WhatsUp Gold v16.0

User Guide

Overview

Devices

Monitoring Devices

Reports

Logs

Admin

Using the SNMP API

Using the Dashboard Screen Manager

Troubleshooting and Maintenance

Copyright notice

Overview

In This Section

WhatsUp Gold Overview

In This Chapter

Welcome to Ipswitch WhatsUp Gold

Welcome to Ipswitch WhatsUp Gold, the powerful network monitoring solution designed to help you protect your changing business infrastructure. WhatsUp Gold provides standards-based monitoring of any network device, service, or application on TCP/IP and Windows networks.

WhatsUp Gold lets you discover devices on your network, initiate monitoring of those devices, and execute actions based on device state changes, so you can identify network failures before they become catastrophic.

Discovery and Mapping

The WhatsUp Gold roles-based discovery process searches for devices on your network and helps determine the type of device based on the device attributes.

Device roles do two things:

- Specify the criteria that a device must match to be identified as the device role.
- Specify the monitoring configuration that is applied to the device when it is added to WhatsUp Gold.

After devices are discovered, you can add them to the WhatsUp Gold database and view monitored devices as a list of devices or as a graphical map.

Polling/Listening

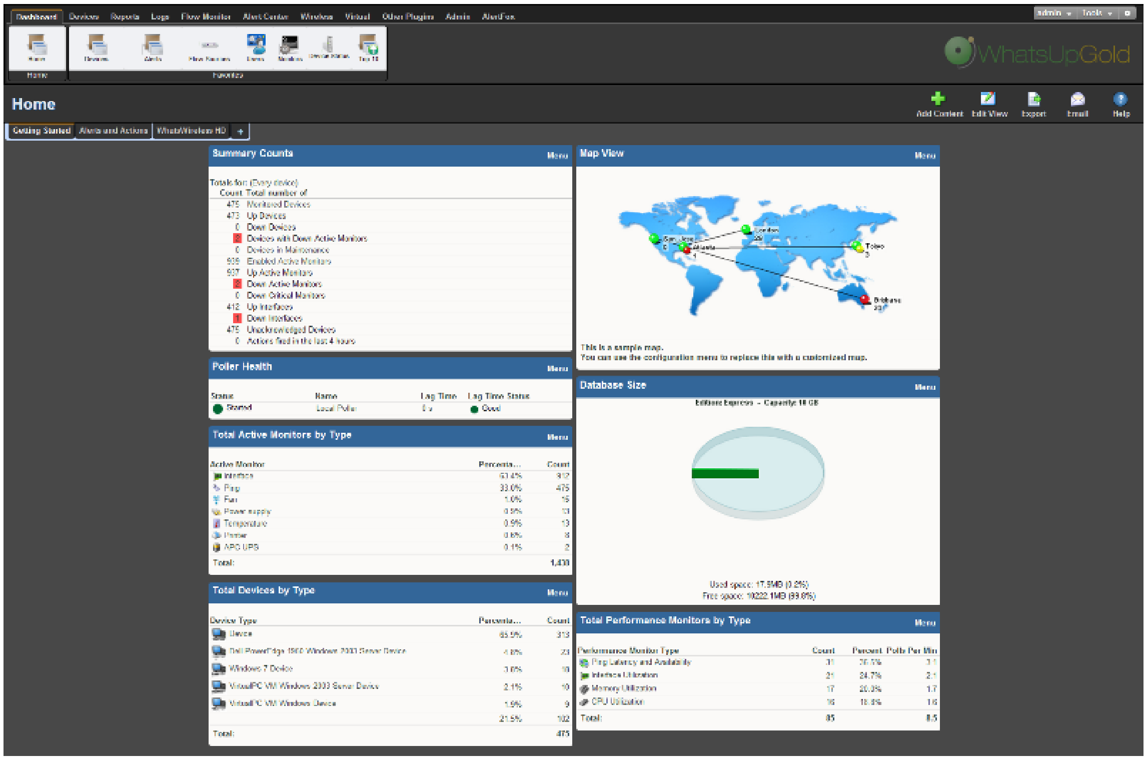
WhatsUp Gold actively polls devices to determine their status. You can use active monitors to poll services on a device and passively listen for messages sent across the network. Performance monitors track device performance by checking and reporting on device resources, such as disk, CPU, and interfaces.

Actions/Alerts

Depending on the responses received from polling, WhatsUp Gold fires actions to notify you of changes on your network. Actions aid in problem resolution through assorted options such as email and cell phone alerts, or service restarts. In addition to actions, WhatsUp Gold Alert Center notifies you of issues on passive and performance monitors, the WhatsUp Gold system, and WhatsUp Gold Flow Monitor through user-configured thresholds and notification policies.

Logs and Dashboards

Logs ensure 360-degree visibility into network status and performance, and historical data for devices and monitors. Dashboard reports let you focus on segments of the network and create your own views of report data. These views position crucial network data in one location, which allows for quick and easy access.



Summary Counts

Totals for: (Every device)

Count	Total number of
475	Monitored Devices
473	Up Devices
0	Down Devices
2	Devices with Down Active Monitors
0	Devices in Maintenance
939	Enabled Active Monitors
937	Up Active Monitors
2	Down Active Monitors
0	Down Critical Monitors
412	Up Interfaces
1	Down Interfaces
475	Unacknowledged Devices
0	Actions fired in the last 4 hours

Poller Health

Status	Name	Lag Time	Lag Time Status
● Started	Local Poller	0 s	● Good

Total Active Monitors by Type

Active Monitor	Percenta...	Count
Interface	63.4%	912
Ping	33.0%	475
Fan	1.0%	15
Power supply	0.9%	13
Temperature	0.9%	13
Printer	0.6%	8
APC UPS	0.1%	2
Total:		1,438

Total Devices by Type

Device Type	Percenta...	Count
Device	65.9%	313
Dell PowerEdge 1950 Windows 2003 Server Device	4.8%	23
Windows 7 Device	3.8%	18
VirtualPC VM Windows 2003 Server Device	2.1%	10
VirtualPC VM Windows Device	1.9%	9
	21.5%	102
Total:		475

Map View

This is a sample map.
You can use the configuration menu to replace this with a customized map.

Database Size

Edition: Express - Capacity: 10 GB

Used space: 17.9MB (0.2%)
Free space: 10222.1MB (99.8%)

Total Performance Monitors by Type

Performance Monitor Type	Count	Percent	Polls Per Min
Ping Latency and Availability	31	36.5%	3.1
Interface Utilization	21	24.7%	2.1
Memory Utilization	17	20.0%	1.7
CPU Utilization	16	18.8%	1.6
Total:	85		8.5

WhatsUp Gold Interfaces

WhatsUp Gold offers two core user interfaces, the Windows console interface and the web interface. You can accomplish discovery and mapping on the console or web interface, then setup of monitors and dashboard views, users and permissions, and do day-to-day monitoring on the web interface.

- **Windows console interface**. The console is a Windows application, through which you can configure and manage WhatsUp Gold and its database.
- **Web interface**. The web interface provides access to WhatsUp Gold functionality (via HTTP or HTTPS) from a web browser.

- **Mobile interface**. You can now conveniently view your network status from a mobile device through WhatsUp Gold Mobile interface.

WhatsUp Gold Editions

WhatsUp Gold is available in three primary editions. Each edition tailors features to meet the diverse network management needs, from small networks to those spanning multiple geographic locations. Learn more about WhatsUp Gold product editions and get a detailed view of the *WhatsUp Gold product comparisons* (http://www.whatsupgold.com/WUGProducts) on the WhatsUp Gold web site.

WhatsUp Gold also offers a variety of optional products to provide a full-line of advanced network monitoring tools:

Optional plug-ins

WhatsUp Gold WhatsConfigured. This configuration management plug-in enables effective management of one of the most critical assets on your network—device configurations. It automates the key configuration and change management tasks required to backup, compare, and upload configuration files for networking devices. WhatsConfigured maintains and controls configuration files and alerts when any configuration changes are detected. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/WhatsConfigured).

WhatsUp Gold Flow Monitor. plug-in for WhatsUp Gold leverages Cisco NetFlow, sFlow, J-Flow, and Border Gateway Protocol (BGP) data from switches, routers, and Adaptive Security Appliances (ASA) to gather, analyze, report, and alert on LAN/WAN network traffic patterns and bandwidth utilization in real-time. It highlights not only overall utilization for the LAN/WAN, specific devices, or interfaces; it also indicates users, applications, and protocols that are consuming abnormal amounts of bandwidth, giving you detailed information to assess network quality of service and quickly resolve traffic bottlenecks. WhatsUp Flow Monitor protects network security by detecting unusual activity, such as that exhibited by viruses, worms, DOS attacks, and other rogue activity directed at your network. Comprehensive reporting takes the raw real-time network traffic data from routers and switches and presents you with useful information to understand trends, utilization, and where network bandwidth is consumed. For more information, see the WhatsUp Gold Flow Monitor User Guide on the *WhatsUp Gold web site* (http://www.whatsupgold.com/NetFlowMonitor).

WhatsUp Gold WhatsVirtual. This plug-in lets you monitor virtual environments using WhatsUp Gold. The WhatsVirtual plug-in provides WhatsUp Gold with the ability to discover, map, monitor, alert, and report on virtual environments. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/WhatsVirtual).

WhatsUp Gold VoIP Monitor. This plug-in for WhatsUp Gold measures your network's ability to provide the quality of service (QoS) necessary for your VoIP calls on your LAN and WAN links. After a simple setup, the VoIP Monitor accesses Cisco IP SLA (service level agreement) enabled devices to monitor VoIP performance and quality parameters including jitter, packet loss, latency, and other performance values. The plug-in’s full integration with WhatsUp Gold allows you to easily view graphs and metrics for bandwidth and interface utilization and troubleshoot network issues that affect VoIP performance. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/products/Voip_Monitor).

Optional applications

WhatsUp Gold WhatsConnected. This application is a Layer 2/3 network mapping tool that discovers, maps and documents your network down to the individual port, making it simple to visualize the physical topology and understand device interconnections. This application is a standalone and is used separately from an instance of WhatsUp Gold. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/products/WhatsConnected).

WhatsUp Log Management. This application suite provides comprehensive event and Syslog log collection, monitoring, analysis, reporting and storage for your network. The suite includes Event Analyst, Event Archiver, Event Alarm and Event Rover. For more information, see the WhatsUp Gold web (http://www.whatsupgold.com/LogManagement)*site*. (http://www.whatsupgold.com/FlowPublish)

AlertFox End-User Monitor. This application provides comprehensive synthetic web transaction monitoring capabilities from an end-user perspective. With just a push of a button, a browser-based recorder captures all the steps involved in a web transaction, so you can periodically exercise and measure mission-critical transactions as often as you need to. AlertFox EUM is offered as Software-as-a-Service (SaaS), has minimal software to install, and requires no long-term financial commitments. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/AlertFoxEUM).

WhatsUp Gold Failover Manager. The WhatsUp Gold Failover Manager is designed to make your network monitoring and management tasks more resilient for high availability operation. It ensures continuous visibility into the health of the monitored infrastructure when the performance or connectivity of the primary WhatsUp Gold server is impaired. In such cases a secondary 'failover' server can be automatically set to take over monitoring tasks. WhatsUp Gold Failover Manager is integrated into the Alert Center for appropriate notifications and escalations. For more information, see the *WhatsUp Gold site* (http://www.whatsupgold.com/FailoverMgr).

WhatsUp Gold Flow Publisher. This application provides a unique insight and visibility into your network traffic for every device, whether they natively support flow monitoring or not. Flow Publisher makes flow monitoring possible for every network segment and for literally every device. By capturing raw traffic from the network and converting it into standard NetFlow records, Flow Publisher puts you in complete control and conversing in a language your users understand. For more information, see the *WhatsUp Gold site* (http://www.whatsupgold.com/FlowPublish).

IP Address Manager. This application provides an automated solution to the cumbersome and error prone task of inventorying network address usage. IP Address Manager discovery scans provide you with an extensive breakdown of your network's subnets, DHCP, and DNS servers. These discovery scans can be scheduled to run automatically to gather up-to-date inventory information on a daily basis. Inventory information can be saved, exported, and distributed in multiple formats as reports. For more information, see the *WhatsUp Gold site* (http://www.whatsupgold.com/IPAMsite).

New in Ipswitch WhatsUp Gold

Refer to the Ipswitch WhatsUp Gold *Release Notes* (http://www.whatsupgold.com/WUG16releasenotes) to learn about the latest product features, editions, system requirements, fixed in this release, known issues, and other

WhatsUp Gold information. Also see *About the WhatsUp Gold web interface* (on page 17) for highlight information about the web user interface.

Using the WhatsUp Gold community site

WUGspace is an WhatsUp Gold IT community centered around valuable technical content for network engineers, IT managers, Architects, and System Administrators. Visit the community for additional product information and help, learn from other users, submit product ideas, and more. Visit the WhatsUp Gold forum on the *WUGspace community site* (http://www.whatsupgold.com/wugspace).

Using the WhatsUp Customer Portal for product account information

For additional help and information about managing product licenses, go to the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses. The WhatsUp Customer Portal:

- Provides quick and easy access to your purchased software downloads
- Streamlines service agreement renewal purchases and software upgrades
- Handles offline activations
- Provides a central location for your support cases

For more information about viewing license information from the WhatsUp Gold web interface, see *Using Application Settings: System* (on page 20).

Finding more information and updates

Following are information resources for WhatsUp Gold. This information may be periodically updated and available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/support/index.aspx).

- **Release Notes**. The release notes provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for installing, upgrading, and configuring WhatsUp Gold. The release notes are available at **Start > Programs > Ipswitch WhatsUp Gold > Release Notes** or on the *WhatsUp Gold web site* (http://www.whatsupgold.com/WUG16releasenotes).
- **Application Help for the console and web interface**. The console and web help contain dialog assistance, general configuration information, and how-to's that explain how to use the features. The Table of Contents is organized by functional area, and can be accessed from the main menu or by clicking **Help** in the console, or the **?** icon in the web interface.
- **Getting Started Guide**. This guide provides an overview of WhatsUp Gold, information to help you get started using the application, the system requirements, and information about installing and upgrading. The Getting Started Guide is available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wug16gsg).

- **WhatsUp Community**. WUGspace is an WhatsUp Gold IT community centered around valuable technical content for network engineers, IT managers, Architects, and System Administrators. Visit the community for additional product information and help, learn from other users, submit product ideas, and more. Visit the WhatsUp Gold forum on the *WUGspace community site* (http://www.whatsupgold.com/wugspace).
- **Additional WhatsUp Gold resources**. For a list of current and previous guides and help available for WhatsUp Gold products, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/support/guides.aspx).
- **Licensing Information**. Licensing and support information is available on the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.
- **Technical Support**. Use the WhatsUp Gold Support Site for a variety of WhatsUp Gold product help resources. From here you can view product documentation, search Knowledge Base articles, access the community site for help from other users, and get other Technical Support information. The Support Site is available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/support/index.aspx).

Getting Familiar with WhatsUp Gold

In This Chapter

Using the WhatsUp Gold Web Interface

Accessing the web interface

✓ **Important**: Make sure that you use IPv4 compatible addresses to access the WhatsUp Gold web interface.

You can connect to the WhatsUp Gold web interface from any supported browser by entering the WhatsUp Gold web address. This web address consists of the hostname of the WhatsUp Gold host and the web server port number.

For example, if your WhatsUp Gold host is named `monitor1.ipswitch.com`, and it is connected to default port 80 then the web address is:
`http://monitor1.ipswitch.com`
- or -
`http://monitor1.ipswitch.com:80`

Note: When you use the default web server port (80), you do not have to include the port in the address, but all other ports require the port number following the url.

There are two default users on the Web server:

Account type	**Username**	**Password**
Administrator	`admin`	`admin`
Guest	`guest`	`<password left blank>`

Note: Microsoft Internet Information Services (IIS) is used for the WhatsUp Gold web server. For more information, see the *Configuring the web server* section of the *Installing and Configuring WhatsUp Gold* (http://www.whatsupgold.com/wugiis_16) guide.

About the WhatsUp Gold web interface

The WhatsUp Gold web interface allows you to view and modify most WhatsUp Gold features from a web browser. From the web interface, you can:

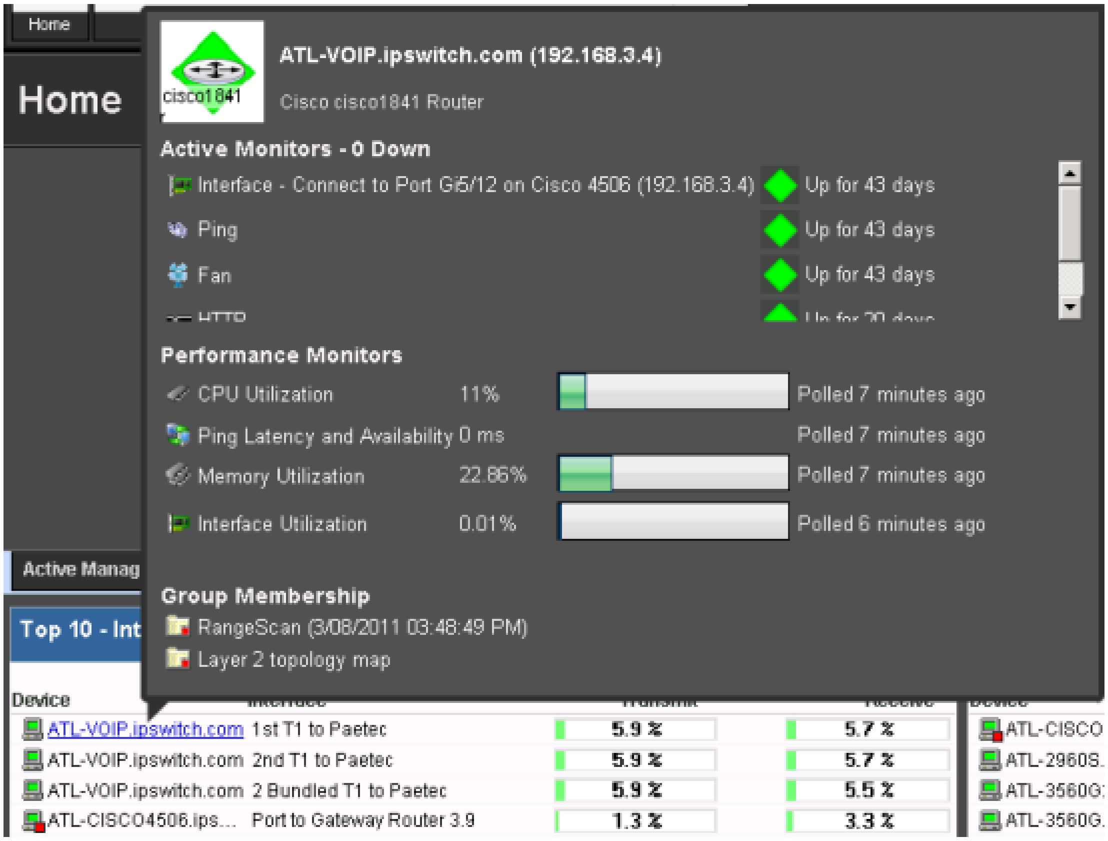
- Discover network devices
- Configure monitors, alerts, and actions
- View reports for devices and groups of devices
- View Layer 2 network topology maps
- Manage admin features

Reporting features are available in the web interface. Full reports and dashboard reports provide information about device status and performance. Full reports are located in the *Reports* (on page 350) and *Logs* (on page 419) tabs and dashboard reports are located in the Dashboard tab under **Home**.

If you have used previous versions of the WhatsUp Gold web interface, you'll notice changes designed to make WhatsUp Gold easier to navigate and use. Here's more about the interface:

- **Application tabs and button names**. Some of the tabs and buttons on the navigation bar have been renamed and shortened to help you access the web interface application features easier.
- **Settings icon (⚙)**. From the new settings icon, you may access the Ipswitch website, training information, application help, *application settings* (on page 20), and the WhatsUp Gold Knowledgebase.
- **More features**. New product features have been added or updated to the WhatsUp Gold family:
- **Wireless** included with WhatsUp Gold Premium Edition
- **Asset Inventory** included with WhatsUp Gold Standard and Premium Editions
- **WhatsVirtual** integrated in WhatsUp Gold when purchased as a plug-in
- **WhatsConfigured** integrated in WhatsUp Gold when purchased as a plug-in
- **How do I logout?** The logout feature has been moved under the username in the top right corner of each page.
- **Tab changes**. The WhatsUp Gold user interface is transitioning to a new look, so the Virtual and Wireless tabs have a different page presentation.
- **How do I collapse the navigation bar to make more viewable content pane space?** Click an active or selected tab to collapse the navigation bar and click again to expand the navigation bar again.

- **Device popups** provide a quick view of device performance, active monitor, and group membership information. From a device list or report view, hover the mouse pointer over a device name to view popup information.



ATL-VOIP.ipswitch.com (192.168.3.4)

Cisco cisco1841 Router

Active Monitors - 0 Down

Interface - Connect to Port Gi5/12 on Cisco 4506 (192.168.3.4)	Up for 43 days
Ping	Up for 43 days
Fan	Up for 43 days
HTTP	Up for 20 days

Performance Monitors

CPU Utilization	11%	Polled 7 minutes ago
Ping Latency and Availability	0 ms	Polled 7 minutes ago
Memory Utilization	22.86%	Polled 7 minutes ago
Interface Utilization	0.01%	Polled 6 minutes ago

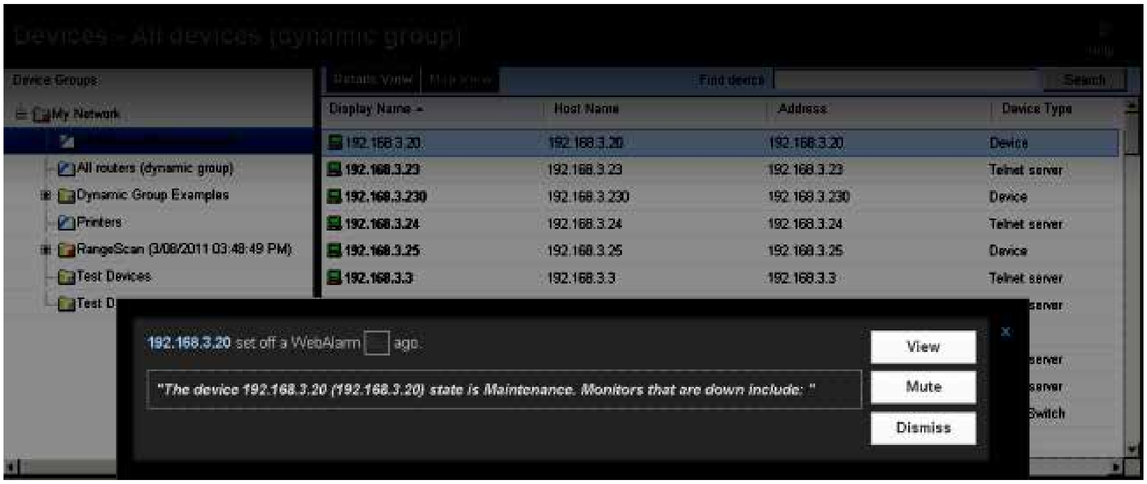
Group Membership

RangeScan (3/08/2011 03:48:49 PM)

Layer 2 topology map

Device	Interface	Transmit	Receive	Device
ATL-VOIP.ipswitch.com	1st T1 to Paetec	5.9 %	5.7 %	ATL-CISCO
ATL-VOIP.ipswitch.com	2nd T1 to Paetec	5.9 %	5.7 %	ATL-2960S.
ATL-VOIP.ipswitch.com	2 Bundled T1 to Paetec	5.9 %	5.5 %	ATL-3560G:
ATL-CISCO4506.ips...	Port to Gateway Router 3.9	1.3 %	3.3 %	ATL-3560G.

- **Message bar** provides informative and unobtrusive notification area for device status and other information at the bottom of the page.

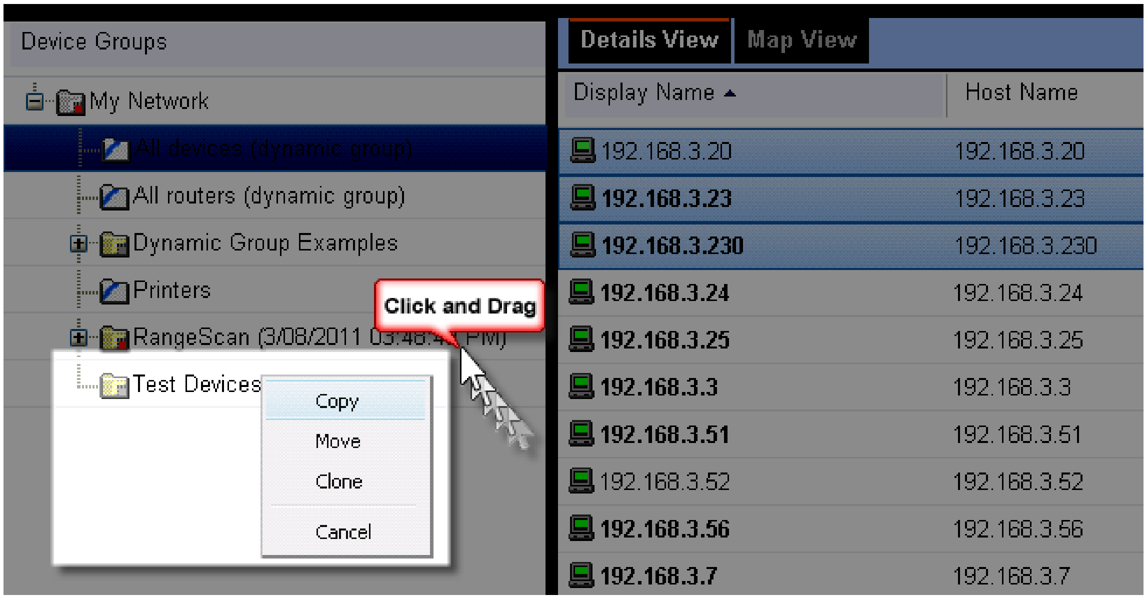


Display Name	Host Name	Address	Device Type
192.168.3.20	192.168.3.20	192.168.3.20	Device
192.168.3.23	192.168.3.23	192.168.3.23	Telnet server
192.168.3.230	192.168.3.230	192.168.3.230	Device
192.168.3.24	192.168.3.24	192.168.3.24	Telnet server
192.168.3.25	192.168.3.25	192.168.3.25	Device
192.168.3.3	192.168.3.3	192.168.3.3	Telnet server

192.168.3.20 set off a WebAlarm ago.

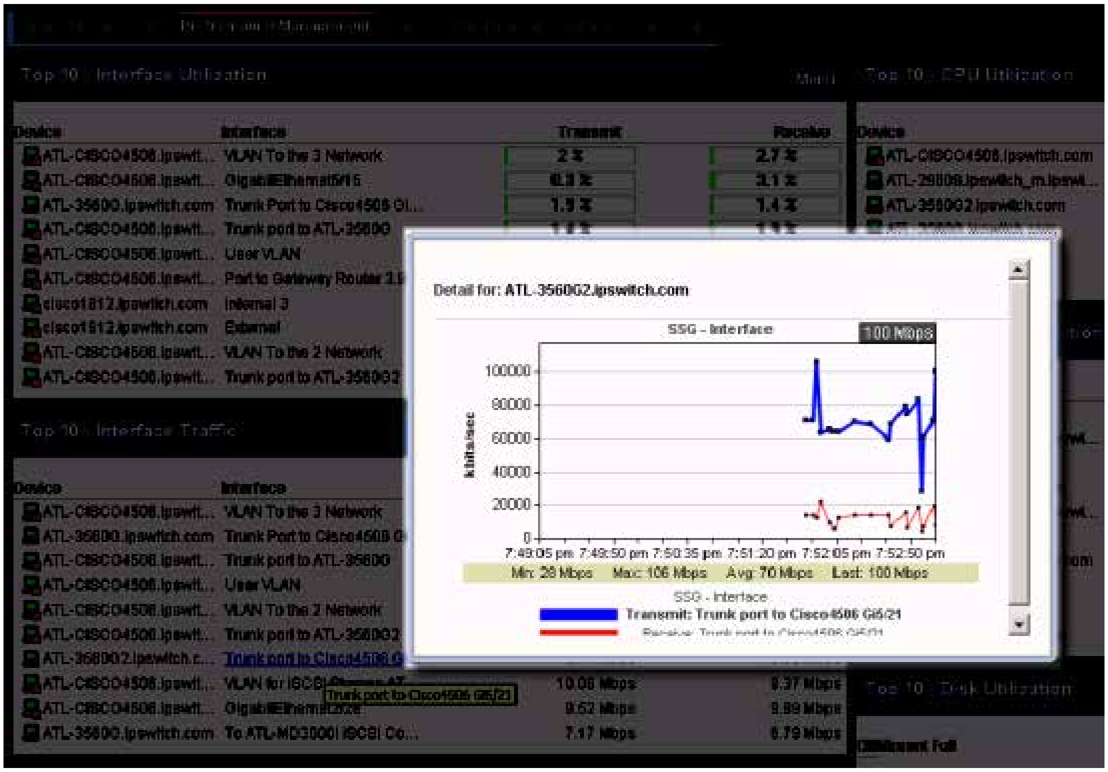
"The device 192.168.3.20 (192.168.3.20) state is Maintenance. Monitors that are down include: "

- **Drag-and-drop capabilities**. Drag devices to a new group, then confirm whether to copy, move, or clone devices.



Display Name ▲	Host Name
192.168.3.20	192.168.3.20
192.168.3.23	192.168.3.23
192.168.3.230	192.168.3.230
192.168.3.24	192.168.3.24
192.168.3.25	192.168.3.25
192.168.3.3	192.168.3.3
192.168.3.51	192.168.3.51
192.168.3.52	192.168.3.52
192.168.3.56	192.168.3.56
192.168.3.7	192.168.3.7

- **Split Second Graphs (InstantInfo popups)** provide real-time information on SNMP and WMI performance counters for the devices on your network. From a device list, reports, or dashboard views, hover the mouse pointer over device items such as the interface, CPU, and memory names to view split second graph information.



Top 10 - Interface Utilization

Device	Interface	Transmit	Receive
ATL-CISCO4506.ipswit...	VLAN To the 3 Network	2 %	2.7 %
ATL-CISCO4506.ipswit...	GigabitEthernet5/15	0.3 %	3.1 %
ATL-3560G.ipswitch.com	Trunk Port to Cisco4506 Gi...	1.5 %	1.4 %
ATL-CISCO4506.ipswit...	Trunk port to ATL-3560G	[illegible]	[illegible]
ATL-CISCO4506.ipswit...	User VLAN		
ATL-CISCO4506.ipswit...	Port to Gateway Router 1.1		
cisco1812.ipswitch.com	Internal 3		
cisco1812.ipswitch.com	External		
ATL-CISCO4506.ipswit...	VLAN To the 2 Network		
ATL-CISCO4506.ipswit...	Trunk port to ATL-3560G2		

Top 10 - CPU Utilization

Device
ATL-CISCO4506.ipswitch.com
ATL-2950G.ipswitch_m.ipswi...
ATL-3560G2.ipswitch.com

Top 10 - Interface Traffic

Device	Interface		
ATL-CISCO4506.ipswit...	VLAN To the 3 Network		
ATL-3560G.ipswitch.com	Trunk Port to Cisco4506 G		
ATL-CISCO4506.ipswit...	Trunk port to ATL-3560G		
ATL-CISCO4506.ipswit...	User VLAN		
ATL-CISCO4506.ipswit...	VLAN To the 2 Network		
ATL-CISCO4506.ipswit...	Trunk port to ATL-3560G2		
ATL-3560G2.ipswitch.c...	Trunk port to Cisco4506 G		
ATL-CISCO4506.ipswit...	VLAN for iSCSI	10.08 Mbps	9.37 Mbps
ATL-CISCO4506.ipswit...	GigabitEthernet2/26	9.62 Mbps	9.89 Mbps
ATL-3560G.ipswitch.com	To ATL-MD3000i iSCSI Co...	7.17 Mbps	6.79 Mbps

Detail for: ATL-3560G2.ipswitch.com

Min: 28 Mbps Max: 106 Mbps Avg: 70 Mbps Last: 100 Mbps

SSG - Interface

Transmit: Trunk port to Cisco4506 Gi6/21

Receive: Trunk port to Cisco4506 Gi6/21

Using Application Settings: System

The System Application Settings page allows you to configure your WhatsUp Gold help preferences. You can also view current product license and plug-in information. To access the System Application Settings, click the settings icon **(⚙) > Application Settings**.

Help

To set your preferred help source, select one of the following:

- **Use online help**. Select this option to use WhatsUp Gold help located on the WhatsUp Gold web site. You must have an internet connection to use this help.
- **Use local help**. Select this option to use WhatsUp Gold help located in the local WhatsUp Gold application folders. This help is included with the WhatsUp Gold installation.

About (license information)

To view current license and plug-in information, click **About WhatsUp Gold...**. The About WhatsUp Gold dialog appears with the following information:

- License Type
- Serial Number
- Edition
- Maximum Devices

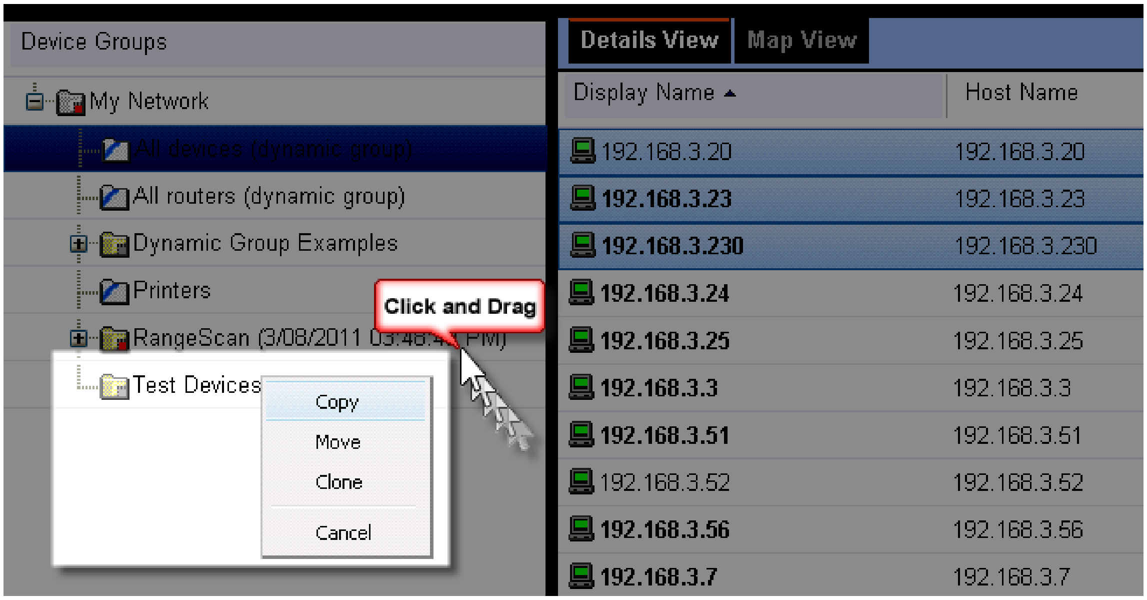
The About WhatsUp Gold dialog also displays the number of devices that are currently monitored in relation to the maximum number of licensed devices that are available. Additionally, the About WhatsUp Gold dialog lists each plug-in for which you are licensed and any other applicable information about the plug-in:

- **Plug-in**. Displays the name of the product.
- **License Type**. Displays the type of license currently active for your WhatsUp Gold installation.
- **Time Remaining**. Displays the amount of time left to use the plug-in before it expires.
- **Current Limit**. Displays the current/maximum numbers of data sources used by the plug-in.

For additional help and information about managing your product license, go to the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Organizing devices, device groups, and maps with drag-and-drop

In the Device and Map views, you can quickly and easily organize devices and device groups by dragging the device you want in a particular group to the device group folder.



Display Name ▲	Host Name
192.168.3.20	192.168.3.20
192.168.3.23	192.168.3.23
192.168.3.230	192.168.3.230
192.168.3.24	192.168.3.24
192.168.3.25	192.168.3.25
192.168.3.3	192.168.3.3
192.168.3.51	192.168.3.51
192.168.3.52	192.168.3.52
192.168.3.56	192.168.3.56
192.168.3.7	192.168.3.7

After you drop the icon or icons, a menu appears, asking if you want to move or copy the devices. If you move the devices, they are deleted from the previous device group. If you copy the devices, the devices appear in both device groups. For more information, see *Managing devices* (on page 96).

Note: When you copy a device using drag-and-drop, a shortcut is created in the new location. Even though a device exists in multiple locations, it only exists once in the database. Therefore, to modify a device, you can change the settings by opening the device properties from any group in which the device appears, and the change is reflected in all other instances of the device. This also means that each device is only polled once, no matter how many times it appears in your device group tree.

About the Task Tray and Desktop Actions icon

WhatsUp Gold installs two task bar icons on your computer; the Status Tray icon and the Desktop Actions Icon.

Status Tray

The Status Tray icon automatically displays popup messages about WhatsUp Gold polling activity as they are generated.

To configure Status Tray message preferences:

1 Click on the icon to launch a dialog that reports the message server status and the number of status messages that are available.

2 Click Advanced View to open the WhatsUp Gold Status Center configuration dialog.

- On the Messages tab, you can click **Clear All** to delete current status messages.
- On the Message Settings tab, you can select the desired check boxes to enable and/or filter message types.
- On the Poller Configuration tab, you can modify the Service Bus IP and the Service Port for the local poller.

Note: If the Service Bus IP or the Service Bus IP is changed, click **Save** and **Restart** to save changes and restart the polling controller.

3 Close the dialog to save any changes made to the Message Settings.

Desktop Actions

The Desktop Actions icon displays to indicate that the application for Sound and Text-to-Speech actions is turned on.

Note: Desktop Actions must be running for the Sound and Text-to-Speech actions to work.

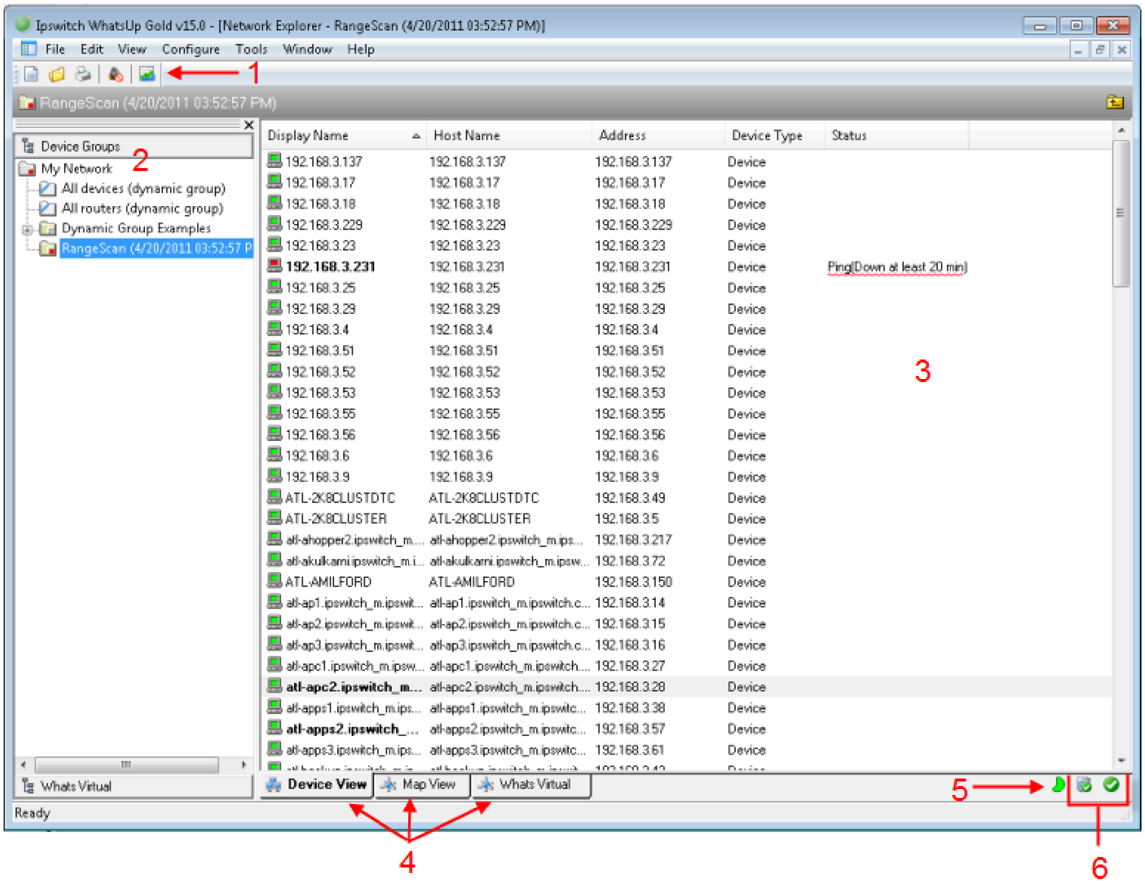
To turn off the Desktop Actions icon , right-click the icon, then click Close.

Note: Sound and Text-to-Speech actions are disabled when you close the Desktop Actions icon.

Using the WhatsUp Gold Console

About the console

The WhatsUp Gold console is a Windows application used for the configuration and management of WhatsUp Gold and its database. The console has six main components, which are indicated on the image below.


Ipswitch WhatsUp Gold v15.0 - [Network Explorer - RangeScan (4/20/2011 03:52:57 PM)]
File
Edit
View
Configure
Tools
Window
Help
1
RangeScan (4/20/2011 03:52:57 PM)
Device Groups
2
My Network
All devices (dynamic group)
All routers (dynamic group)
Dynamic Group Examples
RangeScan (4/20/2011 03:52:57 P
3
Whats Virtual
Device View
Map View
Whats Virtual
5
Ready
4
6

Display Name	Host Name	Address	Device Type	Status
192.168.3.137	192.168.3.137	192.168.3.137	Device	
192.168.3.17	192.168.3.17	192.168.3.17	Device	
192.168.3.18	192.168.3.18	192.168.3.18	Device	
192.168.3.229	192.168.3.229	192.168.3.229	Device	
192.168.3.23	192.168.3.23	192.168.3.23	Device	
192.168.3.231	192.168.3.231	192.168.3.231	Device	Ping(Down at least 20 min)
192.168.3.25	192.168.3.25	192.168.3.25	Device	
192.168.3.29	192.168.3.29	192.168.3.29	Device	
192.168.3.4	192.168.3.4	192.168.3.4	Device	
192.168.3.51	192.168.3.51	192.168.3.51	Device	
192.168.3.52	192.168.3.52	192.168.3.52	Device	
192.168.3.53	192.168.3.53	192.168.3.53	Device	
192.168.3.55	192.168.3.55	192.168.3.55	Device	
192.168.3.56	192.168.3.56	192.168.3.56	Device	
192.168.3.6	192.168.3.6	192.168.3.6	Device	
192.168.3.9	192.168.3.9	192.168.3.9	Device	
ATL-2K8CLUSTDTC	ATL-2K8CLUSTDTC	192.168.3.49	Device	
ATL-2K8CLUSTER	ATL-2K8CLUSTER	192.168.3.5	Device	
atl-ahopper2.ipswitch_m....	atl-ahopper2.ipswitch_m.ips...	192.168.3.217	Device	
atl-akulkarni.ipswitch_m.i...	atl-akulkarni.ipswitch_m.ipsw...	192.168.3.72	Device	
ATL-AMILFORD	ATL-AMILFORD	192.168.3.150	Device	
atl-ap1.ipswitch_m.ipswit...	atl-ap1.ipswitch_m.ipswitch.c...	192.168.3.14	Device	
atl-ap2.ipswitch_m.ipswit...	atl-ap2.ipswitch_m.ipswitch.c...	192.168.3.15	Device	
atl-ap3.ipswitch_m.ipswit...	atl-ap3.ipswitch_m.ipswitch.c...	192.168.3.16	Device	
atl-apc1.ipswitch_m.ipsw...	atl-apc1.ipswitch_m.ipswitch....	192.168.3.27	Device	
atl-apc2.ipswitch_m...	atl-apc2.ipswitch_m.ipswitch....	192.168.3.28	Device	
atl-apps1.ipswitch_m.ips...	atl-apps1.ipswitch_m.ipswitc...	192.168.3.38	Device	
atl-apps2.ipswitch_...	atl-apps2.ipswitch_m.ipswitc...	192.168.3.57	Device	
atl-apps3.ipswitch_m.ips...	atl-apps3.ipswitch_m.ipswitc...	192.168.3.61	Device	

1 **WhatsUp Gold Toolbar**. The icons on this toolbar change according to the view you are currently using. Button functions are identified with mouse-over tooltips. Additional toolbar icons can be enabled for the Map view by selecting **View > Toolbars**.

2 **Device Group Tree**. This is a list of all device groups created through WhatsUp Gold. When you perform a discovery scan, WhatsUp Gold creates a top level folder for that scan. All discovered subnetworks are created in subgroups, but can be organized, deleted, or renamed to fit your needs.

3 **View pane**. This pane displays the selected device group based on the view from the tabs below (Device View or Map View).

4 **View selectors**. Choose the way you want to view your device groups. Each of these views are explained in detail later in this chapter.

- § **Device View**. This view provides an overview of each device and subgroup in a selected device group.

- **Map View**. This view shows a graphical representation of the devices and subgroups in a selected device group.
- **WhatsVirtual**. This tab displays the Whats Virtual plug-in. You must have WhatsVirtual licensed and enabled for this View to display. To upgrade your license to include WhatsVirtual, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

5 **Polling Indicator Icons**. These icons indicate the current state of the poll engine.

Poll engine is connected	Poll engine is not connected	Polling is enabled	Polling is disabled

6 **Database Size Indicator Icon.** This icon shows the current size of your database. The color and shape changes according the database size thresholds:

🟢	49% and below
🟡	50% to 74%
🔴	75% and above

About the Task Tray and Desktop Actions icon

WhatsUp Gold installs two task bar icons on your computer; the Status Tray icon and the Desktop Actions Icon.

Status Tray

The Status Tray icon automatically displays popup messages about WhatsUp Gold polling activity as they are generated.

To configure Status Tray message preferences:

1 Click on the icon to launch a dialog that reports the message server status and the number of status messages that are available.

2 Click Advanced View to open the WhatsUp Gold Status Center configuration dialog.

- On the Messages tab, you can click **Clear All** to delete current status messages.
- On the Message Settings tab, you can select the desired check boxes to enable and/or filter message types.
- On the Poller Configuration tab, you can modify the Service Bus IP and the Service Port for the local poller.

Note: If the Service Bus IP or the Service Bus IP is changed, click **Save** and **Restart** to save changes and restart the polling controller.

3 Close the dialog to save any changes made to the Message Settings.

Desktop Actions

The Desktop Actions icon displays to indicate that the application for Sound and Text-to-Speech actions is turned on.

Note: Desktop Actions must be running for the Sound and Text-to-Speech actions to work.

To turn off the Desktop Actions icon , right-click the icon, then click Close.

Note: Sound and Text-to-Speech actions are disabled when you close the Desktop Actions icon.

Using Discovery Console

Learning about the Discovery Console

The Discovery Console performs network scans to identify network devices and the *role* each device performs on the network. The WhatsUp Gold discovery is based on templates that are configured in the Device Roles, for more information see *Using Device Roles* (on page 56) in the WhatsUp Gold console application. The templates consists of:

§ a set of criteria that a device must meet to match the discovery template. The criteria helps identify a device based on device role, brand/mode, OS, etc.

§ a set of default configuration items to be applied to a device that matches this template.

Before you run a network discovery, you need to configure the discovery settings. You can configure the *discovery settings* (on page 45) in the the Discovery Console, available in the WhatsUp Gold web interface (**Devices > Discovery Console**) or the WhatsUp Gold console (**File > Discover Devices**). The discovery settings are located in the Settings column on the left section of the Discovery Console. For more info, see the *Discovery Console* (on page 43) section.

After running a discovery, use the following sections of the Discovery Console to view and manage discoveries:

§ *Devices Discovered* (on page 51)

§ *Progress Summary information* (on page 50)

§ *Device Information tab* (on page 55)

§ *Scheduled Discoveries tab* (on page 53)

§ *Saved Results tab* (on page 56)

Using WhatsUp Gold Mobile Access

About WhatsUp Gold Mobile Access

WhatsUp Gold provides mobile access to the WhatsUp Gold network management application. You can conveniently view your network's status from a mobile device at anytime. This WhatsUp Gold feature ensures that you are informed about network issues so that you can maintain critical network performance.

Mobile Access supported browsers

Because WhatsUp Gold Mobile Access does not depend on JavaScript to function, most mobile web browsers support it. However, a JavaScript enabled browser enhances WhatsUp Gold's look and navigation.

Note: Cookies are required for the standard web session to function.

Browsers supported to access the WhatsUp Gold Mobile interface: Mobile Safari 4.2, 5.x; Microsoft Internet Explorer Mobile 6.1.x; or Opera Mini 4.2WhatsUp Gold mobile interface

Tip: You may need to adjust your browser's viewing options to optimize for your device's browser.

Managing WhatsUp Gold mobile access

The WhatsUp Gold Mobile Access feature is enabled by default for the WhatsUp Admin account. You can provide access to other WhatsUp Gold users from the Edit User dialog.

Use the following configuration options to manage Mobile Access.

To enable or disable WhatsUp Gold Mobile Access (globally) in the Manage Web Server configuration options:

1 From the WhatsUp Gold web interface, go to **Admin > Server Options**. The Manage Server Options dialog appears.
2 Select the **Enable Mobile Access** option.

To enable or disable WhatsUp Gold Mobile Access users in the Manage Users configuration options:

1 From the WhatsUp Gold web interface, go to **Admin > Users**. The Manage Users dialog appears.
2 Select the user for which you want to grant mobile access to WhatsUp, then click **Edit**. The Edit User dialog appears.
3 Under Account Administration, select **Mobile Access**.

Accessing WhatsUp Gold from a mobile device

You can access the WhatsUp Gold mobile interface from any supported mobile device browser.

