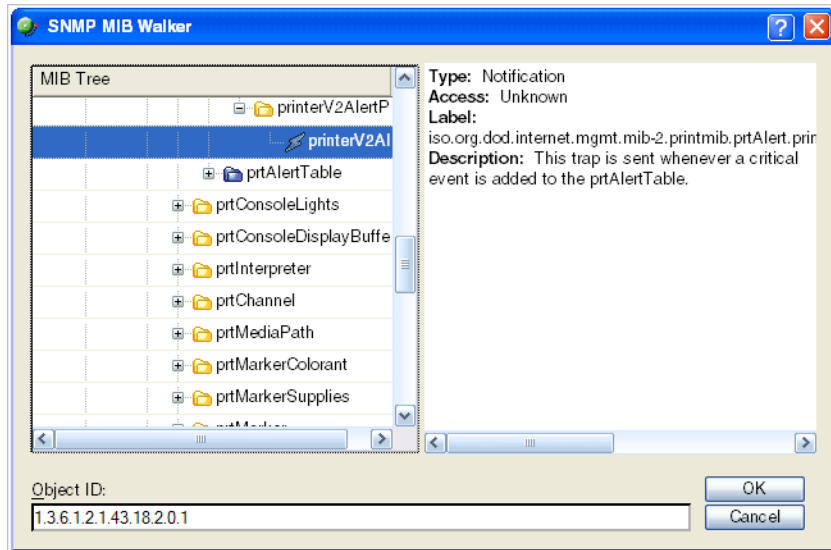
1. Configure the device to send SNMP Traps to your WhatsUp Gold computer. View the device's User Manual or contact your hardware vendor/manufacturer for instructions to configure this.
2. In the WhatsUp Gold console, turn on the SNMP Trap Listener. Click **Configure > Program Options > Passive Monitor Listeners > SNMP Trap > Configure**. The SNMP Configuration dialog opens.
3. Click to select **Listen for messages on port 162**. Click **OK** to turn the listener on, then click **OK**.
Note: If you have Windows Trap Listener enabled on the WhatsUp Gold computer, the SNMP Trap Listener will not work. You must turn the Windows Trap Listener off first.
4. In the web interface Device View or Map View, right-click the printer device you are creating a Passive Monitor for, then select **Properties**. The Device Properties dialog opens.
5. Click **Passive Monitors**. The Device Properties Passive Monitors dialog opens.
6. Click **Add**. The Select Passive Monitor Type dialog opens.

7. Since you do not have an active monitor of this type configured in the Passive Monitor Library, click **Browse (...)**. The Passive Monitor Library dialog opens.
8. Click **New**. The Select Passive Monitor Type dialog appears.
9. In the **What type of monitor would you like to create?** list, select **SNMP Trap**, then click **OK**. The SNMP Passive Monitor Instance dialog opens.



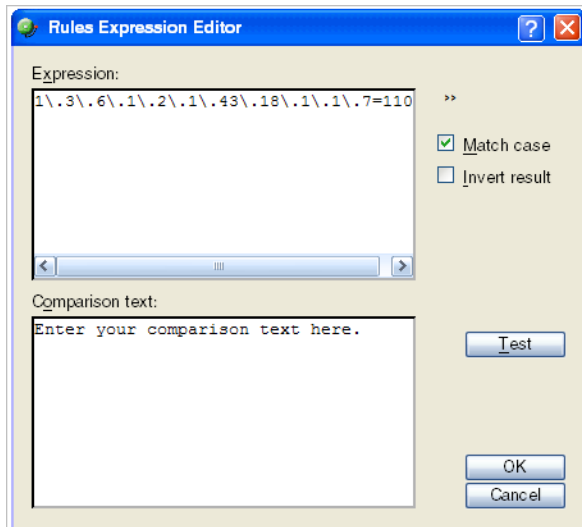
10. In the **Name** box, enter `Printer Alerts`.
11. In the **Generic type (Major)** box, select **6 Enterprise Specific**. If you know your MIB parameters, enter them in the **Generic type (Major)** and **Specific type (Minor)** and **Enterprise OID** boxes).
You can also browse the MIB browser to select the Enterprise OID in the tree. If you don't, you can look for the trap object in the tree and get this information:
 - a. Click the **Browse (...)** button, next to the **Enterprise/OID** box. The SNMP MIB Walker dialog opens.