To access WhatsUp Gold from a mobile device:

1 Enter the WhatsUp Gold web address which includes the hostname of the WhatsUp Gold host, the web server port number, followed by `/NmConsole/Mobile/Start`. The default port number is 80. The mobile access login screen opens.

For example, if your WhatsUp Gold host is named `monitor1.ipswitch.com`, then the web address is:

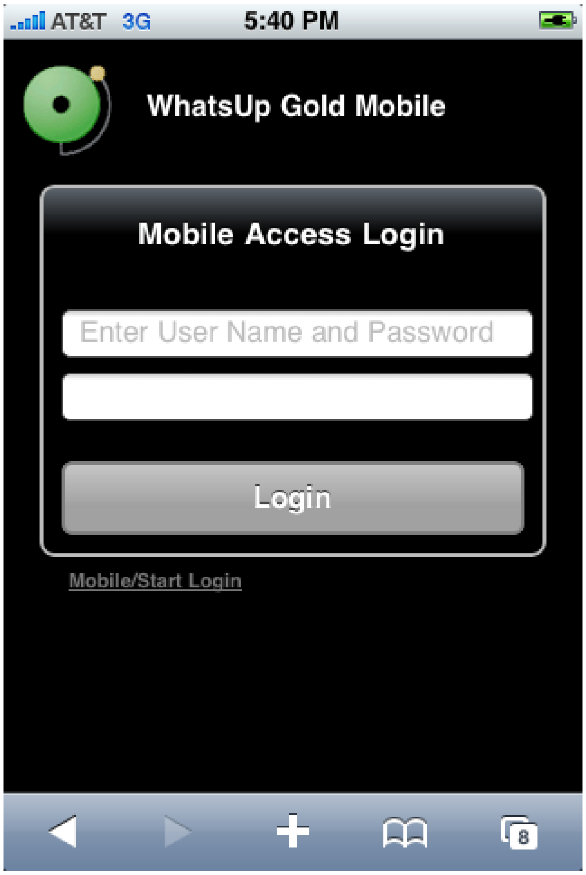
`http://monitor1.ipswitch.com/NmConsole/Mobile/Start/`
- or -

`http://monitor1.ipswitch.com:80/NmConsole/Mobile/Start/`

Note: When you use the default web server port (80), you do not have to include the port in the address. All ports other than 80 require that the port number follow the url in the web address.

Note: If you want WhatsUp Gold Mobile Access to be accessible via the Internet (for example, via mobile phones using 3G or 4G), then make sure it is available on a server with a public IP.

2 Enter your **Username** and **Password**, then click **Login**.



Mobile/Start Login

In addition to the standard login, WhatsUp Gold Mobile Access includes a one-click login feature. Because entering text in a mobile phone can be time consuming, WhatsUp Gold allows you to create up to four one-click logins per mobile device. You can bookmark each login or add to a mobile device Home Screen. One-click logins create an encrypted cookie on the user's mobile phone that includes a username, password, root url (which helps with SSL redirects), and the user's last visited page (excluding dialogs) for session timeouts.

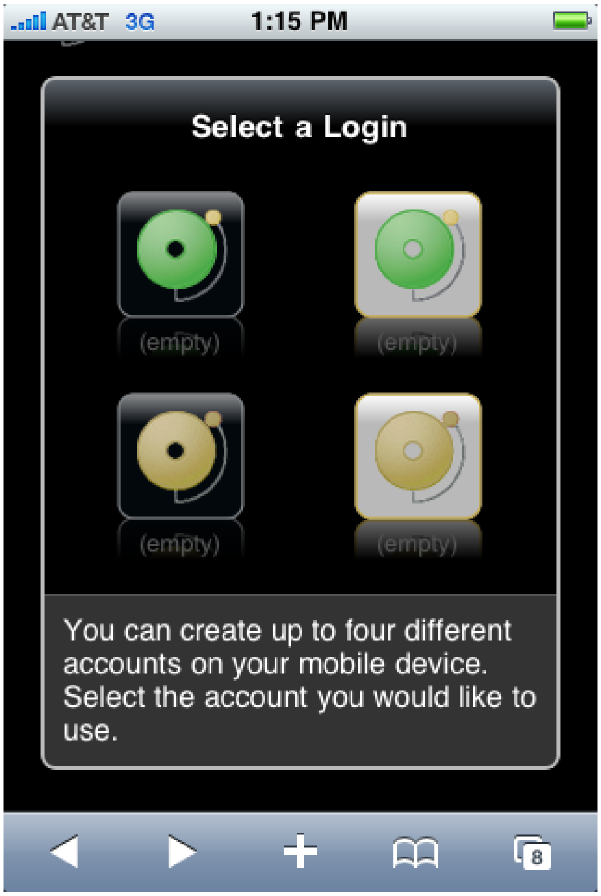
To create a new Mobile/Start Login:

1 Navigate to `NmConsole/Mobile/Start/`

2 Click **Create New Login**. The Mobile Start utility appears.

3 Click **Start**. The Select a Login dialog appears.

> **Tip**: If WhatsUp Gold is configured to use an SSL connection and you are not using a secure connection, you can click **Switch to Secure Login** to login on an SSL connection before creating a one-click login.



You can create up to four different accounts on your mobile device. Select the account you would like to use.

4 Select the login icon you want to use for the one-click login. The Create Login dialog appears.

5 Enter the **Username** and **Password**, then click **Create Mobile Login**. The Login Created dialog appears.

6 Click **Done**.

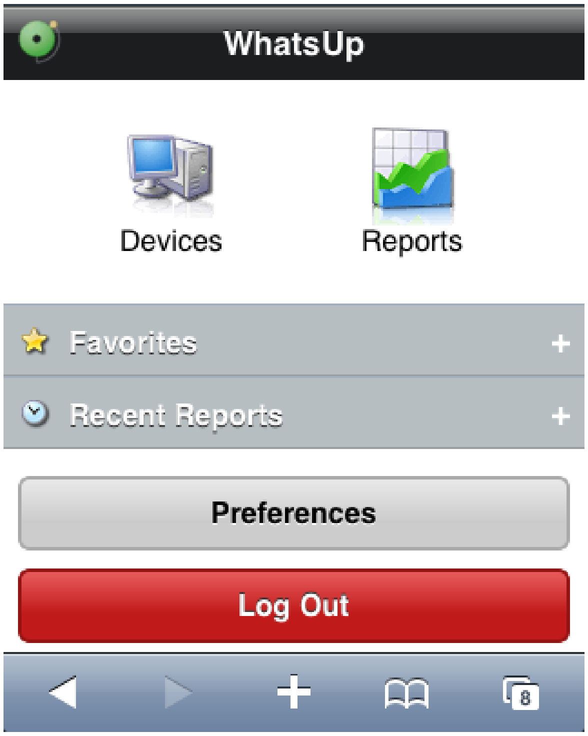
To login via the Mobile/Start Login:

Note: If you want WhatsUp Gold Mobile Access to be accessible via the Internet (for example, via mobile phones using 3G or 4G), then make sure it is available on a server with a public IP.

1. Start the WhatsUp Gold Mobile Access application on your mobile device browser.
2. On the login page, click **Mobile/Start Login**. The Mobile/Start Login page appears.
3. Click the login icon for the account with which you want to login to WhatsUp Gold.

Navigating and using the WhatsUp Gold Mobile Access home screen

After you log in, the WhatsUp Gold Mobile Access home screen opens.

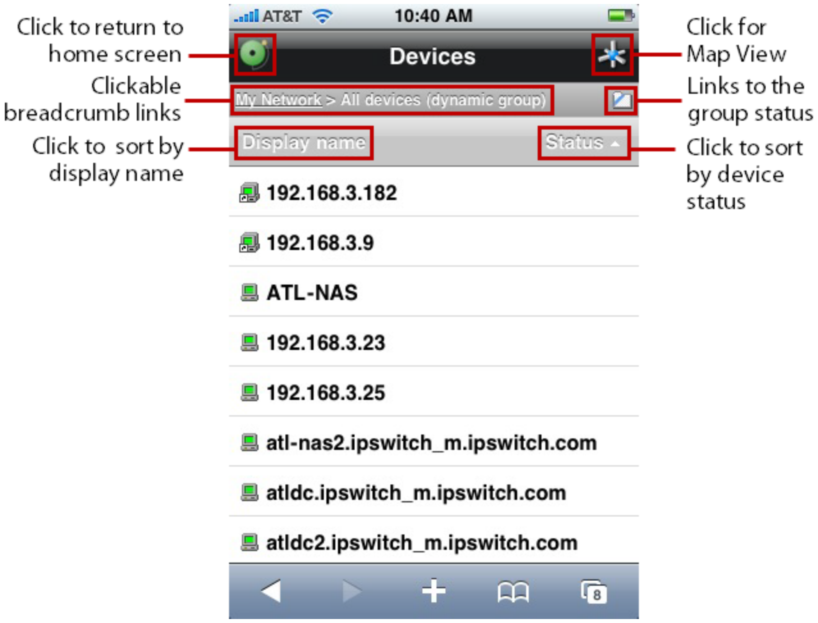


The home screen includes links to key WhatsUp Gold features so that you can view reports and monitor your network devices from remote locations:

- Devices
- Reports
- Favorites
- Recent Reports
- Preferences
- Log Out

Using Mobile Access device list

Click Devices to access the WhatsUp Gold Mobile Access Device View and Map View. Within the Devices view, you can view individual device and device group reports.



Click to return to home screen

Clickable breadcrumb links

Click to sort by display name

Click for Map View

Links to the group status

Click to sort by device status

192.168.3.182

192.168.3.9

ATL-NAS

192.168.3.23

192.168.3.25

atl-nas2.ipswitch_m.ipswitch.com

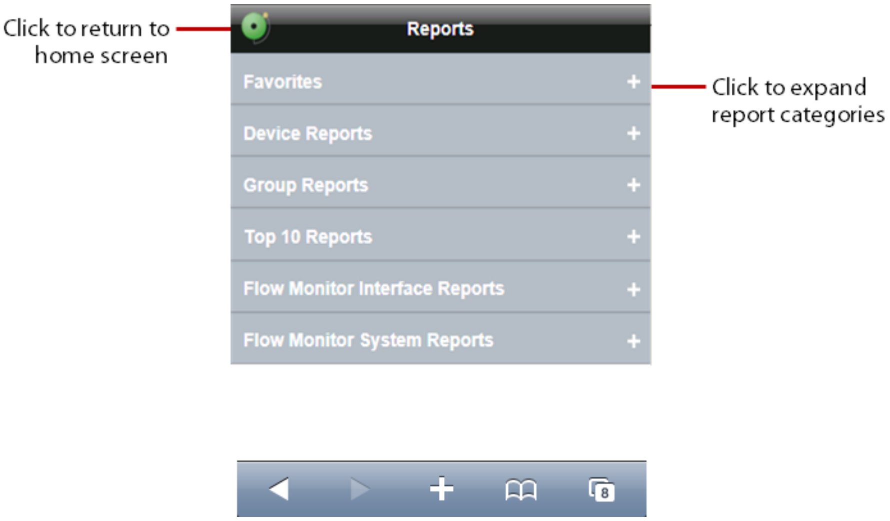
atldc.ipswitch_m.ipswitch.com

atldc2.ipswitch_m.ipswitch.com

Click a device to view device reports or click a device group to view devices within a group.

Using Mobile Access reports

Click Reports to access WhatsUp Gold Mobile Access Reports. Mobile Access is primarily a reporting tool designed to extend remote access to your network information. There are a number of standard WhatsUp Gold reports that are available as WhatsUp Gold mobile reports.



Click to return to home screen

Click to expand report categories

Each report includes options to specify the report data you want to view, such as date range, chart preferences, add to favorites, and other options. If you have the WhatsUp Gold Flow Monitor, Flow Monitor reports are also available in WhatsUp Gold Mobile Access.

Configuring device Notes and Attributes

All device Notes and Attributes information that you want to view from your mobile device reports must be set up in the WhatsUp Gold console or web interface Device Properties dialog. You can add phone numbers, email addresses, and Google Maps addresses to function as links on mobile devices with browsers that support these features.

To add a phone number as a Note or Attribute:

1. From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.
2. In the **Attribute** or **Note** field, use standard html code for a phone number link. For example:
   ```
   <a href="tel:(123) 123-1234">(123) 123-1234</a>
   ```

To add an email address as a Note or Attribute:

1. From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.
2. In the **Attribute** or **Note** field, use standard html code for an email link. For example:
   ```
   <a href="mailto:<John Doe> jdoe@ipswitch.com">John Doe</a>
   ```

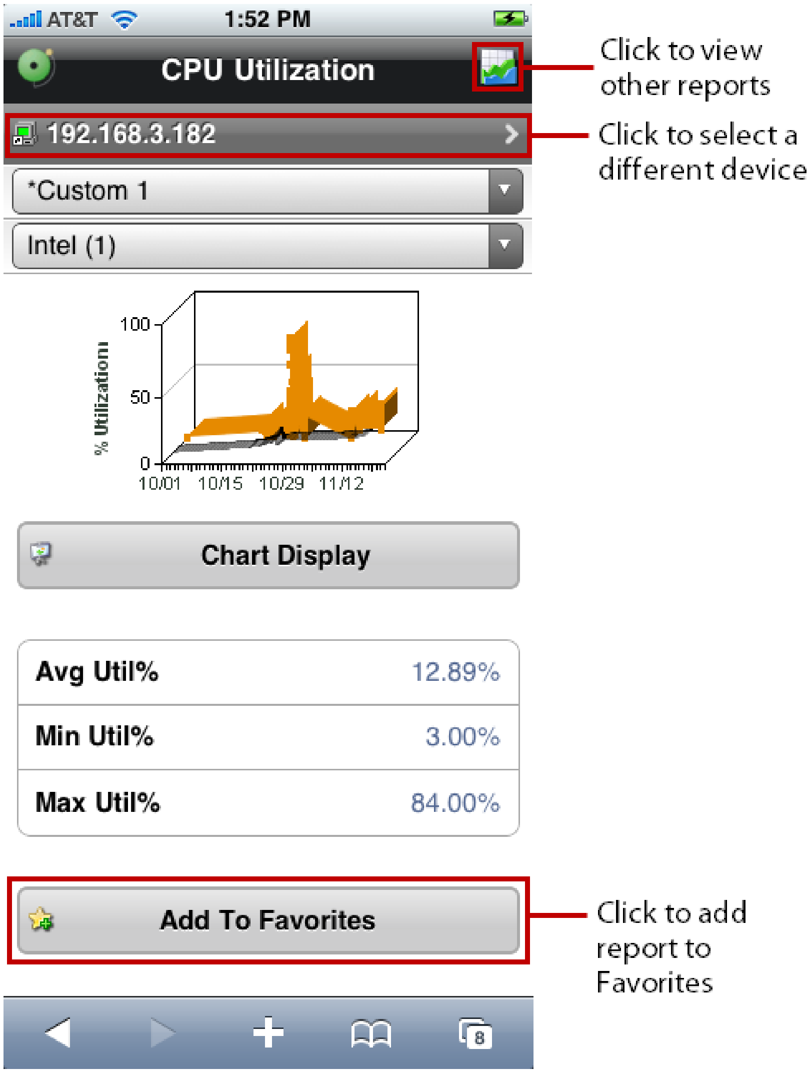
To add a Google Map address as a Note or Attribute:

1 From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.

2 In the **Attribute** or **Note** field, use standard html code for a Google map link. Google map links can be copied from the link field on the address's map view.

Using Mobile Access favorites

WhatsUp Gold Mobile Access Favorites allow you to group your favorite reports by clicking the **Add to Favorites** button at the bottom of each report.



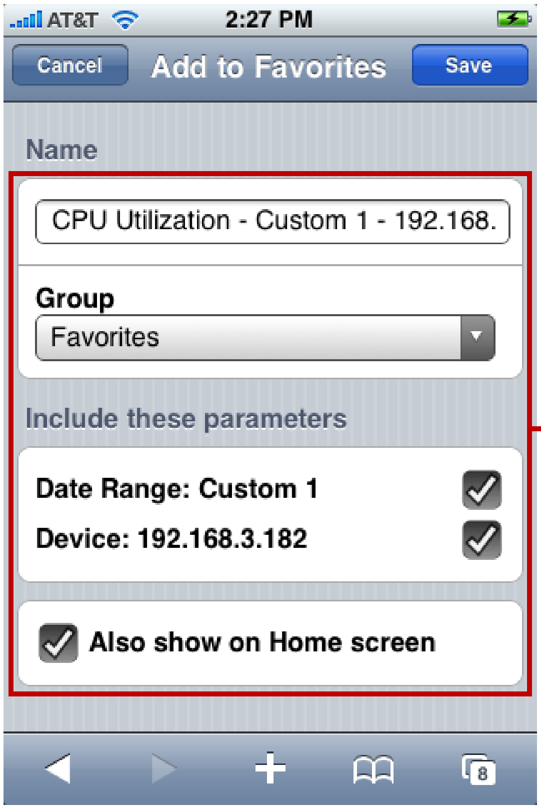
Avg Util%	12.89%
Min Util%	3.00%
Max Util%	84.00%

Click to view other reports

Click to select a different device

Click to add report to Favorites

When you mark a report as a favorite, you can use the options to save the specific report parameters such as the device, date range, and other report range selection criteria for the report. This helps you view your favorite reports with the report preconfigured for your viewing preferences. To add the Favorite report to your mobile device home screen, click **Also show on Home screen**.



Name

CPU Utilization - Custom 1 - 192.168.

Group

Favorites

Include these parameters

Date Range: Custom 1 ☑

Device: 192.168.3.182 ☑

☑ Also show on Home screen

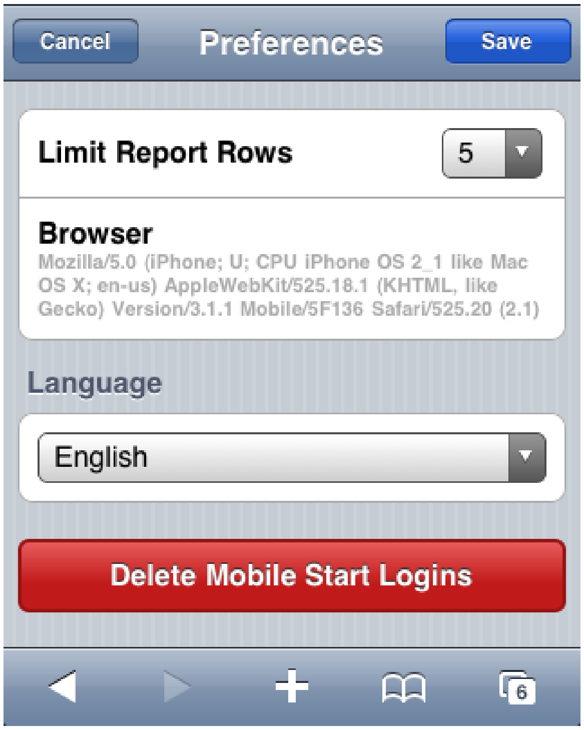
Enter and select report Favorite preferences

On the Home screen, click **Favorites** to expand and view your favorite reports. You can also click **Recent Reports** to view the ten most recent reports you have viewed.

Using Mobile Access preferences

Click the **Preferences** button on the Home screen to set your WhatsUp Gold Mobile Access preferences.

The Preferences dialog provides information about the browser and OS versions. You can also set a limit on the number rows displayed in a report and set the preferred viewing language.



Limit Report Rows 5

Browser
Mozilla/5.0 (iPhone; U; CPU iPhone OS 2_1 like Mac OS X; en-us) AppleWebKit/525.18.1 (KHTML, like Gecko) Version/3.1.1 Mobile/5F136 Safari/525.20 (2.1)

Language
English

In the Preferences dialog, when you click **Delete Mobile Start Logins**, all mobile start logins are deleted; no confirmation is required.

About Polling

In This Chapter

WhatsUp Gold Polling Engine Overview

The Ipswitch WhatsUp Gold Poller is an application used to perform and assign WhatsUp Gold device polling operations to monitor network devices. Specifically, additional pollers installed on your WhatsUp Gold system transmit active monitor and performance monitor data to the WhatsUp Gold server. Extending polling activity across multiple pollers increases the number of devices for which WhatsUp Gold can poll and collect data to send back to the WhatsUp Gold system. This is referred to as clustered polling. Using clustered polling, WhatsUp Gold can efficiently scale polling operations to a larger number of network devices, ultimately providing the capacity to monitor and manage larger networks.

Clustered polling is available to users with licenses for Ipswitch WhatsUp Gold Standard, Premium, Distributed, and Failover editions as well as to trial users working on Evaluation licenses for WhatsUp Gold. Pollers may be installed on any Windows system on the network, other than the WhatsUp Gold server. By default, the WhatsUp Gold poller is installed on the WhatsUp Gold system when you install the WhatsUp Gold application. Additional poller licenses may be purchased and added to your WhatsUp Gold system.

During installation, you must configure each poller to send data to the WhatsUp Gold server by entering a name to identify the poller, the server name or IP address to identify the device running WhatsUpGold, and valid credentials required to access the WhatsUp Gold host computer. You must also use this information to configure WhatsUp Gold to receive data from each poller installed on your network. The poller is configured through the WhatsUp Gold web interface by clicking **Admin > Polling**. This launches the Polling Configuration Library dialog where the local poller and additional poller configurations enabled for clustered polling can be added, edited, or deleted. For more information on configuring pollers using the WhatsUp Gold Polling Configuration Library in WhatsUp Gold, see *Using the Polling Configuration Library* (on page 488).

✓ **Important**: The machine on which the WhatsUp Gold poller is installed MUST have the same access to the network as the WhatsUp Gold machine. Polling data is always reported from the viewpoint of the WhatsUp Gold machine regardless of which device performed the polling task. Therefore, if a poller can only access a portion of the network, devices to which the poller does not have access (even if previously discovered by WhatsUp Gold) are reported as down.

✓ **Important**: If you are licensed for WhatsUp Gold Failover, you should continue to use WhatsUp Gold Failover for full WhatsUp Gold system redundancy. For more information, see *Polling and WhatsUp Gold Failover* (on page 40).

Poller Installation and Removal

WhatsUp Gold Poller installation and configuration

The WhatsUp Gold poller installation file is included on the WhatsUp Gold host machine in the following location: `<WhatsUp Gold Installation Directory>\WhatsUp Poller Installer`. To install on another network machine, you must obtain the install file from this location and place it on the machine(s) that will serve as the poller(s).

The following are prerequisites for installing an additional poller on your WhatsUp Gold system:

- Local admin privileges for the host machine are required to install the WhatsUp Gold poller.
- The Windows account from which you install the poller must have a known password. You will be prompted to enter this password during the poller installation process.

Note: After a remote poller is installed, you can modify the poller User name and Password in the Windows Credential Manager, accessible via the Windows Control Panel. Ensure you log in to the remote polling machine using the same user credentials used during the poller installation. You can also run the remote poller install program (repair install) on the target poller system to change the user name and password.

- .NET 4 is required for installation and is available to install if not already installed on the host machine. If prompted to allow .NET4 installation, click **Yes**.

Note: System polling and reporting times are based on the WhatsUp Gold system clock and time-zone settings.

To install the WhatsUp Gold poller:

1 Double-click the executable file. If the Open File - Security Warning dialog appears, click **Run**. The WUG Poller - InstallShield Wizard launches.

2 Click **Next**. The **License Agreement** dialog appears.

3 Review the Ipswitch License Agreement, select **I accept the terms of the license agreement**, and click **Next** to continue. The Choose Destination Location dialog appears.

4 Click **Next** to install the WhatsUp Gold poller in the default directory or click **Change** to select an different location. The WhatsUp Gold info dialog appears.

5 Enter a unique name to identify the poller in the **Name** box.

✓ **Important**: Following installation, you will need the poller name to successfully add the poller to the configuration library in WhatsUp Gold. See *Configuring the Poller* (on page 39) for additional details.

6 Enter the server name or IP address for the WhatsUp Gold machine in the **Server** box.

Note: The default port shown in the WhatsUp Gold installation info dialog is 9713. This is the port assigned to the WhatsUp Gold host system and should not be altered unless the port on the WhatsUp Gold machine/polling controller has been changed.

Note: In order for a poller to connect to WhatsUp Gold, you'll need to enable communication on the following ports: TCP 9713 - Polling Data Communications and TCP - 9730 Polling Control Communications.

7 Click **Next**. The Login dialog appears.

8 Enter a valid user name and password for the WhatsUp Gold server.

9 Click **Next**. The Password dialog appears.

10 Enter the password for the current Windows account on the machine on which the poller is being installed.

Note: WhatsUp Gold Poller inherits the security attributes in place on the machine on which it is installed. It is recommended that the poller be installed using an administrator-level Windows account.

Note: To modify applicable credentials after installation, access the Windows Vault from the Control Panel of the machine on which the WhatsUp Gold Poller is installed.

11 Click **Next**. The Ready to Install the Program dialog appears.

12 Click **Install**. InstallShield Wizard installs the WhatsUp Gold Poller.

13 After installation is complete, click **Finish** to exist the InstallShield Wizard.

14 Click **Finish**.

WhatsUp Gold Poller Removal

To remove the WhatsUp Gold poller:

1. Access the Windows Control Panel for the machine on which the Polling Engine is installed.
2. Select the **Uninstall a program** hyperlink.
3. Double-click **Ipswitch WhatsUp Gold Polling Engine v16.0** in the list of installed programs.. The WhatsUp Gold Polling Engine InstallShield Wizard launches.
4. Click **Yes** to indicate you want to remove the selected application and all of its features.
5. When the dialog indicates uninstall is complete, select whether or not you want to restart your computer now or later.
6. Click **Finish**.

Configuring WhatsUp Gold to use additional pollers

You can configure WhatsUp Gold to use additional pollers installed on your WhatsUp Gold system using the Polling Configuration Library. To access the Polling Configuration Library from the web interface, go to **Admin > Polling**. Or, if you previously added the Poller Health dashboard report to your WhatsUp Gold home page, you can launch the Polling Configuration Library dialog by clicking on any poller name displayed within the report.

For detailed information on using the Polling Configuration Library, see *Using the Polling Configuration Library* (on page 488).

Poller Health Dashboard

The Poller Health dashboard report displays the status of all configured pollers on your WhatsUp Gold system. For additional detailed information on adding dashboard reports to your WhatsUp Gold home page and the Poller Health dashboard report, see Adding dashboard reports to a dashboard view and Poller Health dashboard report.

Polling Performance Tuning

An average poll lag time of a few seconds or more indicates your system may not be performing optimally. If WhatsUp Gold device polling seems to be experiencing performance lag, use the Poller Health dashboard report to assess and confirm poller performance. The WhatsUp Gold CPU and memory utilization reports can also be used to indicate performance issues. There are a number of ways to improve poller performance by reducing the workload of the WUG machine:

Add pollers to your WhatsUp Gold system

The first option is adding one or more additional pollers to your WhatsUp Gold system depending on the size of your network. When additional pollers are installed, load balancing should be disabled on the local poller using the procedure described previously. This transfers the majority of the polling workload to the additional pollers, reserving the local poller for polling activity on the WhatsUp Gold Server. However, if your network is distributed across a large geographic area, you may benefit from assigning a poller to a specific subnet or device. In this case, load balancing should also be disabled on the specific poller to limit its activity to the assigned device(s).

Disable load balancing on the local poller

The second option is removing the local poller from the load balancing queue reduces the workload of the WhatsUp Gold server and allows it to perform other tasks for which it is responsible.

To disable load balancing on the local poller:

1. Select **Admin > Polling** to access the *Polling Configuration Library* (on page 488).
2. Select the Local Poller and click **Edit**. The Edit Poller Configuration dialog appears.
3. Clear the **Use for load balance** check box.
4. Click **OK**.

Relocate SQL to another machine

The third option is to relocate your SQL instance to a machine separate from your WUG server. For more information, see the *WhatsUp Gold Database Migration and Management Guide* (http://www.whatsupgold.com/wugdbmg_16).

Other modifications

If you are still experiencing polling performance issues, consider the following network environment modifications:

- Add additional memory and increase disk speed on the machine hosting your SQL instance.
- Add or assign a machine on your WhatsUp Gold system dedicated solely to polling operations.

Using Clustered Polling with WhatsUp Gold Failover and Distributed editions

Ipswitch WhatsUp Gold Failover Edition is an optional WhatsUp Gold product that introduces a failover capability to your network that will activate in the event your primary WhatsUp Gold machine fails. If you have WhatsUp Gold Failover Edition, any pollers pointing to the primary WhatsUp Gold machine must be identical in both name and configuration to pollers pointing to the secondary WhatsUp Gold machine so the failover system is redundant, receiving and reporting the same data in a failover scenario. Any variation in name, configuration, or access permissions between pollers assigned to the primary and secondary WhatsUp Gold machines will cause incomplete data to be returned on the WhatsUp Gold failover system.

⚠ **Caution**: Pollers do not failover independently of WhatsUp Gold. If an individual poller fails, it's counterpart on the secondary WhatsUp Gold system will not assume the failed pollers' operations. Your secondary WhatsUp Gold system must mirror your primary WhatsUp Gold system completely.

✓ **Important**: Because pollers assigned to the primary and secondary systems must be named identically and in a failover scenario only one WhatsUp Gold system is active at a time, each poller name only needs to be entered into the polling configuration library once.

Pollers work with a WhatsUp Gold Distributed configuration exactly like a standard WhatsUp Gold configuration. No special configuration is necessary.

Poller usage in WhatsUp Gold

Additional pollers installed on your WhatsUp Gold system transmit active and performance monitor data to the WhatsUp Gold server.

The following functions are supported by other WhatsUp Gold services:

- Actions
- Active Script Active Monitor
- Active Script Performance Monitor
- Discovery
- MIB Walker
- Passive Monitors
- Split Second Graphs
- VoIP Monitor
- WhatsConfigured Tasks
- Wireless Polling
- WhatsVirtual Polling

Devices

In This Section

Discovery Console

In This Chapter

Discovering network devices

Network discovery is the process WhatsUp Gold uses to identify devices on your network that you may want to monitor. Network discovery scans each device to determine its manufacturer, model, and running software and services, also known as the *role* each device plays on the network. WhatsUp Gold uses this information to automatically assign commonly used monitors to each device. For more information, see *Learning about the Discovery Console* (on page 26).

Before you discover the devices on your network, you need to prepare both your devices and WhatsUp Gold so that devices are discovered properly. For more information see, *Preparing devices for discovery* (on page 43) and *Preparing WhatsUp Gold for discovery* (on page 44).

Preparing devices for discovery

In order for WhatsUp Gold to properly discover and identify devices, each device must respond to the protocols that WhatsUp Gold uses during discovery.

Preparing devices to be discovered

To discover that a device exists on an IP address, WhatsUp Gold uses the following methods:

§ Ping (ICMP)

§ Scanning for open TCP ports

If a device does not respond to ping or TCP requests, it cannot be discovered by WhatsUp Gold. We recommend ensuring that all devices respond to at least one of these types of requests prior to running a discovery.

Preparing devices to be identified

After WhatsUp Gold discovers a device on an IP address, it queries the device to determine the manufacturer and model, components (such as fans, CPUs, and hard disks), operating system, and specific services (such as HTTP or DNS). To gain this information, WhatsUp Gold uses SNMP or WMI data from individual devices.

Enabling SNMP on devices

We recommend that important devices be configured to respond to SNMP requests. For information about how to enable SNMP on a specific device, see *Enabling SNMP on Windows devices* (on page 285) in the *WhatsUp Gold Online Help* (http://www.whatsupgold.com/wug16webhelp) or consult the network device documentation. For information about configuring SNMP on network devices, you may also want to view the WUG Guru video *How to enable SNMP on a Windows server* (http://www.whatsupgold.com/wug123snmpvideo).

Enabling WMI on devices

Alternatively, WhatsUp Gold can gather information about Windows computers using WMI. In most cases, however, the information available via WMI is also available via SNMP. Because SNMP requests are more efficient than WMI requests, we recommend using WMI only when SNMP cannot be enabled or does not provide the same information as WMI.

Note: If a firewall exists between WhatsUp Gold and the devices to be discovered (or if the Windows Firewall is enabled on the computer where WhatsUp Gold is installed), make sure that the appropriate ports are open on the firewall to allow WhatsUp Gold to communicate via SNMP and WMI. For more information, see *Troubleshooting SNMP and WMI connections* (on page 565) in the help.

Preparing WhatsUp Gold for discovery

For the best discovery results, configure all of the credentials used by devices on your network before starting a discovery scan. The Credentials Library stores applicable login, community string, or connection string information for devices and applications.

To apply appropriate action policies to discovered devices, we also recommend that you configure the policies in WhatsUp Gold prior to starting a discovery session, and then associate them with a device role. For more information, see *Using Device Roles* (on page 56) in the help.

Configuring credentials

To configure credentials:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.
2 Click **New**. The Select Credential Type dialog appears.
3 Select the type of credential you want to create, then click **OK**. The Add New Credential dialog appears.
4 Enter the information for the credential you want to create, then click **OK**. The Add New Credential dialog closes.
5 Repeat steps 2 through 4 for each credential that you want to use during the discovery process.

For more information about credentials, see *Using Credentials* (on page 68) in the help.

Creating action policies

To create an action policy:

1. From the WhatsUp Gold console, click **Configure > Action Policies**. The Action Policies dialog appears.
   - or -
   From the WhatsUp Gold web interface, go to **Admin > Action Policies**.
2. Click **New**. The New Action Policy dialog appears.
3. Enter a name for the action policy. This name is used to help you identify this action policy in WhatsUp Gold.
4. Click **Add**. The Action Builder wizard appears.
5. Follow the on-screen instructions in the Action Builder wizard to create or select actions for the policy. At the end of the wizard, click **Finish** to close the Action Builder wizard and add the action to the action policy.
6. To add additional actions to the action policy, click **Add** again.
7. After you have added all of the actions to the action policy, verify that they are listed in the correct order. If they are not, you can select actions and use the **Up** and **Down** buttons to change the actions' order in the list.
8. Click **OK**. The New Action Policy dialog closes.

To associate an action policy with a device role:

1. After creating the action policy, on the WhatsUp Gold console click **File > Discover Devices**. The Discovery console appears.
2. From the Discovery console menu, click **Advanced > Device role settings**. The Device Role Settings dialog appears.
3. Select the device role that you want to use in the action policy, then click **Configure**. The Role Settings Editor appears.
4. Select the **Action Policy** tab.
5. Select the action policy you want to include, then click **OK**. The Role Settings Editor dialog closes.

For more information about action policies, see *About Action Policies* (on page 348) in the help.

Configuring and running discovery

Discovering devices on your network is a three-stage process that includes:

§ *Configuring discovery settings* (on page 45)

§ *Running discovery* (on page 49)

§ *Adding discovered devices to WhatsUp Gold* (on page 52)

To begin discovering devices on your network, from the WhatsUp Gold web interface, click **Devices > Discovery Console**. The Discovery Console appears.

Configure discovery settings

Before you can run a discovery scan on your network, you need to configure the discovery settings. These settings are located in the Settings column of the Discovery Console.

Select scan settings

WhatsUp Gold can use several different methods to scan your network. Select the scan type that best suits your network.

§ **SNMP Smart Scan**. This scan type uses one or more SNMP-enabled devices to identify the devices and sub-networks on your network. For more information, see *Using SNMP Smart Scan* (on page 48).

§ **IP Range Scan**. Type the IP range that defines the addresses to include in the network scan. For example, **Start Address** 10.0.0.1 and **End Address** 10.0.0.100. For more information, see *Using IP Range Scan* (on page 48).

§ **Hosts File Scan**. WhatsUp Gold imports devices from a hosts file. For more information, see *Using Hosts File Scan* (on page 48).

✓ **Important**: If you update the `Hosts` text file, you must click **Load/Reload** (console) or **Upload** (web interface) to update the host file information. If you do not, the `Hosts` file changes will not be updated for new Hosts File Scans.

Note: The VMware scan feature is available in WhatsUp Gold when you are licensed for WhatsVirtual or when you are running the WhatsUp Gold product evaluation. To update or purchase a license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

§ **VMware Scan** (available for WhatsVirtual license). This scan connects to VMware servers and uses the VMware vSphere API to gather infrastructure information about your virtual environment. The VMware Scan uses a list of user provided VMware vCenter servers or VMware hosts as targets for the scan.

§ **Rescan existing WUG VMware vCenter servers and hosts (recommended)**. Use this option to rescan previously discovered vCenter servers and hosts. Choosing this option updates the device lists and maps provided in the Device View and Map View.

§ **Add new VMware vCenter servers or hosts**. Enter the IP address of the managing vCenter or VMware hosts. Separate each host name or IP address with a comma.

Note: You can enter a vCenter IP address as a target and WhatsVirtual will discover all VMware hosts and virtual machines the vCenter manages.

Note: If you want detailed information about VMware hosts to be available for the VMware Host Details log, you must add credentials for the VMware hosts.

Note: You must have VMware credentials for all of the servers in the list of targets for the scan.

Note: Ensure that VMware Tools are installed on each virtual machine you want to discover. If VMware tools are not installed on a virtual machine, the device is not discovered during the VMware Scan.

Select Credentials

To correctly identify devices, WhatsUp Gold needs to query the devices using SNMP, WMI, the VMware API or all of these methods. In these sections, select the credentials that you want WhatsUp Gold to use during discovery. You can select multiple credentials. The credentials list contains the credentials currently configured in the Credential Library. To use a credential that is not listed, you must first add the credential to the *Credential Library* (on page 458) in WhatsUp Gold. For more information, see *Using Credentials* (on page 68).

> **Note**: Selecting too many credentials may significantly increase the time required to run discovery. To decrease the amount of time it takes for discovery to run, select only the credentials that are used by the devices you want to discover.

Configure Scan Method

WhatsUp Gold can use two methods to detect that a device exists on an IP address:

§ **Ping**. When using this method, WhatsUp Gold detects devices by issuing a ping request via ICMP and listening for a response.

§ **Advanced**. When using this method, WhatsUp Gold first detects all devices that respond to ping. Then, if a device does not respond to ping, WhatsUp Gold scans common TCP ports for a response.

§ **Ping Timeout (seconds)**. Enter the time, in seconds, for a device to respond to a ping scan. If it does not respond to the scan within this time, the scan continues on to the next IP address. The default is 2 seconds.

§ **Ping Retries**. Enter the number of times to attempt to ping a device before continuing on to the next device. The default is 1 retry.

Configure Advanced Settings

You can modify the timeout and retry settings for SNMP and WMI requests. By default, WhatsUp Gold has a 2 second timeout for SNMP requests, 10 seconds for WMI requests, and retries failed SNMP requests once.

If the **Use SNMP SysName to name devices** option is selected, WhatsUp Gold attempts to identify the SNMP SysName as the first measure to define the device name. If SNMP is not enabled on a device, WhatsUp Gold attempts to resolve the DNS host name of discovered devices if the **Resolve host names** option is selected. If neither the SNMP SysName nor the DNS host name is available, WhatsUp Gold uses the device IP address to name the device. Clear **Resolve host names** and **Use SNMP SysName to name devices** if you do not want WhatsUp Gold to resolve the device name with either of these discovery methods.

By default, WhatsUp Gold automatically scans for virtual machines hosted by discovered VMware servers. If you do not want WhatsUp Gold to scan for the virtual machines hosted by discovered VMware servers, clear **Auto scan virtual environments**.

By default, WhatsUp Gold automatically uses layer 2 discovery to generate layer 2 topology maps and inventory information available in the Device Viewer. If you do not want WhatsUp Gold to use layer 2 discovery, clear **Use layer 2 discovery and generate layer 2 topology map** to disable Layer 2 discovery.

You may also enable wireless device discovery using WhatsUp Gold Wireless by selecting the **Gather information for wireless topology and performance** option.

Using SNMP Smart Scan

To use SNMP Smart Scan, configure these settings:

- **Seed Addresses**. Enter the IP addresses that indicate where you want to start the network discovery scan. The discovery engine reads SNMP data from these devices and continues to scan the network for additional devices based on the SNMP responses from the seed devices.
  - **Add**. Click to enter a new seed address for the discovery scan.
  - **Edit**. Select a seed address to change.
  - **Remove**. Select a seed address to delete.
- **Scan Depth**. Enter an integer value that defines how deep discovery should scan to find network devices. This sets the levels of your network that you want to scan. With a value of 1, the scan discovers and maps your top-level network and any sub-networks of that top-level. To discover a sub-network within that sub-network, you must enter a scan depth of 2 or greater. The default value of 2 means that the scan discovers and maps the top-level network and two sub-network levels.

Using IP Range Scan

To use IP Range Scan, configure these settings:

- **Start Address**. Enter the first IP address in the range you want to discover.
- **End Address**. Enter the last IP address from the range you want to discover.

For example, if you want to discover devices between 192.168.0.1 and 192.168.0.128, enter `192.168.0.1` for **Start Address** and `192.168.0.128` for **End Address**.

Using Hosts File Scan

To use Hosts File Scan:

- Click **Load/Reload** (console) or **Upload** (web interface) to browse to the `Hosts` file location. Discovery scans and imports the IP addresses mapped to host names listed in the `Hosts` text file. You can also select other text files that include a list of IP address.

✓ **Important**: If you update the `Hosts` text file, you must click **Load/Reload** (console) or **Upload** (web interface) to update the host file information. If you do not, the `Hosts` file changes will not be updated for new Hosts File Scans.

Using Layer 2 Scan

Layer 2 discovery uses the WhatsUp Gold discovery engine to discover layer 2 networking information. This information is used to create graphical representations of the physical network connections between discovered devices.

- **Use layer 2 discovery and generate layer 2 topology map**. Select this option to enable Layer 2 discovery.

Using VMware Scan

Note: The VMware scan feature is available in WhatsUp Gold when you are licensed for WhatsVirtual or when you are running the WhatsUp Gold product evaluation. To update or purchase a license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

§ **VMware Scan** (available for WhatsVirtual license). This scan connects to VMware servers and uses the VMware vSphere API to gather infrastructure information about your virtual environment. The VMware Scan uses a list of user provided VMware vCenter servers or VMware hosts as targets for the scan.

§ **Rescan existing WUG VMware vCenter servers and hosts (recommended)**. Use this option to rescan previously discovered vCenter servers and hosts. Choosing this option updates the device lists and maps provided in the Device View and Map View.

§ **Add new VMware vCenter servers or hosts**. Enter the IP address of the managing vCenter or VMware hosts. Separate each host name or IP address with a comma.

Note: You can enter a vCenter IP address as a target and WhatsVirtual will discover all VMware hosts and virtual machines the vCenter manages.

Note: If you want detailed information about VMware hosts to be available for the VMware Host Details log, you must add credentials for the VMware hosts.

Note: You must have VMware credentials for all of the servers in the list of targets for the scan.

Note: Ensure that VMware Tools are installed on each virtual machine you want to discover. If VMware tools are not installed on a virtual machine, the device is not discovered during the VMware Scan.

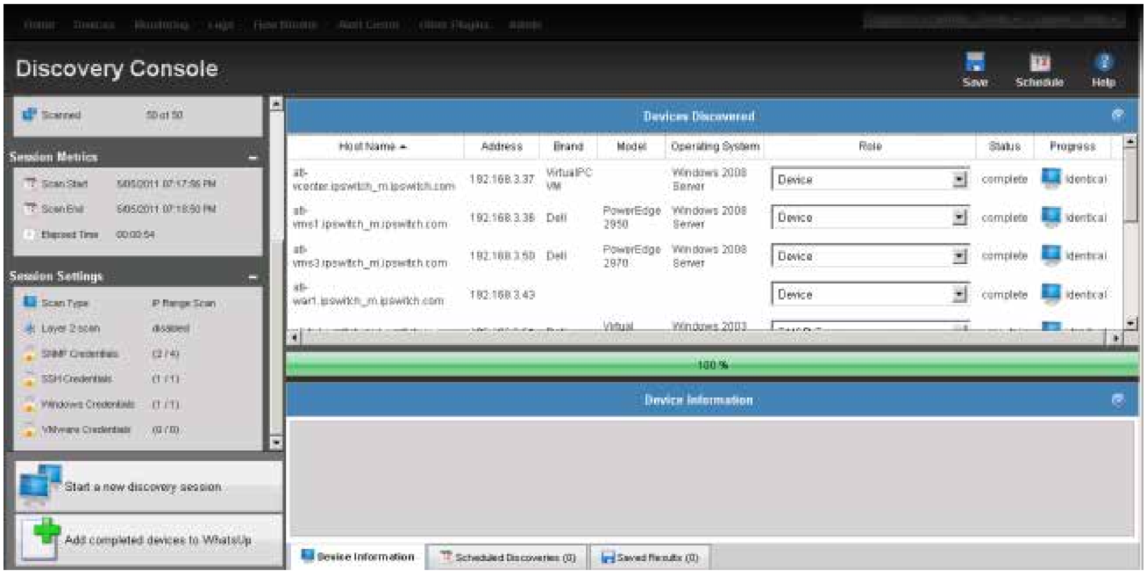
Running discovery

After you have configured discovery settings, click **Start a discovery session** to find devices on your network.

When you begin a new discovery session:

§ The Settings pane is replaced by the Progress Summary pane, which lists information about the running discovery session.

- Discovered devices are added to the list in the Devices Discovered pane. As each device is scanned, additional information about it becomes available, such as its brand, model, and operating system. Based on what it discovers about a device, WhatsUp Gold designates a device role, which defines what monitors WhatsUp Gold attempts to apply to the device.



Scanned 50 of 50

Scan Start 5/05/2011 07:17:56 PM
Scan End 5/05/2011 07:18:50 PM
Elapsed Time 00:00:54

Scan Type IP Range Scan
Layer 2 scan disabled
SNMP Credentials (2 / 4)
SSH Credentials (1 / 1)
Windows Credentials (1 / 1)
VMware Credentials (0 / 0)

Host Name	Address	Brand	Model	Operating System	Role	Status	Progress
at-vcenter.ipswitch_m.ipswitch.com	192.168.3.37	VirtualPC VM		Windows 2008 Server	Device	complete	identical
at-vms1.ipswitch_m.ipswitch.com	192.168.3.38	Dell	PowerEdge 2950	Windows 2008 Server	Device	complete	identical
at-vms3.ipswitch_m.ipswitch.com	192.168.3.50	Dell	PowerEdge 2970	Windows 2008 Server	Device	complete	identical
at-warl.ipswitch_m.ipswitch.com	192.168.3.43				Device	complete	identical

100 %

To view detailed information about a discovered device:

1. Select a fully discovered device from the list in the Devices Discovered pane. You can tell a device has been fully discovered when the Status column lists `complete`. The row highlights when the device is selected.
2. If it is not already selected, select the **Device Information** tab from the bottom of window. This section shows detailed information about the selected device.

To stop a running discovery session:

If a discovery session has not completed fully (reached 100% on the progress bar), you can stop it by clicking **Stop the current discovery session**.

Tip: When you stop a running discovery session, the devices that have been completely discovered remain in the Devices Discovered list and can still be added to WhatsUp Gold. Devices that show a Status of *Canceled*, however, cannot be added to WhatsUp Gold unless you run another discovery session and allow them to be discovered completely.

Viewing progress summary information

After a new discovery session starts, the Progress Summary information displays to the left side of the Discovery Console and provides information about the discovery in progress.

Device Summary

- **Device Limit**. Lists the number of devices that WhatsUp Gold is licensed to manage.
- **Existing Devices**. Lists the number of devices that WhatsUp Gold is monitoring.
- **Discovered Devices**. Lists the number of devices discovered in the current scan.

Network Traffic

- **SNMP Bytes (in/out)**. Indicates the amount of SNMP data WhatsUp Gold has sent and received in the current discovery process.
- **PDU (Protocol Data Unit) (in/out)**. Indicates the amount of data sent and received among peer network devices during the discovery process.
- **Scanned**. Indicates the number of devices scanned and the total number of devices to be scanned.

Session Metrics

- **Scan Start**. Indicates the time the discovery started.
- **Scan End**. Indicates the time the discovery ended.
- **Elapsed Time**. Indicates the time the discovery took to complete.

Session Settings

- **Scan Type**. Indicates the current discovery method used in the current network scan.
- **Layer 2 scan**. Indicates whether Layer 2 discovery was enabled for the discovery scan.
- **SNMP Credentials**. Indicates the number of devices that were discovered with SNMP credentials.
- **Windows Credentials**. Indicates the number of devices that were discovered with WMI credentials.
- **VMWare Credentials**. Indicates the number of devices that were discovered with VMware credentials.

Viewing device discovery information

After the discovery settings are configured and you start a discovery session, the Devices Discovered section on the right side of the Discovery Console displays the progress and results of the discovery scan. Information and the status of each device discovery appears as follows:

- **Host Name**. Lists the the discovered device name by IP address or name.
- **Address**. Lists the discovered device IP address.
- **Brand**. Lists the device hardware manufacturer. The brand information helps narrow the discovery criteria to identify product model information.
- **Model**. Lists the device manufacturer model. The model information helps further refine the discovery criteria to help identify the device role.
- **Operating System**. Lists the operating system the device is running.
- **Role**. Based on the device brand, model, running applications, active ports, and other discovery criteria, a template or several template options are listed as device Role options (configurations). You can also create custom device role configurations so that device roles are identified more accurately, during discovery, for the devices on your network. For more information, see *Using Device Roles* (on page 56).
- **Status**. Lists the status of the discovery that is running.
- **Progress**. Lists the results of the discovery; whether the device found is a new or existing device. If the device is a new device, you can add it to the WhatsUp Gold database (device map) *OR* if the device is an existing device, the device has already been added to the WhatsUp Gold database.

Tip: Each column under Devices Discovered is sortable; click a column title to sort the column.

Adding discovered devices to WhatsUp Gold

After WhatsUp Gold discovers and identifies the role of devices, you can add those devices to a device group. You do not have to wait for the discovery session to reach 100% before you can add devices; after a device is listed as *Complete* in the Status column, it can be added to a device group.

Tip: If a device identifies with an incorrect role or a role other than the one you want to use, you can change it in the drop down in the **Role** column. This box lists all of the roles for which the device met the criteria. If the role you want to use is not in this list, you must modify the device identification on the role. For more information, see *Using Device Roles* (on page 56) in the console application help.

To select a device role:

- In the Devices Discovered **Role** column, for each device listed, select the device role you want to use to define the device configuration. For more information about device role settings, see *Using Device Roles* (on page 56) in the console application help.

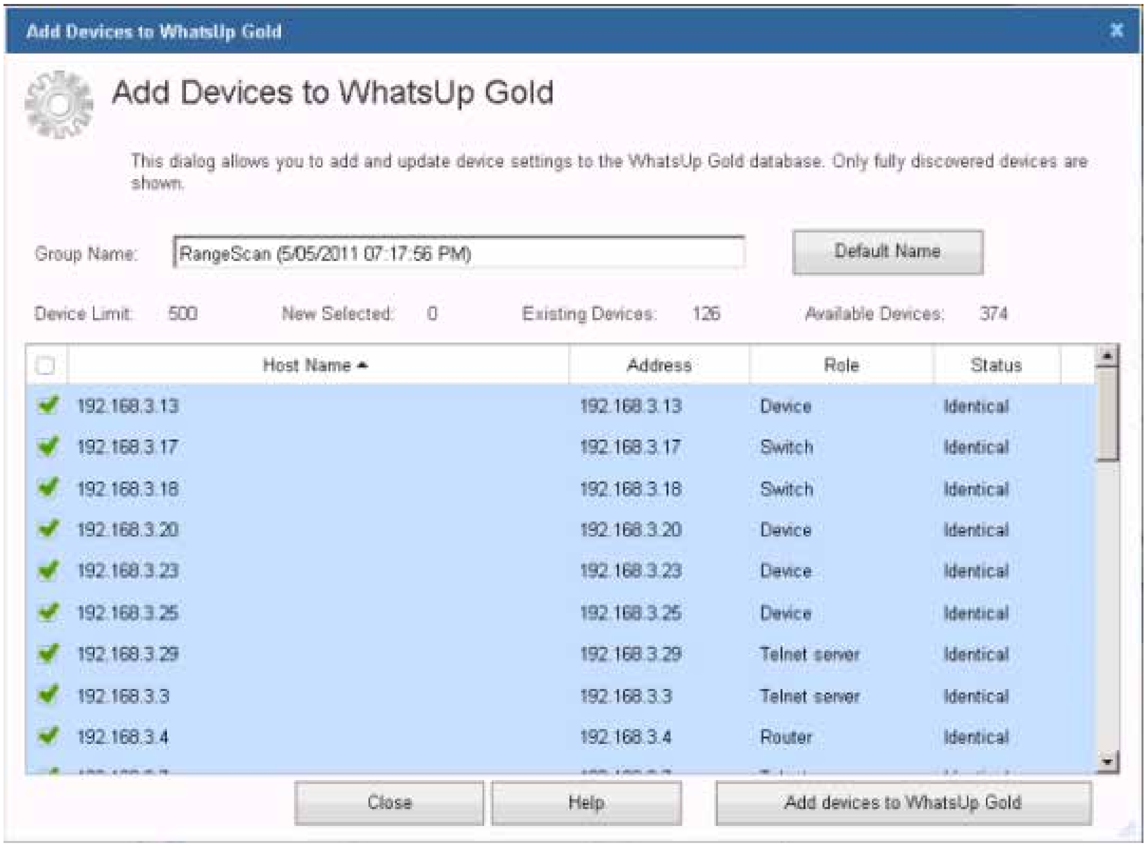
Before adding devices to the database, you can view the following information about devices:

- **Device Limit**. Lists the total number of devices WhatsUp Gold is licensed to monitor.
- **New Selected**. Lists the number of devices you have selected to add to the WhatsUp Gold database.
- **Existing Devices**. Lists the number of devices WhatsUp Gold is currently monitoring.
- **Available Devices**. Lists the number of devices remaining on the license for WhatsUp Gold to monitor.

To add all completed devices to a device group:

Note: Only devices that are listed as *Complete* in the Status column can be added. If any selected devices are in any other status, they are not added to WhatsUp Gold.

1 Click **Add completed devices to WhatsUp**. The Add Devices to WhatsUp Gold dialog appears.



Add Devices to WhatsUp Gold

This dialog allows you to add and update device settings to the WhatsUp Gold database. Only fully discovered devices are shown.

Group Name: RangeScan (5/05/2011 07:17:56 PM)

Device Limit: 500 New Selected: 0 Existing Devices: 126 Available Devices: 374

□	Host Name ▲	Address	Role	Status
✓	192.168.3.13	192.168.3.13	Device	Identical
✓	192.168.3.17	192.168.3.17	Switch	Identical
✓	192.168.3.18	192.168.3.18	Switch	Identical
✓	192.168.3.20	192.168.3.20	Device	Identical
✓	192.168.3.23	192.168.3.23	Device	Identical
✓	192.168.3.25	192.168.3.25	Device	Identical
✓	192.168.3.29	192.168.3.29	Telnet server	Identical
✓	192.168.3.3	192.168.3.3	Telnet server	Identical
✓	192.168.3.4	192.168.3.4	Router	Identical

2 Enter the name of the device group to which you want to add devices into the **Group Name** box. To use a device group that already exists in WhatsUp Gold, type the name exactly as it appears in WhatsUp Gold. If the name does not already exist in WhatsUp Gold, a device group with that name is created. To use a default name, which includes the type of scan and the time the scan started, click **Default name**.

3 Select each device you want to add to WhatsUp Gold. A check mark next to a device indicates that the device will be added to WhatsUp Gold.

4 Click **Add devices to WhatsUp Gold**. A progress dialog appears as the devices are added to the device group.

5 When you are finished adding devices, click **Close**. The Save Device Settings dialog closes.

After discovered devices are added to the device group, WhatsUp Gold begins monitoring them immediately.

Configuring scheduled discovery

After you have optimized discovery settings for your network, you can schedule discovery to run periodically using the configured settings. Each time discovery runs, it detects new devices on your network and suggests adding monitors on devices that have changed since the last discovery. You can also configure email notifications that distribute information about the results of the scheduled discovery. Select the Discovery Settings options on the left to configure the discovery, then use the Schedule Information section to set up the discovery schedule.

To create a scheduled discovery:

1. Click **Devices > Discovery Console**. The Discovery console appears.
2. Click **Schedule**. The Scheduled Discovery Settings dialog appears.
3. Configure the settings for the discovery you want to schedule. For more information, see *Configure discovery settings* (on page 45).
4. Configure the discovery settings, schedule information, and schedule recurrence settings.
5. To have this discovery detect both new devices and new services on existing devices, click **Test for new monitors on existing devices**. If this option is not selected, WhatsUp Gold does not scan for new services on existing devices.
6. To receive an email notification of the discovery's results, click **Send email notification upon completion**.
   a) Click **Email Settings** to configure the email notification. The Email Settings dialog appears.
   b) Enter the information for the email. In **Body**, you can use HTML and *discovery percent variables* (on page 61) (Device Session variables only).
   c) After you have configured the email, click **OK**. The Email Settings dialog closes.
7. Verify that **Schedule enabled** is selected.
8. Click **OK** to save the scheduled discovery. The Scheduled Discovery Settings dialog closes.

To view and edit scheduled discoveries:

1. In the tabbed section at the bottom of the Discovery Console, click **Scheduled Discoveries**. The Scheduled Discoveries tab appears.
2. Select a scheduled discovery in the list that you want to view or edit, then click **Edit**.
3. Change the discovery schedule as required.

To delete a scheduled discovery:

1. In the tabbed section at the bottom of the Discovery Console, click **Scheduled Discoveries**. The Scheduled Discoveries tab appears.
2. Select a scheduled discovery you want to delete, then click **Delete**.

Configuring discovery results email settings

Use this dialog to set up the recipients for the scheduled discovery results. Complete the **To**, **From**, **Subject**, and **Body** for the scheduled discovery notification email. You can configure the SMTP server, port, timeout, SMTP server authentication, and encrypted connections in the global email settings dialog.

A template email message has been created in the Body section of the dialog. You can use plain text or html code to style the message. You can also use other Discovery variables to customize the email message with additional information you want to include. For more information, see the *discovery percent variables* (on page 61) information in the console application help.

When the email is configured, you can click **Test** to make sure the message sends to the recipients and that the message body works correctly.

To configure global email settings:

1. Click **Devices > Discovery Console**. The Discovery Console appears.
2. Click **Schedule**. The Scheduled Discovery Settings dialog appears.
3. Select the **Send email notification upon completion** or **Send email even when no updates found** option, then click **Email Settings**. The Email Settings dialog appears.

Viewing Device Information tab

The Device Information tab provides detailed information returned from SNMP devices discovered on the network. This information helps you view details about each device before adding it to the WhatsUp Gold database.

> **Note**: Device Information varies, dependant upon on the device type and the SNMP information available on the device.
>
> When determining the default display name, WhatsUp Gold polls SNMP objects in the following order: `ifAlias (1.3.6.1.2.1.31.1.1.1.18)`, `ifName (1.3.6.1.2.1.31.1.1.1.1)`, `ifDesc (1.3.6.1.2.1.2.2.1.2)`. If no value is found, the next object is queried until a value is returned.

To view device details:

1. Click **Devices > Discovery Console**. The Discovery Console appears.
2. In the bottom section of the Discovery Console, click the **Device Information** tab.
3. Click to select a device in the Devices Discovered list. The SNMP information extracted from the device displays in the Device Information box.

Viewing scheduled discoveries

The Scheduled Discoveries tab lists all the discovery scans that are scheduled to run. You can edit and delete the discovery schedules as required. The following information about scheduled discoveries is displayed.

- **Scan Name**. Lists the saved scheduled discovery name.
- **Description**. Lists descriptive information about the scheduled discovery.
- **Date Saved**. Lists the date and time the scheduled discovery was saved.
- **Next Scan**. List the time(s) the scheduled discovery scan is scheduled to run.
- **Create**. Click to setup a new scheduled discovery.

You can select an existing scheduled discovery in the list, then **Edit** or **Delete** the scheduled discovery.

> **Note**: The results from the scheduled discovery scan will appear in the **Saved Results** tab.

For more information, see *Configuring scheduled discovery* (on page 53).

Saving discovery results

You can save the results of a network discovery to return to at a later time. This is useful if you are discovering a large network and will be creating device groups and adding devices over more than one session.

To save the results of a discovery session:

✓ **Important**: When you save the device discovery results, the list of devices found in the discovery are saved. This does not save the devices to the WhatsUp Gold database.

1 From the Discovery console, click **Save**. The Save Discovery Results dialog appears.

2 Enter a **Name** and **Description** for the saved discovery session, then click **OK**. The discovery session is saved under the Saved Results tab.

To open a saved discovery session:

⚠ **Caution**: Saved results are not updated when they are opened. If your network changes between the time of the initial scan and when you open the saved results, the saved results will not be accurate.

1 From the Discovery console, select the **Saved Results** tab.

2 Select the saved discovery session that you want to open, then click **View**. The saved discovery session results appear in the Devices Discovered pane.

Using saved discovery results

The Saved Results tab lists all the discovery scans that have been saved for later use. Use the Saved Results tab to view the results of a previous discovery scan or delete the discovery scan from the list. When you view previous scans, you can select and add devices that you have not previously added to the WhatsUp Gold database. For more information, see *Adding discovered devices to WhatsUp Gold* (on page 52).

To access the Discovery Console Saved Results tab:

1 Click **Devices > Discovery Console**. The Discovery Console appears.

2 In the bottom section of the Discovery Console, click the **Saved Results** tab.

The following Saved Scan information is listed:

§ **Name**. Lists the saved discovery name.

§ **Description**. Lists descriptive information about the discovery.

§ **Date Saved**. Lists the date and time the discovery was saved.

§ **Scheduled**. Lists whether the scan is a scheduled scan or a discovery scan. A True value indicates that the scan is a scheduled scan, while False indicates that the scan is a discovery or unscheduled scan.

You can select an existing Saved Scan in the list, then **View** or **Delete** the scan.

Using Device Roles

When WhatsUp Gold discovers devices, it tries to determine the type of each device so that it can monitor them appropriately. To determine a device type, WhatsUp Gold compares the discovered attributes of each device to a set of criteria called *device roles*.

Device roles do two things:

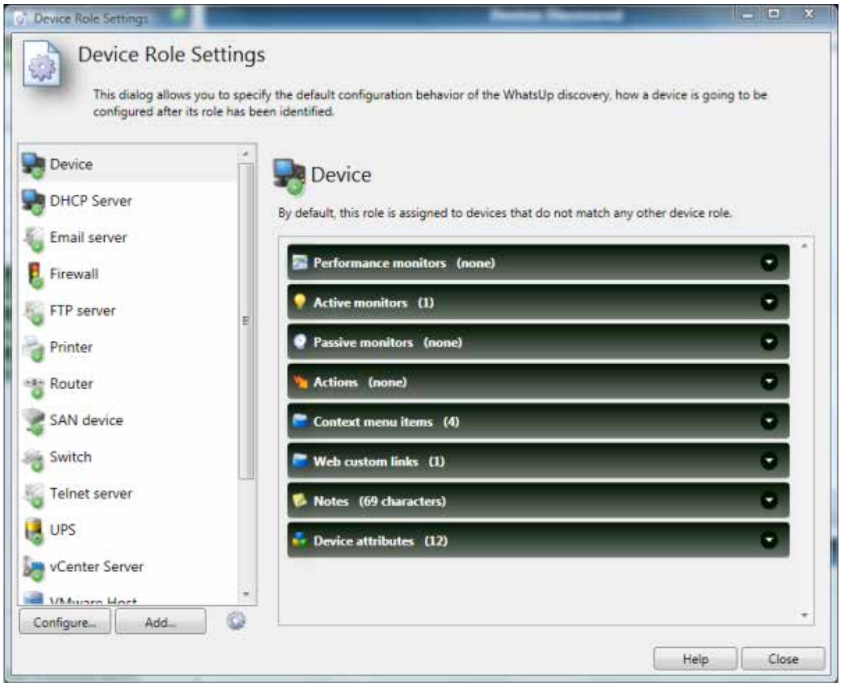
§ Specify the criteria that a device must match to be identified as the device role.

- Specify the monitoring configuration that is applied to the device when it is added to WhatsUp Gold.

WhatsUp Gold provides default device roles that are used to identify most common network devices. If your network includes devices that are not identified by this default set, you can create custom device roles.

Configuring device role settings

When a device is added to WhatsUp Gold, the initial device configuration is specified by device role. You can use the Device Role Settings dialog to configure and modify custom device roles for use with your network.



Device Role Settings

This dialog allows you to specify the default configuration behavior of the WhatsUp discovery, how a device is going to be configured after its role has been identified.

Device

By default, this role is assigned to devices that do not match any other device role.

Performance monitors (none)
Active monitors (1)
Passive monitors (none)
Actions (none)
Context menu items (4)
Web custom links (1)
Notes (69 characters)
Device attributes (12)

Note: The Device Role Settings dialog is only available from the WhatsUp Gold console.

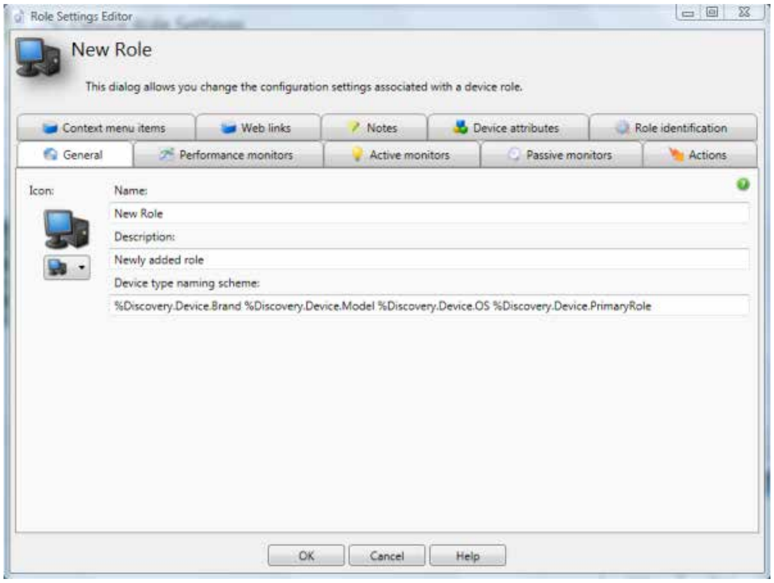
To configure device role settings:

1. Open the Discovery console from the WhatsUp Gold console.
2. Click **Advanced > Device role settings**. The Device Role Settings dialog appears.
3. Select the device role you want to modify, then click **Configure**.

   - or -

   Click **Add** to create a new device role. The New Role dialog appears.

Note: You cannot modify the role identification criteria of a default role. You can, however, duplicate a default role and modify the new role's criteria, then disable the default role.



New Role

This dialog allows you change the configuration settings associated with a device role.

Icon:

Name:

New Role

Description:

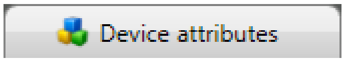
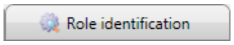
Newly added role

Device type naming scheme:

%Discovery.Device.Brand %Discovery.Device.Model %Discovery.Device.OS %Discovery.Device.PrimaryRole

4 Configure the device properties. The following table lists the device properties that can be configured to be automatically added to discovered devices that match a device role.

To configure this property	Use this tab	Notes
The device's icon and informational overlay text, as seen on the device map	General	Supports *discovery percent variables* (on page 61). For more information, see the General tab console Help.
Performance monitors applied to the device	Performance monitors	For more information, see the Performance monitors tab console Help.
Active monitors applied to the device, including which active monitors are critical	Active monitors	To make an active monitor critical, click the checkbox in the **Critical** column of that monitor. For more information, see *About critical active monitors* (on page 243) and the Active monitors tab console Help.
Passive monitors associated with the device	Passive monitors	We do not recommend enabling the **Any** options. The **Any** options cause WhatsUp Gold to save a large volume of data and can lead to performance problems caused by a large database. For more information, see the Passive monitors tab console Help.
Action policy applied to the device	Actions	For more information, see the Actions tab console Help.
Context menu items available when right-clicking on the device in the console	Context menu items	Supports *discovery percent variables* (on page 61). For more information, see the Context menu items tab

To configure this property	Use this tab	Notes
		console Help.
Web links available for the device in the web interface		Supports *discovery percent variables* (on page 61). For more information, see the Web links tab console Help.
The initial content of the device's Notes box		Supports *discovery percent variables* (on page 61). For more information, see the Notes tab console Help.
Attributes added to the device		Supports *discovery percent variables* (on page 61). For more information, see the Device attributes tab console Help.
The criteria a discovery scan uses to determine whether a device fits a specific role		For more information, see *Configuring device role identification settings* (on page 59).

Configuring device role identification settings

To determine if a device is a certain role, WhatsUp Gold can use several different types of criteria ranging from simple DNS and TCP port checks to complex SNMP queries.

To configure how a role is identified:

1 Open the Discovery console from the WhatsUp Gold console.

2 Click **Advanced > Device role settings**. The Device Role Settings dialog appears.

3 Select the device role you want to modify, then click **Configure**.

- or -

Click **Add** to create a new device role. The New Role dialog appears.

> **Note**: You cannot modify the role identification criteria of a default role. You can, however, duplicate a default role and modify the new role's criteria, then disable the default role.

4 Select the **Role identification** tab.

5 To add a new criterion, click **Add**. The **Select an identification criterion type** dialog appears.

- or -

To edit an existing criterion, click **Edit**. The **Edit Criterion** dialog appears. Skip to step 7 to continue.

6 Select a criterion from the list.

§ **DNS hostname contains**. Select to set criteria that passes if the value of the polled SNMP object (OID) contains the specified hostname value. For example, you can check that a device name contains "ATL," the prefix used in the Atlanta office computer names.

§ **SNMP object contains**. Select to set criteria that passes if the value of the polled SNMP object (OID) contains the specified value. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.1.1.0 (Microsoft branch) with "Version 5.1" system description information to determine the devices that are running Windows XP.

§ **SNMP object has a child which contains**. Select to set criteria that passes if the value of the polled SNMP object (OID) includes a child object. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.17 (dot1dBridge, the root of the bridge MIB). If this OID has a child, it means the device supports the Bridge MIB, and therefore the device must be a switch.

§ **SNMP object has a number of children greater than**. Select to set criteria that passes if the value of the polled SNMP object (OID) includes child objects greater than x number of children. For example, you can check the number of instances of a device interface by discovering instances of the interface table. This criterion could be used to identify "critical" network switches by identifying switches with 200 or more interface tables.

§ **SNMP object has a value**. Select to set criteria that passes if the value of the polled SNMP object (OID) contains the specified value. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.1.6 (sysLocation) with "Server Room" system description information to determine the devices that are network servers.

§ **SNMP object has at least one child**. Select to set criteria that passes if the value of the polled SNMP object (OID) includes at least one child object. For example, you can check that a printer OID includes at least one child printer OID. This criterion determines that the device is definitely a printer device. Printer OIDs must include a printer child OID.

§ **SNMP object is**. Select to set criteria that passes if the value of the polled SNMP object (OID) is equal to the specified value. For example, you could poll the sysContact object to make sure the configured contact information is equal to "Jane Doe."

§ **SNMP object matches regular expression**. Select to set criteria that passes if the value of the polled SNMP object (OID) matches the specified regular expression value. For example, you could check for devices that contain the OID value 1.3.6.1.2.1.1.1.0, the Catalyst switch sysDescr. If this system description matches the regular expression value (.*Catalyst), the criteria is matched.

§ **SNMP object starts with**. Select to set criteria that passes if the value of the polled SNMP object (OID) starts with the specified value. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.1.2.0, an HP enterprise OID. If this OID starts with 1.3.6.1.4.1.11, the root of the HP Enterprise MIB space, it means the specified device is supported.

§ **SNMP SysObjectID is**. Select to set criteria that passes if the value of the polled SysObjectID object the specified value. For example, the criterion could poll the SysObjectID and check that it starts with 1.3.6.1.4.1.9.1.502, a Catalyst switch SysObjectID. This criteria will pass only if the polled device is a Catalyst machine.

§ **SNMP SysObjectID starts with**. Select to set criteria that passes if the value of the polled SysObjectID object starts with the specified value. For example, the criterion could poll the system object ID and check that it starts with 1.3.6.1.4.1.9, the root of the Cisco Enterprise MIB space. This criteria will pass only if the polled device is a Cisco machine.

- **NIC card brand name matches regular expression**. Select to set criteria that passes if the value of the device NIC card brand name matches the specified regular expression value. For example, SNMP is used to identify all NIC MAC addresses and they are converted to NIC vendor strings. The criterion could use the regular expression .**intel* to check for a criteria match on all Intel NIC cards.
- **TCP port is open**. Select to set criteria that passes if the value of the of the device port open is equal to the specified port open value. For example, if you want to find devices that have TCP ports 1234 open, then enter the port number "1234" for the port check criteria.
- **Is always a successful match**. Select to set all criteria to always match when the option is selected.
- **Device is a VMware host server (ESX/ESXi)**. Select to set criteria that passes if the device type is a VMware host server.
- **VMware server is hosting a number of VMs greater than**. Select to set criteria that passes if the number of VMs hosted is greater than the specified value.
- **Name of VM hosted by VMware server is**. Select to set criteria that passes if the name of the VM hosted by the VMware server is the specified name.
- **Name of VM hosted by VMware server contains**. Select to set criteria that passes if the name of the VM hosted by the VMware server contains the specified value.
- **Device is a VMware vCenter Server**. Select to set criteria that passes if the device type is a VMware vCenter Server.

7 After selecting a criterion, click **OK**. The Edit Criterion dialog appears.

8 Configure the settings for the criterion, then click **OK**. For specific information about the criterion's settings, click **Help**.

Note: By default, a device must match ALL role identification criteria to be identified as that device role. To identify devices that match ANY of the role identification criteria, clear **Match all criteria**.

Using the percent variables in the Discovery Console

You can customize discovery, device role, and scheduled discovery information with the variables in the following tables. For more information about where you can use the discovery percent variables, see Configuring device role settings in the WhatsUp Gold console help.

Device Discovery variables	**Description**
`%Discovery.Device.DeviceID`	Returns the device ID.
`%Discovery.Device.Description`	Returns the device description information.
`%Discovery.Device.Contact`	Returns the device contact information.
`%Discovery.Device.Location`	Returns the device location

	information.
%Discovery.Device.Name	Returns the device name information.
%Discovery.Device.OID	Returns the device OID information.
%Discovery.Device.PrimaryRole	Returns the device's primary role setting.
%Discovery.Device.Model	Returns the device product model information.
%Discovery.Device.Brand	Returns the device product brand information.
%Discovery.Device.OS	Returns the device operating system information.
%Discovery.Device.OSVersion	Returns the device operating system version.
%Discovery.Device.PhysicalAddress	Returns the device MAC address.
%Discovery.Device.PhysicalAddressVendor	Returns the device vendor name information.
%Discovery.Device.VMware.Host.Name	Returns the VMware host name.
%Discovery.Device.VMware.Host.FullName	Returns the full name of the VMware host.
%Discovery.Device.VMware.Host.OSType	Returns the VMware host operating system information.
%Discovery.Device.VMware.Host.VIMVersion	Returns the VMware virtual server version.
%Discovery.Device.VMware.Host.APIVersion	Returns the VMware virtual server API version.
%Discovery.Device.VMware.Host.APIType	Returns the VMware virtual server API type.
%Discovery.Device.VMware.Host.Build	Returns the VMware virtual server build number.
%Discovery.Device.VMware.Host.BootTime	Returns the VMware virtual server boot time.
%Discovery.Device.VMware.Host.HardwareVendor	Returns the hardware vendor name of the VMware host server.
%Discovery.Device.VMware.Host.HardwareModel	Returns the hardware model of the VMware host server.
%Discovery.Device.VMware.Host.NumberCPUCores	Returns the number of CPU cores on the VMware host server.
%Discovery.Device.VMware.Host.NumberCPUPkgs	Returns the number of CPU packages on the VMware host server.
%Discovery.Device.VMware.Host.NumberCPUThreads	Returns the number of CPU threads on the VMware host server.
%Discovery.Device.VMware.Host.CPUFrequency	Returns the CPU clock frequency of the VMware host server in Hz.

%Discovery.Device.VMware.Host.CPUModel	Returns the CPU model used by the VMware host server.
%Discovery.Device.VMware.Host.MemorySize	Returns the amount of memory in the VMware host server.
%Discovery.Device.VMware.Host.NumberVMsTotal	Returns the total number of virtual machines hosted by the VMware server.
%Discovery.Device.VMware.Host.NumberVMsPoweredOn	Returns the number of virtual machines hosted by the VMware server that are in the powered on state.
%Discovery.Device.VMware.Host.NumberVMsSuspended	Returns the number of virtual machines hosted by the VMware server that are in the suspended state.
%Discovery.Device.VMware.Host.NumberVMsPoweredOff	Returns the number of virtual machines hosted by the VMware server that are in the powered off state.

Device Session variables	**Description**
%Discovery.Session.ExistingDevices	Returns the total number of devices that reside in the WhatsUp Gold database.
%Discovery.Session.NewDevices	Returns the number of new devices identified in the discovery session.
%Discovery.Session.ModifiedDevices	Returns the number of device roles identified in the discovery session.
%Discovery.Session.LicensedDevices	Returns the number of devices WhatsUp Gold is licensed to manage.
%Discovery.Session.DiscoveredDevices	Returns the total number of devices identified in the discovery session.
%Discovery.Session.StartDate	Returns the discovery session starting date and time.
%Discovery.Session.EndDate	Returns the discovery session ending date and time.
%Discovery.Session.ElapsedTime	Returns the total discovery session scan time from start to finish.

Managing device roles

> **Note**: The Device Role Settings dialog is available from the WhatsUp Gold console Discovery console. For additional information about device roles, see the WhatsUp Gold console help.

Use the Device Role Settings dialog to manage device roles for discovery. From this dialog you can:

- *Create new device roles* (on page 64)
- *Duplicate existing device roles* (on page 64)
- *Modify device roles* (on page 64)
- *Enable or disable device roles* (on page 65)
- *Restore device roles to their original settings* (on page 65)
- *Delete device roles* (on page 65)

The Device Role Settings dialog is accessible from the Discovery console (**Advanced > Device role settings**).

Creating new roles

To create a new device role:

1. From the Discovery console, click **Advanced > Device role settings**. The Device Role Settings dialog appears.
2. Click **Add**. The Role Settings Editor dialog appears.
3. Configure the new device role. When you are done, click **OK**. The Role Settings Editor dialog closes.

Duplicating device roles

To duplicate an existing device role:

1. From the Discovery console, click **Advanced > Device role settings**. The Device Role Settings dialog appears.
2. Select a device role, then click the gear icon (⚙). A menu appears.
3. Select **Duplicate selected role** from the menu. A copy of the selected role is added to the list and selected.
4. To modify it, click **Configure**. The Role Settings Editor dialog appears.
5. Modify the device role.
6. When you are finished modifying the role, click **OK**. The Role Settings Editor dialog closes.

Modifying device roles

To modify an existing device role:

1. From the Discovery console, click **Advanced > Device role settings**. The Device Role Settings dialog appears.
2. Select a device role, then click **Configure**. The Role Settings Editor dialog appears.
3. Modify the device role.

4 When you are finished modifying the role, click **OK**. The Role Settings Editor dialog closes.

Enabling or disabling device roles

To enable/disable a device role:

1 From the Discovery console, click **Advanced > Device role settings**. The Device Role Settings dialog appears.

2 Select a device role, then click the gear icon (⚙). A menu appears.

3 If the device role is disabled, select **Enable selected role**. If the device role is enabled, select **Disable selected role**. The device role's status is immediately updated in the list.

Restoring a device role to its original settings

To restore a default device role to its original settings:

Note: Only default device roles can be restored.

1 From the Discovery console, click **Advanced > Device role settings**. The Device Role Settings dialog appears.

2 Select a device role, then click the gear icon (⚙). A menu appears.

3 Select **Restore selected role to factory defaults**. A confirmation dialog appears.

4 To restore the device role to its default settings, select **Yes**. The device role is restored to its original settings.

Deleting device roles

To delete a device role:

Note: Default device roles cannot be deleted. If you do not want to use a default device role, disable it.

1 From the Discovery console, click **Advanced > Device Role Settings**. The Device Role Settings dialog appears.

2 Select a device role, then click the gear icon (⚙). A menu appears.

3 Select **Delete selected role**. A confirmation dialog appears.

4 To delete the device role, select **Yes**. The device role is removed from the list.

Using Devices

In This Chapter

Viewing devices in WhatsUp Gold

After you have discovered and added devices to WhatsUp Gold, use the Devices tab to view and manage devices in WhatsUp Gold.

In WhatsUp Gold, devices are displayed as resources (computers/workstations, servers, routers, switches, etc.) that are connected to your computer through a LAN (Local Area Network), a wireless network, or over the Internet. WhatsUp Gold watches these devices through a network connection.

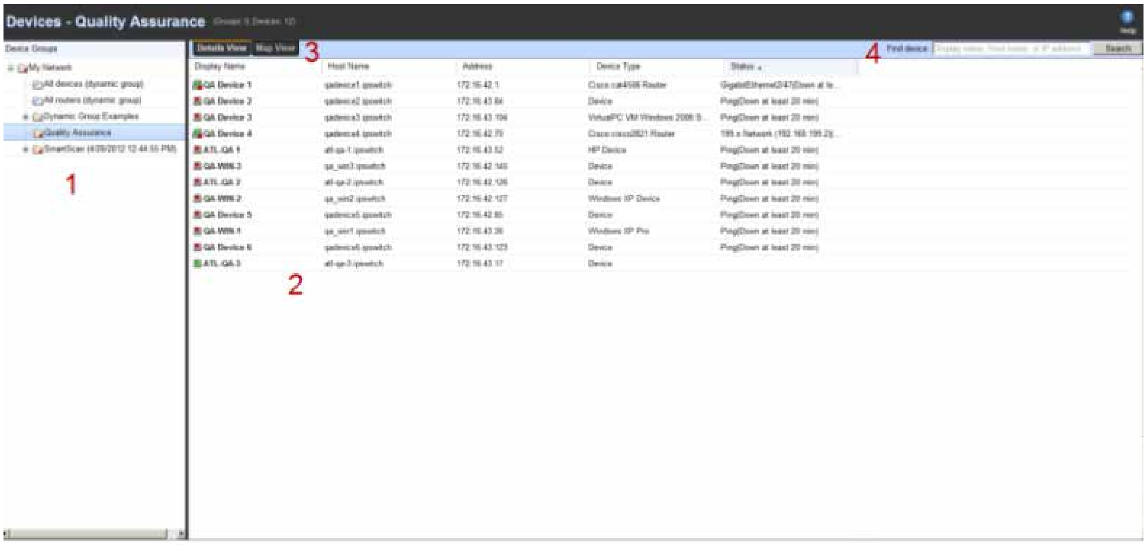
§ After you associate active monitors with devices on your network, the monitors query the network services installed on a device and wait for a response, checking to make sure that the FTP server, web server, email server, etc., is up and responding. If a response is either not received or is not the expected response, the service is considered down. If the query is returned as expected, the service is considered up. Notifications or other actions can be setup in WhatsUp Gold to address the issue. For a more information about service monitors, see the *Active Monitors overview* (on page 153).

You can also configure passive monitors, which listen for specified events to occur on a device and when the event occurs, notifies you or takes other actions. For more information, see the *Passive Monitors overview* (on page 247).

Additionally, you can configure performance monitors to gather device performance information, such as CPU, disk, memory, and interface utilization. For more information, see the *Performance monitors overview* (on page 260).

To view network devices:

§ Click the **Devices** tab, then click **Devices**. The Device list appears.



Devices - Quality Assurance (Groups: 5 Devices: 12)

Device Groups
- My Network
  - All devices (dynamic group)
  - All routers (dynamic group)
  - Dynamic Group Examples
  - Quality Assurance
  - SmartScan (4/26/2012 12:44:55 PM)

Details View | Map View

Find device: Display name, Host name, or IP address | Search

Display Name	Host Name	Address	Device Type	Status
QA Device 1	qadevice1.qaswitch	172.16.42.1	Cisco cat4506 Router	GigabitEthernet2/47(Down at le...
QA Device 2	qadevice2.qaswitch	172.16.43.84	Device	Ping(Down at least 20 min)
QA Device 3	qadevice3.qaswitch	172.16.43.104	VirtualPC VM Windows 2008 S...	Ping(Down at least 20 min)
QA Device 4	qadevice4.qaswitch	172.16.42.70	Cisco cisco2821 Router	195.x Network (192.168.195.2)...
ATL-QA 1	atl-qa-1.qaswitch	172.16.43.52	HP Device	Ping(Down at least 20 min)
QA-WIN 3	qa_win3.qaswitch	172.16.42.140	Device	Ping(Down at least 20 min)
ATL-QA 2	atl-qa-2.qaswitch	172.16.42.126	Device	Ping(Down at least 20 min)
QA-WIN 2	qa_win2.qaswitch	172.16.42.127	Windows XP Device	Ping(Down at least 20 min)
QA Device 5	qadevice5.qaswitch	172.16.42.85	Device	Ping(Down at least 20 min)
QA-WIN 1	qa_win1.qaswitch	172.16.43.38	Windows XP Pro	Ping(Down at least 20 min)
QA Device 6	qadevice6.qaswitch	172.16.43.123	Device	Ping(Down at least 20 min)
ATL-QA 3	atl-qa-3.qaswitch	172.16.43.17	Device	

1 **Device Groups**. Lists network devices by categories. Select the device group you want to view. The selected device group appears in the right panel in the Details View or Map View. For more information, see *Using Device Groups* (on page 72).

2 **Details View** (shown). Lists network devices as a list of devices in a group.

3 **Map View** (not shown). Lists network devices as icon views of devices in a group. The map view provides visual information about the device status. For more information, see *Using the Map View* (on page 92).

4 **Find Device**. Use this search tool to find a device or device group(s) in WhatsUp Gold. For more information, see *Searching for devices* (on page 68).

Each device icon provides information about its device state and the state of the monitors associated to the device. In addition, the Status column indicates which specific monitor is down and the duration of the interruption.

About device icons

The following icons appear in the Device View (console) or Details View (web interface) when viewing the contents of a device group. For more information about device icons and status indicators, see *Using the Map View* (on page 92).

Icon	Description
🟩	(Green) All monitors on the device are considered up.
🟩🟥	Device entry appears in another device group. At least one monitor on the device is unresponsive, but at least one is considered up.
🟧	(Orange) The device is currently in maintenance mode.

A bold device name shows that the device has undergone a state change, and that state change has not been acknowledged. To acknowledge a device state, right-click the device and click **Acknowledge**.

Using Credentials

The Credentials system stores the applicable login, community string, or connection string information for the following devices and applications:

- Windows (WMI Active Monitors, WMI Performance Monitors, and the Web Task Manager)
- SNMP v1, 2, and 3 devices in the WhatsUp Gold database
- ADO database
- VMware
- Telnet
- SSH

Credentials are configured in the Credentials Library (located on the **Admin** tab under **Credentials Library**) and used in several places throughout the application. They can be associated with devices in the Device Properties dialog (right-click a device, select **Properties > Credentials**), or through **Credentials Bulk Field Change** by right-clicking a group of devices in a device list or map.

A device needs SNMP credentials applied to it in order for SNMP-based active monitors to work. Similarly, NT Service Checks must have Windows credentials applied, and WhatsUp Gold database monitors require ADO connection information.

VMware vCenter, and ESXi devices require VMware credentials to access system performance counters.

WhatsConfigured plug-in requires either an SSH or Telnet connection to gather configuration data and to perform various task scripts. For more information, see *Credentials Library* (on page 458).

Searching for devices

Use the Find Device feature to find a device or device group(s) to which a network device belongs. Find Device is a "contains" search. For example, if you enter the numbers 192 for an IP address search, any device whose IP address contains the sequential numbers 192 would be listed in the search results.

To search for a device using the Find Device feature:

1 In the WhatsUp Gold web interface, go to **Devices > Find Device**. The Find Device dialog appears.

- or -

From the Devices tab, click **Search** next to the Find devices box.

2 Enter or select the appropriate information:

§ **Search**. Select the device aspect by which you would like to perform the device search; either *Device Display Name*, *Hostname*, *IP Address*, or *All*. If you select to perform a search by All, WhatsUp Gold searches for the matching criteria in the device's display name, hostname, and IP address.

§ **For**. Enter the device criteria for which WhatsUp Gold will search for a match.

§ **Exact Match**. (Optional) Select to have WhatsUp Gold search for an exact match of the search criteria you enter in the **For** box.

3 Click **Find**. Device search results are displayed in the lower section of the dialog.

Note: By default, Find Device searches for matches that contain your search criteria. For example, if you search for `Device IP Address` and `12`, your search results can contain matches for addresses including 12.0.0.1, 192.168.120.2, 172.16.42.12, 10.122.0.1, 172.16.42.112, and 192.168.212.1.

The dialog displays the following data about devices matching the search criteria.

§ The device's **Display Name**.

§ The device's **Hostname**.

§ The device's **IP Address**.

§ The **Device Group** to which the device belongs. If a device belongs to more than one device group, it is listed multiple times in the list of devices, one time for each group in which it belongs.

Note: Devices are displayed in this list according to a user's group access rights. You must have Group Read rights to at least one group to which a device belongs in order for it to appear in the results list. For more information, see *Group Access and User Rights for the Find feature* (on page 70).

To view a group to which the device belongs:

Select a device from the list, then click **View Group**. The Device List appears in either Details or Map View, with the selected device highlighted.

To edit a device configuration:

Select a device from the list, then click **Properties**. The device *Properties* (on page 117) dialog appears.

To delete a device from a group:

Select a device from the results list that is listed in the group from which you want to remove the device, then click **Delete**. The device is removed from the group.Use this dialog to find a device or device group(s) to which a network device belongs, then manage the device as needed.

Understanding group access and user rights for Find Device

The Find Device feature adheres to the group access and user rights assigned to a WhatsUp Gold user account. User rights and group access rights are configured from the Manage Users dialog.

Note: Group access rights are enabled from the Manage Users dialog, but must be specified from a group's properties. For more information, see Assigning group access rights.

To access the Manage Users dialog from the WhatsUp Gold web interface, go to **Admin > Users**.

A user account must have group read rights to at least one group to which a device belongs in order for it to appear in the results list. Additionally, a user account must have the following rights to use the Find Device feature:

§ An account must have Device Read to edit a device via *Device Properties* (on page 117).

§ An account must have both the Group Write and Manage Groups rights to remove a device from a group.

§ An account must have both the Device Write and Manage Devices rights to remove a device from WhatsUp Gold.

Note: When you attempt to remove a device from a group and it is the last copy of that device in WhatsUp Gold, if you have the appropriate rights, it is removed from WhatsUp Gold.

Searching for devices with interface traffic

If you have Flow Monitor, you can use the device right-click menu Host Search option to display the interfaces over which traffic has been transmitted to or from a specific device.

To search for device interface traffic:

1 Click the **Device** tab, then click **Devices**. The Device page appears.

2 From the Details View or Map View, right-click a device, then click **Host Search**. The Host Search dialog appears.
The top portion of this dialog provides specific information about the device for which you searched.

§ **Host name**. Displays the full host name of the device.

§ **IP address**. Displays the IP address of the device.

§ **Domain**. Displays the domain or group to which the device belongs.

§ **Country**. Displays the country to which the public IP address of this device is assigned.

§ **Last resolved**. Displays the date and time when the last record of the device was recorded on any interface.

The lower portion of this dialog displays specific interfaces over which the device transmitted traffic. This table shows the interface name, the amount of data recorded in the 24 hours prior to that date, and the date traffic was last recorded.

To view data where the selected host generated the traffic:

Select **Sender**. To view data where the selected host received the traffic, select **Receiver**.

By default, the **Traffic** and **Last Data Recorded** columns do not display information. To view information for these columns, select **Show Traffic and Last Data Recorded**.

Using device groups

In This Chapter

Using device groups

In WhatsUp Gold, device groups help you to quickly find and diagnose problems. You can create as many device groups as you wish to organize your network in a way that is meaningful to you and your monitoring needs.

Device group types

Two types of device groups exist in WhatsUp Gold:

§ Non-dynamic groups

§ Dynamic groups

Non-dynamic groups are simply referred to as "device groups." Each time you perform a discovery scan, WhatsUp Gold creates a group containing the devices found in that scan. WhatsUp Gold names the group by combining the type of scan and the date and time the scan took place. For example, "SNMP Scan (2007-08-03 10:24:37)." Devices that are already in the database appear in the new group as shortcuts to the original device reference. The shortcut icon indicates that the device appears in multiple groups. You can configure a device either by clicking the original reference, or by clicking a shortcut to the device. Functionally, shortcuts serve the same purpose as the original device reference, and display the same device status.

SQL queries searching for devices based on user-specified criteria create dynamic groups. By default, all devices discovered on your network are placed into a dynamic group named All devices. Similarly, each time a router is discovered it is placed into a similar dynamic group named All routers.

Device group icons

Device groups use icons to display the current state of the group and to indicate the type of device group.

🟩	All of the monitors on all devices in the group are up.
🟥	The device group contains at least one device that is considered down.
📁	The device group is empty, or devices have not been polled due to a dependency on another device.
▨	Indicates a dynamic group.

Device group maps

The Map View is based on device group folders, and each device group has a separate map. If a device group folder contains a subfolder, or subgroup, you can double-click the folder in Map View to display the subfolder map.

Device group reports

Device groups are particularly important when you are viewing reports pertaining to a specific group, or *group reports* (on page 353). Viewing group reports requires you to select a device group and a monitor to view data for that group. When you create groups, consider ways of easily distinguishing them from one another for this reason. An easy way to distinguish groups is using group names that are meaningful, such as "Atlanta Developers" and "Atlanta Tech Support." As a result, you can easily tell what each device group is when choosing a group on which to view Group Report information.

Device Group Access Rights

Similar to user rights are the WhatsUp Gold group access rights, which link permissions to device groups. For more information, see About group access rights.

Creating device groups

To create a new device group:

> **Note**: You cannot create a new device group within a dynamic group.

1 From the WhatsUp Gold web interface, go to **Devices > New Group**. The Create Group dialog appears.

2 Enter the appropriate information:

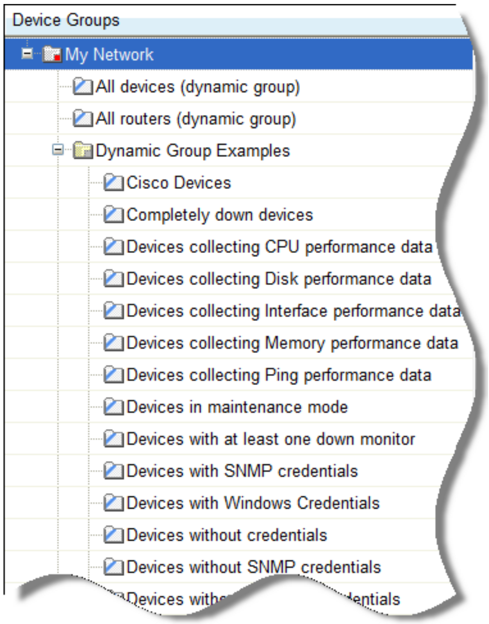
§ **Group Name**. Enter a unique name for the group.

§ **Description**. (Optional) Enter additional information about the group.

3 Click **OK** to add the group to the My Network tree.

About Dynamic Groups

Dynamic groups can be created for specific device types, device attributes, active monitors, or anything else that is stored for individual devices in the database. Dynamic groups act as SQL queries that run on the WhatsUp Gold database, and can display real-time data if viewed through a report that is set to automatically refresh. WhatsUp Gold is preconfigured with dynamic group examples, which you can see in the Devices view, under Device Groups.



Device Groups

- My Network
  - All devices (dynamic group)
  - All routers (dynamic group)
  - Dynamic Group Examples
    - Cisco Devices
    - Completely down devices
    - Devices collecting CPU performance data
    - Devices collecting Disk performance data
    - Devices collecting Interface performance data
    - Devices collecting Memory performance data
    - Devices collecting Ping performance data
    - Devices in maintenance mode
    - Devices with at least one down monitor
    - Devices with SNMP credentials
    - Devices with Windows Credentials
    - Devices without credentials
    - Devices without SNMP credentials
    - Devices with entials

All of the *Dynamic Group examples* (on page 77) are active, so if you have devices that meet the criteria, you will see the device displayed within the group. In the web interface, the dynamic group display is refreshed every 2 minutes. A group is also refreshed when you select it.

To view or edit the criteria for a dynamic group, right-click the group name, then select **Properties**.

Note: Dynamic groups on the web interface do not follow group access rights. Anyone with the ability to view a device group can view any dynamic groups contained in that device group as well. However, only devices that the user has the permission to view appear in the group.

Creating dynamic groups

To create a new dynamic group:

1 Click the **Devices** tab, then click **New Dynamic Group**. The Create Dynamic Group dialog appears.

2 Select a method for configuring the new Dynamic Group. You have three options:

§ **Use the Dynamic Group Builder**. Select this option to use the WhatsUp Gold Dynamic Group Builder to write rules for your Dynamic Group SQL filter. See Configuring Dynamic Groups for more information.

§ **Use SQL (advanced)**. Select this option to write your own Dynamic Group SQL filter. See Configuring Dynamic Groups for more information.

§ **Create a predefined dynamic group**. Select this option to select a predefined dynamic group.

3 Click **OK** to save changes.

Configuring dynamic groups

You can create a new Dynamic Group using the WhatsUp Gold Dynamic Group Builder or by using the more advanced dialog to write your own SQL code.

Note: Dynamic groups in the web interface: Dynamic groups do not follow group access rights. Anyone with the ability to view a device group can view any dynamic groups contained in that device group as well. However, only devices the user has the ability to view appear in the group.

To create a new Dynamic Group using the Dynamic Group Builder:

1 From the WhatsUp Gold web interface, go to **Devices > New Dynamic Group**. The Create Dynamic Group dialog appears.

2 Select **Use the Dynamic Group builder**, then click **OK**.

3 Enter or select the appropriate information:

- **Group Name**. Enter a name for the Dynamic Group as it will appear in the WhatsUp Gold Device List.
- **Description**. (Optional) Enter additional information for the new Dynamic Group. This description is visible to all users who can open the dynamic group.
- **Filter**. Select **All devices** to show all devices that match the criteria of the dynamic group, select **All devices in the parent group** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located, or select **All devices in the parent group and its children groups** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located or any of that group's children groups.

4 Create and edit rules to form an SQL filter for the Dynamic Group.

- Click **Add** to begin writing the rules for your SQL filter. The *Dynamic Group Rule Editor* (on page 85) appears.
- Enter the appropriate information in the *Dynamic Group Rule Editor* (on page 85). As you create rules, they are added to the Dynamic Group Builder dialog where you can add more rules, edit, or delete existing rules by clicking **Add**, **Edit**, or **Delete**.

Note: Parentheses (single, double, triple, and quadruple) are available for use in your filter code - add them by selecting them from the lists before and after your rules.

Note: You can move existing rules up or down within your filter code by selecting a rule and then clicking on **Up** or **Down**.

Validating your filter code

As you configure your rules, the SQL filter is displayed at the bottom of the Builder dialog. When you are satisfied with the filter code that is displayed, click **Validate** to test the filter code syntax. If the test returns no errors, click **OK** to save the configured SQL filter and to add the new Dynamic Group to your Device List.

If the code returns errors, either make the needed changes at this time, then click **OK**. Additionally, you have the option to save the filter code so that you may edit it at a later time. You can then select the Dynamic Group from the Device List and right-click, then select **Properties** to edit the group filter code.

Converting your filter code

You can convert a Dynamic Group created with the Dynamic Group Builder to the SQL dialog by clicking **Convert**. It is important to note that once you convert the Dynamic Group to the SQL dialog, you will not be able to edit the group in the Dynamic Group Builder again—you will only be able to make changes to the group from the SQL dialog. If you aren't an advanced SQL user, we recommend that you make a copy of the Dynamic Group so that you can keep a copy available for edit in the Dynamic Group Builder.