- b. In the MIB Tree, browse to **mgmt > mib-2 > printmib > prtAlert > printerV1Alert > printerV2AlertPrefix > printerV2Alert**. This object defines a trap (or notification) in the MIB. On the right pane, information about this trap may display the Enterprise OID and Major and Minor Numbers. **Enterprise OID: 1.3.6.1.2.1.43.18.2 (printerV2Alert)**
Generic type (Major): 6
Specific type (Minor): 1

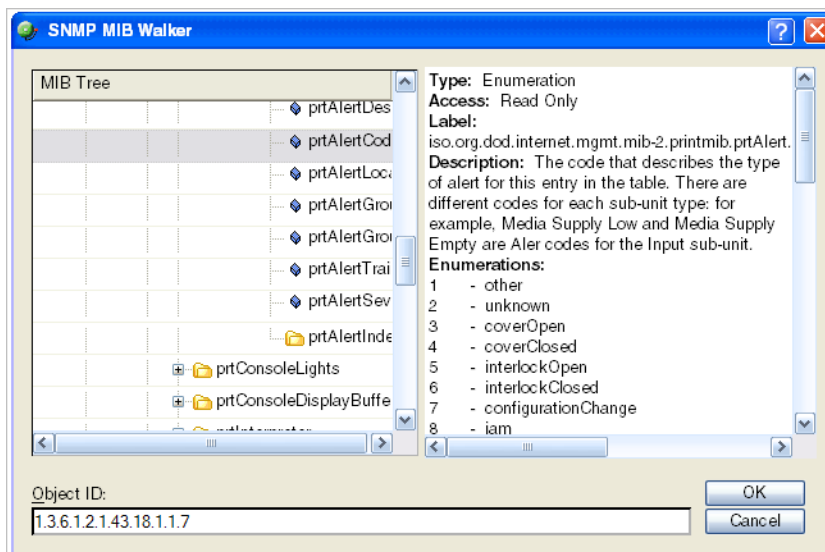


12. Click **OK**. The SNMP Passive Monitor Instance dialog opens.
13. The printerV2Alert is defined with two objects in its payload (prtAlertCode and prtSeverityLevel). We want to match only if the alert code contains a certain value.
- In the **Payload** box, click **Add** to build the expressions you want to match on for the passive monitor payload. The Rules Expression Editor opens.
- In this example, you browsed the MIB Browser and found the OIDs for prtAlertCode (1.3.6.1.2.1.43.18.1.1.7) and prtSeverityLevel (1.3.6.1.2.1.43.18.1.1.2). Since you want to be alerted when an SNMP Trap payload contains the 'Toner Low' message in the prtAlertCode table, configure the Match On to show 1.3.6.1.2.1.43.18.1.1.7=1104. 1104 is the code for 'toner low.' Click **OK**.

Note: Since the '.' character is used as a match expression, you have to add a \ to the expression before each '.' Character. For example:
 1\.3\.6\.1\.2\.1\.43\.18\.1\.1\.7=1104



Note: The printer alert information is available in the MIB browser by browsing to 1.3.6.1.2.1.43.18.1.1.7. A list of possible values display under **Enumeration Values**.



14. You also want to know when a critical warning is sent from the printer, so click **Add** again. The Rules Expression Editor opens.
15. In the Expression box, enter 1\.3\.6\.1\.2\.1\.43\.18\.1\.1\.2=3. We know from the description of the instance that 3 is the code for 'critical warning.' Click **OK**. The SNMP Passive Monitor Instance dialog opens.

16. Click **OK** to add the monitor to the Passive Monitor Library, then click **Close** to record the selection of the new monitor type.
17. Right-click the device you want to add the newly created Passive Monitor to, then select **Properties**. The Device Properties dialog opens.
18. Click **Passive Monitors**, then click **Add**. The Select Passive Monitor Type dialog opens.
19. In the **Which Passive Monitor type would you like to add?** list, select **SNMP Trap** and in the **Which Passive Monitor would you like to add?** list, select **Printer Alerts** (the Passive Monitor created earlier in this procedure), then click **Next**. The Setup Actions for Passive Monitors dialog opens.
20. Click **Add**, the Select or Create Action dialog opens. Select from the options, **Select an action from the Action Library** or **Create an action**, then follow the remaining dialogs to build a list of actions. When a trap is received that matches the Passive Monitor payload, these actions are fired to alert you.

About Ipswitch

Founded in 1991, Ipswitch, Inc., develops easy-to-use, affordable, software products that extend mission-critical IT resources for businesses and improve efficiency for consumers. Its product family includes WS_FTP Professional, the world's most popular FTP client; WS_FTP Server with 128-bit SSL encryption, the first industrial-strength, full-featured FTP server for Windows NT/2000/XP; WhatsUp Gold, a leading network mapping, monitoring, notification and reporting tool; IMail Anti-Virus, an add-on product powered by Symantec's CarrierScan™; and Ipswitch Instant Messaging, a secure Instant Messaging solution specifically designed for businesses.