To create a new Dynamic Group using the Advanced SQL dialog:

1 Enter the appropriate information:

§ **Group name**. Enter a name for the dynamic group. This name appears on the device list.

§ **Description**. (Optional) Enter additional information that describes the dynamic group.

§ **SQL Filter**. Enter the SQL query statement that retrieves the list you want from the database. For the dynamic group to appear in your device list, the first line must be '`SELECT DISTINCT nDeviceID`'.

2 Click **OK** to save and add the Dynamic Group to your Device List.

Validating your filter code

When you are satisfied with the filter code that is displayed, click **Validate** to test the filter. If it runs as you expect, click **OK** to save the configured SQL filter and to add the new Dynamic Group to your Device List. If the code does not run as you expect, but you would still like to save the filter code so that you may edit it at a later time, click **OK.** You can then select the Dynamic Group from the Device List and right-click, then select **Properties** to edit the group filter code.

If you do not know how to formulate SQL queries, you can use the WhatsUp Gold Dynamic Group Builder, or cut and paste filter entries from existing dynamic groups, then edit them to read data from other tables.

WhatsUp Gold is preconfigured with dynamic group examples, which you can see in the Devices view, under Device Groups. In addition to the preconfigured dynamic groups, we have provided several sample filters for you to create some very interesting dynamic groups.

Note: You can learn more about the database structure by downloading the database schema file on the *WhatsUp Gold support page* (http://www.whatsupgold.com/support/index.aspx).

Dynamic Group examples

WhatsUp Gold is preconfigured with dynamic group examples, which you can see in the Devices view, under Device Groups. For more information on these groups, see *Configuring Dynamic Groups* (on page 75).

The following examples show several dynamic group filters that you can use to create some interesting dynamic groups for your devices. To use these examples, select the text of the filter, and then copy and paste the text into the **Filter** box of the *Dynamic Group* (on page 75) dialog.

> **Note**: You may have to remove the copyright information from the cut and paste if it appears when you copy from this help file.

To show all devices that have had a state change in the last three hours:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

    JOIN PivotActiveMonitorTypeToDevice

      ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

    JOIN ActiveMonitorStateChangeLog

      ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

         ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

WHERE  Device.bRemoved = 0

    AND DATEDIFF(Hh,ActiveMonitorStateChangeLog.dStartTime,GETDATE()) <= 3
```

To show all devices with multiple interfaces:

```
SELECT DISTINCT NetworkInterface.nDeviceID

FROM Device

     JOIN NetworkInterface

       ON Device.nDeviceID = NetworkInterface.nDeviceID

WHERE   Device.bRemoved = 0
```

```
GROUP BY Network Interface.nDeviceID

HAVING   COUNT(NetworkInterface.nDeviceID) > 1
```

To show all devices that have gone down in the last two hours and are still down:

```
SELECT DISTINCT Device.nDeviceID

FROM      Device

              JOIN PivotActiveMonitorTypeToDevice

                ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

              JOIN ActiveMonitorStateChangeLog

        ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

             ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

      JOIN MonitorState

        ON Device.nWorstStateID = MonitorState.nMonitorStateID

WHERE Device.bRemoved = 0

              AND PivotActiveMonitorTypeToDevice.bDisabled = 0

              AND DATEDIFF(hh, ActiveMonitorStateChangeLog.dStartTime, GETDATE()) <= 2

              AND MonitorState.nInternalMonitorState = 1
```

To show all the devices (in one specific group) that have had an action fire in the last two days:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

       JOIN ActionActivityLog

         ON Device.nDeviceID = ActionActivityLog.nDeviceID

       JOIN PivotDeviceToGroup
```

```
          ON Device.nDeviceID = PivotDeviceToGroup.nDeviceID

        JOIN DeviceGroup

          ON PivotDeviceToGroup.nDeviceGroupID = DeviceGroup.nDeviceGroupID

WHERE  Device.bRemoved = 0

        AND DATEDIFF(Dd,ActionActivityLog.dDateTime,GETDATE()) <= 2

        AND DeviceGroup.sGroupName = 'My Key Resources Group'
```

To show all devices with disks that are 90% full or fuller:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

        JOIN PivotStatisticalMonitorTypeToDevice

          ON Device.nDeviceID = PivotStatisticalMonitorTypeToDevice.nDeviceID

        JOIN StatisticalDiskIdentification

          ON PivotStatisticalMonitorTypeToDevice.nPivotStatisticalMonitorTypeToDeviceID =

               StatisticalDiskIdentification.nPivotStatisticalMonitorTypeToDeviceID

        JOIN StatisticalDiskCache

          ON StatisticalDiskIdentification.nStatisticalDiskIdentificationID  =

               StatisticalDiskCache.nStatisticalDiskIdentificationID

WHERE  Device.bRemoved = 0

        AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1

        AND StatisticalDiskCache.nDataType = 1

        AND (((nUsed_Avg / nSize) >  0.90)

              AND (NOT nSize = 0
            OR nSize IS

                NULL))
```

To show all devices in maintenance or with at least one down active monitor and match the specified device types:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

    JOIN MonitorState

      ON Device.nWorstStateID = MonitorState.nMonitorStateID

WHERE  Device.bRemoved = 0

    AND MonitorState.nInternalMonitorState IN (1,2)

    AND Device.nDeviceTypeID IN (3,4,38,63,64,65,66,67,68,71,72)
```

To show only devices on which all active monitors are down:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

    JOIN MonitorState

      ON Device.nWorstStateID = MonitorState.nMonitorStateID

WHERE  Device.bRemoved = 0

    AND MonitorState.nInternalMonitorState = 1

    AND Device.nWorstStateID = Device.nBestStateID
```

To show only those devices on which all active monitors have been down for 20 minutes or more:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device
```

```
    JOIN PivotActiveMonitorTypeToDevice

      ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

    JOIN ActiveMonitorStateChangeLog

      ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

         ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

    JOIN MonitorState

      ON PivotActiveMonitorTypeToDevice.nMonitorStateID =

         MonitorState.nMonitorStateID

WHERE  Device.bRemoved = 0

    AND PivotActiveMonitorTypetoDevice.bRemoved = 0

    AND PivotActiveMonitorTypeToDevice.bDisabled = 0

    AND MonitorState.nInternalMonitorState = 1

    AND DATEDIFF(Mi,ActiveMonitorStateChangeLog.dStartTime,GETDATE()) >= 20

    AND Device.nWorstStateId = Device.nBestStateId
```

To show devices to which a particular performance monitor is assigned:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

    JOIN PivotStatisticalMonitorTypeToDevice

      ON Device.nDeviceID = PivotStatisticalMonitorTypeToDevice.nDeviceID

    JOIN StatisticalMonitorType

      ON StatisticalMonitorType.nStatisticalMonitorTypeID =

         PivotStatisticalMonitorTypeToDevice.nStatisticalMonitorTypeID
```

```
WHERE  Device.bRemoved = 0

       AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1

       AND StatisticalMonitorType.sStatisticalMonitorTypeName

           LIKE '%Interface Utilization%'
```

To show devices to which a particular passive monitor is assigned:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

       JOIN PivotPassiveMonitorTypeToDevice

         ON Device.nDeviceID = PivotPassiveMonitorTypeToDevice.nDeviceID

       JOIN PassiveMonitorType

         ON PassiveMonitorType.nPassiveMonitorTypeID =

              PivotPassiveMonitorTypeToDevice.nPassiveMonitorTypeID

WHERE  Device.bRemoved = 0

       AND PivotPassiveMonitorTypeToDevice.bRemoved = 0

       AND PassiveMonitorType.sMonitorTypeName LIKE '%Cold Start%'
```

To show devices to which a particular active monitor is assigned:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

       JOIN PivotActiveMonitorTypeToDevice

         ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

       JOIN ActiveMonitorType

         ON ActiveMonitorType.nActiveMonitorTypeID =
               PivotActiveMonitorTypeToDevice.nActiveMonitorTypeID

WHERE  Device.bRemoved = 0

       AND PivotActiveMonitorTypeToDevice.bRemoved = 0

       AND ActiveMonitorType.sMonitorTypeName LIKE '%Ping%'
```

To find a device by its display name, host name, or IP address:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

    JOIN NetworkInterface

     ON Device.nDeviceID = NetworkInterface.nDeviceID

       AND Device.nDefaultNetworkInterfaceID =

           NetworkInterface.nNetworkInterfaceID

    JOIN DeviceType

     ON Device.nDeviceTypeID = DeviceType.nDeviceTypeID

WHERE  (Device.sDisplayName LIKE '%Mail Server%'

     OR NetworkInterface.sNetworkName LIKE '%server1.ipswitch.com%'

     OR NetworkInterface.sNetworkAddress LIKE '%1.2.3.4%')

    AND Device.bRemoved = 0
```

To show devices whose actions (or whose active monitors' actions) have a specific word in their name:

Note: To search for a different action, change the action name after LIKE. Be sure to leave both % symbols.

```
SELECT DISTINCT Device.nDeviceID

FROM   Device
```

```
        JOIN ActionPolicy

                        ON Device.nActionPolicyID = ActionPolicy.nActionPolicyID

        JOIN PivotActionTypeToActionPolicy

                        ON ActionPolicy.nActionPolicyID =

                                PivotActionTypeToActionPolicy.nActionPolicyID

                        JOIN ActionType

                         ON PivotActionTypeToActionPolicy.nActionTypeID =

                                ActionType.nActionTypeID

WHERE  Device.bRemoved = 0

        AND ActionType.sActionTypeName LIKE '%Critical%'

UNION

SELECT DISTINCT Device.nDeviceID

FROM   Device

        JOIN PivotActiveMonitorTypeToDevice

          ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

        JOIN ActionPolicy

          ON PivotActiveMonitorTypeToDevice.nActionPolicyID =

                ActionPolicy.nActionPolicyID

        JOIN PivotActionTypeToActionPolicy

          ON ActionPolicy.nActionPolicyID =

                PivotActionTypeToActionPolicy.nActionPolicyID

      JOIN ActionType
```

```
          ON PivotActionTypeToActionPolicy.nActionTypeID =

             ActionType.nActionTypeID

WHERE  Device.bRemoved = 0

    AND PivotActiveMonitorTypeToDevice.bRemoved = 0

    AND ActionType.sActionTypeName LIKE '%Critical%'

UNION

SELECT DISTINCT Device.nDeviceID

FROM   Device

    JOIN ActionPolicy

         ON  ActionPolicy.nActionPolicyID=0 and bGlobalActionPolicy=1

    JOIN PivotActionTypetoActionPolicy P

         ON P.nActionPolicyID = ActionPolicy.nActionPolicyID

    JOIN [ActionType]

         ON P.nActionTypeID = ActionType.nActionTypeID

WHERE  ActionType.sActionTypeName LIKE '%Critical%'
```

Using the Dynamic Group Rule Editor

Use this dialog to create or edit rules for use in the SQL filter for the new group.

Select the desired rule components from the list and enter in a variable in the empty field. This is a list of rule types available for use with the WhatsUp Gold Dynamic Group Builder.

String rules

§ **Active monitor**. Checks the Active Monitors configured for a device found at **Device Properties > Active Monitors**.

§ **Device attribute**. Checks for a device **Attribute name** that matches the criteria entered in **Attribute value**. Device attributes are configured on the **Device Properties > Attributes** dialog.

§ **Display name**. Checks the **Display name** field found at Device **Properties > General**.

- **IP address**. Checks the **IP address** field found at **Device Properties > General**. Also checks any additional network interface in the Additional Network Interfaces dialog.
- **Host name**. Checks the **Host name** field found at **Device Properties > General**. Also checks any additional network interface in the Additional Network Interfaces dialog.
- **Device type**. Checks the **Device type** field found at **Device Properties > General**.
- **SNMP OID**. Checks the **SNMP OID** field found at **Device Properties > Credentials**.

You can choose from six search criteria for the string rule types:

- contains
- does not contain
- is
- is not
- starts with
- ends with

After choosing a search criteria, you enter a variable to complete the string rule. An example string rule could read, "Match the following rule where: Device type contains Windows," where "Device type" is the rule type, "contains" is the search criteria, and "Windows" is the variable. This string rule would search for all device types on the network that contain the word "Windows."

"Yes/No" rules

- **Has an SNMP credential.** Checks the **SNMP v1/v2/v3 credentials** field found at **Device Properties > Credentials** to see if devices have SNMP credentials.
- **Has a Windows credential.** Checks the **Windows credentials** field found at **Device Properties > Credentials** to see if devices have Windows credentials.

Note: Does not apply to Passive Monitors that use credentials.

You have two search criteria to choose from for Yes/No rules:

- Yes
- No

You do not have to enter a variable for Yes/No rules, because the variable exists in the rule type itself. For example, if you're searching for devices that do not have SNMP credentials, the variable is the SNMP credential. The criteria is whether a device has an SNMP credential (No). An example yes/no rule could read, "Match the following rule where: Has a Windows credential, Yes," where "Has a Windows credential" is the variable and "Yes" is the search criteria. This rule would search for devices that have Windows credentials.

"IP address is within" rules

You can create two types of IP addresses within rules:

- the range
- a subnet

The range. To create a Dynamic Group consisting of devices within a certain range of IP addresses, you can create a rule that searches for devices with addresses that fall between two IP addresses, a lower number address, and a higher number address. For example, you could create a rule that reads, "Match the following rule where: IP address is within the range 192.160.1.1. and 192.165.25.255." The rule would search for all devices with IP addresses that fall between the two addresses and create a new Dynamic Group with these devices.

A subnet. To create a Dynamic Group consisting of devices within a certain subnet, you can create a rule that searches for devices on a specific IP address' subnet. You will be required to know an IP address and a subnet mask. You can either the subnet mask or the prefix length of that subnet in the **Mask** field.

Using the **A subnet** option requires that you have some knowledge of CIDR notation.

Note: The "IP address is within" rules do not support IPv6 addresses. A full rule should read something like, "Match the following rule where: IP address starts with 192.6."

Click **OK** to add the rule to the Dynamic Group Builder dialog.

Creating Layer-2 Groups

You can create Layer-2 groups and apply dynamic map filters to layer-2 maps so that the maps update dynamically, each time device information is changed.

As a part of selecting (filtering) devices to display in the dynamic topology maps, you use Map Devices and Connected Devices selection filters to build the a custom map. For example, using the Map Devices filtering options, you can select devices in the IP range of 10.0.0.1 - 10.0.0.100 to appear on a map. Any device added to the network, within the range, will be added to the map. You can also apply Connected Devices filters to show devices connected to the core mapped devices. For example, you can filter a map to show all servers connected to switches on the topology map.

This feature helps ensure that your layer-2 topology maps are up-to-date with the most recent network configuration.

Use the The Layer-2 Group Properties dialog to:

- Define the devices you want to show on the group map so that each time the map is updated dynamically, any new devices that match the criteria is added to the map.
- Configure the topology layout and display settings; for example, radial, hierarchy, manual map layout options.
- Configure monitor settings for the group/map.

To create a new layer-2 group and manage group map settings:

1 On the WhatsUp Gold web interface, in Map View, right-click inside the map. From the right-click menu, click **Map Options > Group/Layout Settings**. The Layer-2 Group Properties dialog appears.

- or -

On the WhatsUp Gold web interface, in Map View, right-click inside the map. From the right-click menu, click **New > New Layer-2 Group**. The Layer-2 Group Properties dialog appears.

2 Enter a **Device Group Name** for the new group/map.

3 Use the dialog's three tabs to configure map settings:

Devices tab

Select the **Update Mode**:

§ **Dynamic**. Select this option to apply map filters to the topology map each time device information is changed.

§ **Manual**. Select this option to disable device filtering for maps. When the device filters are disabled, you can add devices to the map with the topology map right-click menu.

Use the **Map Devices** and **Connected Devices** boxes to design a filter for the devices you want to include on the map. Click **Edit** to open the Edit Devices Filter dialog and make device filter selections. For more information, see *Configuring Device Filters* (on page 90).

If you want to see layer-2 links for devices in the map, select the **Show Layer-2 Links** option.

If you want to see association links for devices in the map, select the **Show Association Links** option.

Layout tab

To understand the layout modes, you must be familiar with the layout strategy used by the WhatsUp Gold topology engine. For each map, the topology viewer automatically selects a root device, which becomes the starting point of the diagrams. The root device is selected based on finding the device on the diagram with the most network connections.

Using the connectivity model, the topology viewer sets the *root* as the parent and then assigns all connected devices as children. This process continues until all devices on the topology map are given a parent/child relationship.

With the parent/child relationships calculated, the topology viewer provides three layout modes for any topology map. These modes describe the manner in which each child node (or device) is given its position on the topology map. The layout modes are described as follows:

§ **Radial**. In the radial layout mode, connected child devices are given positions in a radial (or circular) pattern around their parent device. You can modify the layout results by changing the following layout attributes:

  § **Level Spacing**. This setting dictates the amount of space between the parent and child device. Increase this value to provide more spacing between the parent and children devices.

  - § **Node Angle**. This setting dictates the amount of space between each child (or sibling) devices. Increase this value to fan out the children.

> **Note**: When increasing the node angle, if a large number of devices are shown connected to one parent, the radial layout may overlap (make a full circle). In this case you may need to decrease the node angle and increase the level spacing.

- § **Hierarchy**. In this mode, connected child devices are given positions in a hierarchical (or tree like) pattern in relationship to their parent. You can modify the layout results by changing the following layout attributes:

  Direction. This setting indicates the placement of the root device and the direction the children will be placed from the root device.

  - § **Down**. The root device is placed at the top of the topology map, and children are placed respectively below the root device.
  - § **Up**. The root device is placed at the bottom of the topology map, and children are placed respectively above the root.
  - § **Left**. The root device is placed at the right of the topology map, and children are placed respectively to the left of the root.
  - § **Right**. The root device is placed at the left of the topology map, and children are placed respectively to the right of the root.

  Alignment. This setting indicates the placement of the root (or parent) device in relationship to its children.

  - § **Center**. The root/parent device is centered (either vertically/horizontally) with respect to its children.
  - § **Left**. The root/parent device is located to the far left (either vertically/horizontally) with respect to its children.
  - § **Right**. The root/parent device is located to the far right (either vertically/horizontally) with respect to its children.

  Level Spacing. This setting dictates the amount of space between the parent and child devices. Increase this value to provide more spacing between the parent and children devices.

  Node Spacing. This setting dictates the amount of space between each child (or sibling) devices. Increase this value to create more space between sibling devices.

- § **Manual**. In this mode, the automatic layout methods are turned off and you are given complete control over device placement on the topology map. The topology maps provide a drag-and-drop capability to simplify creating and arranging a custom topology map. The following is a list of drag-and-drop operations in manual layout mode.

  - § **Left Mouse Click**. Selects a device on the topology map.
  - § **Left Mouse Click + Mouse Move**. Selects and drags a device to a new position on the topology map.
  - § You can use the manual layout mode to add new devices to the topology map. The method to add a device is the same as adding a device in radial or hierarchical

layout mode. After the devices are placed on the topology map, you can manually move devices on the map or select the radial or hierarchy layout settings to readjust the map.

Monitors tab

Select the **Monitor Settings** you want to apply to the map. You can select to:

- Enable Ping/SNMP Interface Active Monitors
- Create Ping Latency and Availability Performance Monitors
- Create Interface Utilization Performance Monitors
- Enable Performance Monitors

4 Click **OK** to save changes.

Configuring Device Filters

Device filters allow you to filter device group maps so that only the network information you want is displayed. You can customize the filter to display information about:

- All of your devices, including endpoint devices, such as servers and workstations.
- Only your network devices.
- Only those devices that have SNMP credentials.

You can create filters for categories of devices, individual IP addresses, IP ranges, subnets, VLANs, or combinations of these elements.

Creating a Device Filter

The following procedures provide instructions on how to create device filters using the Edit Device Filters dialog.

To create or edit a device filter:

1 Select the range of devices you want to include in the filter from the **Start with** list. This option sets the device range by restricting the devices filtered to one of the following groups of devices:

- **All Devices**. Select this option if you want the filter to be applied to all of the devices in the current discovery file.
- **All Network Devices**. Select this option if you want the filter to be applied to devices that are used to create the network, such as routers and switches.
- **All SNMP Devices**. Select this option if you want the filter to be applied only to those devices with an SNMP credential in the credential library.
- **All Servers**. Select this option if you want the filter to be applied to all discovered server devices.
- **All Virtual Machines**. Select this option if you want the filter to be applied to all discovered virtual machines.
- **All Virtual Servers**. Select this option if you want the filter to be applied to all discovered virtual server devices.

- **All Wireless LAN Controllers**. Select this option if you want the filter to be applied to all discovered LAN controller devices.
- **All Wireless APs**. Select this option if you want the filter to be applied to all discovered wireless APs.
- **All Wireless AP Clients**. Select this option if you want the filter to be applied to all discovered wireless AP clients.
- **All Workstations**. Select this option if you want the filter to be applied to all discovered workstation devices.

2 Use the options in the **Filter by** section to select specific hosts or VLANs to include in the filter.

The Advanced filtering options filter for individual or ranges of IP addresses, host names, NetBIOS names, subnets, or VLANs. The following buttons call dialogs to enter values for the advanced filtering criteria:

a) Click **Name/IP Address** to restrict the filter to specific hostnames, IP addresses, IP address ranges or subnets. The Device Filter - Host/IP Address Include Scope dialog appears.

Enter the hosts, IP addresses, and subnets you want to include in your filter:

- **Host / System / NetBIOS Names**. Enter the hostname, system name or NetBIOS name of the device or devices you want the filter to select. When you list a name in this box, the filter will return only those devices with that name in the box. You can use a * character as a wildcard in this box. Click **Clear** to clear the **Host / System / NetBIOS Names** box.
- **IP addresses / Subnets**. Enter the IP address, IP address range or subnet address (CIDR format) of the device or devices you want the filter to select. When you list one or more addresses or and address range for this option, the filter will return only those devices that match or fall within the indicated address range. Click **Clear** to clear the **IP addresses / Subnets** option.

b) Click **VLANs** to specify the the VLANs and indexes to include in the filter. The Device Filter - VLANs dialog appears.

Enter the VLAN name or index from which you want the filter to select devices. Click **Clear** to clear the VLAN names or indexes.

3 Also in the **Filter by** section of the dialog, select the categories of devices you want to include in your device filter.

If you select any category, only devices that match that category appears. If you have not selected any devices, all devices that meet the other filter criteria appears.

Click inside the box in the column heading to select all of the categories. When all categories are selected, all devices are returned.

4 Click **OK** to save changes.

Using Maps

In This Chapter

Using the Map View

As you discover devices on your network, WhatsUp Gold creates a map of the initial discovery device group. You can configure this map, or create other device groups and configure maps for these groups as you see fit. Regardless of the groups for which you configure maps, you can configure all maps in a variety of ways:

- Organize devices into user-specified groups, for example, all HTTP servers.
- Customize individual device icons such as workstations, containers, routers, and bridges.
- (WhatsUp Gold console) Indicate relationships among devices by using annotation objects such as rectangles, ellipses, text, network clouds, and "attached" or "free" lines.
- Show status of network link lines.

To access the Map View:

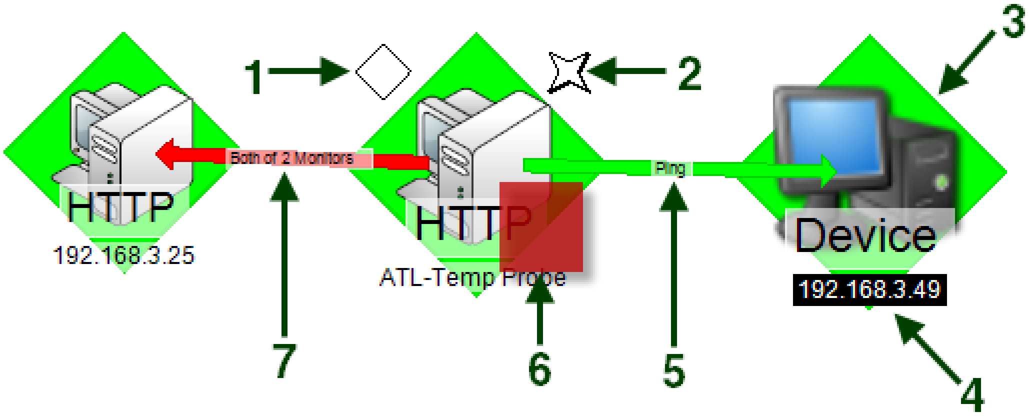
From the WhatsUp Gold web interface, go to **Devices > Devices > Map View**.
 - or -
From the WhatsUp Gold console, go to **View > Map View**.

Interpreting the Map View

The Map View consists of device icons, annotations, and graphical indicators which are used to represent the state of your network. The device icon is a graphical representation of the device and provides the hostname or IP address of the device. The device icon can be modified adding annotations, which you can add manually in the WhatsUp Gold console application, and by graphical indicators which are automatically applied to device icons.

Graphical Indicators

While annotations are added manually, graphical indicators are automatically applied to the device icon by WhatsUp Gold in response to state changes, or to dependencies between devices. The following diagram illustrates graphical indicators as they appear on a device icon in the Map View.



1 **Passive monitor indicator**. A diamond shape at the upper left of the device icon, displays the state of the passive monitors associated with the device.

2 **SNMP indicator**. A four pointed star located at the upper right of the device icon, is present when the device has SNMP credentials stored in the Credentials Library.

> **Note**: The presence of the SNMP indicator does not indicate that SNMP is enabled on the device, or that the device is reporting SNMP traps to WhatsUp Gold.

3 **Device state indicator**. The background color and shape directly behind the device icon, provides an indication of the state of the device as determined by the active monitors monitoring the device.

4 **Device status change indicator**. A reverse of the normal background and foreground, indicates that the device has undergone a state change that has not yet been acknowledged.

5 **Up dependency indicator**. A green arrow that originates at the dependent device and terminates at the device on which it dependent. The active monitors on which the device is dependent are displayed on the arrow.

6 **Active monitor indicator**. A square located at the lower right of the device icon, indicates the state of the active monitors associated with the device. If the indicator is green, there is a recent Up state change in an active monitor. If the indicator is red, there is a recent Down state change in an active monitor.

7 **Down dependency indicator**. A red arrow that originates at the dependent device and terminates at the device on which it dependent. The active monitors on which the device is dependent are displayed on the arrow.

Map View Options

In the WhatsUp Gold web interface, the default Map View display is scaled to fit within the maximum width and height in pixels set in the *Manage Server Options* (on page 467) dialog.

You can display a device map at 100% scale by clicking **Full Size**. To return the device map to the default size, click **Scale To Fit**.

Note: If you navigate away from and then back to the Map View, the display reverts to the default scaled option.

You can determine the look of the device map in both the WhatsUp Gold console and web interfaces. In the console, right-click on the device map, select **Display**, and then choose which map elements to enable. In the web interface, right-click on the device map, select **Map Options > Display Options**, and then choose which map elements to enable. The options available are:

- Device Icons
- Polling Dependency Arrows
- Unconnected Links
- Clip Device Names
- Wrap Device Names
- Remove Link Comments

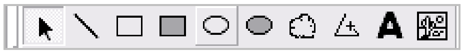
Note: The menu in the console also contains a **Snap to Grid** option. Snap to Grid is not present in the web interface map view right-click menu because the effect of the feature only visible in the console.

Annotations

Annotations, available in the WhatsUp Gold console application, are graphical objects that let you customize and visually organize a map view. You can use these annotations to draw connections between devices, add images and backgrounds, provide textual information, and add visual enhancements to the Map View. Map annotations include:

- Circles
- Lines
- Rectangles
- Text
- Network clouds
- Polygons
- Images

The Annotation toolbar is located at the top middle of the WhatsUp Gold console Map View.



Use this toolbar to add annotations and manipulate their properties, such as border width and color.

About Map View device limitations

By default, WhatsUp Gold does not display maps with more than 256 devices. You can change this default within the registry keys, with the understanding that it will cause lengthy delays by specifying larger device defaults.

> ✓ **Important**: The more devices you allow on a map, the longer time you will wait for the map to load.

To change map device limitations:

1 Locate the registry key which controls this setting.

- For 32-bit operating systems, open `HKEY_LOCAL_MACHINE\Software\Ipswitch\Network Monitor\WhatsUp Gold\Settings`.
- For 64-bit operating systems, open HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ipswitch\Network Monitor\WhatsUp Gold\Settings

2 Change the `MapView-MaxDevices` registry key to a number greater than `256` (Decimal).

> **Note**: If you want to change the text that displays when you reach the maximum device limit, you can change it in the `MapView-MaxDevicesMessage` registry value. The default text is:
>
> `There are more devices on this Map than can be |drawn in a reasonable time. Use the Device List |to manage devices for this Group. | |To increase the maximum of (%ld) devices that |can be drawn per Map, look in the online help |system for Map Device Limits.`
>
> The pipes (|) in the default text indicate line breaks in the text and the (%ld) is a variable for the `MapView-MaxDevicesMessage` value.

Managing devices

In This Chapter

Learning about devices

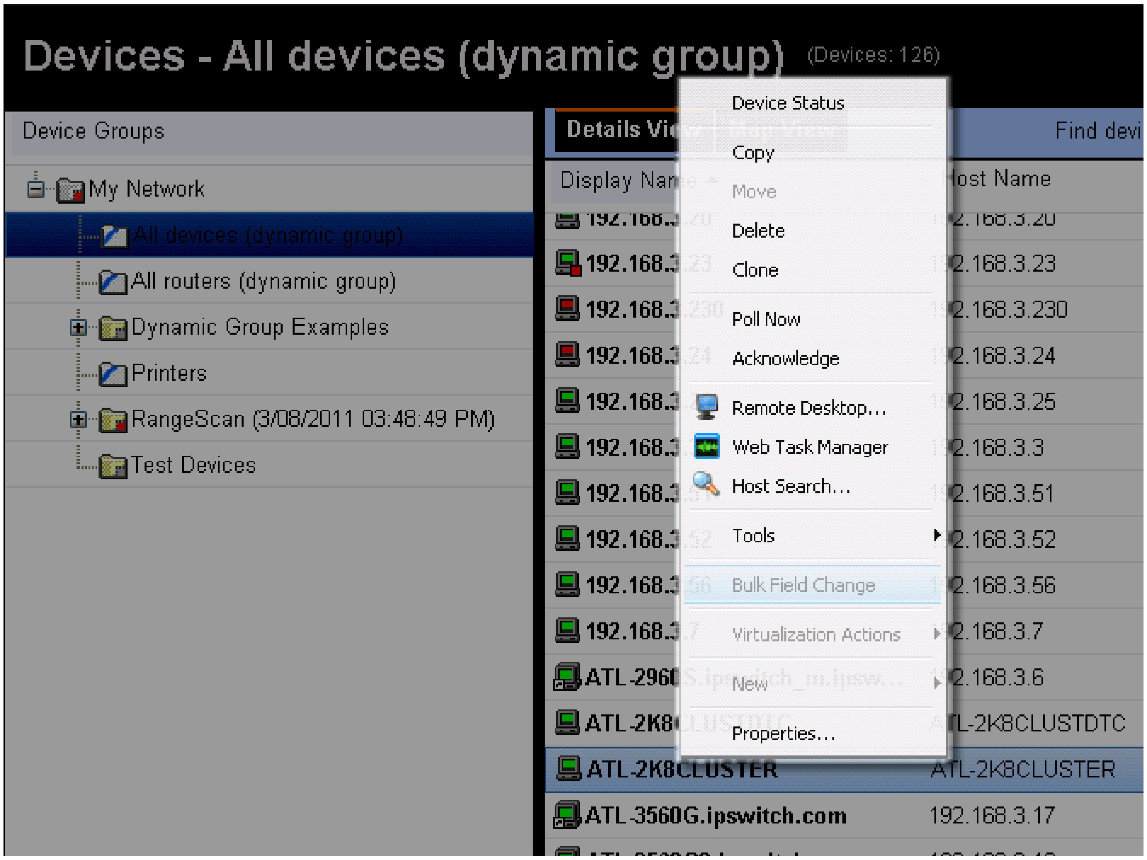
From the device right-click menu, you can perform a number of tasks on the selected device. You can Copy, Move, Paste, and Clone devices; poll a device; acknowledge a device states; access devices via Remote Desktop Connection, search for interface traffic to and from devices, use tools for troubleshooting device issues, apply bulk changes to multiple devices at one time, set actions on virtual machines, add a new device, and view device properties.

To view the Details View right-click menu:

To access the Details View right-click menu:

1 From the WhatsUp Gold web interface, go to **Dashboard > Devices > Details View**.

2 Right-click a device or multiple devices in the Details View. The following menu appears:



Adding a single new device to WhatsUp Gold

There are two ways to add devices to WhatsUp Gold:

- Discover devices automatically. For more information, see *Learning about the Discovery Console* (on page 26)
- Manually add individual devices.

When you add devices individually, the device is added to the WhatsUp Gold database immediately doing a discovery scan. The new device is generically categorized as a workstation. This option may be useful for testing purposes, as it allows you to add the same device to a database multiple times.

To add a single device to WhatsUp Gold:

1. In the WhatsUp Gold web interface, go to **Devices > New Device**. The Add New Device dialog appears.
2. Enter the **IP address or host name of the new device**.
3. If you want to add a device without scanning for additional device information, select **Add device immediately without scanning**. The new device is generically categorized as a workstation.
4. If you want to apply a device role to a new device, select **Force device role**. For more information, see *Using Device Roles* (on page 56).
5. Click **Advanced** to select a number of additional options for which to scan the device. You can select additional options to resolve the device host name, use advanced SNMP and ping timeout and retry settings. Additionally, select SNMP, SSH, WMI or VMware credentials for the new device. For more information, see *Setting Advanced single device discovery settings* (on page 97).
6. Click **OK** to save changes. WhatsUp Gold attempts to resolve the IP address or hostname, then scans that device for device roles (if selected). When the scan is complete, Device Properties dialog appears, allowing you to further configure the device as needed.

Note: If WhatsUp Gold already contains the number of devices that your license allows, a message appears telling you that you must upgrade your license or remove existing devices to add a new device.

Setting Advanced device discovery settings

Select the following advanced single device discovery properties to use for the device you are adding to WhatsUp Gold.

- **Resolve host names**. Select this option to have WhatsUp Gold attempt to populate the list of discovered devices with host names, instead of IP addresses. If the **Use SNMP SysName to name devices** option is selected (see below), it is used first to identify device names. If SNMP information is not available, the **Resolve host names** option is used to identify device names (if the option is selected).
- **Use advanced ping**. Select this option to use TCP port checks and ICMP pings to scan on networks. If the TCP connection or ICMP ping is successful, the device at the IP address is discovered.

- **Timeout (ms)**. Enter the amount of time the scan should wait for the ping or SNMP information in milliseconds (ms).

> **Note**: Refer to the information for Use advance ping options, to determine when this setting applies to ping.

- **Retry count**. Enter the number of times WhatsUp Gold should attempt to make the ping or SNMP identification.

> **Note**: Refer to the information for Use advance ping options, to determine when this setting applies to ping.

- **Use SNMP SysName to name devices**. Select this option to discover each device name by accessing the device SNMP SysName. This method is used first to identify device names. If not available, the **Resolve host names** option is used to identify device name (if the option is selected).
- **SNMP credentials**. Select the appropriate SNMP credentials. This box populates with credentials currently available in the WhatsUp Gold Credentials Library. If you select an inappropriate set of credentials, or none is selected, WhatsUp Gold determines device type based on the monitors discovered during the scan.

> **Tip**: Click browse (**...**) in the console or **Credentials** in the web interface to open the WhatsUp Gold Credentials Library to configure a new set of credentials to use for discovery.
>
> **Tip**: Credentials are configured in the Credentials Library. When a device is discovered using a credential, that credential is then associated to that device. You can change this on **Device Properties > Credentials**. If you select **All,** discovery uses all configured credentials in the Credentials Library. The credential that is successful is then associated with the device.

- **SSH credentials**. Select the appropriate SSH credentials. This box populates with credentials currently available in the WhatsUp Gold Credentials Library.
- **Windows credentials**. Select a Windows credential to use when attempting to discover devices where you have to provide a Windows user name or password when connecting. This box is populated from credentials currently available in the WhatsUp Gold Credentials Library.
- **VMware credentials**. Select the VMware credential to use when discovering VMware vCenter, ESX and ESXi devices. This box is populated from credentials currently existing in the Credentials Library.

Changing a device name

Changing the name of a device changes how it appears in the list views.

To change a device name:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

3 Click **General**. The General section of the Device Properties dialog appears.

4 Enter the new, unique name in the **Display Name** box.

5 Click **OK** to save changes.

Changing a device IP address

To change a device IP address:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

3 Click **General**.

4 Type the new IP address in the **Address** box.

5 Click **OK** to save changes.

Adding additional network interfaces to a device

To configure a network interface:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- or -
From any page where a device is selected using the device picker, click **Properties** in the title bar.

3 Click **General**. The General dialog appears.

4 Click **Additional Network Interfaces**. The Network Interfaces dialog appears.

5 Click **Add**. The Add Network Interface dialog appears.

6 Enter the network information for the new interface.

7 Click **OK** to save the new interface information and return to the General section.

To change the default network interface on a device:

1 In the General section of Device Properties, click **Additional Network Interfaces**.

2 On the Network Interfaces dialog, select the interface you want to make the default.

3 Click **Set Default.**

4 Click **OK** to return to the General section.

Adding notes to a device

To add a note to a device:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 In the Device List or Map View, right-click a device, then choose **Properties**. The Device Properties dialog appears.

Click **Notes.** The Notes dialog opens.

3 Enter the note in the **Notes** box.
Use the Notes box to include information about the selected device. For example, you can record historical information about a device, physical location information, or notes relating to the actions configured for the device.

Note: There is no automatic word wrap. Add a return to display information in the dialog without requiring you to scroll to view it.

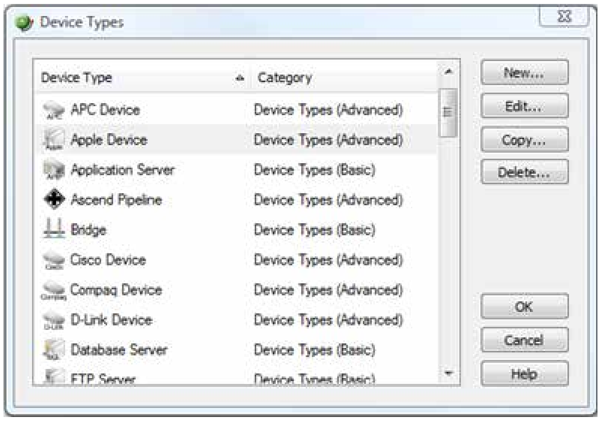
4 Click **OK** to save changes.

Using device types

Important: Prior to the WhatsUp Gold v14 release Device Types were used to identify the role a device performed on the network for the active and passive monitors, menu items, and icons associated with each device. WhatsUp Gold v14 and later has moved Device Type information to be managed in the Discovery Console Device Role Settings.

The Device Types dialogs now have limited functionality. Active monitors, passive monitors, and action policies are no longer editable in the Device Type dialog. The device General and Menu Items information is editable. For more information, see *Discovering and Viewing Network Data* (on page 43).

The device type icons represent network devices on maps. The WhatsUp Gold console provides device types for more than 40 device types with an option to create additional custom types.



Device Type	Category
APC Device	Device Types (Advanced)
Apple Device	Device Types (Advanced)
Application Server	Device Types (Basic)
Ascend Pipeline	Device Types (Advanced)
Bridge	Device Types (Basic)
Cisco Device	Device Types (Advanced)
Compaq Device	Device Types (Advanced)
D-Link Device	Device Types (Advanced)
Database Server	Device Types (Basic)
FTP Server	Device Types (Basic)

To configure device types (WhatsUp Gold console only):

1 Open the Device Types Library:

In either Device View or Map View on the WhatsUp Gold console, click **Configure > Device Types**. The Device Types Library dialog appears.

2 In the Device Type Library, do *one* of the following:

§ Click **New** to configure a new device type.

§ Select a device type, then click **Edit** to reconfigure the selected device type.

§ Select a device type, then click **Copy** to make a duplicate of the selected device type.

§ Select a device type, then click **Delete** to remove it from the Device Type Library.

3 Click **OK** to save changes.

To change a device type from the WhatsUp Gold console or web interface:

1 In Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **General**. The General Properties appear.

3 Select a new **Device Type** from the list on the right side of the dialog.

4 Click **OK** to save changes.

5 The device's type and coinciding icon updates on the map.

Refreshing device details

You can refresh devices using layer 2 discovery methods from the Device Groups list, Device Details, and Map View with the **Refresh Device Details** right-click menu command.

To refresh device details using layer 2:

Right-click a single device or device group, then click **Refresh Device Details**. WhatsUp Gold begins rediscovering the devices and progress displays on the Rediscover Devices dialog.

- or -

Select several devices and right-click the selection, then click **Refresh Device Details**. WhatsUp Gold begins rediscovering the devices and progress displays on the Refresh Devices dialog.

The Refresh Details Progress dialog displays the following information:

§ **Discovery Status**. The discovery scan progress; either *Canceled*, *Initializing*, *Finalizing*, *Running*, *Complete*, *Initialization*, *Run Failed*, *Finalization*, *Failed*, or *Unknown*.

§ **Elapsed Time**. The amount of time that has passed since the discovery scan began.

§ **Device Count**. The number of devices WhatsUp Gold has discovered.

The bottom of the dialog displays a discovery progress bar.

Copying a device

Use the copy feature to create a *shortcut* to the device in another group, much like a Windows shortcut. The copy provides access to the original device from a group other than the original group in which it is located.

To copy a device:

1 From the WhatsUp Gold web interface, in the Details View or Map View, right-click the device for which you want to copy. The right-click menu appears.

2 Click **Copy**. The Select a Device Group dialog appears.

3 Select the group that you want to copy the device into, then click **OK**. The group that you copied the device to opens.

> **Tip**: You can also drag-and-drop to copy device(s) from one group to another. Select the device(s) you want to copy, then drag-and-drop to the group where you want the device copied.

Moving a device

Use the move feature to move devices to another group. Moving removes devices from the original group and locates them in another group.

To move a device:

1 From the WhatsUp Gold web interface, in the Details View or Map View, right-click the device for which you want to move. The right-click menu appears.

2 Click **Move**. The Select a Device Group dialog appears.

3 Select the group that you want to move the device into, then click **OK**. The group that you copied the device to opens.

> **Tip**: You can also drag-n-drop to move device(s) from one group to another. Select the device(s) you want to move, then drag-n-drop to the group where you want the device moved.

Deleting a device

Use the delete device feature to remove devices from WhatsUp Gold. Once removed, the device is not monitored.

To remove a device:

1 From the WhatsUp Gold web interface, in the Details View or Map View, right-click the device for which you want to delete. The right-click menu appears.

2 Click **Delete**. A message appears asking you to confirm that you want to delete the selected device(s).

3 Click **OK**.

Cloning a device

The WhatsUp Gold cloning feature, available in the web interface, allows you to do a *deep copy* of a device. The term *deep copy* means that the device is copied to a new device with all active monitors, passive monitors, actions, attributes, etc. applied to the new device. This functionality makes it easy to create a new device with monitors, actions, and attributes set up based on ones you have already taken the time to set up for a previously created device. This reduces the time required to set up new monitors, actions, and attributes for a new device.

> **Note**: Any monitors and action policies associated with the device you are cloning from are not duplicated for the new cloned device, rather the new cloned device has the existing monitors and action policies applied to it.

Methods to clone a device

There are two ways to clone a device: from the device right-click menu or dragging-and-dropping a device from a device list or a map view to a new device group.

After you have cloned a device, you need to change the device host name and address in the Device Properties - General dialog settings so that WhatsUp Gold can monitor the new device and all of the active monitors, passive monitors, actions, and attributes that are applied to the new device. For more information, see *Changing the cloned Device Properties* (on page 104).

To clone a device:

1 From the WhatsUp Gold web interface, in the Details View or Map View, right-click the device for which you want to clone attributes. The right-click menu appears.
2 Click **Clone**. The Clone selected items from x to ... dialog appears.
3 Select the group that you want to clone the device into, then click **OK**. A status dialog appears indicating the cloning process status.
4 Click **Close** to complete the cloning process.

Note: The new cloned device display name is as shown in the following device name example:
- Original name: `Device-WHO`
- First clone (in new group): `Device-WHO`
- Second clone: `Device-WHO - Clone`
- Third clone: `Device-WHO - Clone (2)`
- Subsequent clones: `Device-WHO - Clone (nnn)`

Tip: You can also use the Device Properties - Notes dialog to verify if a device is a cloned device. Right-click the device you want to check, then click **Properties > Notes**. If the device is a cloned device, a message appears; for example, `This device was cloned on 6/24/2010 10:12:37 AM`.

5 Change the cloned device properties as required. For more information, see *Changing the cloned Device Properties* (on page 104).

Cloning a device using drag-n-drop

To clone a device using drag-n-drop:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.
2 In either the Details View or Map View, click the device (or multiple devices) for which you want to clone attributes, then drag the device(s) to the device group where you want the device(s) to appear. The Copy, Move, Clone, Cancel menu appears.
3 Click **Clone**. A status dialog appears indicating the cloning process status.
4 Click **Close** to complete the cloning process.

Note: The new cloned device display name is as shown in the following device name example:
- Original name: `Device-WHO`
- First clone (in new group): `Device-WHO`
- Second clone: `Device-WHO - Clone`
- Third clone: `Device-WHO - Clone (2)`
- Subsequent clones: `Device-WHO - Clone (nnn)`

Tip: You can also use the Device Properties - Notes dialog to verify if a device is a cloned device. Right-click the device you want to check, then click **Properties > Notes**. If the device is a cloned device, a message appears; for example, `This device was cloned on 6/24/2010 10:12:37 AM`.

5 Change the cloned device properties as required. For more information, see Changing the cloned Device Properties.

Changing the cloned Device Properties

After you have cloned a device, you need to change the device host name and address in the Device Properties - General dialog settings so that WhatsUp Gold can monitor the new device and all of the active monitors, passive monitors, actions, and attributes that are applied to the new device.

To change the cloned Device Properties:

1 From the group where the new cloned device resides, right-click the device, then click **Properties**. The Device Properties dialog appears.

2 Click **General**. The General dialog appears.

3 Enter the new device **Host name**, **Address**, and other information you want to change for this device, then click **OK**.

Polling overview

Polling is the active watching, or monitoring, of your network by WhatsUp Gold. This is done in a variety of ways, depending on the service monitors you have configured on your devices. The default polling method is done through Internet Control Message Protocol (ICMP). The default polling interval for WhatsUp Gold is 60 seconds.

A small amount of data is sent from the WhatsUp Gold computer across the network to the device it is watching. If the device is up, it echoes the data back to the WhatsUp Gold computer. A device is considered down by WhatsUp Gold when it does not send the data back.

Changing how you poll devices

After a device is added to the database, WhatsUp Gold begins monitoring that device using ICMP (Internet Control Message Protocol). WhatsUp Gold sends a message to the device, then waits for the echo reply. If no reply is received, WhatsUp Gold considers it an unresponsive device and changes the status color of the device.

By default, WhatsUp Gold uses the device IP address as the message target. If you prefer, you can use the Host name or the Windows name of the computer instead, and you can change how WhatsUp Gold polls the devices.

To change how you poll a device:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

3 Click **General**.

4 Select the protocol used to poll the device from the **Polling type** list.

5 Select **IP address** or **Host name** from the **Poll using** list.

6 If you selected Host name in the **Poll using** list, enter the device host name the **Host name** box.

7 Click **OK** to save changes.

It is useful to poll using the host name if you want to monitor a device that has a dynamic IP address instead of a static address. To monitor this type of device, choose **Host name** from the **Poll using** list. Doing so allows WhatsUp Gold to locate the host using DNS on the network even if the device IP address changes.

Using Maintenance mode

This feature lets you place devices in Maintenance mode. Any device placed in Maintenance mode will not be polled, actions will not be triggered, and logging activity is disabled, but it remains in the device list with an identifying icon. By default, the maintenance state is represented by an orange background color.

	Details View
idmr	Map View

To put a device into maintenance mode:

1. From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.
2. In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
3. Click **Polling**.
4. Select **Force this device into maintenance mode now**.
   - or -
   Change the scheduled maintenance setting for the device:
   - Click **Add** to schedule a new maintenance time for the device.
   - Select an existing entry, then click **Edit** to change a scheduled time.
   - Select an existing entry, then click **Remove** to delete a scheduled time from the list.
5. Click **OK** to save the change.

Changing the device polling frequency

The default polling interval is 60 seconds. You can change this setting on each device.

To change the polling frequency for a device:

1. From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.
2. In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
3. Click **Polling**. The Polling, Maintenance and Dependencies page appears.
4. Change the interval in the **Poll Interval** box.
5. Click **OK** to save changes.

Stopping and starting monitor polling

To stop and start polling on a per-monitor basis:

1. From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.
2. In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

3 Click **Active Monitors**. The Active Monitors page appears.

4 Double-click the Active Monitor with the polling setting you want to change. The Active Monitor Properties dialog appears.

5 Change the polling status of the monitor:
Select **Enable polling for this active monitor** to start polling.
- or -
Clear **Enable polling for this active monitor** to stop polling.

6 Click **OK** to save changes.

> **Note**: Some active monitors have additional settings and advanced options you can optionally change from the Active Monitor Properties dialog.

Dependencies overview

By default, WhatsUp Gold polls all of the devices and active monitors on your Device List, often creating unnecessary overhead by polling devices whose state could be assumed based on the status of other devices. The dependency feature reduces polling overhead in these cases by allowing you to create conditions under which a device will not be polled. These conditions determine if a dependent device is to be polled based on the state of another device which is the target of the dependency. The state of the target device is determined by the state of one or more of its active monitors. You can establish dependencies on either the up or down states of these active monitors, resulting in Up dependencies, or Down dependencies.

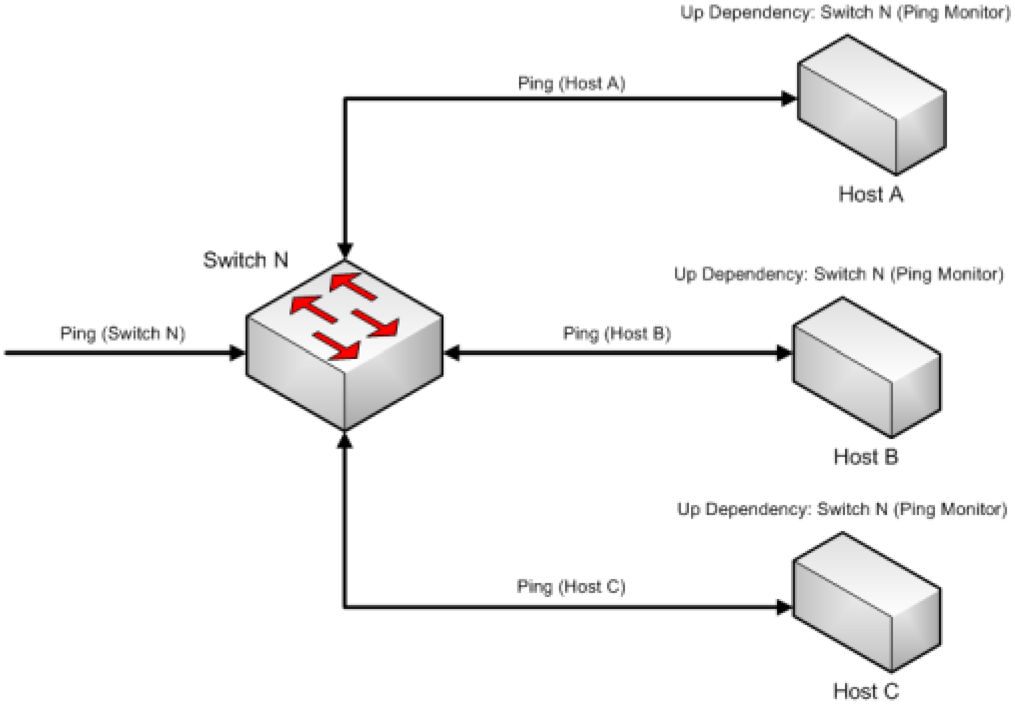
Up Dependencies

An up dependency establishes a condition so that a device is polled only if the selected active monitors on a second device are in the up state. The device can be thought of as being “behind” the device to which it has a dependency, so that it will only be polled if the device "in front" of it is up.

Example

In this example, an active monitor has been configured for each of the devices, and is denoted using **Ping (***device_name***)**. Without dependencies, WhatsUp Gold attempts to poll the Ping monitors on the hosts even if the switch has been powered down, or is otherwise unreachable. This situation results in network and system overhead that could be avoided by creating up dependencies on the hosts.

By adding an up dependency on each host so that the polling of the hosts is dependent on the Ping monitor on Switch N being up, denoted **Up Dependency: Switch N (Ping Monitor**), you create the condition where WhatsUp Gold discontinues polling the hosts when Switch N is powered down or otherwise unavailable to the **Ping(Switch N)** monitor. This reduces the overhead required to monitor the dependent host devices, while providing information about their accessibility based on the accessibility of Switch N.


Up Dependency: Switch N (Ping Monitor)
Ping (Host A)
Host A
Switch N
Up Dependency: Switch N (Ping Monitor)
Ping (Switch N)
Ping (Host B)
Host B
Up Dependency: Switch N (Ping Monitor)
Ping (Host C)
Host C

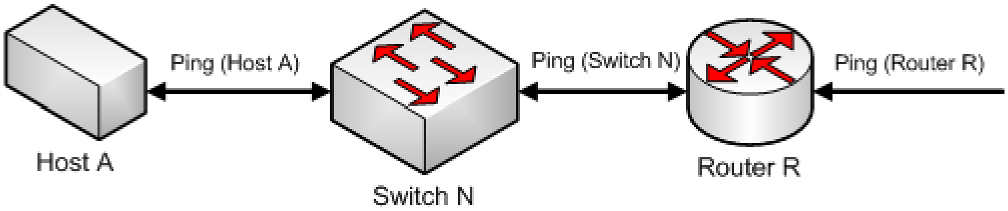
Down Dependencies

A down dependency establishes a rule so that a device is polled only if the selected active monitors on a second device are in the down state. The device can be thought of as something is "in front of" the device to which it has a dependency. The dependant devices in front will not be polled unless the device further down the line is down.

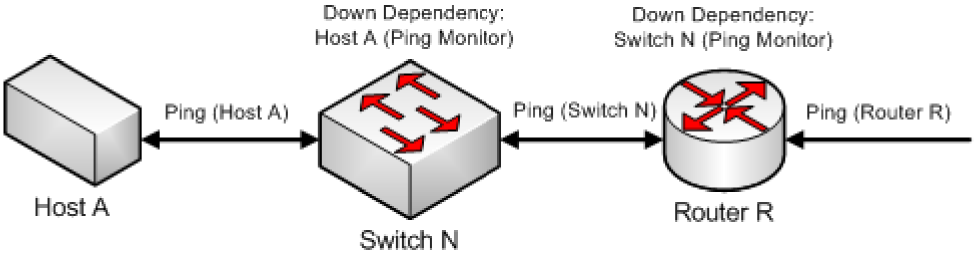
Example

In this example, a network segment has a group of devices, each with a dependency on another for its connectivity. Each of these devices has a Ping monitor used to determine the state of the device, denoted **Ping (***device***)**. If Host A can be pinged from another network segment, then it can be assumed that Router R, and Switch N are up and available, so to operate separate ping monitors on these devices creates unneeded overhead as long as Host A is up. However if Host A is powered down, or otherwise unreachable by the Ping monitor, we must rely on the Ping (Switch N) and Ping (Router R) monitors to ensure that these devices are up and accessible.

In this example, a network segment has a group of devices, each with a dependency on another for its connectivity. Each of these devices has a Ping monitor used to determine the



Adding a down dependency on Switch N to the Ping monitor on Host A, **Down Dependency: Host A (Ping Monitor)**, and a down dependency on Router R to the Ping monitor on Switch N, **Down Dependency: Switch N (Ping Monitor)**, creates a chain of dependencies that will monitor the network segment and reduce the active monitors that must operate on the segment when it is fully operational.



With these dependencies added, if **Ping (Host A)** should go into a down state, the down dependency on Switch N will cause WhatsUp Gold to begin polling Switch N. If the polling of Switch N is successful, it will continue to be polled until Host A is recovered. However, if Switch N is also unreachable and **Ping (Switch N)** goes into a down state, the down dependency on Router R will cause WhatsUp Gold to begin polling Router R. When **Ping (Switch N)** returns to an up state, Router R will no longer be polled. Likewise when **Ping (Host A)** returns to an up state, Switch N will no longer be polled.

Down dependencies and the "assumed up" state

A down dependency on a device can lead to an "assumed up" state, where a monitor on the dependent device indicates that it is up, regardless of its actual state.

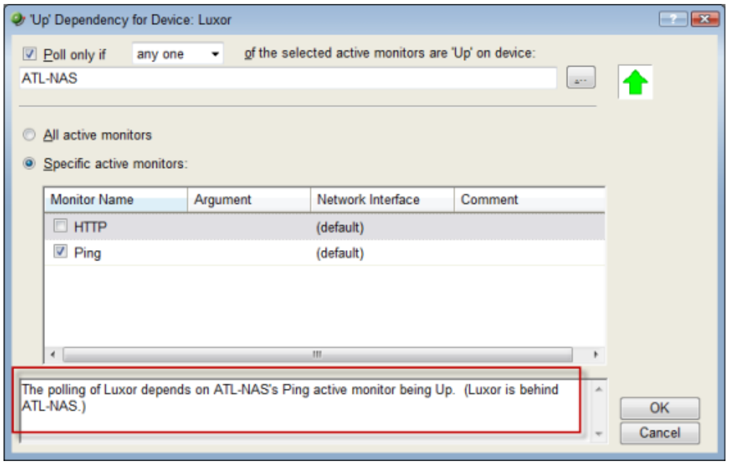
This condition occurs when the dependent device is in an inactive state, and is able to respond to an echo request from a ping of the device. Because of the down dependency, the dependent device is not being polled and is "assumed up", yet the actual state of the monitored service or process is unknown, and may have even failed.

An example of the dependent system would be a passive, or standby server, in support of a high-availability (HA) database cluster that has a down dependency on the active server. If the database management system (DBMS) on the standby server fails to start on a reboot, WhatsUp Gold will not show this failure until the active server fails and the standby server is polled.

Reading dependencies

There are several ways to "read" dependencies to ensure they are applied as you want them.

1 Review the description of the dependency in the Device Properties dialog.



'Up' Dependency for Device: Luxor

☑ Poll only if any one of the selected active monitors are 'Up' on device:

ATL-NAS

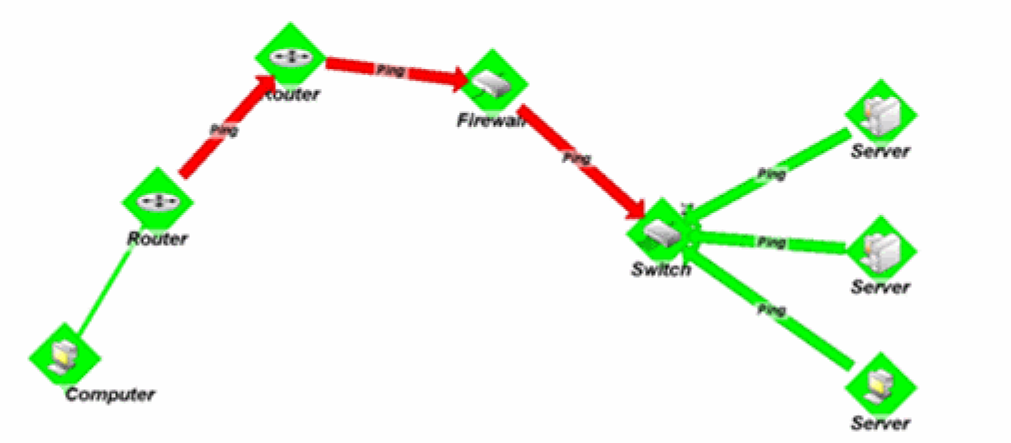
○ All active monitors

● Specific active monitors:

Monitor Name	Argument	Network Interface	Comment
□ HTTP		(default)	
☑ Ping		(default)	

The polling of Luxor depends on ATL-NAS's Ping active monitor being Up. (Luxor is behind ATL-NAS.)

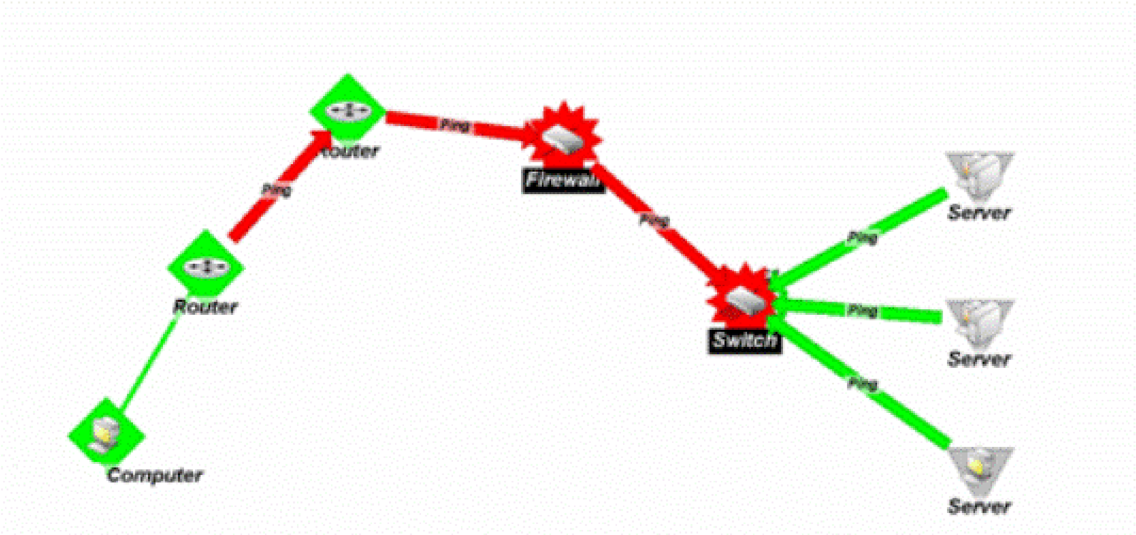
2 Read the dependency arrows in the Map View.



The map above displays several Up and Down dependencies. The green arrows indicate an Up dependency, and the red arrows indicate a Down dependency.

Using the "behind" and "in front" terminology you can follow the graphical arrow in the map above to read a dependency. For example, the server dependencies are read as, "only poll the servers if the switch is up." The servers are behind the switch, and will only be polled if the switch is also responding to polls. If the switch goes down, the server is assumed unavailable and is no longer be polled. Since the server is unavailable, the server's state then changes to Unknown.

For another example, the router dependency on the firewall is read as, "only poll the firewall if the switch is down." If a break in communication takes place between the router and the firewall, the switch changes to the Down state because it is Down dependent on the firewall. If the switch goes down, the state of the servers changes to Unknown, because they are Up dependent on the switch. Then, since the switch is down, the firewall is polled and changes to the Down state. After the firewall is considered down, the router is polled.



Down dependencies are useful in showing the break position in a chain of machines. If the chain is not broken at any point, the machines in the chain are not polled and are assumed up.

Setting Dependencies

There are two ways to set dependencies in WhatsUp Gold:

- Using Device Properties
- Using the Map View

To set dependencies in the Device Properties:

1 Go to the properties for a device:

   - On the console, from Device View, double-click a device.
   - On the web interface, click the **Devices** tab, then double-click a device. The Device Status Dashboard for that device appears. Click the **Properties** button. The Device Properties dialog appears.

2 Click **Polling**. The Polling, Maintenance, and Dependencies dialog appears.

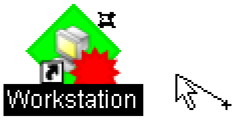
3 Click either the **Up Dependency** or the **Down Dependency** button to bring up the appropriate Device Dependencies dialog, and to configure the up or down dependency.

To set dependencies in the Map View:

1 Go to Map View:

§ In the console, click the **Map View** tab. Map View appears.

2 Right-click a device, select **Set Dependencies**, then select either **Set Up Dependency on** or **Set Down Dependency on**. The cursor changes to the Set Dependency arrow.



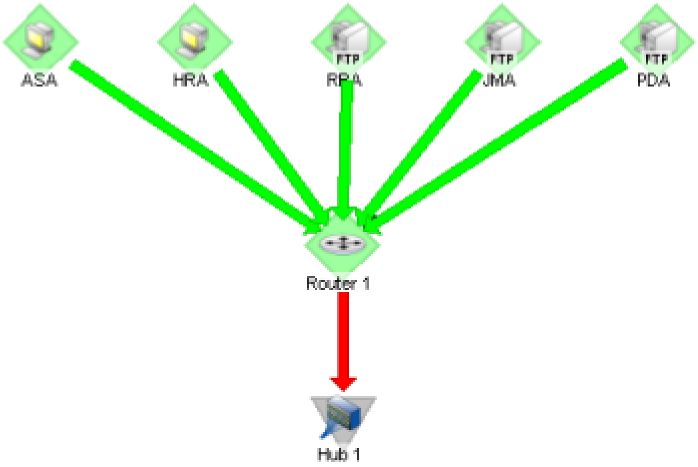
3 Click on any device in the current group to set the dependency.

Note: You cannot set a dependency across groups. However, you can make shortcuts to the devices you want to set a dependency on in a group, then set the dependency to the shortcut.

Tip: To view the dependency between the two devices in Map View, click **Display > Polling Dependency Arrows**.

Viewing Dependencies

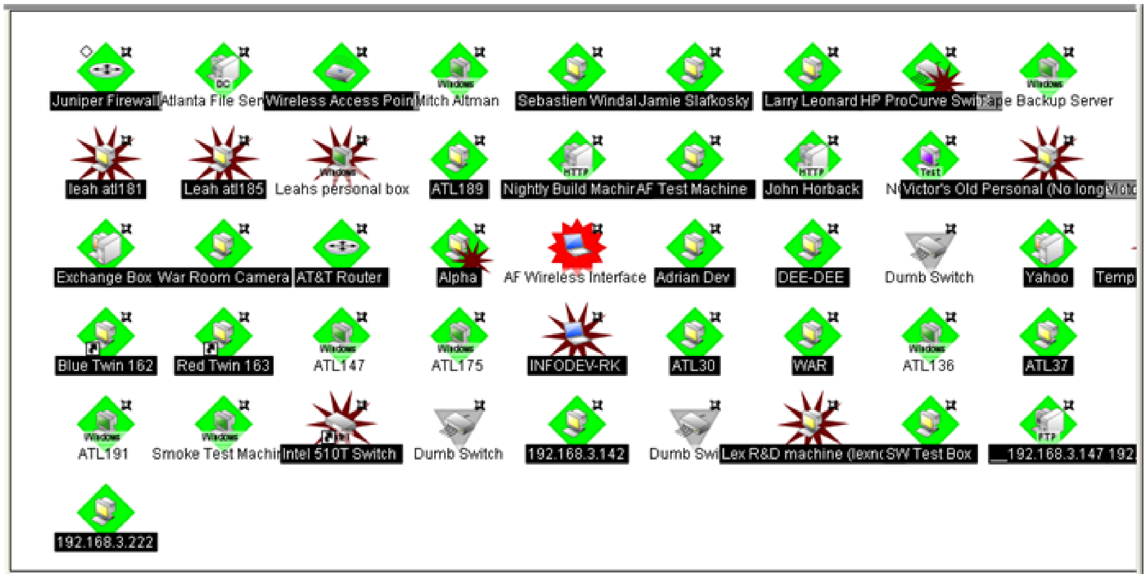
After you have set up your dependencies, you can view dependency lines in the Map view, as long as the devices appear in the same group. If the devices are not in the same group, you can refer to the Polling, Maintenance, and Dependencies dialog (**Device Properties > Polling**) to view the dependencies.



In the example above, the devices have an up dependency on the router, and the router has a down dependency on the hub. If the router's active monitors fail, the hub would be polled, and the devices behind the router would not be polled. When the router's active monitors are successful, the hub is not polled, but the devices behind the router are.

Using Acknowledgements

When a device state changes, regardless of any action that has been placed on the device, WhatsUp Gold uses the Acknowledgement feature to make you aware that a state change occurred. The name of the device name appears in bold in the Details View and in white on a black background in the Map View.



After the device is in Acknowledgement mode, it remains so until you actively acknowledge it.

Note: Acknowledging a device state change does not keep that device from firing actions. To stop a device from firing actions, you must put the device into maintenance mode.

Acknowledging a State Change

Once a device is in acknowledgement mode, it will remain until you actively acknowledge the status. You can use the State Change Acknowledgement monitor report to view all devices that have changed state but remain unacknowledged.

To acknowledge a state change:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 In either the Details View or the Map View, right-click the device you want to acknowledge. The right-click menu appears.

3 Select **Acknowledge**. The device state change is acknowledged and the device is removed from the State Change Acknowledgement monitor report.

Accessing a remote desktop to view and manage devices

WhatsUp Gold provides a right-click menu link to the Remote Desktop/Terminal Services client that allows you to connect to devices remotely. If the client is installed on the WhatsUp Gold computer, and the Remote Desktop/Terminal Services is installed and activated on the device you want to connect to, you are prompted for the user name and password for that device.

This application allows you to access and troubleshoot device and monitor issues that WhatsUp Gold identifies.

Note: Remote desktop access is browser dependent, some web browsers do not support this feature. For more information about the remote desktop feature, see the help for the remote desktop client.

To connect to a remote desktop:

1 From the WhatsUp Gold web interface, click the **Device**s tab, then click **Devices**.

2 From the Details or Map View, right-click a device, then click **Remote Desktop**. The Remote Desktop Connection dialog appears.

3 Log into the remote device to manage as needed.

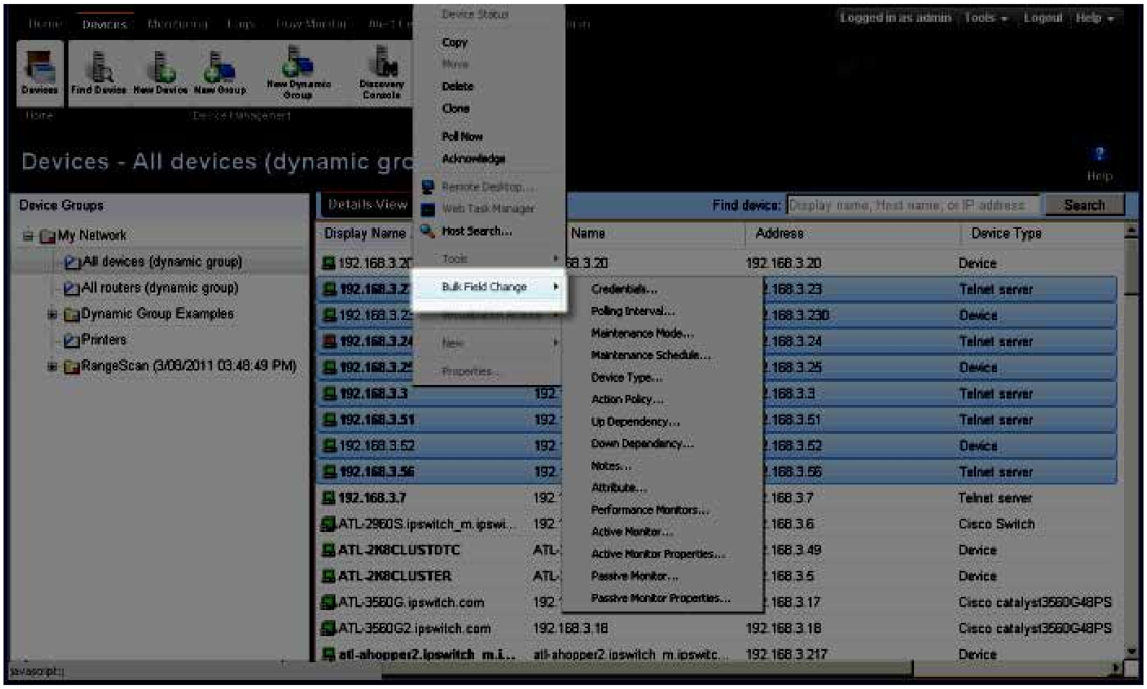
Configuring multiple devices with the Bulk Field Change feature

The Bulk Field Change feature gives you the ability to make changes to multiple devices and device groups. You must have administrative privileges to the devices or device groups that you want to make changes to.

To edit multiple devices:

1 Select the devices or device groups you want to change, right-click and click **Bulk Field Change**. The Bulk Field Change context menu appears.

Note: When you select a device group, every device in the group, and any subgroup of the group, will reflect the Bulk Field Change.



2 Select the box you want to change. The following items can be modified through Bulk Field Change.

- Credentials
- Polling Interval
- Maintenance Mode
- Maintenance Schedule (web interface only)
- Device Type
- Action Policy
- Up Dependency
- Down Dependency
- Notes
- Attribute
- Performance Monitors
- Active Monitor
- Active Monitor Properties
- Passive Monitor (web interface only)
- Passive Monitor Properties (web interface only)

3 Enter the configuration information you want set. Refer to the help for more information on configuration options.

4 Click **OK** to save changes.

Understanding Web Alarms

A Web Alarm is an action type that plays a sound over the web interface when a device state change occurs. All users logged in via the web interface will see these alarms. The type is configured in the Actions Library, and can be associated to any device or monitor like any other action.

Managing a Web Alarm action:

- You can edit the default Web Alarm action through the Action Library (**Admin > Actions**). Select the **Default Web Alarm**, then click **Edit.**

Managing a Web Alarm:

When a web alarm alert fires, a dialog appears in the web interface. This dialog allows you to dismiss or mute the alarms that have been fired. Click the **Dismiss** or **Dismiss All** buttons to stop the alarm that is currently sounding. Dismissing the web alarm does not stop the sound for future occurrences of the Web Alarm.

To disable Web Alarms:

- Click **Admin > Preferences**. The Admin Preferences dialog appears.
- Clear the **Enable web alarms** option.

✓ **Important**: For Web Alarms to work properly, your browser must support embedded sound files.

Note: If there are web alarms in the list with different sounds configured for each, the oldest web alarm's sound takes priority. To hear a new or different sound for a web alarm, dismiss the previous web alarm from the list.

Note: To associate a sound file with an Alarm, the sound file must be placed in the `\Program Files\Ipswitch\WhatsUp\HTML\Nm.UI\WebSounds` directory.

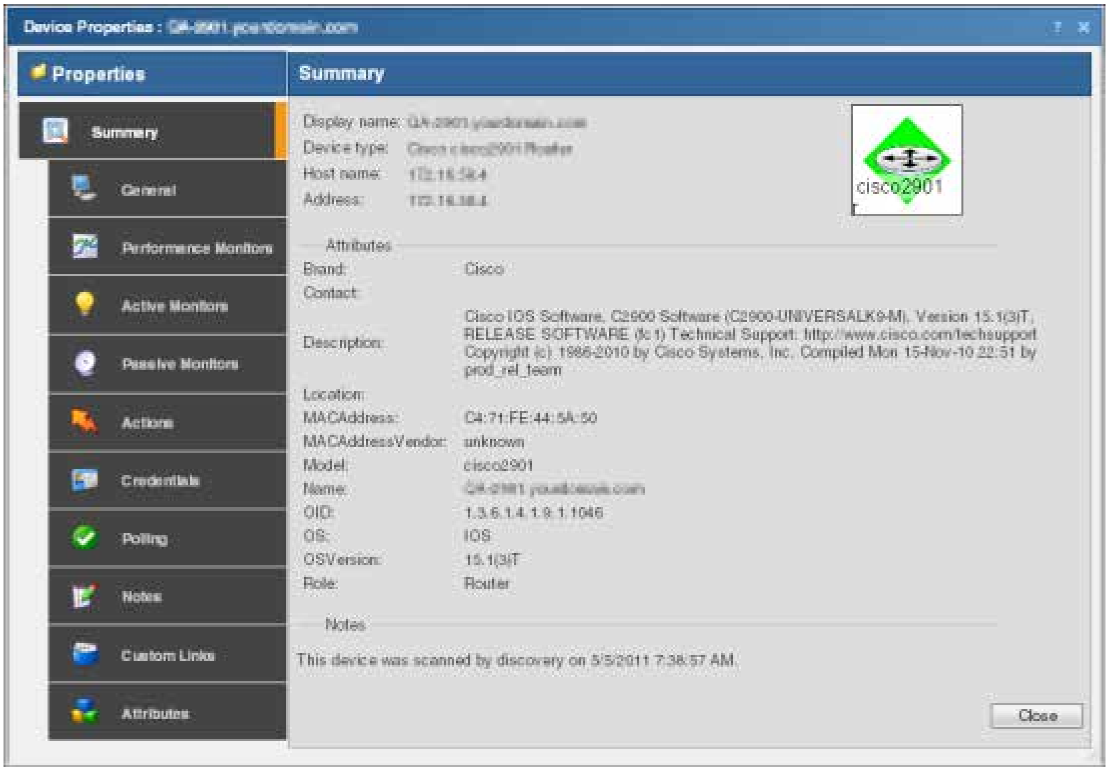
You can double-click an entry in this dialog to view the device Device Status report.

Using Device Properties

In This Chapter

Working with Device Properties

Use the Device Properties dialog to manage each device, credentials, applied monitors, actions, notes, and other details about the device.



Summary

Display name: QA-2901.yourdomain.com
Device type: Cisco cisco2901 Router
Host name: 172.16.58.4
Address: 172.16.58.4

Attributes

Brand:	Cisco
Contact:	
Description:	Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(3)T, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2010 by Cisco Systems, Inc. Compiled Mon 15-Nov-10 22:51 by prod_rel_team
Location:	
MACAddress:	C4:71:FE:44:5A:50
MACAddressVendor:	unknown
Model:	cisco2901
Name:	QA-2901.yourdomain.com
OID:	1.3.6.1.4.1.9.1.1046
OS:	IOS
OSVersion:	15.1(3)T
Role:	Router

Notes

This device was scanned by discovery on 5/5/2011 7:38:57 AM.

To access device properties for a device:

- Click the **Devices** tab, click either the **Details View** or **Map View**, then right-click a device and click **Properties**.

The Device Properties dialog includes the following features:

- **Summary**. View device information configured elsewhere in the Device Properties dialog.
- **General**. Configure basic device information.
- **Performance Monitors**. Configure, manage and apply performance monitors for the current device.
- **Active Monitors**. Configure, manage and apply active monitors to the current device. Applies monitors that log device responses to active inquiries (such as ping or HTTP responses).
- **Passive Monitors**. Configure, manage and apply passive monitors to the current device. Applies monitors that log received status information sent from devices (such as syslog, SNMP, and Windows event information).
- **Actions**. Select and configure action policies or alerts for this device. Configures device responses (such as sending email notifications) when particular conditions are met (such as no ping response for five minutes).

- **Credentials**. Manage SNMP, Windows, ADO, Telnet, SSH, and VMware credentials associated with the current device. Provides access to the Credentials Library and lets you link credentials with devices to allow reports requiring credentials to access those devices.
- **Polling**. Configure how applied monitors interact with the device to determine the status. Controls polling interval settings, including frequency, up and down dependencies, and adjusting poll intervals for maintenance schedules.
- **Virtualization**. Identify vCenter servers, VMware hosts, and configure a list of the virtual devices associated with a VMware server.
- **Notes**. Enter notes and free-form information pertaining to the selected device.
- **Custom Links**. Enter hyperlinks associated with the selected device.
- **Attributes**. Add device information for the selected device. This information is displayed in the Attributes section of the Summary section of Device Properties.
- **Tasks** (optional with WhatsConfigured). Use to schedule tasks, and modify and compare WhatsConfigured configuration archives assigned to this device.

Using Device Properties - Summary

The Device Properties Summary page is a display-only page which gathers information from device MIBs and other areas of the Device Properties dialog.

The following Summary items are configured in the General tab:

- **Display name**
- **Device name**
- **Host name**
- **Address**

The following items are gathered from MIBs on the device. If SNMP is not enabled on the device, then values for these items are not displayed.

- **Brand**
- **Contact**
- **Description**
- **Location**
- **MACAddress**
- **MACAddressVendor**
- **Model**
- **Name**
- **OID**
- **OS**
- **OSVersion**
- **Role**

Using Device Properties - General

The General section of the Device Properties dialog box provides, and lets you modify, basic information for the selected device.

- **Display name**. An identifying name for the current device. This name is populated during discovery, but can be changed by the user at any time. Changing the name will not change how the device is polled, only how it is displayed in WhatsUp Gold.
- **Polling type**. Select the type of polling you want WhatsUp Gold to use for this device.
- ICMP (TCP/UDP)
- IPX
- NetBIOS

> **Note**: If NetBIOS is selected, the Host Name box must contain a valid NetBIOS name. If IPX is selected, the Address box must contain a valid IPX address. If NetBIOS or IPX is selected, you cannot monitor TCP/IP services on this device.

- **Poll using**. Select if you want WhatsUp Gold to use the IP address or the Host name (DNS) of the device for polling.
- **Host name (DNS name)**. This should be the official network name of the device if the polling method is ICMP. The network name must be a name that can be resolved to an IP address. If the polling method is NetBIOS or IPX, this must be the NetBIOS or IPX name.
- **Address**. Enter an IP or IPX address.
- **Additional Network Interfaces**. Click to configure an additional Network Interface for the current device.
- **Device**. Select the appropriate device type from the pull-down menu. The icon displayed will represent the device in all views.

Device Properties - Performance Monitors

Use Performance Monitors dialog to configure and manage performance monitors for the selected device. For more information, see *Using Performance Monitors* (on page 260).

> **Note**: For some performance monitors, the SNMP credential on the device must be configured. For WMI performance monitors, the Windows credential is required.

- **Enable global performance monitors**. Select options in this list to enable monitors. The following monitors are populated by entries in the *Performance Monitor Library* (on page 261), but cannot be edited or changed from their default settings. These monitors are ready to be added to devices.
- **CPU Utilization**. Monitors the CPU utilization on the selected device.
- **Disk Utilization**. Monitors the available disk space for the selected device.
- **Interface Utilization**. Monitors all interfaces on the selected device.

- **Memory Utilization**. Monitors memory utilization on the selected device.
- **Ping Latency and Availability**. Monitors how often and quickly the device responds to a Ping check.

  If you select a specific performance monitor without configuring the monitor manually, the default collection type is automatically selected. The collection type refers to the item on the current device that is being monitored (This does not pertain to the custom WMI and SNMP monitors that may appear):

  - CPU - All
  - Disk - All
  - Interface - All, Default, or Specific
  - Memory - All
  - Ping - All

  For example, if you have multiple CPUs running on the device, WhatsUp Gold gathers statistics on all of them by default.
- **Configure**. Click to configure additional data stream options for the global performance monitor.

> **Note**: If an error occurs, a warning message appears directing you to the problem. If it is a timeout error, you are prompted to open the Advanced dialog to change the **Timeout** value. For any other error, you are returned to this dialog.

- **Library**. Click for options to create (**New**), **Edit**, **Copy**, or **Delete** performance monitor library items to use on all devices.
- **Enable individual performance monitors (for this device only)**. Use this section of the dialog to add customized APC UPS, Printer, Active Script, SNMP, or WMI performance monitors to only be used on this device. The monitors added here do not appear in the Performance Monitor Library, and cannot be used on other devices unless it is manually created for that device.
- Click **New** to configure a new monitor.
- Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.
- Select a performance monitor type, then click **Delete** to remove it from the list.

For information on the Active Script Performance Monitor, see *Adding and Editing an Active Script Monitor* (on page 155).

> **Note**: If you are attempting to monitor a Cisco device with either the CPU or Memory Performance Monitors, the Cisco device must support Cisco IOS 12.2(3.5) or later.

Using Device Properties - Active Monitors

Use the Active Monitors dialog to display and manage Active Monitors for this device. For more information, see *Using Active Monitors* (on page 153).

To add an active monitor to this list:

- Click **Add** to configure a new active monitor. Use the wizard to select active monitor settings.
- Select an active monitor, then click **Edit** to change the configuration.
  - or -
  Double-click an active monitor to edit the configuration.
- Select an active monitor, then click **Disable** to disable the monitor on the device.
- Select an active monitor, then click **Enable** to enable the monitor on the device.
- Select an active monitor, then click **Remove** to remove the monitor from the device.
- Click **Configure** to select critical monitors for this device and set their polling order.

Using Device Properties - Passive Monitors

Some measurable network conditions occur at intervals instead of providing an up or down status. For example, an application may log a message to the system Event log (such as an antivirus application alerting when a virus is found). Because these types of messages or events can occur at any time, a Passive Monitor Listener listens for them, and notifies WhatsUp Gold when they occur. For more information, see *Using Passive Monitors* (on page 247).

This dialog displays all Passive Monitors configured for this device.

- Click **Add** to configure a new Passive Monitor.
- Select a Passive Monitor, then click **Edit** to change the configuration

- or -

Double-click a Passive Monitor to edit the configuration.

- Select a Passive Monitor, then click **Remove** to remove the monitor from the device.

Using Device Properties - Actions

You can select an Action Policy to use on this device or configure alerts specifically for this device. For more information, see *About actions* (on page 304).

Select a policy from the **Apply this Action policy** list. You can also create a new, or edit an existing action policy by clicking browse (...) next to the list.

Configured alerts appear in the **Apply individual actions** list, displaying the action type that is to be fired and the state change that will trigger the action. You may have multiple actions on a single device.

This dialog displays all Actions configured for this device.

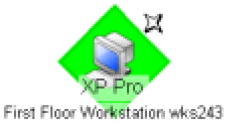
- Click **Add** to configure a new Action.
- Select an Action, then click **Edit** to change the configuration
  - or -
  Double-click an Action to edit the configuration.

- Select an Action, then click **Remove** to remove the action from the device. Removing the action from the list also deletes all records for this action (on this device) from the Action Log.

Using Device Properties - Credentials

The Credentials dialog displays **SNMP, Windows, ADO, Telnet, SSH, and VMware credentials** information for the current device.

In the Device Dashboard Map View, devices that are SNMP-manageable devices appear on the map view with an icon with a white star in the top right corner.



Credentials

- **SNMP v1/v2/v3**. Select the SNMP credentials to connect to this device. If the Identify devices via SNMP option was selected during discovery (or if an SNMP discovery was performed) the correct SNMP credential was used during the discovery process, and if the device is an SNMP manageable device, then the correct credential is selected automatically. If any of these conditions are not met, None is selected.
- **Windows**. Select the Windows credential to connect to this device. Click browse (**...**) to browse the Credentials Library.
- **ADO**. Select the ADO credentials for database connection string information to be used when a database connection is required for WhatsUp Gold database monitors.
- **Telnet**. If you use WhatsConfigured, Telnet credentials may be used to connect and run command-line interface (CLI) commands with WhatsConfigured tasks.
- **SSH**. Select SSH credentials to connect with remote devices that WhatsUp Gold monitors with SSH monitors. Also, if you use WhatsConfigured, SSH credentials may be used to connect and run command-line interface (CLI) commands with WhatsConfigured tasks. WhatsConfigured uses SSH as default credentials, then will attempt to use Telnet credentials when SSH credentials are not available.
- **VMware**. Select the VMware credentials to be used when connecting to a VMware host or vCenter server.
- **Edit**. Click to open the Select Credentials dialog, then select the credential from the list or click browse (**...**) to browse the Credentials Library.
- **Device Object ID (OID)**. Enter the SNMP object identifier for the device. This identifier is used to access a device and read SNMP data available for the device.

For more information, see *Using credentials* (on page 68).

Using Device Properties - Polling

About polling

Polling is the term used for monitoring discovered devices in WhatsUp Gold. Polling can occur in several ways, depending on the monitors configured for network devices. The default polling method uses Internet Control Message Protocol (ICMP). The default polling interval for WhatsUp Gold is 60 seconds.

A small amount of data is sent from the WhatsUp Gold computer across the network to the device it is watching. If the device is up, it echoes the data back to the WhatsUp Gold computer. A device is considered down by WhatsUp Gold when it does not send the data back.

The Polling dialog

The Polling dialog lets you configure polling options and/or schedule maintenance times for the selected device.

- **Poll interval**. This number determines how often WhatsUp Gold polls the selected device. Enter the number of seconds you want to pass between polls.

> **Note**: Polling dependencies & blackouts only apply to the collection of device active monitors.

- **Up dependency**. Click to configure additional options, based on when another device is operational, that determine when the selected device is polled.
- **Down dependency**. Click to configure additional options, based on when the selected device is not operational, that determine when other devices are polled.

Maintenance

Use this section of the dialog to manually set the device Maintenance state, or schedule the maintenance state for a certain time period. Any device placed in Maintenance mode will not be polled, actions will not be triggered, and logging activity is disabled, but it remains in the device list with an identifying icon. By default, the maintenance state is represented by an orange background color.

- **Force this device into maintenance mode now**. Select this option to put the selected device in maintenance mode. Clear the option to resume polling the device.
- **Recurring maintenance times**. This box displays all scheduled maintenance periods for the device.
- Click **Add** to schedule a new maintenance time for the device.
- Select an entry, then click **Edit** to change a scheduled time.
  - or -
  Double-click a Schedule to edit its configuration.
- Select an entry, then click **Remove** to delete a scheduled time.

For more information, see *Polling overview* (on page 104) and *Dependencies overview* (on page 106).

Using Device Properties - Virtualization

The Virtualization dialog allows for the identification of vCenter servers, VMware hosts, and provides a list of the virtual devices associated with the VMware server. You can use this dialog to identify the virtualization component, and associate virtual devices with the component. Also, if the device is a vCenter server you can control event collection and select the event types you want to receive from the server.

Role selection

During discovery, the most likely role for the virtual device is determined and the result is displayed in the role selection area of the Virtualization tab. You can manually define the role of the VMware server by choosing one of the following options:

- **This device is not a VMware server**. Select this option if the device being configured is not a VMware host or vCenter server.
- **This device is a VMware host**. Select this option if the device being configured is a VMware host.
- **This device is a VMware vCenter**. Select this option if the device being configured is a vCenter server.

Event collection configuration

If the virtual device you are configuring is a vCenter server, a Configure event collection button appears in the dialog which provides the the option to configure event collection.

> **Note**: To collect events, the WhatsVirtual event listener must be configured to listen for events from the vCenter. From the WhatsUp Gold console click **Configure > Program Options > General** dialog to configure WhatsVirtual to listen for events.

Click **Configure event collection** to open the **Configure VMware event listener** dialog and select the event types you want to collect for the vCenter server.

> **Note**: The current status of the Virtualization event listener is displayed beside the **Configure event collection** button.

Virtual devices managed by this VMware server

The virtual devices managed by VMware server list provides the following information about each virtual device.

- **Device name**. The name of the device as it appears in the **Display name** box of the General dialog of the Device Properties menu.
- **Device IP address**. The IP address of the virtual machine.
- **Virtual machine VMware name**. The name of the virtual machine within the VMware system.

Click **Add** to manually add a virtual machine to the list of virtual devices hosted on the VMware server. The Associate WUG device to a virtual machine dialog appears.

Select a virtual device from the list and click **Remove** to remove the device from the list of virtual devices managed by the VMware server.

Click **OK** to accept the virtualization settings, otherwise click **Cancel** to discard any changes you have made.

Using Device Properties - Notes

The Notes dialog provides an option to enter free-form messages to the device database.

The dialog displays the following information:

§ **Notes**. The first line of the Notes box displays the time and date when WhatsUp Gold added the device to the database.

Use the **Notes** box to include information about the selected device. For example, you can record historical information about a device, physical location information, or notes relating to the actions configured for the device.

Using Device Properties - Custom Links

In the WhatsUp Gold web interface, you can use this dialog to create a custom link for a device.

To view custom links created for a device, you need to add the Device Custom Links dashboard report to its Device Status dashboard view. For more information, see Adding dashboard reports to a dashboard view.

§ Click **Add** to add a new custom link.

§ Select a custom link in the list, then click **Edit** to change the settings.

- or -

Double-click a custom link to edit its configuration.

§ Select a custom link in the list, then click **Remove** to remove it from the list.

Using Device Properties - Attributes

The Attributes dialog lists information about the associated device, such as contact person, location, serial number, etc. The first three attributes in the list (Contact, Description, and Location) are added by WhatsUp Gold when the device is added to the database, either by the Device Discovery wizard, or through another means.

To add attributes to a device:

1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- or -
From any page where a device is selected using the device picker, click **Properties** in the title bar.

2 Click **Attributes**. The Attributes dialog appears.

3 Use the following options:

§ Click **Add** to add a new device attribute. The Add Attribute dialog appears.

> **Note**: When you add or edit an attribute, ensure **Attribute name** does not contain a space. For example, use Phone_Number as an attribute name, instead of Phone Number. WhatsUp Gold returns an 'No Such Attribute' error when an attribute variable such as `%Device.attribute.[attribute_name]` is used in a message and the attribute name contains a space.

- Select a device attribute in the list, then click **Edit** to change the settings.
- Select a device attribute in the list, then click **Remove** to remove it from the list.

4 Enter information in the **Attribute name** and **Attribute value** boxes.

5 Click **OK** to save changes.

Using the DeviceIdentifier attribute

When a Beeper Action fires, it looks for and returns a device attribute called DeviceIdentifier. You can add this attribute to a device via its Properties (**Device Properties > Attributes**).

If the Beeper Action does not find the DeviceIdentifier in a device's attributes, WhatsUp Gold uses the last two octets of the IP address to identify the device. For example, a numeric message is sent to a beeper when a device returns to the up state after being down:

0-149-238

The first digit is the number configured in the Up, Down, or passive monitor code, the second two sets of numbers identify the device using the last two octets of the device's IP address.

To configure a DeviceIdentifier attribute for a device:

1 Open the device's Properties:

- Right-click a device, then click **Properties**. The Device Properties dialog appears.
- Click **Attributes**. The Attributes dialog appears.

2 Click **Add**. The Add Attribute dialog appears.

3 In **Attribute name**, enter DeviceIdentifier.

4 In **Attribute value**, enter the desired numeric value.

> **Note**: The DeviceIdentifier attribute value should contain only numeric characters or the asterisk (*); alphabet characters, spaces, and other special characters are not recognized by the Beeper Action.

5 Click **OK** to save changes.

Using Device Property - Menus

In the WhatsUp Gold console, you can use the Menu dialog to create a custom context menu for a device. Context menus are custom menu items that appear when you right-click a device; they serve as *shortcuts* to launch applications.

The menu item can launch programs based on the command line you enter. You can also append command line arguments, including *WhatsUp Gold percent variable arguments* (on page 342) to include device IP address, device host name, and other types of percent variable arguments. When you select the new menu item, the associated command is launched with the arguments that were included in the device's custom menu configuration.

- **Customize the menu on this device (don't use device type menu)**. Select this option to create and/or modify a context menu for this device. This will override any separate context menu that has already been created for the device type of the device.
- **Menu list**. This box displays the commands that are currently configured for the device. After an item has been configured, it appears on the context (right-click) menu. When you click the menu item, the menu item is executed.
- Click **Add** to add a new menu item.
- Select a Menu Name, then click **Edit** to change the settings.
  - or -
- Double-click a Menu Name to edit its configuration.
- Select an Menu Name, then click **Remove** to delete it from the list.

Important: Menu items can only be configured on the WhatsUp Gold console.

Using WhatsConfigured Device Properties - Tasks

The Tasks section of the Device Properties dialog displays, and lets you modify and run WhatsConfigured scheduled tasks, and modify and compare WhatsConfigured configuration archives assigned to this device.

Note: To add tasks to a device and/or view configuration information, WhatsConfigured must be activated. To update your license to purchase WhatsConfigured plug-in, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Tasks attached to this device

Each scheduled task is listed by **Name**, **Description**, and the time it was **Last Run**.

- Click **Add** to add a scheduled task to this device.
- Select a task, then click **Remove** to delete a scheduled task from this device.
- Select a task, then click **Run Now** to perform the selected task immediately. The task will run only for the currently selected device. To run a task for all devices to which it is assigned, use the **Run Now** option in the WhatsConfigured Task Library.

Configuration archives saved for this device

Each archived configuration is listed by its **Time Created** and **Activity**.

- Select a configuration, then click **Restore** to restore the device to the selected configuration.

- Select a configuration, then click **Delete** to remove the configuration from the device's list of archives.
- Select a configuration, then click **View** to see the configuration details.
- Select two configurations, then click **Compare** to view the two configuration files side-by-side.

Using Device Properties - Wireless

Use the Wireless dialog to enable or disable monitoring of the selected device with the WhatsUp Gold Wireless feature.

To enable monitoring by WhatsUp Gold Wireless, click to select the **Monitor this device with Wireless** check box, then click **Close**.

Using Network Tools

WhatsUp Gold includes several network troubleshooting tools. These tools allow you to take a closer look at the status of your network devices.

Note: Network Tools are only available on the WhatsUp Gold web interface.

The following tools help you check the connectivity of networked devices:

- *Ping Tool* (on page 129)
- *Traceroute Tool* (on page 130)
- *Lookup Tool* (on page 131)
- *Telnet Tool* (on page 132)

The following tools help you identify information about MIB objects that network devices support:

- *SNMP MIB Walker Tool* (on page 132)
- *SNMP MIB File Explorer Tool* (on page 135)

The following tools help you identify problems with network devices so you can take corrective action to resolve issues:

- *MAC Address Tool* (on page 136)
- Diagnostic Tool
- *Web Performance Monitor* (on page 138)
- *Web Task Manager* (on page 140)

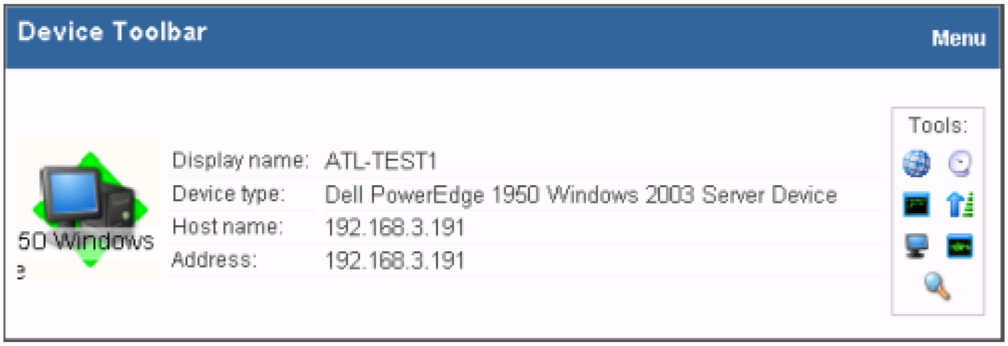
Note: The Web Performance Monitor and Web Task Manager tools are not available in WhatsUp Gold Standard Edition.

Accessing Network Tools

There are multiple ways to access the network tools.

- **Web interface Tools menu**
- From the web interface, select **Tools**. The Tools menu appears.
- **Details View and Map View**
- From either the Details View or Map View, right-click on a device, then select **Tools**.
- **Device Toolbar Dashboard Report**

1. From either the Details View or Map View, double-click on a device. The Device Status dashboard view appears.
2. Locate the *Device Toolbar* dashboard report for the selected device. On the right side of report, small icons are linked to some of the network tools.



Device Toolbar

Display name: ATL-TEST1
Device type: Dell PowerEdge 1950 Windows 2003 Server Device
Host name: 192.168.3.191
Address: 192.168.3.191

3. Click an icon to launch the network tool in the context of the selected device.

Using the Ping tool

The Ping tool sends out an ICMP (Internet Control Message Protocol) echo request to the networked device identified in **Address/Hostname**.

Tool results

The results of this request appears after the request has been made.

- **Destination**. The address specified in Address/Hostname.
- **Packets**. The number of data packets sent, received, and lost during the device ping.
- **RTT**. Round trip time in milliseconds; the amount of time it takes for the ping request to be returned from the remote device.
- **Status**. Success or failure. If failure, a reason is stated for the failure. For example, "Failure: Request timed out."

To use the Ping Tool:

1 Enter or select the appropriate information:

- **Address/Hostname**. The target of the Ping echo request. Enter the host name or IP address of the device you want to check.

> **Note**: The Ping tool supports IPv6 addresses.

- **Timeout**. Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The Ping fails if this time limit is exceeded.
- **Count**. Enter the number of data packets sent by the Ping tool.
- **Packet size**. Enter the size (in bytes) of the packets you want the Ping tool to send. 32 bytes is the default.

2 Click **Ping** to run the tool.

Using the Traceroute tool

This tool sends out echo requests to a specific device, then traces the path it takes to get to that IP address or host name. This tool is often used to determine where, on the network, a data transmission interruption occurs.

Tool results

The results of this request appear in the bottom of the page after the tool has run:

- **Result**. Success or Failure. This is the general result of each hop in the Trace Route process.
- **Ping 1/2/3**. The tool sends out three ping requests to each hop in the route to the device. These columns show the round trip time for each of the requests.
- **Address**. The IP address of each device encountered on the path.
- **Host name**. The host name of each device encountered on the path.

To use the Traceroute Tool:

1 Enter or select the appropriate information:

- **Address/Host name**. Enter the host name or IP address of the device you want to trace the route to.

> **Note**: The Trace Route tool supports IPv6 addresses.

- **Timeout**. Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The Trace Route fails if this time limit is exceeded.
- **Max hops**. Enter the maximum number of hops you want to limit the route to. It is generally felt that 32 hops should be enough to find any device on the internet.

2 Click **Traceroute** to run the test.

Using the Lookup tool

This is a debugging tool that lets you query your Internet domain name system (DNS) server for information about a domain and its registered hosts. Lookup can show you what happens when an application on your network uses your DNS server to find the address of a remote host.

To use the Lookup Tool:

1 Enter or select the appropriate information:

- **Address/Host name**. Enter the host name or IP address of the device you want to trace the route to.
- **Lookup Type**. Select the lookup type from the drop-down list.

> **Note**: The available list options vary depending on the DNS Server option that is selected (Stack, Default, or Custom).

  - **A**. Look up the host's Internet address from the hostname.
  - **AAAA**. Look up for the host IPv6 address from a hostname.
  - **All**. Display all available information about the host.
  - **CNAME**. Display alias names for the host.
  - **HINFO**. Display the CPU type and operating system type of the host.
  - **MX**. Display the hostname of the mail exchanger for the domain.
  - **NS**. Display the hostnames of name servers for the named zone.
  - **PTR**. Look up the hostname from the Internet address.
  - **SOA**. Display the domain's Start of Authority information, which indicates the primary name server for the domain and additional administrative information.
  - **SRV**. Look up any SRV record configured on this DNS server. SRV records specify the location of services on the network.
  - **TXT**. Look up any arbitrary text information the DNS server may have for this domain name or host.
  - **ZONE**. Display the zone listing for the domain. The zone listing describes the domains for which the name server is the primary name server) and lists all registered hosts in the domain.
- **Timeout**. Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The Trace Route fails if this time limit is exceeded.
- **DNS Server**. Select the method of the look up:
  - **Stack**. Use the OS TCP/IP stack look up routines.
  - **Default**. Use the default DNS server configured on the computer WhatsUp Gold is running on.
- **Custom**. Query a custom DNS server. You must then enter the hostname or IP address of the domain name server you want to use.

2 Click **Lookup** to run the tool.

Using the Telnet tool

Telnet is a simple service monitor that checks for a Telnet server on port 23. If no telnet service responds on this port, then the service is considered down.

To begin the service check, click the **Telnet** button. Refer to the Telnet application Help for more information.

Important: The Telnet protocol handler is disabled by default in Microsoft Internet Explorer 7. To re-enable it, see *Re-enabling the Telnet protocol handler* (on page 567).

Using the SNMP MIB Walker

This network tool lets you discover, or explore in detail, the SNMP objects that a device supports and that can be monitored with WhatsUp Gold. The SNMP MIB Walker actively polls for objects. It does not require MIB files for the polled objects to be loaded.

An SNMP walk is a succession of SNMP getnext reads starting with the configured Object ID (the root of the subtree walked) until there are no next objects in the MIB subtree or until the specified number of lines in the MIB have been walked. As results return from the MIB Walker, you can click an object (node) for more detailed information about the SNMP object and to walk further down the list of objects. You can also hover the mouse cursor over a node to display SNMP object details.

To use the SNMP MIB Walker:

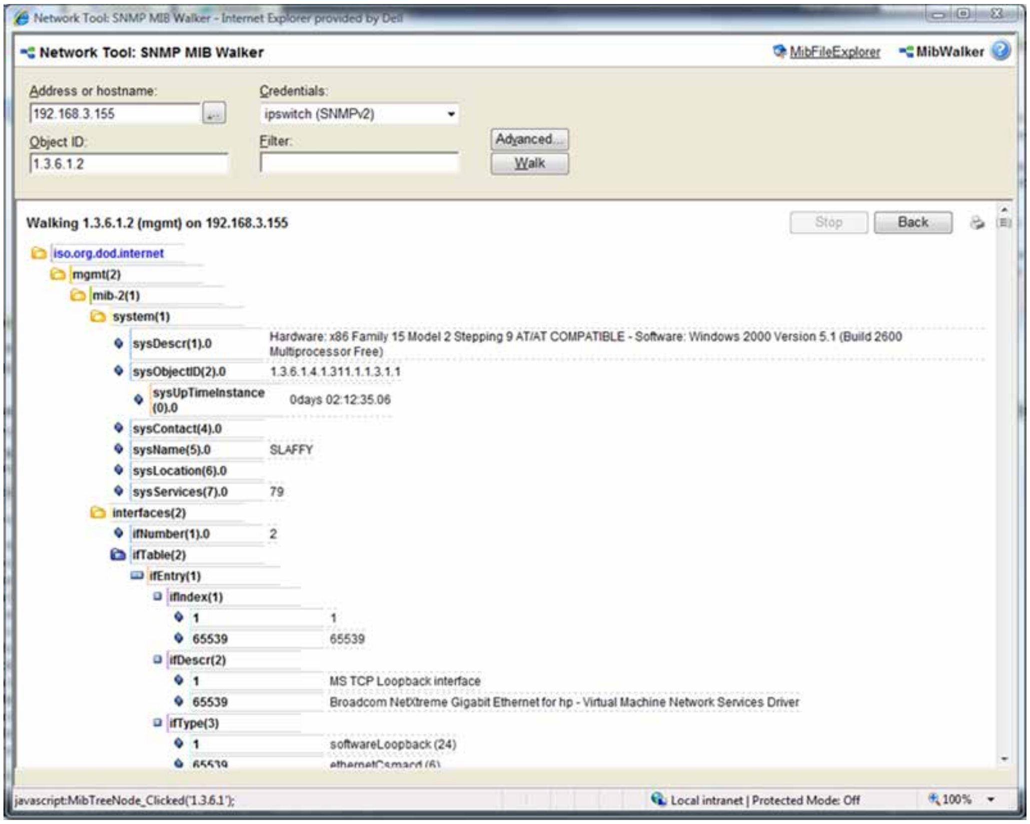
1 Enter or select the appropriate information:

- **Address or hostname**. Enter an IP address hostname for the device.
- **Credentials**. Select the appropriate credentials for the device from the list. For more information, see *Using Credentials* (on page 68).
- **Object ID**. Enter the numeric or label ID for the object for which you want information. A default OID is displayed in the box.
- **Filter**. (Optional) Enter a filter to narrow down the search by returning only OIDs whose values match the filter criteria.

Tip: This is a regular expression, non-case-sensitive filter. For more information, see *Regular Expression Syntax* (on page 175).

- Click the **Advanced** button to change the value for the search timeout and retries, output types (tree, list-numeric OIDs, list-labels), and the maximum number of lines displayed.

2 After you have entered all of the information, click **Walk** to perform the search. The SNMP MIB Walker returns a list of SNMP objects that are available on the selected device.


Network Tool: SNMP MIB Walker - Internet Explorer provided by Dell
Network Tool: SNMP MIB Walker
MibFileExplorer
MibWalker
Advanced...
Walk
Stop
Back
Local intranet | Protected Mode: Off
100%

Address or hostname: 192.168.3.155

Credentials: ipswitch (SNMPv2)

Object ID: 1.3.6.1.2

Filter:

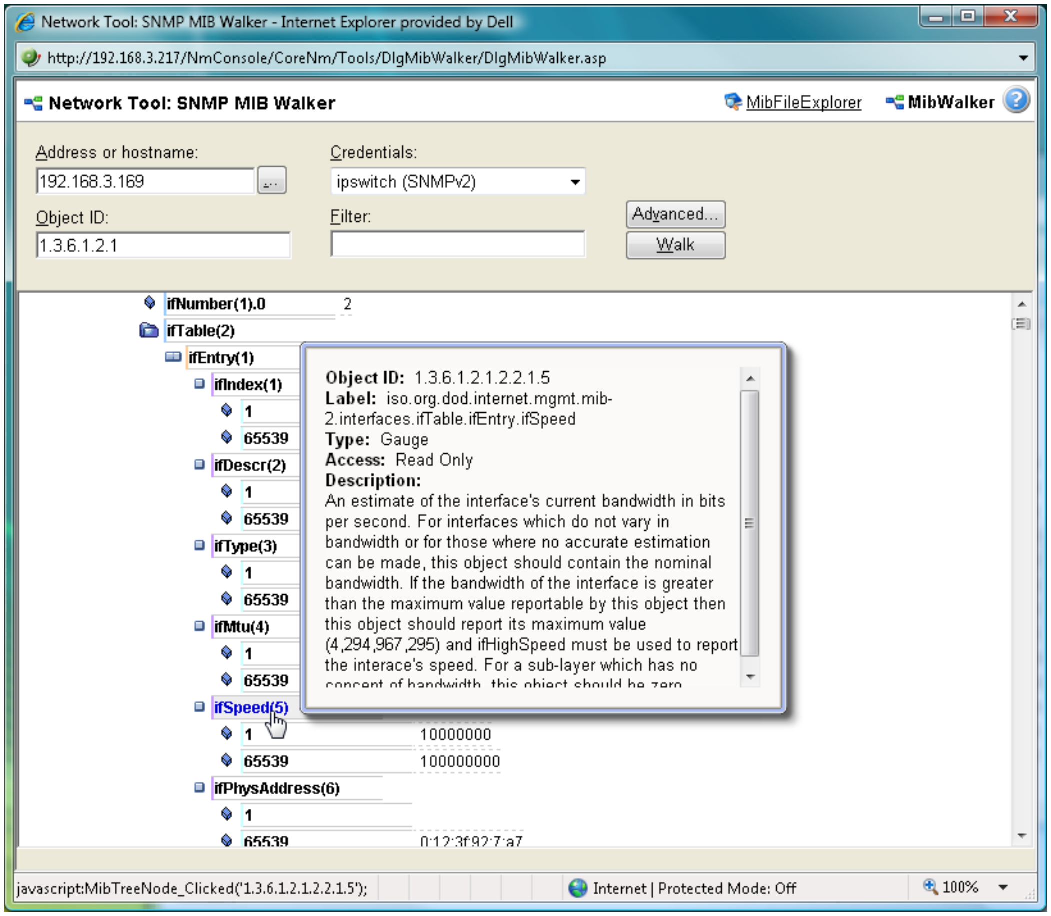
```
Walking 1.3.6.1.2 (mgmt) on 192.168.3.155

iso.org.dod.internet
  mgmt(2)
    mib-2(1)
      system(1)
        sysDescr(1).0         Hardware: x86 Family 15 Model 2 Stepping 9 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600
                              Multiprocessor Free)
        sysObjectID(2).0      1.3.6.1.4.1.311.1.1.3.1.1
          sysUpTimeInstance
          (0).0                 0days 02:12:35.06
        sysContact(4).0
        sysName(5).0          SLAFFY
        sysLocation(6).0
        sysServices(7).0      79
      interfaces(2)
        ifNumber(1).0         2
        ifTable(2)
          ifEntry(1)
            ifIndex(1)
              1                 1
              65539             65539
            ifDescr(2)
              1                 MS TCP Loopback interface
              65539             Broadcom NetXtreme Gigabit Ethernet for hp - Virtual Machine Network Services Driver
            ifType(3)
              1                 softwareLoopback (24)
              65539             ethernetCsmacd (6)
```

javascript:MibTreeNode_Clicked('1.3.6.1');

To terminate the walk, click **Stop**. If you are performing multiple walks, click **Back** to view the previous walk.

After the SNMP Walker returns a list of the supported SNMP objects, you can use this information to create custom performance monitors and active script performance monitors for devices. For more information, see *Creating custom performance monitors* (on page 286).

To view detailed information about a specific MIB object, mouse over the object for which you need more information. The information displays in a popup bubble.


Network Tool: SNMP MIB Walker - Internet Explorer provided by Dell
http://192.168.3.217/NmConsole/CoreNm/Tools/DlgMibWalker/DlgMibWalker.asp
Network Tool: SNMP MIB Walker
MibFileExplorer
MibWalker
Advanced...
Walk
javascript:MibTreeNode_Clicked('1.3.6.1.2.1.2.2.1.5');
Internet | Protected Mode: Off
100%

Address or hostname: 192.168.3.169

Credentials: ipswitch (SNMPv2)

Object ID: 1.3.6.1.2.1

Filter:

```
ifNumber(1).0        2
ifTable(2)
  ifEntry(1)
    ifIndex(1)
      1
      65539
    ifDescr(2)
      1
      65539
    ifType(3)
      1
      65539
    ifMtu(4)
      1
      65539
    ifSpeed(5)
      1              10000000
      65539          100000000
    ifPhysAddress(6)
      1
      65539          0:12:3f:92:7:a7
```

Object ID: 1.3.6.1.2.1.2.2.1.5
Label: iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifSpeed
Type: Gauge
Access: Read Only
Description:
An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interace's speed. For a sub-layer which has no concept of bandwidth, this object should be zero

About MIB Output Types

You can change the format for the way MIB objects are displayed in the Advanced Parameters dialog. Whether the OID information is output as numeric OIDs or descriptive labels, each node may have additional sub-nodes that can be drilled down (walked) for more information. Each time you click a node, if there are child nodes, the node you clicked becomes the root node for the drill-down. The child nodes are expanded and attributes are displayed. MIB objects can be listed in one of three format options:

- **Tree**. Lists the MIB object in a tree structure format. This format is most useful in showing the OID hierarchy.
- **List - Numeric OIDs**. Lists the objects in a tabular format showing OIDs in a row numeric format. This format is especially helpful if you do not have the MIB file for the device objects. It provides the raw OID information that you can use in Custom Performance Monitors and Active Script Peformance Monitors. Also, you can click the individual OID digits to display more or less MIB object information. As you click OID digits, the digits further to the left expand the sub-node information of the respective digits. As you click OID digits further to the right, the sub-node information expands for the respective digit and therefore more granular sub-node information.
- **List - Labels**. Lists the objects in a tabular format with user friendly labels. If the MIB for the object is not loaded, labels will default to numeric OIDs. Click an OID label name to expand the sub-nodes and view more information.

Note: You can switch to the WhatsUp Gold MIB Explorer by clicking on the MIB Explorer link on the upper-right side of this dialog.

Using the SNMP MIB Explorer

This network tool lets you search for, or explore through, SNMP objects defined in MIB files. The MIB File Explorer has three search/explore options.

As results return from the MIB File Explorer you can click an object (node) for more detailed information about the SNMP object. You can also hover the mouse cursor over a node to display SNMP object details.

To search by object ID:

Enter an object label or object ID in the **Object ID** box, then click **Detail**.

To search by MIB module:

Select a module from the **MIB Module** list, then click **Display**.

To search objects by type or description:

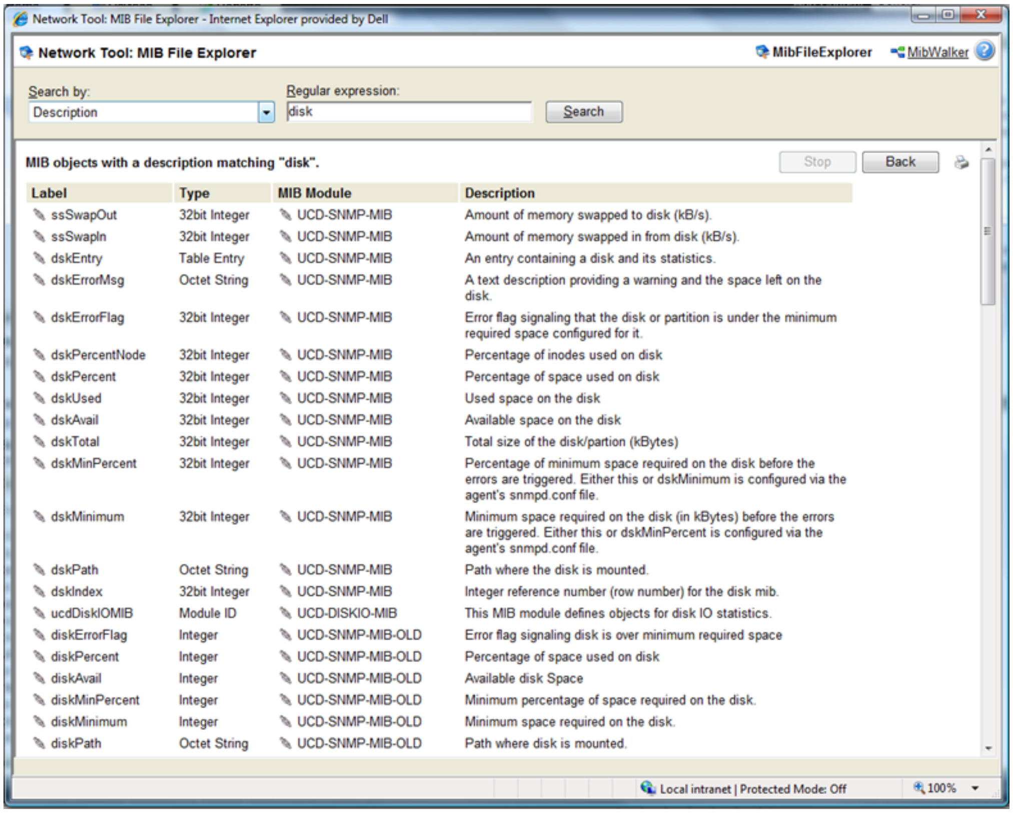
First, select **Type** or **Description** from the **Search Object** list, then proceed appropriately:

§ To search by object **Type**:

§ Select a type from the list, then click **Find**.

§ To search by object **Description**:

§ Enter a regular expression in the **Description** box. This is a regular expression, non-case-sensitive filter. For more information, see *Regular Expression Syntax* (on page 175). After entering the description in the box, click **Find**.


Network Tool: MIB File Explorer - Internet Explorer provided by Dell
Network Tool: MIB File Explorer
MibFileExplorer
MibWalker
Search by:
Description
Regular expression:
disk
Search
Stop
Back
Local intranet | Protected Mode: Off
100%

MIB objects with a description matching "disk".

Label	Type	MIB Module	Description
ssSwapOut	32bit Integer	UCD-SNMP-MIB	Amount of memory swapped to disk (kB/s).
ssSwapIn	32bit Integer	UCD-SNMP-MIB	Amount of memory swapped in from disk (kB/s).
dskEntry	Table Entry	UCD-SNMP-MIB	An entry containing a disk and its statistics.
dskErrorMsg	Octet String	UCD-SNMP-MIB	A text description providing a warning and the space left on the disk.
dskErrorFlag	32bit Integer	UCD-SNMP-MIB	Error flag signaling that the disk or partition is under the minimum required space configured for it.
dskPercentNode	32bit Integer	UCD-SNMP-MIB	Percentage of inodes used on disk
dskPercent	32bit Integer	UCD-SNMP-MIB	Percentage of space used on disk
dskUsed	32bit Integer	UCD-SNMP-MIB	Used space on the disk
dskAvail	32bit Integer	UCD-SNMP-MIB	Available space on the disk
dskTotal	32bit Integer	UCD-SNMP-MIB	Total size of the disk/partion (kBytes)
dskMinPercent	32bit Integer	UCD-SNMP-MIB	Percentage of minimum space required on the disk before the errors are triggered. Either this or dskMinimum is configured via the agent's snmpd.conf file.
dskMinimum	32bit Integer	UCD-SNMP-MIB	Minimum space required on the disk (in kBytes) before the errors are triggered. Either this or dskMinPercent is configured via the agent's snmpd.conf file.
dskPath	Octet String	UCD-SNMP-MIB	Path where the disk is mounted.
dskIndex	32bit Integer	UCD-SNMP-MIB	Integer reference number (row number) for the disk mib.
ucdDiskIOMIB	Module ID	UCD-DISKIO-MIB	This MIB module defines objects for disk IO statistics.
diskErrorFlag	Integer	UCD-SNMP-MIB-OLD	Error flag signaling disk is over minimum required space
diskPercent	Integer	UCD-SNMP-MIB-OLD	Percentage of space used on disk
diskAvail	Integer	UCD-SNMP-MIB-OLD	Available disk Space
diskMinPercent	Integer	UCD-SNMP-MIB-OLD	Minimum percentage of space required on the disk.
diskMinimum	Integer	UCD-SNMP-MIB-OLD	Minimum space required on the disk.
diskPath	Octet String	UCD-SNMP-MIB-OLD	Path where disk is mounted.

After the MIB File Explorer returns a list of the supported MIB objects, you can use this information to create custom performance monitors and active script performance monitors for devices. For more information, see *Creating custom performance monitors* (on page 286).

Note: You can switch to the WhatsUp Gold MIB Walker by clicking on the MIB Walker link on the upper-right side of this dialog.

Using the MAC Address tool

The MAC Address tool enables you to discover what MAC addresses are present on your network and gives you the opportunity to obtain physical connectivity information for devices on your network. This tool is useful to solve IP address conflicts within your network by providing you with specific switch information.

Tool results

After running the tool, the results of the test are displayed at the bottom of the page.

If **Get connectivity information using SNMP** is not selected when the tool is run, the results include the following columns:

§ **IP Address**. The IP addresses of devices on your network.

- **MAC Address**. The MAC addresses of devices on your network.
- **Hostname**. The hostnames of devices on your network.

If **Get connectivity information using SNMP** is selected when the tool is run, the results include the following columns:

- **IP Address**. The IP addresses of devices on your network.
- **MAC Address**. The MAC addresses of devices on your network.
- **Hostname**. The hostnames of devices on your network.
- **Port**. The port numbers of the switch ports that are connected to the devices that own the listed MAC addresses.
- **Index**. The unique value assigned to each interface. This number typically corresponds with the interface port number.

> **Note**: If **Port** and **Index** report values of `-1`, WhatsUp Gold did not understand the response from the switch or the request timed out. Verify that credentials are correct and that you can view other SNMP information from the switch, and then run the MAC Address tool again.

- **Description**. The interface description of the interface to which a device is connected. Listed as a letter and a numeral, such as "B4". The interface description allows you to identify the physical connector on the switch.

To use the MAC Address Tool:

1 Enter or select the appropriate information:

- **Local subnet.** Select the network on which you would like to find MAC addresses.

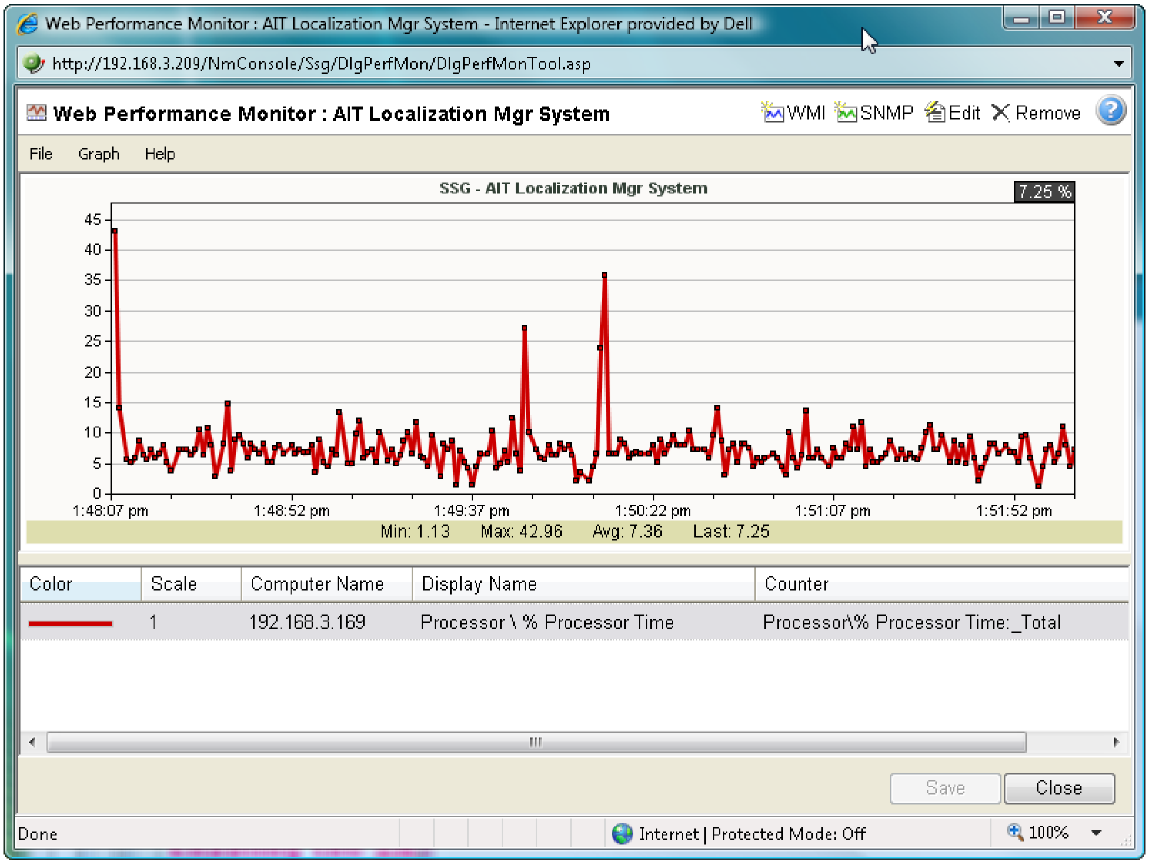
> **Note**:: WhatsUp Gold allows you to search for MAC addresses within your network, but since Layer 2 MAC address information is only visible to local networks, only local networks can be probed for MAC address information. Therefore, only the local networks to which the WhatsUp Gold computer is connected will be available from this field.

- **Get connectivity information using SNMP**. If you would like switch-specific connectivity information for a device in the network, select this option. If this option is selected, the following options are enabled. If this option is cleared, the following options are disabled.
  - **Switch IP address**. Enter the switch IP address.
  - **SNMP credential**. Select the SNMP credential that you use to poll this device. If the credential you want to use is not listed, you can add it using the Credential Library.
  - **Timeout (seconds)**. Enter the amount of time for the tool to wait on a response from the switch. The MAC address discovery fails if this time limit is exceeded.
  - **Retries**. Enter the maximum number of retries when polling the switch using SNMP.

2 Click **Discover** to discover the MAC addresses present on your network.

Using the Web Performance Monitor

The Web Performance Monitor extends the functionality of the Microsoft Windows Performance Monitor to the Web. It is a data collecting and graphing utility designed specifically for the WhatsUp Gold web interface that graphs and displays real-time information on user-specified SNMP and WMI performance counters. It can be used for a quick inspection of a specific network device.


Web Performance Monitor : AIT Localization Mgr System - Internet Explorer provided by Dell
http://192.168.3.209/NmConsole/Ssg/DlgPerfMon/DlgPerfMonTool.asp
Web Performance Monitor : AIT Localization Mgr System
WMI
SNMP
Edit
Remove
File
Graph
Help
SSG - AIT Localization Mgr System
7.25 %
45
40
35
30
25
20
15
10
5
0
1:48:07 pm
1:48:52 pm
1:49:37 pm
1:50:22 pm
1:51:07 pm
1:51:52 pm
Save
Close
Done
Internet | Protected Mode: Off
100%

Min: 1.13 Max: 42.96 Avg: 7.36 Last: 7.25

Color	Scale	Computer Name	Display Name	Counter
🟥	1	192.168.3.169	Processor \ % Processor Time	Processor\% Processor Time:_Total

The graphs can be saved to the database and displayed on dashboard views using the Split Second Graph - Performance Monitor dashboard report or on the Web Performance Monitor tool. Multiple SNMP and WMI counters can be displayed on a single graph, and the color and scale of each graphed item can be individually configured.

Graphs created with the Web Performance Monitor are saved on a per-user account basis, meaning, graphs are only accessible by the user account that created and saved them.

The Web Performance Monitor has two purposes:

- To provide a Web enabled WMI and SNMP performance counter poller and grapher. It supports WMI for Windows servers, and SNMP for network devices such as switches, routers, and UNIX devices.
- To build and edit graphs for use by the Performance Monitor dashboard report. You can use this dashboard report to display any saved graph.

To add a WMI performance counter to the Web Performance Monitor:

1 Click **Tools > Web Performance Monitor**. The Web Performance Monitor appears.

2 Click **Graph > Add WMI Counter**.

- or -

Click the WMI button in the upper right corner of the dialog (see the Toolbar buttons table below). The Add WMI Performance Counter dialog appears.

3 Enter the appropriate information into the dialog boxes.

4 Click **OK** to save changes.

To add an SNMP performance counter to the Web Performance Monitor:

1 Click **Tools > Web Performance Monitor**. The Web Performance Monitor appears.

2 Click **Graph > Add SNMP Performance Monitor**.

- or -

Click the SNMP button in the upper right corner of the dialog (see the Toolbar buttons table below). The Add SNMP Performance Counter dialog appears.

3 Enter the appropriate information into the dialog boxes.

4 Click **OK** to save changes.

Web Performance Monitor menu items

The Web Performance Monitor menu is located at the top left corner of the window.

File menu

§ **File > New Graph**. This menu item resets the graph back to a blank graph.

§ **File > Edit Graph Name**. This menu item lets you change the name of the selected graph.

§ **File > Load Graph**. This opens the Load Graph dialog, which displays a list of saved graph files on the Web server.

§ **File > Save Graph**. This saves the current graph to the database. If no filename is specified, it launches the Save Graph dialog, which allows a filename to be specified. All files are saved to the WhatsUp database.

§ **File > Save Graph As**. This opens the Save Graph dialog which prompts you for a filename, and then saves the current graph to disk.

§ **Windows Properties**. This opens the Configure Window Properties dialog. Use this dialog to configure the graph and window properties for the Web Performance Monitor.

Graph menu

§ **Graph > Add WMI Performance Counter**. This launches the Add WMI Performance Counter dialog.

§ **Graph > Add SNMP Performance Counter**. This launches the Add SNMP Performance Counter dialog.

§ **Graph > Edit Selected Counter**. This launches the appropriate dialog for editing the selected WMI or SNMP performance counter.

- **Graph > Remove Selected Counter**. This removes the selected counter from the list and graph. No changes are saved to disk until the OK button is clicked or the graph is manually saved (**File > Save Graph** - or - **Save Graph As**).

Help menu

- **Help > Help**. This launches help for the Web Performance Monitor.

Web Performance Monitor Toolbar buttons

The Web Performance Monitor Toolbar is located at the top right corner of the window.

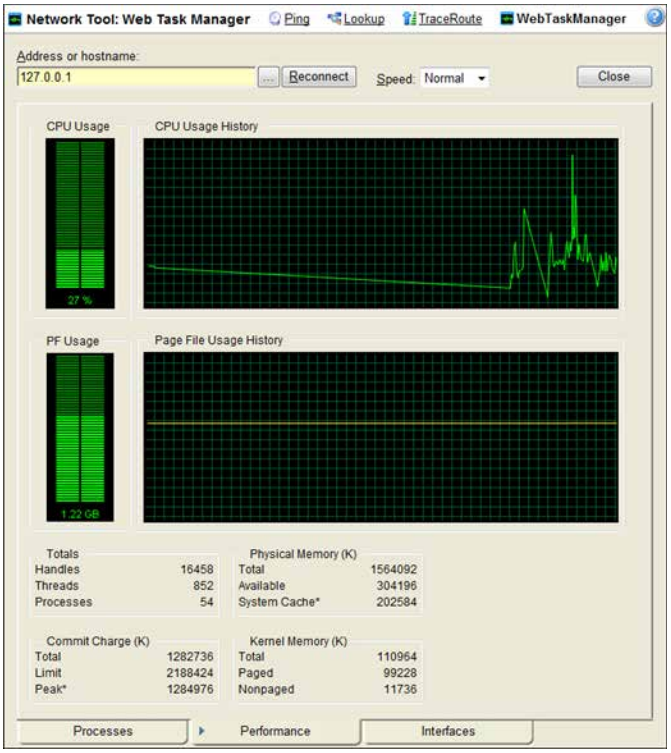
Button	Function
WMI	Opens the Add WMI Performance Counter dialog.
SNMP	Opens the Add SNMP Performance Counter dialog.
Edit	Opens the appropriate dialog for editing the selected WMI or SNMP performance counter.
✕ Remove	Removes the selected graph item from the list and graph.
?	Opens the help topic for the Web Performance Monitor

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 565).

Using the Web Task Manager

The Web Task Manager extends the functionality of the Microsoft Windows Task Manager to provide network device overview information about processes occurring on a device, device performance, and device interface activity. The Web Task Manager graphs and displays real-time information using SNMP or WMI device connections.

You can use the Web Task Manager to identify device issues and take corrective action on a device.



Address or hostname: 127.0.0.1

Speed: Normal

Totals	
Handles	16458
Threads	852
Processes	54

Physical Memory (K)	
Total	1564092
Available	304196
System Cache*	202584

Commit Charge (K)	
Total	1282736
Limit	2188424
Peak*	1284976

Kernel Memory (K)	
Total	110964
Paged	99228
Nonpaged	11736

There are three tabs that provide device information:

- **Processes** (on page 143). Provides key indicator process information for a selected device that WhatsUp Gold is monitoring. For example, you can view a list of **.**exe files that are running and the amount of CPU and memory used by each program.
- **Performance** (on page 145). Provides dynamic performance information for a selected device that WhatsUp Gold is monitoring. For example, you can view details about the CPU and memory usage.
- **Interfaces** (on page 148). Provides information about a selected device's interfaces that WhatsUp Gold is monitoring. For example, you can view a list of interfaces that the device uses to learn about how much data is transmitted and received via each interface.

To use the Web Task Manager:

1. Click the **Devices** tab, then click **Devices**. The Device page appears.
2. From the Details View or Map View, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.
3. Enter or select the appropriate information for the following boxes:
   - **Address or hostname**. Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.
   - Browse (**...**). Click to open the *Web Task Manager Credentials dialog* (on page 142) and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the Credentials Library.

- **Speed**. Select the speed at which you want to monitor the device performance.
  - **Normal**. Updates device information every one second.
  - **Medium**. Updates device information every five seconds.
  - **Slow**. Updates device information every ten seconds.
  - **Paused**. Stops updating device information.
- **Connect using** (Processes tab). Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the Credentials Library are used to connect and read information on the selected device.

Note: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 565).

Note: Some differences exist in column names between the Web Task Manager and Windows Task Manager in Windows Vista and Windows 2008. The `Mem Usage` column in Web Task Manager is named `Working Set (Memory)` in Windows Task Manager on Windows Vista and Windows 2008. The `VM Size` column in Web Task Manager has no corresponding column in Windows Task Manager on Windows Vista and Windows 2008.

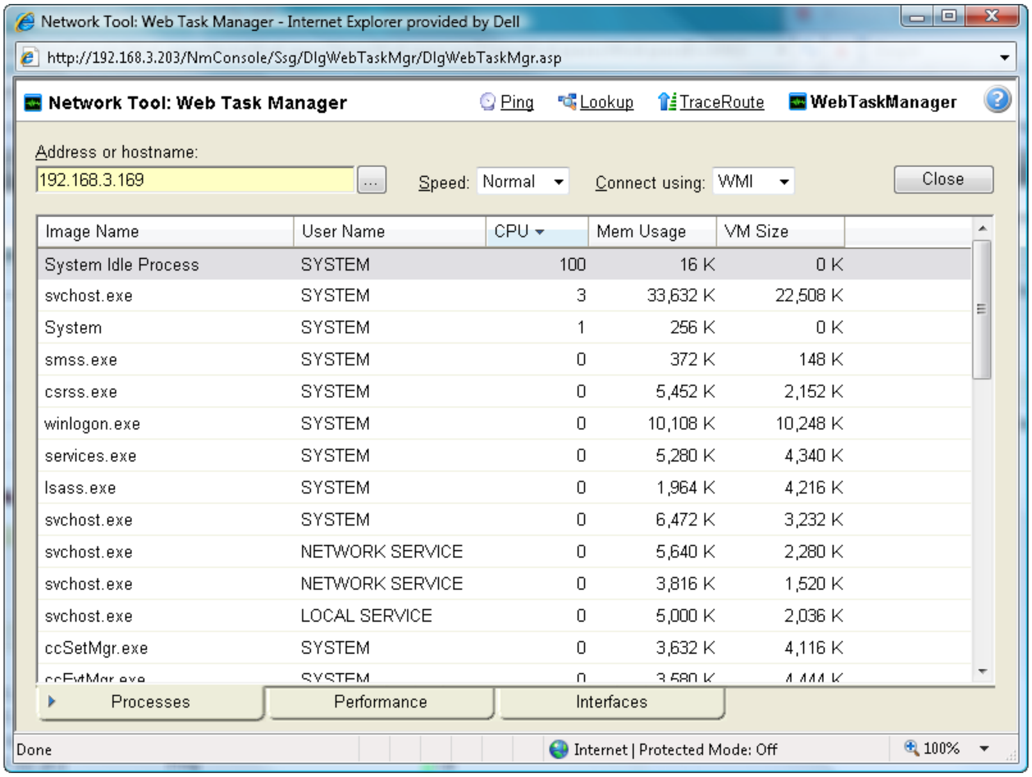
Setting up Web Task Manager device credentials

Use the Web Task Manager Credentials dialog to select credentials for the device you want to monitor with the Web Tools Task Manager.

- **Address or hostname**. Enter a device IP address to select a device for which you want to view process, performance, or interface information. Click the browse (**...**) button to select a device.
- **Windows**. Select the Windows credential to connect to this device. Click the browse (...) button to browse the Credentials Library.
- **SNMP v1/v2/v3**. Select the SNMP credentials to connect to this device. If the Identify devices via SNMP option was selected during discovery (or if an SNMP discovery was performed) the correct SNMP credential was used during the discovery process, and if the device is an SNMP manageable device, then the correct credential is selected automatically. If any of these conditions are not met, *None* is selected.
- **ADO**. Select the ADO credentials for database connection string information to be used when a database connection is required for WhatsUp Gold database monitors.
- **Edit**. Click to open the Select Credentials dialog, then select the credential from the list or click the browse (**...**) button to browse the Credentials Library.

How To example: Using the Web Task Manager - Process tab

The Web Task Manager Processes tab provides key indicator process information for a selected device that WhatsUp Gold is monitoring. This information helps you learn about device processes and identify trends and issues that occur on a particular network device. You can use the Web Task Manager Process tab to view the processes running on WMI- or SNMP-enabled network devices.


Network Tool: Web Task Manager - Internet Explorer provided by Dell
http://192.168.3.203/NmConsole/Ssg/DlgWebTaskMgr/DlgWebTaskMgr.asp
Network Tool: Web Task Manager
Ping
Lookup
TraceRoute
WebTaskManager
Close
Processes
Performance
Interfaces
Done
Internet | Protected Mode: Off
100%

Address or hostname: 192.168.3.169

Speed: Normal

Connect using: WMI

Image Name	User Name	CPU	Mem Usage	VM Size
System Idle Process	SYSTEM	100	16 K	0 K
svchost.exe	SYSTEM	3	33,632 K	22,508 K
System	SYSTEM	1	256 K	0 K
smss.exe	SYSTEM	0	372 K	148 K
csrss.exe	SYSTEM	0	5,452 K	2,152 K
winlogon.exe	SYSTEM	0	10,108 K	10,248 K
services.exe	SYSTEM	0	5,280 K	4,340 K
lsass.exe	SYSTEM	0	1,964 K	4,216 K
svchost.exe	SYSTEM	0	6,472 K	3,232 K
svchost.exe	NETWORK SERVICE	0	5,640 K	2,280 K
svchost.exe	NETWORK SERVICE	0	3,816 K	1,520 K
svchost.exe	LOCAL SERVICE	0	5,000 K	2,036 K
ccSetMgr.exe	SYSTEM	0	3,632 K	4,116 K
ccEvtMgr.exe	SYSTEM	0	3,580 K	4,444 K

After you have identified a process that is causing device performance issues, such as an application executable like `Outlook.exe` running multiple instances of the program, you can correct the problem to bring the device performance back to normal.

Note: Unlike the Windows Task Manager, you cannot terminate processes using the Web Task Manager. To terminate a task, you must log in to the computer where the task is running and use the Windows Task Manager to end the process.

To use the Web Task Manager:

1 Click the **Devices** tab, then click **Devices**. The Device page appears.

2 From the Details View or Map View, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.

3 Enter or select the appropriate information for the following boxes:

- **Address or hostname**. Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.

- Browse (**...**). Click to open the Web Task Manager Credentials dialog and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the Credentials Library.
- **Speed**. Select the speed at which you want to monitor the device performance.
  - **Normal**. Updates device information every one second.
  - **Medium**. Updates device information every five seconds.
  - **Slow**. Updates device information every ten seconds.
  - **Paused**. Stops updating device information.
- **Connect using**. Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the Credentials Library are used to connect and read information on the selected device.

Note: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

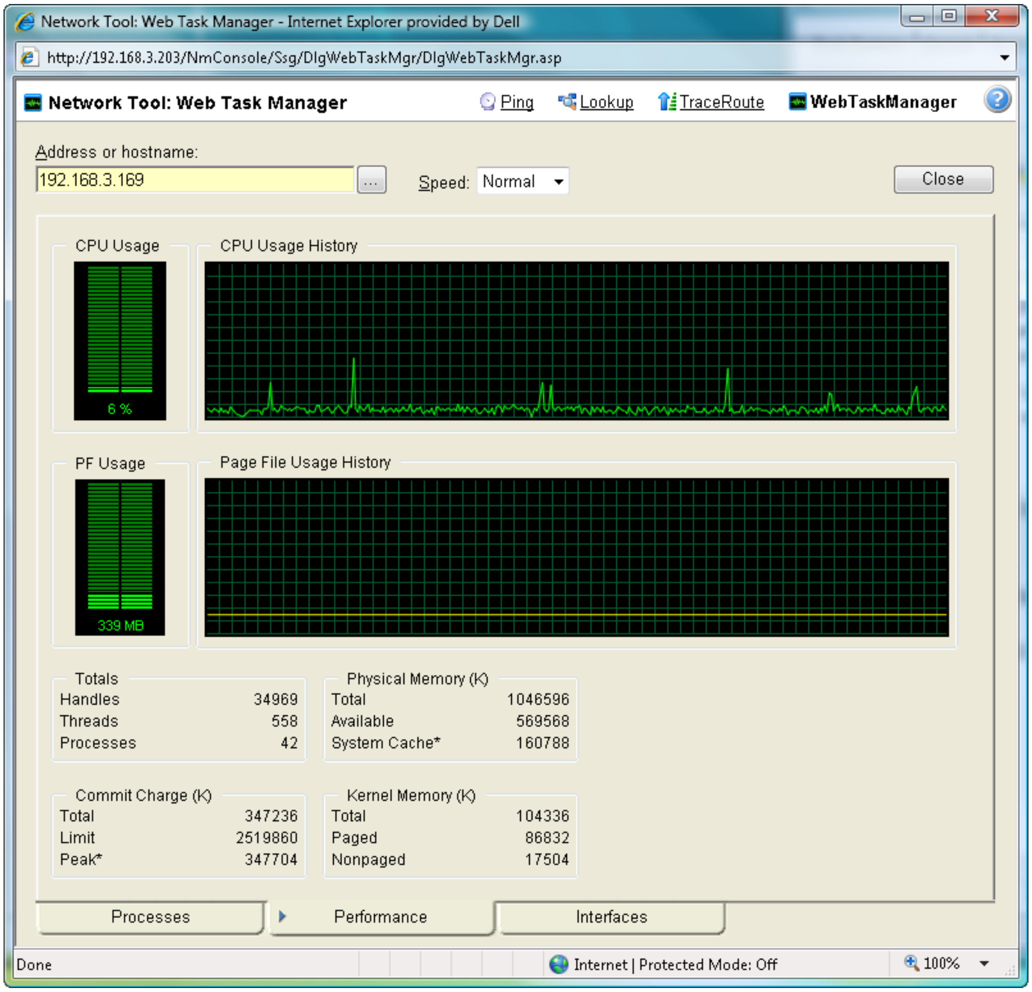
4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 565).

Note: Some differences exist in column names between the Web Task Manager and Windows Task Manager in Windows Vista and Windows 2008. The `Mem Usage` column in Web Task Manager is named `Working Set (Memory)` in Windows Task Manager on Windows Vista and Windows 2008. The `VM Size` column in Web Task Manager has no corresponding column in Windows Task Manager on Windows Vista and Windows 2008.

Using the Web Task Manager - Performance tab

The Performance tab provides dynamic performance information for a selected device that WhatsUp Gold is monitoring. This information helps you learn about device performance and identify trends, spikes, or other issues that occur on a particular network device. You can use the Web Task Manager to view device performance for devices that are WMI or SNMP enabled network devices.



http://192.168.3.203/NmConsole/Ssg/DlgWebTaskMgr/DlgWebTaskMgr.asp

Address or hostname: 192.168.3.169

Speed: Normal

Totals	
Handles	34969
Threads	558
Processes	42

Physical Memory (K)	
Total	1046596
Available	569568
System Cache*	160788

Commit Charge (K)	
Total	347236
Limit	2519860
Peak*	347704

Kernel Memory (K)	
Total	104336
Paged	86832
Nonpaged	17504

After you have identified a performance issue that is causing device performance issues, such as the Page File Usage indicating that the system memory is nearly at full capacity, you can correct the problem to bring the device performance back to normal.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To use the Web Task Manager:

1 Click the **Devices** tab, then click **Devices**. The Devices page appears.

2 From the details or icon view, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.

3 Enter or select the appropriate information for the following fields:

- **Address or hostname**. Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.
- Browse (**...**). Click to open the *Web Task Manager Credentials dialog* (on page 142) and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the *Credentials Library* (on page 458).
- **Speed**. Select the speed at which you want to monitor the device performance.
  - **Normal**. Updates device information every one second.
  - **Medium**. Updates device information every five seconds.
  - **Slow**. Updates device information every ten seconds.
  - **Paused**. Stops updating device information.
- **Connect using** (Processes tab). Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the *Credentials Library* (on page 458) are used to connect and read information on the selected device.

> **Note**: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).

5 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 565).

The following are examples of information that is provided when you connect to and view a WMI enabled device. Note, this information varies by operating system:

- **CPU Usage**. This graph indicates the percentage of time the processor is operating. Use this graph to view how much the processor is operating.
- **CPU Usage History**. This graph indicates how much the processor has operated over time. You can change the Speed option (High, Normal, Slow, Paused). The Speed option determines how often updates occur to the CPU Usage History.
- **PF Usage**. This graph indicates how much page file memory is used.
- **Page File Usage History**. This graph indicates how much the page file memory is used over time. If page file memory usage is high, you may want to increase the available page file memory.

- **Totals**. This provides the total number of Handles, Threads, and Processes occurring on the selected device.
- **Commit Charge (K)**. Provides information about the memory (Total, Limit, and Peak) allocated to the operating system and applications running on the device.
- **Physical Memory (K)**. Provides information about the amount of physical memory (Total, Available, and System Cache) installed on the device.
- **Kernel Memory (K)**. Provides information about how much memory (Total, Paged, and Nonpaged) the operating system kernel and device drivers are using.

> **Note**: Values reported for Peak and System Cache will differ from values reported by the Windows Task Manager on the actual device. In the Web Task Manager, Peak reflects the peak value for the time that the Web Task Manager has been open only, and System Cache does not include the size of the free page list.

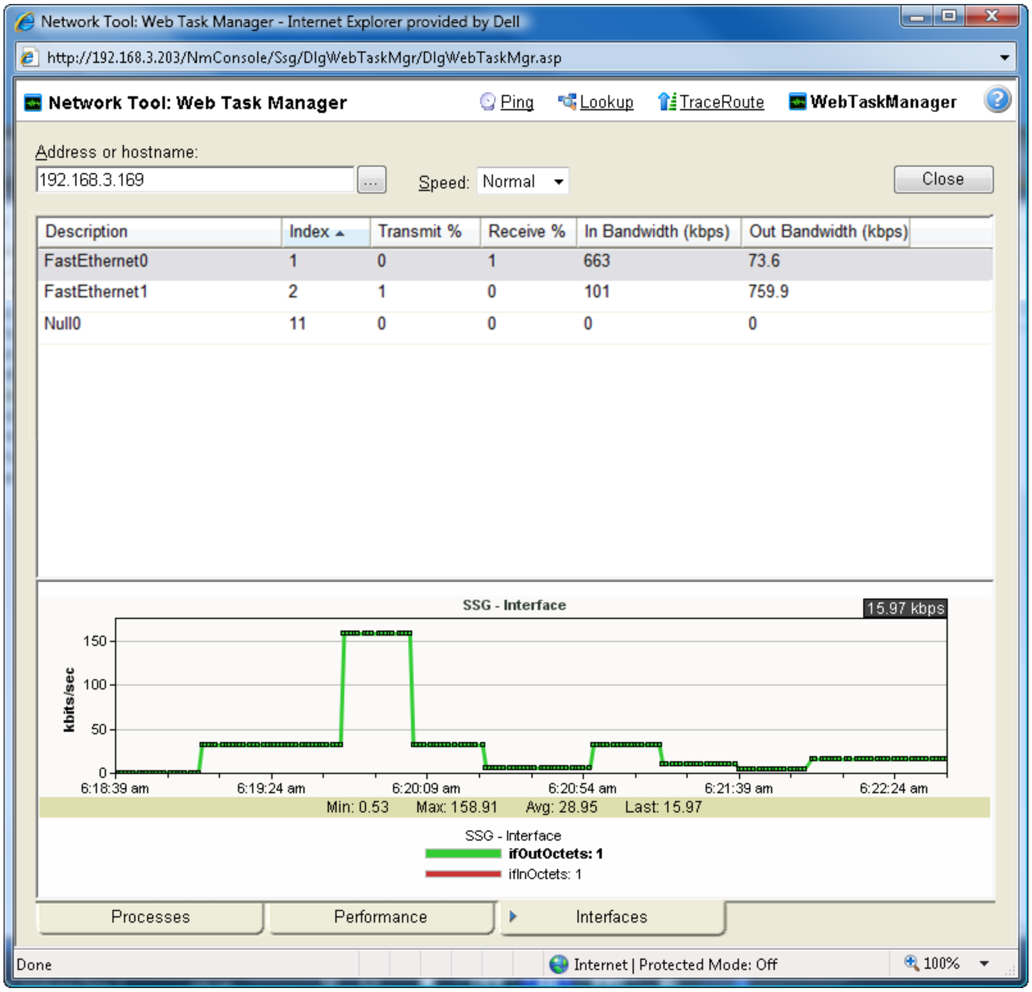
The following information are examples of the information that is provided when you connect to and view a SNMP enabled device. Note, this information varies by operating system:

- **In (PKTS)**. Provides detailed information about the network packets that this device receives.
- **Out (PKTS)**. Provides detailed information about the network packets that this device sends.
- **System**. Provides general system information about CPU performance, the number of interfaces that are running on the device, the total amount of time the device has been operating in the up mode, and the version number of Cisco software running on the device (if applicable).

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 565).

Using the Web Task Manager - Interfaces tab

The Interfaces tab provides information about the interfaces available on a selected device that WhatsUp Gold is monitoring. This information helps you determine how much data is transmitted and received via each interface, and therefore may help you locate an interface that using an unexpected amount of bandwidth.



Address or hostname: 192.168.3.169

Speed: Normal

Description	Index ▲	Transmit %	Receive %	In Bandwidth (kbps)	Out Bandwidth (kbps)
FastEthernet0	1	0	1	663	73.6
FastEthernet1	2	1	0	101	759.9
Null0	11	0	0	0	0

After you have identified the interface that is causing bandwidth performance issues, such as a file sharing application exposing shared files on a computer for others on the Internet to access and download, you can correct the problem to bring the device performance back to normal.

The Web Task Manager includes the following columns:

- **Description**. This column is the text description of the interface as configured on the device.
- **Index**. This column is the unique numerical identifier of the interface as defined on the device.
- **Transmit %**. This column indicates what percentage of the interface's capacity is currently being used to transmit data.

- **Receive %**. This column indicates what percentage of the interface's capacity is currently being used to receive data.
- **In Bandwidth (kbps)**. This column shows the amount of data received by the device in kilobits per second.
- **Out Bandwidth (kbps)**. This column shows the amount of data transmitted by the device in kilobits per second.

To use the Web Task Manager:

1. Click the **Devices** tab, then click **Devices**. The Devices page appears.
2. From the details or icon view, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.
3. Enter or select the appropriate information for the following fields:
   - **Address or hostname**. Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.
   - Browse (**...**). Click to open the *Web Task Manager Credentials dialog* (on page 142) and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the *Credentials Library* (on page 458).
   - **Speed**. Select the speed at which you want to monitor the device performance.
     - **Normal**. Updates device information every one second.
     - **Medium**. Updates device information every five seconds.
     - **Slow**. Updates device information every ten seconds.
     - **Paused**. Stops updating device information.
   - **Connect using** (Processes tab). Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the *Credentials Library* (on page 458) are used to connect and read information on the selected device.

> **Note**: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

4. At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).
5. For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 565).

Using Layer 2 Trace

In troubleshooting situations, it is often critical to understand the path that network data takes to access another network device. The Layer 2 Trace tool provides a method to trace the physical network path from one device to another.

Using previously discovered network connectivity data, the Layer 2 Trace tool finds the path between the two devices and then displays each network interface that is used to build the path. The trace tool also allows for a quick check of the status and availability of each step along the layer 2 path.

To access the Layer 2 Trace tool:

On the WhatsUp Gold web interface, go to **Tools > Layer 2 Trace**.

To use the Layer 2 Trace tool:

1. On the WhatsUp Gold web interface, go to **Tools > Layer 2 Trace**. The Layer 2 Trace dialog appears.
2. Click **Source**. The Select Device dialog appears.
3. Select a starting device for the layer 2 trace, then click **OK**. The IP address for the selected device is listed for the Source Device.
4. Click **Destination**. The Select Device dialog appears.
5. Select a destination device for the layer 2 trace, then click **OK**. The IP address for the selected device is listed for the Destination Device.
6. Click **Trace**. The step-by-step layer 2 path from the source device to the destination device displays in list format. The results of the search display in the Layer 2 Trace tool columns.
   - **Device**. Lists the devices that the network path traverses.
   - **IP Address**. Lists the IP address of each device on the network path.
   - **Interface Name**. Lists the interfaces that the network path traverses.
   - **Ping Status**. Lists the device ping status.

> **Note**: After a trace is completed, you can click **Ping** to view the current status of the Layer 2 path. This tool pings each device identified in the trace and uses SNMP to query the interface for its status.

7. Click **Clear** to remove the information from the Layer 2 Trace table and start a new trace.
   - or -
   Click **Close** to close the dialog.

Using IP/MAC Address Finder

The IP/MAC Finder tool provides an easy way to locate an IP or MAC address on the network. Using the previously discovered network devices, IP/MAC Finder will find and display network interfaces that have sighting information for the supplied IP or MAC address. To get the most up-to-date sighting information, you can use the Refresh button which sends SNMP requests to each network device to quickly update the sighting information.

When enough network data is available, IP/MAC Finder indicates to which network interface the IP or MAC address is physically connected.

To access the IP/MAC Finder tool:

On the WhatsUp Gold web interface, go to **Tools > IP/MAC Address Finder**.

To use the IP/MAC Finder tool:

1 From the WhatsUp Gold web interface, go to **Tools > IP/MAC Address Finder**. The IP/MAC Address Finder appears.

2 Enter the appropriate information in the following fields.

§ **IP Address**. Enter the IP address of a device for which you want to find sightings on the network. Leave this option blank if you are only scanning for a MAC address.
- or -
Click **Select** to select a device, in the Select Devices dialog, for which you want to identify a MAC address. For more information, see About the Select button.

§ **MAC Address**. Enter The MAC address for which you are scanning the network. Leave this option blank if you are only scanning for an IP address.

3 Select **Use Network Devices Only** to display the IP/MAC sightings found only on *network* device types.
- or -
Deselect **Use Network Devices Only** to display all IP/MAC sightings found on *all* device types.

4 Click **Find** to search the network to locate where the IP or MAC device is on the network. The results of the search are displayed in the Sighting Information list:

§ **Device**. Lists the name of the network device that has sighting information for the IP or MAC address.

§ **IP Address**. Lists the IP address of the sighting device.

§ **Interface Name**. Lists the network interface that is routing or forwarding traffic to the IP or MAC address.

§ **Is Linked To**. Lists the network devices to which the device is linked.

§ **Sighting Type**. Lists where the information was seen, such as an ARP Cache, a forwarding database, or the device itself.

5 Click **Clear** to remove the information from the IP/MAC Finder table and start a new device sighting.
- or -
Click **Close** to close the dialog.

Monitoring Devices

In This Section

Using Active Monitors

In This Chapter

Active Monitors overview

Active monitors poll target devices for information such as ping accessibility, device services, such as Web or email servers, and more. Active monitors regularly query or poll the device services for which they are configured and wait for responses. If a query is returned with an expected response, the queried service is considered "up." If a response is not received, or if the response is not expected, the queried service is considered "down" and a state change is issued on the device.

In an effort to help you manage your network after you install the application, WhatsUp Gold includes a number of pre-configured active monitors. These pre-configured monitors display in the Active Monitor Library. As you configure new active monitor types, they are added to the library.

The Active Monitor Library displays active monitors configured and available to apply to network devices. For more information, see *Configuring Active Monitors* (on page 155).

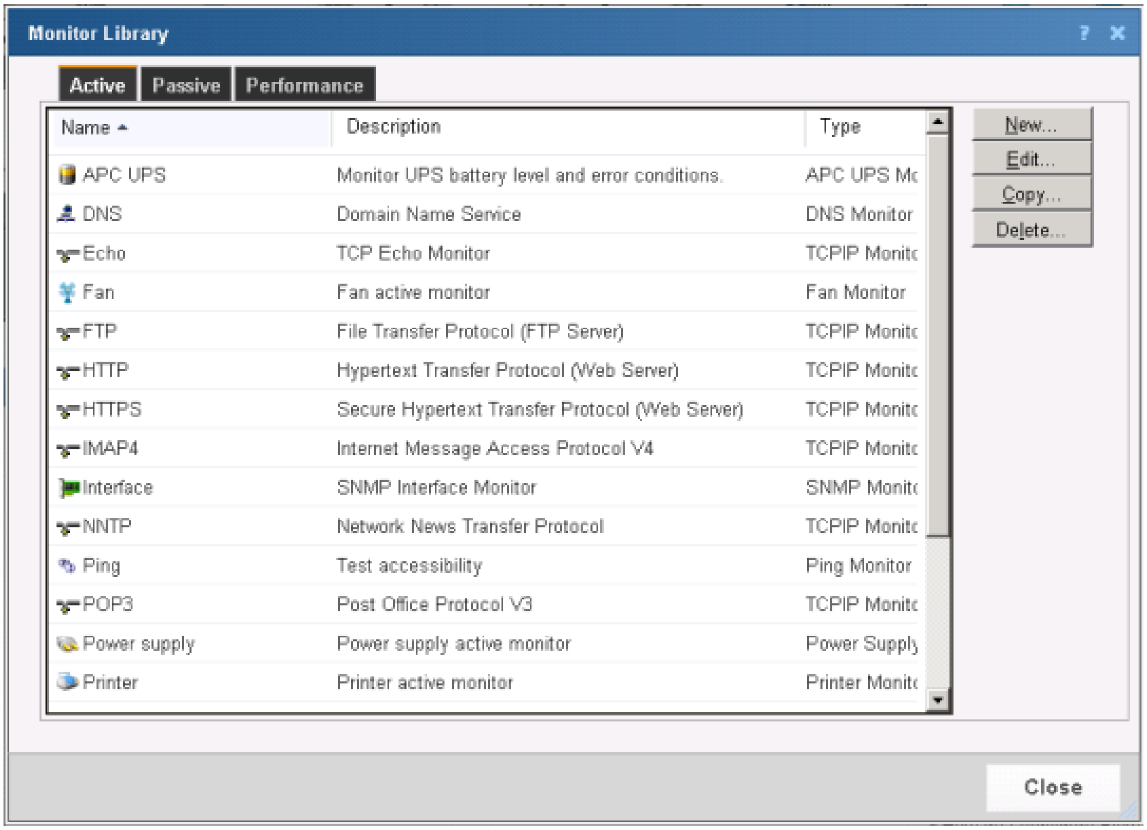
About the Active Monitor Library

The Active Monitor Library displays all active monitors currently configured for use in WhatsUp Gold. To help you manage your network easily after your initial installation of the application, WhatsUp Gold includes a number of pre-configured active monitors. These pre-configured monitors display in the Active Monitor Library. As you configure new active monitor types, they are added to the library.

To access the Active Monitor Library:

1 From the **Admin** panel, click **Monitor Library**. The Monitor Library dialog appears.

2 If not already selected, click the **Active** tab to open the Active Monitor Library.



Name	Description	Type
APC UPS	Monitor UPS battery level and error conditions.	APC UPS Mc
DNS	Domain Name Service	DNS Monitor
Echo	TCP Echo Monitor	TCPIP Monitc
Fan	Fan active monitor	Fan Monitor
FTP	File Transfer Protocol (FTP Server)	TCPIP Monitc
HTTP	Hypertext Transfer Protocol (Web Server)	TCPIP Monitc
HTTPS	Secure Hypertext Transfer Protocol (Web Server)	TCPIP Monitc
IMAP4	Internet Message Access Protocol V4	TCPIP Monitc
Interface	SNMP Interface Monitor	SNMP Monitc
NNTP	Network News Transfer Protocol	TCPIP Monitc
Ping	Test accessibility	Ping Monitor
POP3	Post Office Protocol V3	TCPIP Monitc
Power supply	Power supply active monitor	Power Supply
Printer	Printer active monitor	Printer Monitc

Use the Active Monitor Library to configure new or existing active monitors:

- Click **New** to configure a new Active Monitor Type.
- Select an existing type from the list, then click **Edit** to change an active monitor type.
- Select an active monitor type from the list, then click **Copy** to make a copy of an active monitor.
- Select an active monitor type from the list, then click **Delete** to remove an active monitor from the library.

Caution: When you delete an active monitor from the Active Monitor Library, any instance of that active monitor is also deleted and all related report data is lost.

Selecting an Active Monitor Type

Select one of the following active monitor types, then click **OK**.

- *Active Script Monitor* (on page 155)
- *APC UPS Monitor* (on page 180)
- *DNS Monitor* (on page 157)
- *Email Monitor* (on page 183)
- *Exchange 2003 Monitor* (on page 188)
- *Exchange Monitor* (on page 192)

- *Fan Monitor* (on page 196)
- *File Properties Monitor* (on page 197)
- *Folder Monitor* (on page 200)
- *FTP Monitor* (on page 203)
- *HTTP Content* (on page 206)
- *Network Statistics Monitor* (on page 211)
- *NT Service Monitor* (on page 158)
- *Ping Monitor* (on page 159)
- *Power Supply Monitor*
- *PowerShell Monitor* (on page 214)
- *Printer Monitor*
- *Process Monitor* (on page 219)
- *SNMP Monitor* (on page 162)
- *SQL Query Monitor* (on page 223)
- *SQL Server 2000 Monitor* (on page 228)
- *SSH Monitor* (on page 165)
- *TCP/IP Monitor* (on page 168)
- *Telnet Monitor* (on page 166)
- *Temperature Monitor* (on page 232)
- *VoIP Monitor (available with the VoIP Monitor plug-in)* (on page 233)
- *WAP Radio Monitor* (on page 178)
- *WMI Formatted Monitor* (on page 235)
- *WMI Monitor* (on page 237)

Configuring Active Monitors

All active monitor types are stored in and configured from the Active Monitor Library. In order to function as designed, active monitors must be assigned to devices. When an active monitor is assigned, an individual instance of the monitor is placed on the device to which it is assigned. Subsequent changes made to the active monitor in the Active Monitor Library affect all instances of the monitor.

Adding and editing an Active Script Active Monitor

The Active Script monitor lets you write either VBScript or JScript code to perform specific customized checks on a device. If the script returns an error code, the monitor is considered down. A variety of active script resources are available on the *Active Scripts Resource page* (http://www.whatsupgold.com/script_library).

Note: Ipswitch does not support any custom scripts you create, only the ability to use them in the Active Script monitor. For more information, see *Extending WhatsUp Gold with scripting* (on page 512).

To add a new Active Script active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **Active Script Monitor**, then click **OK**. The New Active Script Monitor dialog appears.
5. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
   - **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
   - **Script Type**. Select either VBScript or JScript.
   - **Use in rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using Rescan on the Device Properties dialog, if the protocol or service is active on the device.
   - **Script text**. Enter your monitor code here.
6. Click **OK** to save changes.
7. After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Active Script active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Select the monitor you would like to edit, then click **Edit**. The Edit Active Script Monitor dialog appears.
4. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
   - **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
   - **Script Type**. Select either VBScript or JScript.
   - **Use in rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device

during a rescan, which is launched using Rescan on the Device Properties dialog, if the protocol or service is active on the device.

- **Script text**. Enter your monitor code here.

5 Click **OK** to save changes.

Adding and editing a Domain Service (DNS) Monitor

The Domain Name Server (DNS) monitor is a simple service monitor that checks for the DNS on port 53. If a DNS service does not respond on this port, the service is considered down.

To add a new DNS active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Click **New**. The Select Active Monitor Type dialog appears.
4 Select **DNS Monitor**, then click **OK**. The Add DNS Monitor dialog appears.
5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.

6 Click **OK** to save changes.
7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing DNS active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Select the monitor you would like to edit, then click **Edit**. The Edit DNS Monitor dialog appears.
4 Enter or select the appropriate information:

- **Name**. Enter a name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs

and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

§ **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.

5 Click **OK** to save changes.

Adding and editing an NT Service Monitor

The NT Service monitor checks the status of a service on a Windows machine and attempts a restart of the service (if the appropriate Administrator permissions exist).

Note: A running Windows Management Instrumentation (WMI) service on the targeted machine is required for this NT Service Monitor to work properly. Windows 2000 Service Pack 2 or higher, XP, and 2003 are installed with the WMI service. WMI is not installed with Windows NT, but can be downloaded from Microsoft and installed on Windows NT.

To add a new NT Service active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **NT Service Monitor**, then click **OK**. The NT Service Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 Select a **Protocol** to use to connect to the device.

7 (Optional) When using the SNMP protocol to connect to the device, click **Advanced** to set the advanced options.

8 Click browse (**...**) to open the Browse for Service dialog, allowing you to locate *any* server/workstation running the service.

9 Select the **Restart on failure** option to have the monitor attempt to restart the service when it enters a down state.

10 Select the **Use in Rescan** option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.

Note: WhatsUp Gold uses Windows Management Instrumentation (WMI) to verify the status of the NT Service Active Monitors you have configured. WhatsUp Gold currently only supports monitoring on Windows 2000 Service Pack 2 or higher, Windows XP Professional, and Windows 2003 or higher.

11 Click **OK** to save changes.

12 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing NT Service monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit NT Service Monitor dialog appears.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 Select a **Protocol** to use to connect to the device.

6 (Optional) When using the SNMP protocol to connect to the device, click **Advanced** to set the advanced options.

7 Click browse (**...**) to open the Browse for Service dialog, allowing you to locate *any* server/workstation running the service.

8 Select the **Restart on failure** option to have the monitor attempt to restart the service when it enters a down state.

9 Select the **Use in Rescan** option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.

Note: WhatsUp Gold uses Windows Management Instrumentation (WMI) to verify the status of the NT Service Active Monitors you have configured. WhatsUp Gold currently only supports monitoring on Windows 2000 Service Pack 2 or higher, Windows XP Professional, and Windows 2003 or higher.

10 Click **OK** to save changes.

Troubleshooting

Having problems with your WMI monitor returning *false negatives* (on page 566)?

Adding and editing a Ping Monitor

The Ping monitor can be configured to send an ICMP (ping) command to a device. This is the default monitor added to all devices during discovery. If the device does not respond, the monitor is considered down.

To add a new Ping active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Ping Monitor**, then click **OK**. The Add Ping Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
- **Retries**. Enter the number of times WhatsUp Gold attempts to send the command before the device is considered down.
- **Payload size**. Enter the length in bytes of each packet sent by the ping command.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.

6 Click **OK** to save changes.

7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Ping active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Ping Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
- **Retries**. Enter the number of times WhatsUp Gold attempts to send the command before the device is considered down.
- **Payload size**. Enter the length in bytes of each packet sent by the ping command.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.

5 Click **OK** to save changes.

Adding and editing a Power Supply Monitor

The Power Supply monitor checks Cisco switches/routers, Dell servers, Dell Power Connect switches/routers, and HP ProCurve and switches/routers, HP ProLiant servers, and other device power supplies to see that they are enabled and return a value that signals they are in an up state. The monitor first checks to see if a device is a Cisco, Dell, or HP device, then checks any enabled power supply devices. If a power supply is disabled, the monitor ignores it; if a power supply does not return a value of 1 - Normal (for Cisco switches/routers), 3 - OK (for Dell server devices), 1 - OK (for Dell switches/routers), 4 - Good (for HP ProCurve switches/routers), or 2 - OK (for HP ProLiant servers), the monitor is considered down.

Note: Not all types of device power supplies may be monitored using the Power Supply monitor. Check the make and model of your device power supply before attempting to monitor.

This monitor is pre-configured and exists in the Active Monitor Library upon installation of WhatsUp Gold. Unlike many pre-configured active monitors, the Power Supply monitor default configuration cannot be modified. However, you can modify the monitor name and description, as well as the SNMP timeout and number of retries used while attempting to connect to devices.

To add a new Power Supply active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Click **New**. The Select Active Monitor Type dialog appears.
4 Select **Power Supply Monitor**, then click **OK**. The New Power Supply Monitor dialog appears.
5 Enter the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
6 (Optional) Click **Advanced** to set the advanced options.
7 Click **OK** to save changes.
8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Power Supply active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Select the monitor you would like to edit, then click **Edit**. The Edit Power Supply Monitor dialog appears.
4 Enter the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 (Optional) Click **Advanced** to set the advanced options.

6 Click **OK** to save changes.

Adding and editing a SNMP Active Monitor

The Simple Network Management Protocol (SNMP) is the protocol governing network management and monitoring of network devices and their functions. In this monitor, WhatsUp Gold utilizes SNMP to gather specific information about the functions of SNMP-enabled network devices by querying a device to verify that it returns an expected value. Depending on the state you choose, the monitor is considered either up or down according to the returned value.

To add a new SNMP active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **SNMP Monitor,** then click **OK**. The Add SNMP Monitor dialog appears.

5 Enter the appropriate information in the following fields:

- **Name**. Enter a name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.

6 Click browse (**...**) to select the appropriate SNMP object in the MIB Browser.

7 Select **Check Type.**

8 Complete the check type detailed information.

When **Constant Value** is selected:

- **Value**. Depending on the Object ID you selected, enter the appropriate value.
- **If the value matches, then the monitor is**: select **Up** or **Down**.

When **Range of Values** is selected:

- **Low Value**. Depending on the Object ID you selected, enter the appropriate value.
- **High Value**. Depending on the Object ID you selected, enter the appropriate value.

When **Rate of Change in Value** is selected:

- **Rate of Change** (in variable units per second). Enter the desired value.
- **If the value is above the rate, then the monitor is**: select **Up** or **Down**.

9 Click **OK** to save changes.

10 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing SNMP active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit SNMP Monitor dialog appears.

4 Enter the appropriate information in the following fields:

- **Name**. Enter a name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.

5 Click browse (**...**) to select the appropriate SNMP object in the MIB Browser.

6 Select **Check Type.**

7 Complete the check type detailed information.

When **Constant Value** is selected:

- **Value**. Depending on the Object ID you selected, enter the appropriate value.
- **If the value matches, then the monitor is**: select **Up** or **Down**.

When **Range of Values** is selected:

- **Low Value**. Depending on the Object ID you selected, enter the appropriate value.
- **High Value**. Depending on the Object ID you selected, enter the appropriate value.

When **Rate of Change in Value** is selected:

- **Rate of Change** (in variable units per second). Enter the desired value.
- **If the value is above the rate, then the monitor is**: select **Up** or **Down**.

8 Click **OK** to save changes.

Selecting an object in the MIB Tree

In order to select the appropriate object in the MIB tree, you need to be familiar with the MIB names for the SNMP objects for which you want to monitor. For more information, see RFC 1213.

Example A.

If you want to monitor the volume of data traveling from your router, you select ifOutOctets in the MIB object tree and insert 1.3.6.1.2.1.2.2.1.16 in the MIB box.

Example B.

If you are interested in the operating status value of a port on your router, you select ifOperStatus and insert 1.3.6.1.2.1.2.2.1.8 in the MIB box.

Example C.

If you are interested in errors from a specific port on your router, you select ifInErrors, and inserting 1.3.6.1.2.1.2.2.1.14 in the MIB box.

For more information, see *Extending WhatsUp Gold with scripting* (on page 512).

Example: Monitoring Network Printer Toner Levels

To avoid running out of printer ink in the middle of print jobs, or wasting toner by switching toner cartridges before they are empty, through WhatsUp Gold you can create a custom SNMP active monitor that notifies you when toner levels are low.

To configure a printer monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click **New**, select **SNMP Monitor**, then click **OK**. The Add SNMP Monitor dialog appears.You need to create an active monitor for each printer type in use. It may be that the office uses the same printer type in each office. In this example, we are using a Hewlett Packard LaserJet 4050N. Check your network printers for their specific maximum capacity toner levels.

3 Enter a **Name** and **Description** for the monitor. For example, TonerMonitor and Toner monitor for the Hewlett Packard LaserJet 4050N.

4 For the **Object ID** and **Instance**, click browse (**...**), then locate the **prtMarkerSuppliesLevel** (OID 1.3.6.1.2.1.43.11.1.1.9) **SNMP** object in the MIB object tree. This SNMP object is found in the MIB tree at:
mgmt > mib 2 > printmib > prtMarkerSupplies > prtMarkerSuppliesEntry > prtMarkerSuppliesLevel

5 Select **Range of Values** from the type drop down menu and enter 4600 (the maximum capacity toner level) as the **High value** and 100 as the **Low Value**, then click **OK**. The action fails when the printer toner level reaches 99.

6 Test the newly created active monitor and make appropriate changes if needed.

7 Assign the active monitor to the printer device, click **Properties > Active Monitors**. The Device Properties Active Monitor dialog appears.

8 Click **Add**.

9 During the configuration wizard, create or select an action to notify you when the printer's toner levels are low.

10 Repeat steps 4-6 for each network printer that requires monitoring.

Example: Monitoring TCP Connections Established for a Device

Too many TCP connections can signal that a device is being maliciously used, in the case of a workstation, or that your web server is close to maxing out, indicating the need to initiate a backup server. You can create an SNMP active monitor to watch a range of established TCP connections for a particular device. If the number of connections goes above the range you specify, you can be notified by an associated action.

To configure a TCP monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click **New**, select **SNMP Monitor**, then click **OK**. The Add SNMP Monitor dialog appears.

3 Enter a **Name** and **Description** for the monitor. For example, Number of TCP `connections less than 2000`.

4 For the **Object ID** and **Instance**, click browse (**...**), then locate the **TcpCurrEstab** (1.3.6.1.2.1.6.9) SNMP object in the MIB object tree.

5 Select **Range of Values** from the Check type list and enter 1999 (the maximum number of established TCP connections) as the **High value** and 0 as the **Low Value**, then click

OK. Any associated actions fail when the number of established TCP connections reaches 2000.

6 Test the newly created active monitor and make appropriate changes if needed.

7 Assign the active monitor to the web server:

a) Right-click on the device on the appropriate device, then click **Properties > Active Monitors**. The Device Properties Active Monitor dialog appears.

b) Click **Add**.

c) Using the configuration wizard, create or select an action to notify you when the number of established TCP connections reaches 2000.

Adding and editing an SSH Active Monitor

The Secure Shell (SSH) monitor connects to a remote device using SSH to execute commands or scripts. The success or failure of the monitor is dependant upon values returned by the commands or scripts that can be interpreted by WhatsUp Gold as up or down.

To add a new SSH active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **SSH Monitor**, then click **OK**. The New SSH Active Monitor dialog appears.

5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Command to run**. Enter the command you want to run and execute on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.

Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

§ **The monitor is considered Up if the following output ____.** Either Contains or Does not contain. Select the appropriate output criteria. For example, if you are checking to see that a specific network connection is present on the remote device, you would select that the output contains that specific connection. If the network connection you specify is not present when the monitor checks, the monitor is considered down.

§ **Use regular expression**. Select this option to have WhatsUp Gold use regular expression when searching for the output of command or script. If you do not choose to use regular expression, WhatsUp Gold looks for specific text outputs, rather than outputs including a regular expression.

§ **SSH credential**. Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned.

If the appropriate SSH credential is not listed, or the device has no SSH credentials are assigned, browse (**...**) to the WhatsUp Gold Credentials Library to configure a set of credentials.

6 Click **OK** to save changes.

7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing SSH active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit SSH Active Monitor dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Command to run**. Enter the command you want to run and execute on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.

Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

§ **The monitor is considered Up if the following output ____.** Either Contains or Does not contain. Select the appropriate output criteria. For example, if you are checking to see that a specific network connection is present on the remote device, you would select that the output contains that specific connection. If the network connection you specify is not present when the monitor checks, the monitor is considered down.

§ **Use regular expression**. Select this option to have WhatsUp Gold use regular expression when searching for the output of command or script. If you do not choose to use regular expression, WhatsUp Gold looks for specific text outputs, rather than outputs including a regular expression.

§ **SSH credential**. Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials are assigned, browse (**...**) to the WhatsUp Gold Credentials Library to configure a set of credentials.

5 Click **OK** to save changes.

Adding and editing a Telnet Monitor

Telnet is a simple service monitor that checks for a Telnet server on port 23. If no telnet service responds on this port, then the service is considered down.

To add a new Telnet active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **Telnet Monitor**, then click **OK**. The Add Telnet Monitor dialog appears.
5. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
   - **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
   - **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
6. Click **OK** to save changes.
7. After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Telnet active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Select the monitor you would like to edit, then click **Edit**. The Edit Telnet Monitor dialog appears.
4. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
   - **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
   - **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
5. Click **OK** to save changes.

Using telnet to determine "Expect on Connect" string

Telnet to the desired port on the host when you are certain it is working properly, and note the host response. You can enter just an identifying portion of a `SimpleExpect` or `Expect` keyword.

For example, if you expect to get "220 hostname.domain.com Imail v1.3" back from the host, you could use "220 host" as a response string (i.e. `SimpleExpect=220 host`, or `Expect=^220 host`).

> **Note**: Some services are based on binary protocols (such as DNS) and do not provide you with a simple response string to use. You can use a packet capture tool to view these types of responses.

Adding and editing a TCPIP Monitor

The TCPIP monitor is used to monitor a TCP/IP service that either does not appear in the list of standard services, or uses a non-standard port number.

To add a new TCPIP active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **TCIPIP Monitor**, then click **OK**. The Add TCPIP Monitor dialog appears.
5. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
   - **Network type**. Select the network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP; the HTTPS monitor uses the SSL type.
   - **Port number**. Enter the TCP or UDP port that you want to monitor.
   - **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
   - **Script**. Enter your script using as many Send, Expect, SimpleExpect, and Flow Control keywords as you would like. For more information, see *Script Syntax*. (on page 171)
6. (Optional) Click **Expect** to open the Rules Expression editor. Whatever is placed in the Expression box appends to the end of the script as an Expect expression.
7. Select the **Use in Rescan** option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.
8. Click **OK** to save changes.

9 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing TCPIP active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Select the monitor you would like to edit, then click **Edit**. The Edit TCPIP Monitor dialog appears.
4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Network type**. Select the network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP; the HTTPS monitor uses the SSL type.

§ **Port number**. Enter the TCP or UDP port that you want to monitor.

§ **Timeout**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

§ **Script**. Enter your script using as many Send, Expect, SimpleExpect, and Flow Control keywords as you would like. For more information, see *Script Syntax* (on page 171).

5 (Optional) Click **Expect** to open the Rules Expression editor. Whatever is placed in the Expression box appends to the end of the script as an Expect expression.
6 Select the **Use in Rescan** option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.
7 Click **OK** to save changes.

Types of TCPIP Monitors

WhatsUp Gold is installed with the following types of TCP/IP monitors already configured.

§ **Echo**. Checks to make sure an Echo server is running on the assigned port.

§ **FTP**. Checks to make sure an FTP server is running on the assigned port.

§ **HTTP**. Checks to make sure an HTTP server is running on the assigned port.

§ **HTTPS**. Checks to make sure the Secure HTTP server is running on the assigned port, and that WhatsUp Gold can negotiate a connection using SSL protocols. This monitor does not check on the validity of SSL certificates.

§ **HTTP Content Scan**. Performs advanced monitoring of a specific web page to make sure specific content appears in the page's code. Supports advanced HTTP processes such as form submission and non-standard HTTP headers. For information on creating a basic HTTP Content Scan monitor, see New/Edit HTTP Content Monitor.

§ **IMAP4**. Checks to make sure a IMAP4 server is running on the assigned port.

- **NNTP**. Checks to make sure a NNTP server is running on the assigned port.
- **POP3**. Checks to make sure a POP3 mail server is running on the assigned port.
- **Radius**. Checks to make sure a Radius server is running on the assigned port.
- **SMTP**. Checks to make sure a SMTP mail server is running on the assigned port.
- **Time**. Checks to make sure a Time server is running on the assigned port.

Types of TCP/IP monitors

WhatsUp Gold is installed with the following types of TCP/IP monitors already configured.

- **Echo**. Checks to make sure an Echo server is running on the assigned port.
- **FTP**. Checks to make sure an FTP server is running on the assigned port.
- **HTTP**. Checks to make sure an HTTP server is running on the assigned port.
- **HTTPS**. Checks to make sure that the Secure HTTP server is running on the assigned port, and that WhatsUp Gold can negotiate a connection using SSL protocols. This monitor does not check on the validity of SSL certificates.
- **HTTP Content Scan**. Monitors a specific web page to make sure that specific content appears in the code for the page.
- **IMAP4**. Checks to make sure a IMAP4 server is running on the assigned port.
- **NNTP**. Checks to make sure a NNTP server is running on the assigned port.
- **POP3**. Checks to make sure a POP3 mail server is running on the assigned port.
- **Radius**. Checks to make sure a Radius server is running on the assigned port.
- **SMTP**. Checks to make sure a SMTP mail server is running on the assigned port.
- **Time**. Checks to make sure a Time server is running on the assigned port.

Using the Rules Expression Editor

WhatsUp Gold knows the proper connecting commands for checking the *standard* services listed on the Services dialog, but to monitor a *custom* service, you may want to specify what commands to send to the service and what responses to expect from the service in order for WhatsUp Gold to consider the service UP. You need to determine the proper command strings to expect and send for a custom service.

You can use a rule expression to test a string of text for particular patterns.

- Enter an expression in the **Expression** box. Use the **>**, **Match case**, and **Invert result** options to the right of the **Expression** box to help build the expression.
- In the **Comparison text** box, enter text to test compare against the expression you built in the **Expression** box.
- Click **Test** to compare the expression against potential payloads you can receive.

After creating and testing the expression, click **OK** to insert the string into the **Match on** box.

Note: If you have multiple payload "match on" expressions, they are linked by "OR" logic - not "AND" logic. Example: If you have two expressions, one set to "AB" and the other to "BA", it will match against a trap containing any of the following: "AB" or "BA" or "ABBA".

i) Script Syntax

You create a script using keywords. In general, Script Syntax is `Command=String`. The command is either `Send`, `Expect`, `SimpleExpect`, or `Flow Control`.

> **Note**: A script can have as many send and receive lines as needed. However, the more you have, the slower the service check.

Keywords

> **Note**: To comment out a line, use the # symbol as the first character of the line.

- To send a string to a port, use the *Send* (on page 172)= keyword.
- To expect a string from a port, use the *SimpleExpect* (on page 171)= or the *Expect* (on page 171)= keyword.
- To receive a conditional response for an error or success, use *Flow Control Keywords* (on page 174).

Examples

If you have a TCP service to check, you need to do the following:

- expect something on connection
- send a command
- check for a response
- send something to disconnect

ii) Script Syntax: Expect=Keyword

Expect=Keyword gives you flexibility to accept variable responses and pick out crucial information using special control characters and regular expressions. If you do not need flexibility, or are new to writing your own custom TCP/UDP scripts, you may want to use the *SimpleExpect* (on page 171) keyword.

There are 4 variations of the Expect Keyword:

- **Expect**. Returns true when the expected value is matched.
- **Expect(MatchCase)**. Only returns true when the case matches the expected value.
- **DontExpect**. Returns true when the value is not found.
- **DontExpect(MatchCase)**. Returns true when the value is not found.

The Expect syntax is `Expect=Response,` where the Response is either specified as an exact text string, or a mixture of *regular expression rules* (on page 175) and text. The **Add/Edit Expect Rule** button helps you construct and test a regular expression response string. It automatically chooses the variation of Expect for you based on options you select.

> **Note**: **Add/Edit Expect Rule** does not aid in the generation of SimpleExpect keywords.

WhatsUp Gold v7 or v8 users: The ~, ^, ! and = = codes have been replaced with variations on the Expect keyword itself. Migrated definitions are automatically converted.

Example 1:

```
#
# Note: script comments start with a # character
#
# Send a simple text command
#
Send = Hello There
#
# Expect a nice response that begins with, "Hi, How are you"
#
Expect=^Hi, How are you
```

Example 2:

```
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
#
# Expect a large response, but we only care to check that somewhere
# in the response John Doe is mentioned
#
Expect=John Doe
```

Example 3:

```
#
# Send a binary escape (27) and an x y and z and then a nak (21)
#
Send=\x1Bxyz\x15
#
# Expect something that does *not* contain 123 escape (27)
#
DontExpect=123\x1B
```

iii) Script Syntax: Send=Keyword

To Send command on a connection, use a Send=keyword. The script syntax is Send=Command. The Command is exactly the message you want to send. You may use a combination of literal characters and binary representations.

WhatsUp Gold understands the C0 set of ANSI 7-bit control characters. A Binary can be represented as \\x##, where the ## is a hexadecimal value. Those familiar with the table may also choose to use shorthand such as \A (\x01) or \W (\x17)

You can also use \r and \n as the conventions for sending the carriage return and line feed control characters to terminate a line.

The following table shows the keywords you can use.

Keyword	Description
\\x##	Binary value in Hexadecimal. For example, \\x1B is escape

`\\`	The "\" character
`\t`	The tab character (\x09)
`\r`	The return character (\x0D)
`\n`	The new line character \x0A)

WhatsUp Gold versions 7 and 8 users: The %### decimal syntax for specifying binary octets has been replaced with the \x## hexidecimal syntax.

Example 1:

```
#
# Note: script comments start with a # character
#
# Send a simple text command
#
Send=Hello There
```

Example 2:

```
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
```

Example 3:

```
#
# Send a binary escape (27) an x y and z and then a nak (21)
#
Send=\x1Bxyz\x15
```

iv) Script Syntax: SimpleExpect Keyword

The SimpleExpect Keyword lets you specify expected responses from a service. Responses can even be binary (i.e. non-printable ASCII character) responses. If you know exactly (or even approximately) what to expect you can construct a simple expect response string to match against.

This keyword allows you some flexibility in accepting variable responses and picking out only crucial information. If you need additional flexibility you may want to consider using the regular expression syntax available in the *Expect* (on page 171) keyword.

The SimpleExpect script syntax is `SimpleExpect=Response`, where the response is a series of characters you expect back from the service. The following table displays keywords that match logic and wildcards to compare responses byte-by-byte expanding escape codes as you go.

Command Options:

Keyword	Description
\x##	Binary value (in Hexadecimal) for example \x00 is null

.	Matches any character
\%	The "%" character
\.	The "." character
\\	The "\" character

Note: Only the number of characters specified in the expect string are used to match the response. The response is expected to start with these characters. Any extra trailing characters received are just ignored.

Example 1:

```
#
# Note: script comments start with a # character
#
# Send=Hello There
#
# Expect a nice response
#
SimpleExpect=Hi, how are you?
```

Example 2:

```
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
#
# Expect a large response, be we only care to check that first word
# received is "Customer"
#
SimpleExpect=Customer
```

Example 3:

```
#
# Send a binary escape (27) an x y and z and then a nak (21)
#
Send=\x1B\x15
#
# Expect any byte (we don't care) then an abc and an ack (6)
#
SimpleExpect=.abc\x06
```

v) Script Syntax: Flow Control Keywords

The following Flow Control keywords are used in a script to return "error" or "success" responses of steps within that script.

- **IfState**. This checks for the current state (ok or error) and jumps to a label if true.
  Valid syntax: `IfState {ERR|OK} label`
  Example:
  `IfState ERR End`
  `IfState OK Bye`
- **Goto**. This immediately jumps to a label.
  Valid syntax: `Goto End`
  Example:
  `Goto End`
- **Exit**. This immediately ends the script with an optional state (ok or error). The optional state overrides the current state.
  Valid syntax: `Exit {ERR|OK}`
  Example:
  `Exit ERR`
  `Exit OK`
- **:Label**. This defines a label that can be the target of a jump. A label is defined by a single word beginning with the ":" character.
  Valid syntax: `:`(with a name following)
  Example:
  `Bye`
- **OnError**. This allows for a global handling of an error situation
  Valid Syntax: `OnError {EXIT|CONTINUE|GOTO} label`
  Example:
  `OnError EXIT (Default behavior)`
  `OnError CONTINUE`
  `OnError GOTO Logoff`

vi) Send to Disconnect Examples

For a service like FTP, to disconnect would be `QUIT/r/n`. If a command string is not specified, the connection is closed by sending a FIN packet and then an RST packet.

The `/r` (carriage return) and `/n` (line feed) are the conventions for sending these control characters to terminate a string. You can use:

- `/r = 0x0a`
- `/n = 0x0d`
- `/t = 0x09` or `/xnn` where nn is any hexadecimal value from 00 to FF

The disconnect string is:

`Send=QUIT/r/n`

vii) Regular Expression Syntax

This table lists the meta-characters understood by the WhatsUp Gold Regex Engine.

Matching a Single Character

Meta-character	Matches
`.` dot	Matches any one character

[...]	character class	Matches any character inside the brackets. Example, [abc] matches "a", "b", and "c"
[^...]	negated character class	Matches any character except those inside the brackets. Example, [^abc] matches all characters except "a", "b", and "c". See below for alternate use - the way ^ is used controls its meaning.
-	dash	Used within a character class. Indicates a range of characters. Example: [2-7] matches any of the digits "2" through "7". Example: [0-3a-d] is equivalent to [0123abcd]
\	escaped character	Interpret the next character literally. Example: 3\.14 matches only "3.14". whereas 3.14 matches "3214", "3.14", "3z14", etc.
\\xnn	binary character	Match a single binary character. nn is a hexadecimal value between 00 and FF. Example: \\x41 matches "A" Example: \\x0B matches Vertical Tab

Quantifiers

Meta-character		Matches
?	question	One optional. The preceding expression once or not at all. Example: colou?r matches "colour" or "color" Example: [0-3][0-5]? matches "2" and "25"
*	star	Any number allowed, but are optional. Example: .* Zero or more occurrences of any character
+	plus	One required, additional are optional. Example, [0-9]+ matches "1", "15", "220", and so on
??, +?, *?		"Non-greedy" versions of ?, +, and *. Match as little as possible, whereas the "greedy" versions match as much as possible Example: For input string <html>content</html> <.*?> matches <html> <.*> matches <html>content</html>

Matching Position

Meta-character		Matches
^	caret	Matches the position at the start of the input. Example: ^2 will only match input that begins with "2".

	Example: ^[45] will only match input that begins with "4" or "5"
$ dollar	At the end of a regular expression, this character matches the end of the input. Example: >$ matches a ">" at the end of the input.

Other

Meta-character	Matches
| alternation	Matches either expression it separates. Example: H|Cat matches either "Hat" or "Cat"
(...) parentheses	Provides grouping for quantifiers, limits scope of alternation via precedence. Example: (abc)* matches 0 or more occurrences of the the string abc Example: WhatsUp (Gold)|(Professional) matches "WhatsUp Gold" or "WhatsUp Professional"
\0, \1, ... backreference	Matches text previously matched within first, second, etc, match group (starting at 0). Example: <{head}>.*?</\0> matches "<head>xxx</head>".
! negation	The expression following ! does not match the input Example: a!b matches "a" not followed by "b".

Abbreviations

Abbreviations are shorthand Meta-characters.

Abbreviation	Matches
\a	Any alphanumeric character: ([a-zA-Z0-9])
\b	White space (blank): ([\\t])
\c	Any alphabetic character: ([a-zA-Z])
\d	Any decimal digit: [0-9]
\D	Any non decimal digit: [^0-9]
\h	Any hexadecimal digit: ([0-9a-fA-F])
\n	Newline: (\r|(\r?\n))
\p	Any punctuation character: ,./\';:"!?@#$%^&*()[]{}-_=+|<>!~
\P	Any non-punctuation character
\q	A quoted string: (\"[^\"]*\")|(\'[^\']*\')
\s	WhatsUp Gold style white space character: [\\t\\n\\r\\f\\v]
\S	WhatsUp Gold style non-white space character: [^ \\t\\n\\r\\f\\v]
\w	Any word characters (letters and digits): ([a-zA-Z0-9_])
\W	Non-word character: ([^a-zA-Z0-9_])
\z	An integer: ([0-9]+)

viii) Text String Example

Example 1

To check an IRC (Internet Relay Chat) service, you can send the command `Version/r/n` and the expected response from the IRC service is: `irc`.

```
Name: IRC; Port: 6667; TCP.

Send=Version/r/n

Expect=irc

Send=QUIT/r/n
```

Note: You can use *Telnet* (on page 168) to find the proper value for **SimpleExpect**, or an **Expect** string for a particular service. Packet Capture tools can also be very useful.

Adding and editing a WAP Radio Monitor

The Wireless Access Point (WAP) Radio active monitor, included in the WhatsUp Gold Premium, Distributed, and MSP Editions, uses Simple Network Management Protocol (SNMP) to query WAP devices and report the status of the wireless access point. This monitor indicates that the wireless radio is in either an up or down state. Currently, the WAP Radio active monitor supports Cisco Aironet WAPs.

Important: The Cisco WAP you want to monitor must support Cisco Dot 11 and IEEE 802.11 MIBs for WhatsUp Gold WAP Monitor features to operate.

To determine the monitor status, the monitor first looks at the ifType (OID 1.3.6.1.2.1.2.2.1.3) value. The ifType value of 71 - IEEE 80211 must be present for the monitor to continue checking the WAP radio device status. If the ifType value is true, then the ifAdminStatus (OID: 1.3.6.1.2.1.2.2.1.7) value is checked. Finally, if the ifAdminStatus value for the interface is in the down or testing state, the active monitor is considered down and the ifOperStatus (OID: 1.3.6.1.2.1.2.2.1.8) value is checked. If the ifOperStatus value is 1 - up or 5 - dormant, the WAP radio is determined to be in the up state; otherwise the device is considered to be in the down state.

This monitor is pre-configured and exists in the Active Monitor Library upon installation of WhatsUp Gold. Unlike many pre-configured active monitors, the WAP Radio monitor's default configuration cannot be modified. However, you can modify the monitor name and description, as well as the SNMP timeout and number of retries used while attempting to connect to devices.

To add a new WAP Radio active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **WAP Radio Monitor**, then click **OK**. The New WAP Radio Monitor dialog appears.

5 Enter the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 (Optional) Click **Advanced** to set the advanced options.

7 Click **OK** to save changes.

8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing WAP Radio active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

Select the monitor you would like to edit, then click **Edit**. The Edit WAP Radio Monitor dialog appears.

3 Enter the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

4 (Optional) Click **Advanced** to set the advanced options.

5 Click **OK** to save changes.

Using Premium active monitors

WhatsUp Gold Premium Edition provides all of the network monitoring capabilities of WhatsUp Gold and extends the product to allow additional monitoring capabilities, including:

- APC UPS monitor watches your American Power Conversion Uninterruptible Power Supply (APC UPS) device and alerts you when selected thresholds are met or exceeded, output states are reached, and/or abnormal conditions are met.
- Email monitor lets you periodically verify that mail servers are not only up, but are receiving and delivering messages properly.
- Microsoft® Exchange™ and Microsoft SQL Server monitors let you manage the availability of key application services, rather than just the network visibility of the host server.
- Fan monitor checks select Cisco, Dell, and HP device fans and cooling devices, such as active and passive cooling components, to see that they are enabled and return a values that signal they are working properly.
- File Properties monitor
- Folder monitor
- FTP monitor

- HTTP Content monitor
- Network Statistics monitor
- Power Supply monitor
- PowerShell monitor
- Printer monitor
- Process monitor
- SQL Query
- SQL Server 2000 monitor
- General application monitoring using Microsoft's WMI lets you monitor any performance counter value and trigger an alarm if the value changes, goes out of range, or experiences an unexpected rate of change.

Adding and editing an APC UPS Monitor

An APC UPS monitor watches your American Power Conversion Uninterruptible Power Supply (APC UPS) device and alerts you when selected thresholds are met or exceeded, output states are reached, and/or abnormal conditions are met. For example, an alert can be sent when the UPS battery capacity is below 20%, when the battery temperature is high, when the battery is in bypass mode due to a battery overload state, and many other UPS alert conditions.

> **Note**: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new APC UPS active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **APC UPS Monitor**, then click **OK**. The Add APC UPS Monitor dialog appears.
5. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
   - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
   - **Thresholds**. Select the threshold(s) on which you want to be alerted. By default, all of the thresholds are selected for use in the monitor.
   - **Configure**. (Optional) Select to set the individual threshold settings.
   - **Monitor the following output states**. Select the output state(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the output states. By default, the following output states are selected for use in the monitor:
     - Abnormal Condition Present
     - Bad Output Voltage

- Battery Charger Failure
- Battery Communication Lost
- High Battery Temperature
- In Bypass due to Fan Failure
- In Bypass due to Internal Fault
- Low Battery
- No Batteries Attached
- Overload
- Replace Battery
- Software Bypass

Tip: Use the list's vertical scroll bar to browse the output states.

- **Monitor the following abnormal conditions**. Select the abnormal condition(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the abnormal conditions. By default, all of the abnormal conditions are selected for use in the monitor.

Tip: Use the vertical scroll bar to browse the list of abnormal conditions.

6 (Optional) Click **Advanced** to set the SNMP timeout and number of retries.
7 Click **OK** to save changes.
8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing APC UPS active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Select the monitor you would like to edit, then click **Edit**. The Edit APC UPS Monitor dialog appears.
4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Thresholds**. Select the threshold(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the thresholds. By default, all of the thresholds are selected for use in the monitor.
- **Configure**. (Optional) Select to set the individual threshold settings.
- **Monitor the following output states**. Select the output state(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the

output states. By default, the following output states are selected for use in the monitor:

- Abnormal Condition Present
- Bad Output Voltage
- Battery Charger Failure
- Battery Communication Lost
- High Battery Temperature
- In Bypass due to Fan Failure
- In Bypass due to Internal Fault
- Low Battery
- No Batteries Attached
- Overload
- Replace Battery
- Software Bypass

Tip: Use the list's vertical scroll bar to browse the output states.

- **Monitor the following abnormal conditions**. Select the abnormal condition(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the abnormal conditions. By default, all of the abnormal conditions are selected for use in the monitor.

Tip: Use the vertical scroll bar to browse the list of abnormal conditions.

5 (Optional) Click **Advanced** to set the SNMP timeout and number of retries.
6 Click **OK** to save changes.

Monitoring mail servers

The Email monitor lets you monitor that a mail server is available and functioning correctly.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

This monitor checks a mail server by first sending the server an email via SMTP. The monitor then attempts to delete previously sent emails using either POP3 or IMAP. If no emails from the monitor are present in the inbox to delete, the mail server is considered down.

The Email active monitor supports encryption with SSL/TLS and SMTP Authentication which ensures that the monitor sends emails to a secure email account.

The Email monitor's email delivery check is done across two polls. Therefore, it is important that you pick a meaningful polling interval. For example, if you want to be notified when your mail server is taking more than two minutes to send and receive email, use a two-minute polling interval.

Note: WhatsUp Gold can monitor any POP3 server that supports these commands: USER, PASS, LIST, TOP, QUIT, RETR, and DELE. WhatsUp Gold can monitor any IMAP server that supports these commands: LOGIN, SELECT, SEARCH, STORE, CLOSE, and LOGOUT.

Adding and editing an Email Monitor

Email monitors check a mail server by first sending the server an email via SMTP. The monitor then attempts to delete previously sent emails using either POP3 or IMAP. If no emails from the monitor are present in the inbox to delete, the mail server is considered down.

The email active monitor supports encryption with SSL/TLS and SMTP Authentication which ensures that the monitor sends emails to a secure email account.

✓ **Important**: You must use a separate email account for every monitor that you create. Failure to do so will result in false negatives. For example, if you want to check both IMAP and POP3 on the same server, and create two instances of the monitor, one configured with POP3 and one with IMAP, you must use two separate email accounts. Otherwise, one monitor will delete all emails previously sent from both instances of the monitor and will incorrectly report the mail server as down.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Email active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Email Monitor**, then click **OK**. The Add Email Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

Outgoing mail

- **SMTP server**. Enter the address of the server on which SMTP is running. Use the default, %Device.Address, to use the device IP address on which the monitor is attached.
- **Port**. Enter the port on which the SMTP service is listening. The standard SMTP port is 25.
- **Mail to**. Enter the address to which the Email Monitor sends email.
- **Mail from**. Enter the address you want listed as "From" in the email sent by the Email Monitor.

Incoming mail

- **Mail server**. Enter the address of the server on which the POP3 or IMAP service is running.
- **Account type**. Enter the protocol (POP3 or IMAP) you want the monitor to use to check for correct email delivery.
- **Username**. Enter the username of the account in which the monitor uses to log in.
- **Password**. Enter the password for the account in which the monitor uses to log in.
- **Advanced**. (Optional) Select to configure additional options, including authentication and encryption options by Setting Advanced Properties for an Email Active Monitor.

6 Click **OK** to save changes.

7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Email active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Email Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

Outgoing mail

- **SMTP server**. Enter the address of the server on which SMTP is running. Use the default, %Device.Address, to use the device IP address on which the monitor is attached.
- **Port**. Enter the port on which the SMTP service is listening. The standard SMTP port is 25.
- **Mail to**. Enter the address to which the Email Monitor sends email.
- **Mail from**. Enter the address you want listed as "From" in the email sent by the Email Monitor.

Incoming mail

- **Mail server**. Enter the address of the server on which the POP3 or IMAP service is running.
- **Account type**. Enter the protocol (POP3 or IMAP) you want the monitor to use to check for correct email delivery.
- **Username**. Enter the username of the account in which the monitor uses to log in.
- **Password**. Enter the password for the account in which the monitor uses to log in.
- **Advanced**. (Optional) Select to configure additional options, including authentication and encryption options by Setting Advanced Properties for an Email Active Monitor.

5 Click **OK** to save changes.

Example: Email Monitor

This example creates an Email Monitor that checks to see if an account on Google's Gmail service is working properly. To test and use the Email Monitor created in this example properly, you need a working Gmail account configured to allow POP3 and SMTP access.

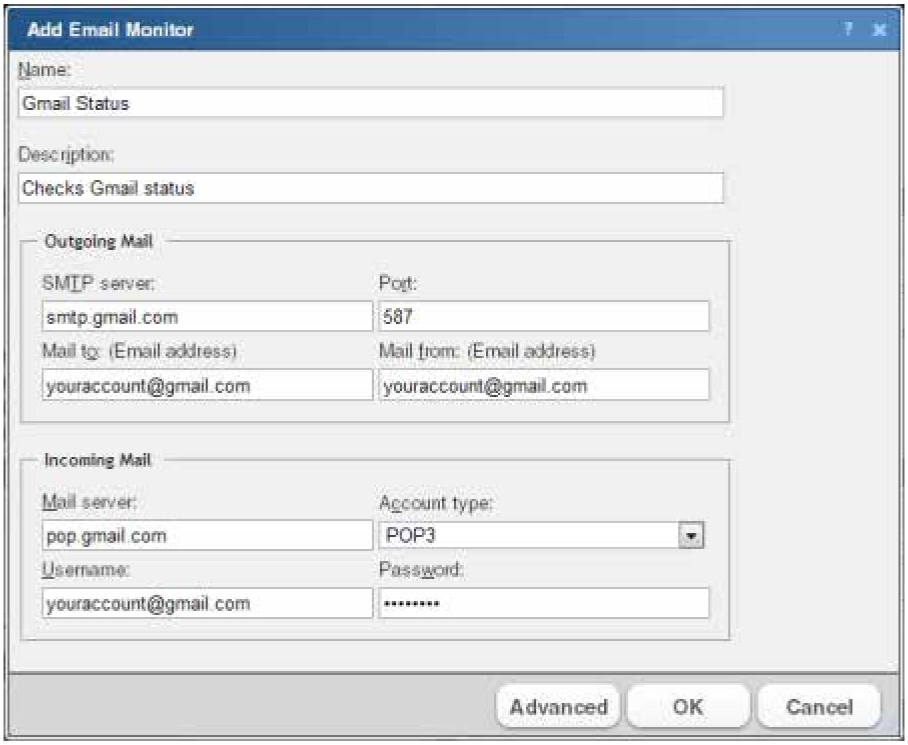
To create an Email monitor for a Gmail account:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab inside the dialog.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select the Email monitor, then click **OK**. The Add Email Monitor dialog appears.



Name: Gmail Status

Description: Checks Gmail status

SMTP server: smtp.gmail.com

Port: 587

Mail to: (Email address) youraccount@gmail.com

Mail from: (Email address) youraccount@gmail.com

Mail server: pop.gmail.com

Account type: POP3

Username: youraccount@gmail.com

Password: ••••••••

5 Enter or select the appropriate information in the dialog boxes:

a) Enter `Gmail Status` in **Name**.

b) In **Description**, enter `Checks Gmail status`.

In the **Outgoing mail** section of the dialog:

c) Enter `smtp.gmail.com` in **SMTP server**.

d) Enter `587` for the Port.

e) If you have a Gmail account, enter it in **Mail to**, in the following format: `youraccount@gmail.com`. If you do not have a Gmail account, create one on the Gmail site.

f) Enter the same Gmail account in **Mail from**.

In the **Incoming mail** section of the dialog:

g) Enter `pop.gmail.com` in the **Mail server** box.

h) Choose **POP3** from the **Account type** list.

i) Again, enter your Gmail account in **Username**.

j) Enter the password for your Gmail account in **Password**.

6 Click **Advanced**. The Advance Monitor Properties dialog appears.

7 Enter or select the appropriate information:

In the **SMTP advanced properties** section of the dialog:

a) Select **Use SMTP authentication**.

b) Enter your Gmail account in **Username**.

c) Enter the password for your Gmail account in **Password**.

d) Select **Use an encrypted connection (SSL/TLS)**.

e) Use the default **Timeout** of 5 seconds.

In the **POP3 advanced properties** section of the dialog:

f) Enter **995** for the Port

g) Select **Use an encrypted connection (Use SSL with TLS)**.

h) Use the default **Timeout** of 5 seconds.

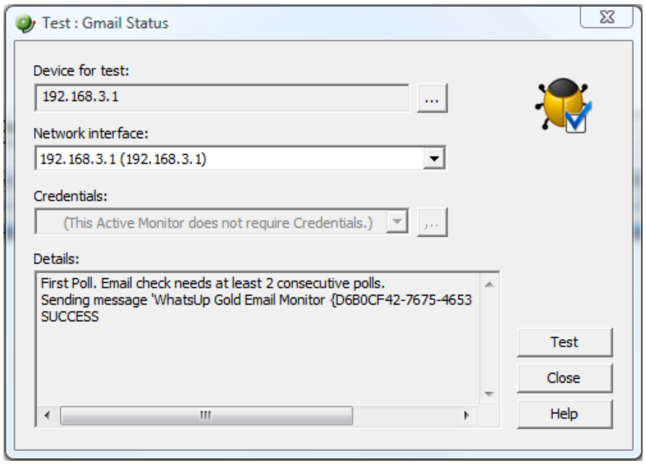
i) Click **OK** to save changes and return to the Add Email Monitor dialog.

j) Click **OK** on the Add Email Monitor dialog to add the Gmail Monitor to the Active Monitor Library.

8 Test the Gmail Status monitor.

a) From the WhatsUp Gold console, go to **Configure** > **Active Monitor Library**. The Active Monitor Library dialog appears.

b) Select the Gmail Status monitor, then click **Test**.



Test : Gmail Status

Device for test: 192.168.3.1

Network interface: 192.168.3.1 (192.168.3.1)

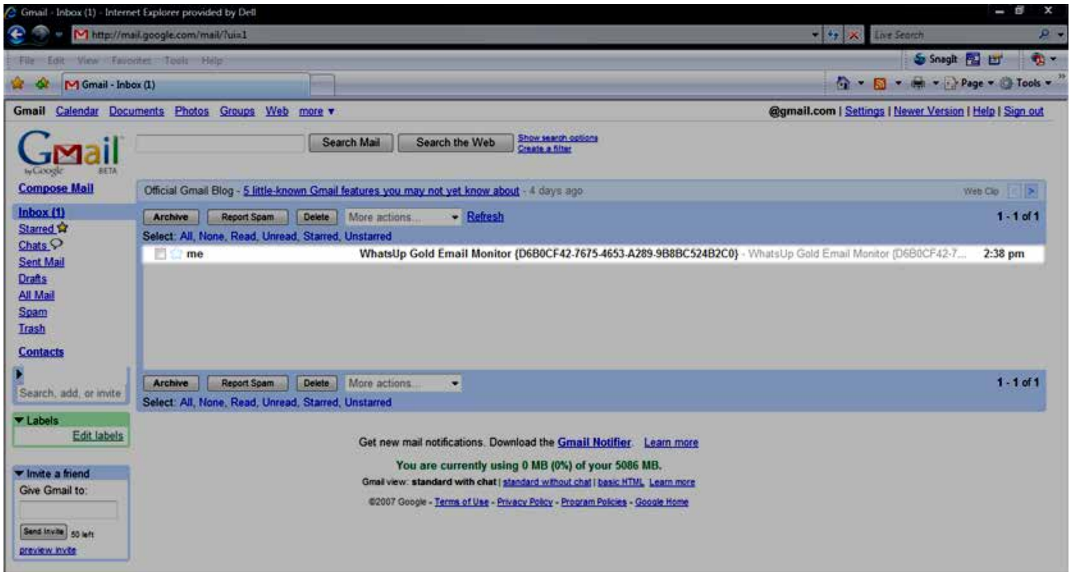
Credentials: (This Active Monitor does not require Credentials.)

Details:

```
First Poll. Email check needs at least 2 consecutive polls.
Sending message 'WhatsUp Gold Email Monitor {D6B0CF42-7675-4653
SUCCESS
```

The Test dialog will list the test as either SUCCESS or FAILED.

You can log in to the Gmail account used for the Gmail Status monitor and actually see the email sent by WhatsUp Gold via the Email Monitor.



Official Gmail Blog - 5 little-known Gmail features you may not yet know about - 4 days ago

me WhatsUp Gold Email Monitor {D6B0CF42-7675-4653-A289-9B8BC524B2C0} - WhatsUp Gold Email Monitor {D6B0CF42-7... 2:38 pm

Get new mail notifications. Download the Gmail Notifier. Learn more

You are currently using 0 MB (0%) of your 5086 MB.

Gmail view: standard with chat | standard without chat | basic HTML Learn more

©2007 Google - Terms of Use - Privacy Policy - Program Policies - Google Home

Monitoring Microsoft Exchange 2003 servers

The Exchange 2003 Monitor lets you monitor the Microsoft® Exchange™ 2003 Server applications. The Exchange 2003 monitor provides real-time information about the state and health of Microsoft Exchange servers on your network.

The Exchange 2003 Monitor supports monitoring of Microsoft Exchange Server versions 2000 and 2003, which can be on any machine in your network.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.

Why use it?

WhatsUp Gold can monitor and report the status of the standard services associated with any mail server, such as SMTP, POP3, and IMAP. If any of these services fail, your users are unable to get mail. It is a good idea to set up monitoring on these services so that you are the first to know if they fail. The Exchange Monitor extends monitoring to parameters reported by Microsoft Exchange, allowing you to get an early warning of a degradation in performance. For example, you can monitor the SMTP queues to see if performance is within an expected range, and if not, you can intervene before the SMTP service fails.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Getting Started with Exchange 2003 monitors

This topic describes the overall process for configuring an Exchange 2003 Monitor, assigning it to a device, and getting feedback from the monitor.

A basic approach to using the Exchange 2003 Monitor:

1. Determine which *Exchange 2003 parameters* (on page 189) to monitor.
2. Determine which *Exchange 2003 services* (on page 190) to monitor.
3. Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination.

   To start, it may be easier to create one monitor for each parameter or service that you want to monitor. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions. For example, a single monitor to check disk space, named Exchange2003Disk, is reported in logs with this name. If Exchange2003Disk is reported down, you know it's a disk space problem.
4. *Adding and Editing an Exchange 2003 Monitor* (on page 188) with your selected parameters and/or services.
5. Add the Exchange 2003 Monitor to the device that represents your Microsoft Exchange 2003 server.
6. Set up an Action to tell you when the monitor goes down or comes back up.

Note: The monitor is reported down if any of the parameters or services in that monitor are down.

Adding and Editing an Exchange 2003 Monitor

The Exchange active monitor lets you monitor the Microsoft® Exchange™ 2003 Server application. The Exchange 2003 Monitor provides real-time information about the state and health of Microsoft 2003 Exchange servers on your network. The Exchange 2003 Monitor supports monitoring of Microsoft Exchange Server version 2003 only, which can be on any machine in your network. To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.

Important: Use the Exchange 2003 Monitor to monitor Exchange 2003 servers only.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Exchange 2003 active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **Exchange 2003 Monitor**, then click **OK**. The New Exchange 2003 Server Monitor dialog appears.
5. Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Thresholds to monitor**. Select the thresholds you want to monitor. To configure the setting for a threshold, highlight the parameter, and click **Configure**.
- **Services to monitor**. Select the services you want to monitor. By default, all services are selected.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.

6 Click **OK** to save changes.

7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Exchange 2003 active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Exchange 2003 Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Thresholds to monitor**. Select the thresholds you want to monitor. To configure the setting for a threshold, highlight the parameter, and click **Configure**.
- **Services to monitor**. Select the services you want to monitor. By default, all services are selected.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.

5 Click **OK** to save changes.

ix) Exchange 2003 parameters

You can set thresholds on the following parameters:

Select this parameter:	If you want to:
CPU	Monitor CPU state on the Exchange host.
Memory	Monitor free memory on the Exchange host.
Disk	Monitor available disk space on the Exchange host.
System	Monitor operating system performance on the Exchange host,

	including context switches, CPU queue length, and system calls.
Links	Monitor message-handling links between mail servers. A link can contain zero or more ExchangeQueue objects, depending on the current message traffic along the link. In the Exchange System Manager, these links are called queues.
Queues	Monitor the dynamic queues created to transfer individual messages between mail servers. An ExchangeQueue is part of an ExchangeLink. ExchangeQueue objects are not the same as the queues listed in the Exchange System Manager.
Cluster	Monitor the state of the clustered resources on the Exchange server. This parameter will return a value of Unknown - 0; OK - 1; Warning - 2; Error - 3.
Custom Thresholds	Browse and select from the large number of additional parameters that Microsoft Exchange reports.

x) Exchange 2003 services

You can monitor the following critical Exchange services to determine whether the service is available (Up) or is disabled (Down).

Select this process:	**If you want to:**
Information Store	Monitor the MAPI message store service. The information store can contain messages, forms, documents, and other information created by users and applications. It provides each user with a server-based mailbox and stores public folder contents.
Site Replication Service	Monitor the Site Replication service.
Management	Monitor the Management service.
MTA Stacks	Monitor the Mail Transport Agent (MTA) service. The MTA service provides the engine for sending messages and distributing information between Microsoft Exchange Server systems or between Microsoft Exchange Server and a foreign system. Each MTA is associated with one information store. It is accessed using MAPI calls only and has no direct programmer interface with Microsoft Exchange Server. The MTA conforms to the 1988 X.400 specification.
System Attendant	Monitor the System Attendant service.
Routing Engine	Monitor the Routing Engine, which determines the routes for delivering messages to remote addresses. It forwards the message to remote Exchange addresses using SMTP. If some addresses are on a foreign messaging system, the routing engine assigns the message to a gateway that handles the address type of the recipient and passes the message to the message transfer agent (MTA).
Event	Monitor the Event service, which reports warnings and errors.
POP3	Monitor the POP3 service, which lets a mail client access mail on the server.
IMAP4	Monitor the IMAP4 service, which lets a mail client access mail on the server.

xi) Example: Exchange Server 2003 Monitor

To monitor the condition of the operating system on the Exchange server, you can create a monitor called ExchangeSystemCheck and add several parameters. The purpose of this monitor is to give an indication of the general state of the system on which your Exchange server is running. To this end, you can configure the monitor to check thresholds for the CPU, Memory, and System parameters. The monitor will also check the state of the System Attendant service.

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab inside the dialog.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Exchange 2003 Monitor** and click **OK**. The New Exchange Server 2003 Monitor dialog appears.

a) In the **Name** box, enter `ExchangeSystemCheck` to indicate that this monitor performs a check on system parameters.

b) Under **Thresholds to monitor**, select the CPU, Memory, and System parameters; then under **Services to monitor**, select the System Attendant service. Make sure these items have a check in the box to the left. Clear the selections for the other parameters and services.

c) Highlight the **CPU** parameter, then click **Configure**. The CPU Threshold dialog opens. Enter an appropriate threshold and click **OK**.

d) Highlight the **Memory** parameter, then click **Configure**. The Memory Threshold disappears. Enter an appropriate threshold for the amount of free memory and click **OK**.

e) Highlight the **System** parameter, then click **Configure**. The System Threshold dialog appears. Enter an appropriate threshold and click **OK**.

f) Click **OK** to add the ExchangeSystemCheck monitor to the Active Monitor library.

5 Add the ExchangeSystemCheck monitor to your Exchange server device.

a) In your device list, find the device that represents the Exchange server. Right-click the device, then select **Properties**. Select **Active Monitors**.

b) Click **Add**. The Active Monitor wizard appears.

c) Select the ExchangeSystemCheck monitor, and continue with the wizard to configure any actions for the monitor. For more information on setting up an action, see *Configuring an action* (on page 306).

After you complete the wizard, the monitor immediately begins to monitor the Exchange server.

Monitoring a Microsoft Exchange 2007 Server

The Exchange Monitor lets you monitor the Microsoft® Exchange™ Server application. The Exchange Monitor provides real-time information about the state and health of Microsoft Exchange servers on your network.

The Exchange Monitor supports monitoring of Microsoft Exchange Server version 2007 and later, which can be installed on any machine in your network.

Important: Do not use the Exchange Monitor to monitor Exchange 2003 servers.

To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.

Why use it?

WhatsUp Gold can monitor and report the status of the standard services associated with any mail server, such as SMTP, POP3, and IMAP. If any of these services fail, your users are unable to get mail. It is a good idea to set up monitoring on these services so that you are the first to know if they fail. The Exchange Monitor extends monitoring to parameters reported by Microsoft Exchange, allowing you to get an early warning of a degradation in performance. For example, you can monitor the SMTP queues to see if performance is within an expected range, and if not, you can intervene before the SMTP service fails.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Getting Started with Exchange monitors

This topic describes the overall process of configuring an Exchange Monitor, assigning it to a device, and getting feedback from the monitor.

A basic approach to using the Exchange Monitor:

1. Determine which *Exchange roles and performance thresholds* (on page 194) to monitor.
2. Determine which *Exchange services* (on page 194) to monitor.
3. Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination.

   To start, it may be simpler to create one monitor for each parameter or service that you want to monitor. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions.
4. *Configure an Exchange Monitor* (on page 192) with your selected parameters and/or services.
5. Add the Exchange Monitor to the device that represents your Microsoft Exchange server.
6. Set up an Action to tell you when the monitor goes down or comes back up.

Note: The monitor will be reported down if any of the parameters or services in that monitor are down.

Adding and Editing an Exchange Monitor

The Exchange active monitor lets you monitor the Microsoft® Exchange™ Server application. This monitor provides real-time information about the state and health of Microsoft Exchange servers on your network. The Exchange Monitor supports monitoring of Microsoft Exchange Server version 2007 and later, which can be on any machine in your network. To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.

Important: Do not use the Exchange Monitor to monitor Exchange 2003 servers.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Exchange active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Exchange Monitor**, then click **OK**. The New Exchange Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Performance aspects to monitor**. Select the category that matches the Exchange server role(s). Highlight the category and click **Configure** to set the individual thresholds. The threshold configuration dialog for the highlighted category opens.
- **Services to monitor**. Select the services you want to monitor.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.

6 Click **OK** to save changes.

7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

For more information on configuring an Exchange Monitor, go to *Getting Started with Exchange Monitors*.

To edit an existing Exchange active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Exchange Monitor dialog appears.

4 Enter or select the appropriate information for the following boxes:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Performance aspects to monitor**. Select the category that matches the Exchange server role(s). Highlight the category and click **Configure** to set the individual thresholds. The threshold configuration dialog for the highlighted category opens.
- **Services to monitor**. Select the services you want to monitor.
- **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using **Rescan** on the Device Properties dialog, if the protocol or service is active on the device.

5 Click **OK** to save changes.

xii) Exchange Roles and Performance Monitoring

Exchange Server Roles are used to group the performance monitoring parameters used by WhatsUp Gold to indicate the state of the Exchange server. A server role is a unit that logically groups the required features and components needed to perform a specific function in the messaging environment. By mirroring these roles in the Exchange Server monitor, the configuration of the monitor becomes a simple exercise of setting the threshold values associated with each Exchange Server Role you want to monitor.

Hub Transport Server Role thresholds

Mailbox Server Role thresholds

Outlook Web Access Server Role thresholds

xiii) Exchange Services

You can monitor the following critical Exchange services to determine if the service is available (Up) or is disabled (Down).

Select this process:	**If you want to:**
Active Directory Topology Service	Monitor the Active Directory Topology service (`MSExchangeADTopology`). This service provides Active Directory topology information to several Exchange Server components.
Anti-spam Update	Monitor the Anti-Spam Update service (`MSExchangeAntispamUpdate`). Used to automatically download anti-spam filter updates from Microsoft Update.
Edge Sync	Monitor the Edge Sync service (`MSExchangeEdgeSync`). Connects to ADAM instance on subscribed Edge Transport servers over secure Lightweight Directory Access Protocol (LDAP) channel to synchronize data between a Hub Transport server and an Edge Transport server. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
File Distribution	Monitor the File Distribution service (`MSExchangeFDS`). Used to distribute offline address book and custom Unified Messaging prompts. This service is dependent upon the Microsoft Exchange Active Directory Topology and Workstation services.
IMAP4	Monitor the IMAP4 service (`MSExchangeIMAP4`). Provides IMAP4 services to IMAP clients. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
Information Store	Monitor the MAPI Information Store service (`MSExchangeIS`). Manages Exchange Server databases. Provides data storage for messaging clients. This service is dependent upon the following services: Event Log, NT LM Security Support Provider, Remote Procedure Call (RPC), Server, and Workstation.
Mailbox Assistants	Monitor the Mailbox Assistants service (`MSExchangeMailboxAssistants).` This service provides functionality for Calendar Attendant, Resource Booking Attendant, Out of Office Assistant, and Managed Folder Mailbox Assistant. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
Mail Submission	Monitor the Mail Submission service

	(MSExchangeMailSubmission). Submits messages from a Mailbox server to a Hub Transport server. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
Monitoring	Monitor the Monitoring service (MSExchangeMonitoring). Provides a remote procedure call (RPC) server that can be used to invoke diagnostic cmdlets. This service does not have any dependencies.
POP3	Monitor the POP3 service (MSExchangePOP3). Provides POP3 services to POP3 clients. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
Replication Service	Monitor the Replication service (MSExchangeRepl). Provides log shipping functionality for local continuous replication (LCR) and cluster continuous replication (CCR). This service is dependent upon the Microsoft Exchange Active Directory Topology service.
System Attendant	Monitor the System Attendant service (MSExchangeSA). Provides monitoring, maintenance, and directory lookup services for Exchange Server. This service is dependent upon the following services: Event Log, NT LM Security Support Provider, Remote Procedure Call (RPC), Server, and Workstation.
Search Indexer	Monitor the Search Indexer service (MSExchangeSearch). Provides content to the Microsoft Search (Exchange Server) service for indexing. This service is dependent upon the Microsoft Exchange Active Directory Topology service and the Microsoft Search (Exchange Server) service.
Service Host	Monitor the Service Host service (MSExchangeServiceHost). Configures the RPC virtual directory in Internet Information Services (IIS), and registry data for ValidPorts, NSPI Interface Protocol Sequences, and AllowAnonymous for Outlook Anywhere. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
Transport	Monitor the Transport service (MSExchangeTransport). Provides Simple Message Transfer Protocol (SMTP) server and transport stack. This service is dependent upon the Microsoft Exchange Active Directory Topology service.
Transport Log Search	Monitor the Transport Log Search service (MSExchangeTransportLogSearch). Provides message tracking and transport log searching. This service has no dependencies.
Speech Engine Service	Monitor the Speech Engine service (MSSpeechService). Provides speech processing services for Unified Messaging. This service is dependent upon the Windows Management Instrumentation service.
Unified Messaging	Monitor the Unified Messaging service (MSExchangeUM). Provides Unified Messaging features, such as the storing of inbound faxes and voice mail messages in a user's mailbox, and access to that mailbox via Outlook Voice Access. This service is dependent upon the Microsoft Exchange Active Directory Topology service and the Microsoft Exchange Speech Engine service.

xiv) Example: Exchange Server monitor

To monitor the operating system on the Exchange server, you can create a monitor called ExchangeMailServer to monitor an Exchange server operating in the Mailbox Server role. The purpose of this monitor is to give an indication of the performance of the Exchange server in regards to the threshold values and services associated with the Mailbox Server role. To this end, you can configure the monitor to monitor the thresholds associated with the

Mailbox Server role, as well as to monitor the Information Store, Mailbox Assistants and Mail Submission services.

1 From the **Admin** panel, select **Monitor Library**. The Monitor Library dialog appears.

2 Click the **Active** tab.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Exchange Monitor**, then click **OK**. The New Exchange Server Monitor dialog appears.

   a) In the **Name** field, enter `ExchangeMailServer` to identify that this monitor checks system parameters.

   b) In the **Category** field, select **Mailbox Server**.

   c) Highlight the Mailbox Server role, then click **Configure**. The Configure Mailbox Server Thresholds menu appears.

   d) In the **RPC Averaged Latency must not exceed:** field, enter an appropriate threshold for the average latency for Remote Procedure Calls, then click **OK**. The New Exchange Monitor page appears.

   e) Under **Services to monitor**, select the System Attendant service. Make sure these items have a check in the box to the left. You need to clear the selections for the other parameters and also for the other processes.

   f) Click **OK** to add the `ExchangeMailServer` monitor to the Active Monitor library.

5 Add the `ExchangeMailServer` monitor to your Exchange server device.

   a) In your device list, find the device that represents the Exchange server. Right-click the device, then select **Properties**. Select **Active Monitors**.

   b) Click **Add**. The Active Monitor wizard appears.

   c) Select the `ExchangeMailServer` monitor, and continue with the wizard to configure any actions for the monitor.

   After you complete the wizard, the monitor immediately begins to monitor the Exchange server.

Adding and editing a Fan Monitor

The Fan Monitor checks select Cisco, Dell, and HP device fans and cooling devices, such as active and passive cooling components, to see that they are enabled and returning values that signal they are working properly. The monitor first checks to see if a device is a Dell, Cisco, or HP device, then checks any enabled fans and other cooling devices. If a fan is disabled, the monitor ignores it; if a fan does not return a value of 1 - Normal (for Cisco devices), 3 - OK (for Dell Servers), 1 - Normal (for Dell PowerConnect switches and routers), devices), 4 - OK (for HP ProCurve Servers), 2 - OK (for ProLiant switches and routers) the monitor is considered down.

Note: Not all types of device fans and cooling components can be monitored using the Fan Monitor. Check the make and model of your device fan or cooling component before attempting to monitor.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Fan active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Fan Monitor** , then click **OK**. The New Fan Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 (Optional) Click **Advanced** to set the advanced options.

7 Click **OK** to save changes.

8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Fan active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Fan Monitor dialog appears.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 (Optional) Click **Advanced** to set the advanced options.

6 Click **OK** to save changes.

Adding and editing a File Properties monitor

This monitor checks to see if a file in a local folder, or on a network share, meets the conditions specified in the monitor's configuration.

Note: The File Properties monitor only checks files in folders local to a device on which WhatsUp Gold is installed, or files in network shares accessible from the WhatsUp Gold device.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new File Properties active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **File Properties Monitor**, then click **OK**. The New File Properties Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Path of the file to monitor**. Enter the Universal Naming Convention (UNC) file path that WhatsUp Gold uses to access the file. For example: `\\192.168.3.1\website\product\index.htm`

✓ **Important**: Mapped drive paths are not permitted for the File Properties monitor.

6 Complete the information in the **Monitor is up if** section:

- **File**. Select the appropriate option: exists or does not exist. If you select exists, the monitor is up if the selected file is found in the folder on the local directory. If you select does not exist, the monitor is up if the file is not found in the folder on the local directory.
- **File size is**. (Optional) Click to select this check box, then:
  - Select the appropriate variable to determine the success or failure of the monitor scan, and enter a numerical value for the file size.
  - Click **File Properties** to obtain the file's current size. This current value populate the file size value field and is used to set the file size threshold.
- **Last modified date is**. (Optional) Select this option to make the monitor dependent on the date on which the file is last modified. Click to select the check box, then click **File Properties** to populate the box with the most recent date and time on which the file was modified.
- **File checksum using ____ is _____**. Select this option to make the monitor dependent on the file's checksum. Click to select the check box, then:
  - Select the algorithm (SHA1, SHA224, SHA256, SHA384, SHA512) WhatsUp Gold uses to calculate the checksum.
  - Click **File Properties** to populate the box with the file's current checksum.

Warning: Selecting this option can greatly increase the amount of time it takes to complete the monitor scan and can possibly have an adverse affect on WhatsUp Gold performance. The probability of lengthy monitor scans and slower performance increases when you use algorithms other than SHA1 when you are scanning large files, or when you scan files located on network shares.

7 Click **OK** to save changes.

8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing File Properties active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit File Properties dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Path of the file to monitor**. Enter the Universal Naming Convention (UNC) file path that WhatsUp Gold uses to access the file. For example: `\\192.168.3.1\website\product\index.htm`

✓ **Important**: Mapped drive paths are not permitted for the File Properties monitor.

5 Complete the information in the **Monitor is up if** section:

- **File**. Select the appropriate option: exists or does not exist. If you select exists, the monitor is up if the selected file is found in the folder on the local directory. If you select does not exist, the monitor is up if the file is not found in the folder on the local directory.
- **File size is**. (Optional) Click to select this check box, then:
  - Select the appropriate variable to determine the success or failure of the monitor scan, and enter a numerical value for the file size.
  - Click **File Properties** to obtain the file's current size. This current value populate the file size value box and is used to set the file size threshold.
- **Last modified date is**. (Optional) Select this option to make the monitor dependent on the date on which the file is last modified. Click to select the check box, then click **File Properties** to populate the box with the most recent date and time on which the file was modified.
- **File checksum using ____ is _____**. Select this option to make the monitor dependent on the file's checksum. Click to select the check box, then:
  - Select the algorithm (SHA1, SHA224, SHA256, SHA384, SHA512) WhatsUp Gold uses to calculate the checksum.
  - Click **File Properties** to populate the box with the file's current checksum.

! **Warning**: Selecting this option can greatly increase the amount of time it takes to complete the monitor scan and can possibly have an adverse affect on WhatsUp Gold performance. The probability of lengthy monitor scans and slower performance increases when you use algorithms other than SHA1 when you are scanning large files, or when you scan files located on network shares.

6 Click **OK** to save changes.

About file checksum

File checksums are fingerprint-like fixed data strings assigned to files when they are saved. Checksum algorithms, such as *SHA1* and *SHA512*, are used to monitor checksum files to detect accidental modification of a file, such as corruption during the storage or transmission process. These algorithms match checksums against each other to look for discrepancies; if any exist, the file is known to have been modified.

The File Properties monitor can monitor current checksum for a file to ensure that it has not been modified by matching the checksum specified in the monitor-configuration to the current checksum. If the monitor finds mismatched checksums, the file is corrupted.

Adding and editing a Folder Monitor

The Folder monitor checks to see if a local or network share folder meets the conditions specified in the monitor configuration.

Note: The Folder monitor only checks folders local to a machine on which WhatsUp Gold is installed, or folders on a network share accessible from the WhatsUp Gold device.

Note: This monitor uses the Windows credentials assigned to the device.

Note: If folder or directory contents change during a poll, the change is ignored and is not counted toward folder/file size.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Folder active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Folder Monitor**, then click **OK**. The New Folder Monitor dialog appears.

5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Path of the folder to monitor**. Enter the Universal Naming Convention (UNC) file path that WhatsUp Gold uses to access the file. For example: `\\192.168.3.1\website\product\`

§ **Include sub-folders**. Select this option to include all folders within the parent folder in the monitor scan.

Important: Selecting this option can greatly increase the amount of time it takes to complete the monitor scan and possibly have an adverse affect on WhatsUp Gold performance.

6 Select the appropriate information for the **Files to include** section:

§ **Include all files**. Select this option to include all files within the parent folder in the monitor scan.

§ **Include files with names matching following wildcard expression**. Select this option, then enter a wildcard expression. Files that match the wildcard expression are included in the monitor scan. For example, enter ***.exe** to check for executable (**.**exe) files in the selected folder.

Note: This option only works for a single wildcard expression at a time. If you enter more than one expression, the monitor reads the entry as one wildcard expression.

Important: When enabled, this option has the probability to greatly slow WhatsUp Gold performance, dependent on the wildcard expression specified. The probability of slower performance increases when this option is used in conjunction with the Include sub-folders option.

7 Select the appropriate information in the **Monitor is up if** section:

§ **Folder**. Select the appropriate option: **exists** or **does not exist**. If you select exists, the monitor is up if the selected folder is found. If you select does not exist, the monitor is up if the folder is not found.

§ For the following options, select the appropriate variables to determine the success or failure of the monitor scan:

§ **Actual folder size is**. Select this option to make the monitor dependent on the actual folder size. Click to select the check box, then:

  § Select the appropriate **Variable** to determine the success or failure of the monitor scan.

  § Click the **Folder Properties** button to populate the **Value** box.

  § Select the **Folder Size Unit** (default is bytes).

§ **Folder size on disk is**. Select this option to make the monitor dependent on the folder size on the disk. Click to select the check box, then:

  § Select the appropriate **Variable** to determine the success or failure of the monitor scan.

  § Click the **Folder Properties** button to populate the **Value** box.

  § Select the **Folder Size Unit** (default is bytes).

§ **Number of files is**. Select this option to make the monitor dependent on the number of files in the folder. Click to select the check box, then:

  § Select the appropriate **Variable** to determine the success or failure of the monitor scan.

- Click the **Folder Properties** button to populate the **Value** box.

8 Click **OK** to save changes.

9 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Folder active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Folder Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Path of the folder to monitor**. Enter the Universal Naming Convention (UNC) file path that WhatsUp Gold uses to access the file. For example: `\\192.168.3.1\website\product\`
- **Include sub-folders**. Select this option to include all folders within the parent folder in the monitor scan.

✓ **Important**: Selecting this option can greatly increase the amount of time it takes to complete the monitor scan and possibly have an adverse affect on WhatsUp Gold performance.

5 Select the appropriate information for the **Files to include** section:

- **Include all files**. Select this option to include all files within the parent folder in the monitor scan.
- **Include files with names matching following wildcard expression**. Select this option, then enter a wildcard expression. Files that match the wildcard expression are included in the monitor scan. For example, enter ***.exe** to check for executable (`.`exe) files in the selected folder.

Note: This option only works for a single wildcard expression at a time. If you enter more than one expression, the monitor reads the entry as one wildcard expression.

✓ **Important**: When enabled, this option has the probability to greatly slow WhatsUp Gold performance, dependent on the wildcard expression specified. The probability of slower performance increases when this option is used in conjunction with the Include sub-folders option.

6 Select the appropriate information in the **Monitor is up if** section:

- **Folder**. Select the appropriate option: **exists** or **does not exist**. If you select exists, the monitor is up if the selected folder is found. If you select does not exist, the monitor is up if the folder is not found.

- For the following options, select the appropriate variables to determine the success or failure of the monitor scan:
- **Actual folder size is**. Select this option to make the monitor dependent on the actual folder size. Click to select the check box, then:
  - Select the appropriate **Variable** to determine the success or failure of the monitor scan.
  - Click the **Folder Properties** button to populate the **Value** box.
  - Select the **Folder Size Unit** (default is bytes).
- **Folder size on disk is**. Select this option to make the monitor dependent on the folder size on the disk. Click to select the check box, then:
  - Select the appropriate **Variable** to determine the success or failure of the monitor scan.
  - Click the **Folder Properties** button to populate the **Value** box.
  - Select the **Folder Size Unit** (default is bytes).
- **Number of files is**. Select this option to make the monitor dependent on the number of files in the folder. Click to select the check box, then:
  - Select the appropriate **Variable** to determine the success or failure of the monitor scan.
  - Click the **Folder Properties** button to populate the **Value** box.

7 Click **OK** to save changes.

Adding and editing an FTP Monitor

The FTP active monitor performs upload, download, and delete tasks on designated FTP servers to ensure that the FTP servers are functioning properly. You can configure a single monitor to perform all three tasks, but note that if any one of the tasks fails, the entire monitor is considered down.

Note: We recommend that you create a separate FTP monitor for each FTP server you are monitoring, unless the same username and password are used for each of the servers.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new FTP active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **FTP Monitor**, then click **OK**. The Add FTP Monitor dialog appears.

5 Enter the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 Enter or select the appropriate information in the **Server Settings** section:

§ **FTP Server**. Enter the device address of the FTP server for which the FTP monitor is configured. The monitor performs tasks on this FTP server.

§ **Port**. Enter the port over which the monitor should use to connect to the FTP server. The default port is 21.

§ **Username**. Enter the username used to log in to the FTP server for which the monitor is configured.

§ **Password**. Enter the password used to log in to the FTP server for which the monitor is configured.

> **Important**: You must specify an account with the appropriate user permissions for the file actions you select. For more information, see FTP user permissions.

§ **Use Passive Mode**. Select this option to instruct WhatsUp Gold to use passive (PASV) mode as it attempts to connect to the FTP server and then to perform the selected tasks. If you do not select this option, the monitor uses Active mode. This option is selected by default. For more information, see Active and Passive modes.

7 Enter or select the appropriate information in the **File Actions** section:

§ **Upload**. Select this option to have the active monitor upload a file to the designated FTP server. This option is selected by default.

§ **Download**. Select this option to have the active monitor download a file from the designated FTP server. This option is selected by default.

§ **Delete**. Select this option to have the active monitor delete a file from the designated FTP server. This option is selected by default.

> **Note**: You cannot select the **Download** or **Delete** options if you have not selected the **Upload** option.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

§ **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.

8 Click **OK** to save changes.

9 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing FTP activ emonitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit FTP Monitor dialog appears.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 Enter or select the appropriate information in the **Server Settings** section:

§ **FTP Server**. Enter the device address of the FTP server for which the FTP monitor is configured. The monitor performs tasks on this FTP server.

§ **Port**. Enter the port over which the monitor should use to connect to the FTP server. The default port is 21.

§ **Username**. Enter the username used to log in to the FTP server for which the monitor is configured.

§ **Password**. Enter the password used to log in to the FTP server for which the monitor is configured.

Important: You must specify an account with the appropriate user permissions for the file actions you select. For more information, see FTP user permissions.

§ **Use Passive Mode**. Select this option to instruct WhatsUp Gold to use passive (PASV) mode as it attempts to connect to the FTP server and then to perform the selected tasks. If you do not select this option, the monitor uses Active mode. This option is selected by default. For more information, see Active and Passive modes.

6 Enter or select the appropriate information in the **File Actions** section:

§ **Upload**. Select this option to have the active monitor upload a file to the designated FTP server. This option is selected by default.

§ **Download**. Select this option to have the active monitor download a file from the designated FTP server. This option is selected by default.

§ **Delete**. Select this option to have the active monitor delete a file from the designated FTP server. This option is selected by default.

Note: You cannot select the **Download** or **Delete** options if you have not selected the **Upload** option.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

§ **Use in Rescan**. Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.

7 Click **OK** to save changes.

Adding and editing an HTTP Content Monitor

This monitor requests a URL and checks the HTTP response against the expected content. If the response does not return the expected content, the monitor fails. You can use this monitor to ensure that your web pages are available for viewing or that they are rendering on certain browsers. For example, you can check to see that a web page contains specific content that is to be listed after a certain date, such as "Ipswitch introduces its newest release, WhatsUp Gold v16." If the monitor does not find the content that you request it to find, the monitor fails and you know to update your web page.

Note: You can access some HTTPS sites, such as Gmail's login screen, using the HTTP content monitor.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new HTTP Content active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **HTTP Content Monitor**, then click **OK**. The Add HTTP Content Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 Enter or select the appropriate information in the **HTTP server settings** section:

§ **URL**. Enter the URL address that you want to check using the monitor. The URL must begin with a proper URI, such as http:// or https://.

Note: The URL can include the full path to the document, including the document's file name and any query string parameters. For example, http://www.domain.com/nmconsole/reports.htm?ReportID=100.

§ **Authentication username**. If required, enter the username the web site uses for authentication.

§ **Authentication password**. Enter the password that coincides with the username that the web site uses for authentication.

Note: The HTTP Content Monitor only supports basic authentication.

- **Proxy server**. If the content that you want WhatsUp Gold to check is behind a proxy server, enter the IP address of the proxy server.
- **Proxy port**. Enter the port on which the proxy server listens.
- **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

7 Enter or select the appropriate information in the **Web page content** section:

- **Web page content to find**. Enter the content you want WhatsUp Gold to look for on the web page it checks. Enter either plain text or a regular expression.
- **Use regular expression**. Select this option to use regular expression in Web page content search.

Note: The HTTP Content Monitor uses standard regular expression processing as supported by the .NET framework.

8 Complete one or more of the following actions:

- Click **Request URL contents** to populate the dialog box with the Web page contents of the URL you entered above.
- Click **Advanced** to configure the user agent and custom headers.
- Check **Use in Rescan** to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.

9 Click **OK** to save changes.

10 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing HTTP Content active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit HTTP Content Monitor dialog appears.

4 Enter the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 Enter or select the appropriate information in the **HTTP server settings** section:

- **URL**. Enter the URL address that you want to check using the monitor. The URL must begin with a proper URI, such as http:// or https://.

> **Note**: The URL can include the full path to the document, including the document's file name and any query string parameters. For example, http://www.domain.com/nmconsole/reports.htm?ReportID=100.

- **Authentication username**. If required, enter the username the web site uses for authentication.
- **Authentication password**. Enter the password that coincides with the username that the web site uses for authentication.

> **Note**: The HTTP Content Monitor only supports basic authentication.

- **Proxy server**. If the content that you want WhatsUp Gold to check is behind a proxy server, enter the IP address of the proxy server.
- **Proxy port**. Enter the port on which the proxy server listens.
- **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

6 Enter or select the appropriate information in the **Web page content** section:

- **Web page content to find**. Enter the content you want WhatsUp Gold to look for on the web page it checks. Enter either plain text or a regular expression.
- **Use regular expression**. Select this option to use regular expression in Web page content search.

> **Note**: The HTTP Content Monitor uses standard regular expression processing as supported by the .NET framework.

7 Complete one or more of the following actions:

- Click **Request URL contents** to populate the dialog box with the Web page contents of the URL you entered above.
- Click **Advanced** to configure the user agent and custom headers.
- Check **Use in Rescan** to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.

8 Click **OK** to save changes.

Example: Monitoring and alerting on web page content

The HTTP Content monitor checks a specified web page to make sure that content appears on the page. If the results of the web page content are not what is expected, you can be notified through an associated action. For example, to check whether a page is up and available, you can look for a text string contained in the web page. The following script checks for the words "WhatsUp Gold Tech Support" on the WhatsUp Gold main Support page.

```
Send=GET /support/index.aspx HTTP/1.0\r\nAccept:
*/*\r\nHost:www.whatsupgold.com\r\nUser-Agent: WhatsUp/1.0\r\n\r\n

Expect=WhatsUp Gold Tech Support
```

- If this HTTP Content monitor shows as *up*, the web page is displaying as expected.
- If this HTTP Content monitor shows as *down*, the web page is down, missing, or has been changed.

To configure a web page monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab inside the dialog.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **HTTP Content Monitor**, then click **OK**. The Add HTTP Content Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a name for the monitor as it will appear in the Active Monitor Library.
- **Description**. Enter a short description for the monitor as it will appear in the Active Monitor Library.

HTTP server settings

- **URL**. Enter the URL address that you want to check using the monitor. The URL must begin with a proper URI, such as `http://` or `https://`.

Note: The URL can include the full path to the document, including the document's file name and any query string parameters. For example, `http://www.domain.com/nmconsole/reports.htm?ReportID=100` .

- **Authentication username**. If required, enter the username the web site uses for authentication.
- **Authentication password**. Enter the password that coincides with the username that the web site uses for authentication.

Note: The HTTP Content Monitor only supports basic authentication.

- **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
- **Proxy server**. If the content that you want WhatsUp Gold to check is behind a proxy server, enter the proxy server's IP address.
- **Proxy port**. Enter the port on which the proxy server listens.

Web page content

- **Web page content to find**. Enter the content that you would like WhatsUp Gold to look for on the web page it checks. Enter either plain text or a regular expression.
- **Use regular expression**. Select this option to use regular expression in **Web page content to find**.

Note: The HTTP Content Monitor uses standard regular expression processing as supported by the .NET framework.

Note: Refer to the script above as an example for setting up a check for expected content on a specific web page URL.

To configure a web page monitor and email alert for a device:

1 Right-click the device (web server) that hosts the web page content for which you want to monitor. The Device Properties dialog appears.

2 Click **Active Monitors**. The Active Monitors dialog appears.

3 Click **Add**. The Select Active Monitor Type dialog appears.

4 Select the monitor to add to the device from the list. Look for the monitor name that you assigned to the monitor created in the previous steps. This is your HTTP Content monitor.

5 Complete the settings for the monitor:

a) Leave the default settings selected (**Enable polling for this Active Monitor** and **Use default network interface**), then click **Next**. The Setup Actions for Monitor State Changes dialog appears.

b) Select **Apply individual actions**, then click **Add**. The Select or Create Action dialog appears.

c) Select **Select an action from the Action Library**, then click **Next**. The Select Action and State dialog appears.

d) In the **Select an action from the Action Library** list, select an existing email action or click browse (**...**) to *create a new email action* (on page 311).

e) In the **Execute the actions on the following state change** list, select **Down**, and then click **Finish** to save the changes and return to the Setup Actions for State page.

f) Click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.

g) Click **Finish**. The Device Properties dialog appears.

h) Click **OK** to save changes.

The active monitor and resulting email action are now enabled. When the web page cannot return the web content, the page is triggered as down and the HTTP Content monitor fails, triggering the email action that tells you that the page is down and that the Web server cannot return web content.

Adding and editing a Network Statistics Monitor

This monitor uses Simple Network Management Protocol (SNMP) to query a device to collect data on three device protocols, Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP), and alerts you when the thresholds you specify are met or exceeded. For example, you can use the IP received discarded threshold monitor to watch for situations where a router with Quality of Service (QOS) has priorities set for Voice over IP (VoIP).

For more information, see *Example - Using a Network Statistic Monitor* to check for IP data received and discarded.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Network Statistics active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Click **New**. The Select Active Monitor Type dialog appears.
4 Select **Network Statistics Monitor**, then click **OK**. The New Network Statistics Monitor dialog appears.
5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Thresholds to monitor**. Select the IP, TCP, and/or UDP thresholds you want to monitor.

Tip: To configure individual settings, highlight a selected threshold, then click **Configure**.

Note: You can only configure one threshold at a time.

§ **Object ID**. The OID of the most recently selected parameter.

§ **Description**. The description of the most recently selected parameter.

6 Click **OK** to save changes.
7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Network Statistic active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Select the monitor you would like to edit, then click **Edit**. The Edit Network Statistic Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Thresholds to monitor**. Select the IP, TCP, and/or UDP thresholds you want to monitor.

> **Tip**: To configure individual settings, highlight a selected threshold, then click **Configure**.
>
> **Note**: You can only configure one threshold at a time.

- **Object ID**. The OID of the most recently selected parameter.
- **Description**. The description of the most recently selected parameter.

5 Click **OK** to save changes.

Example: Using a Network Statistics Monitor to check for IP data received and discarded

You can use the Network Statistics Monitor to verify that various types of packet and connection statistic information for network protocols, such as IP, TCP, and UDP, are within the thresholds that you define as acceptable. By doing so, you can ensure that devices handle specific types of network data as expected.

For example, you can use the *IP received discarded* threshold monitor to watch for situations where a router with Quality of Service (QOS) has priorities set for Voice over IP (VoIP). In these situations, other IP datagrams that a router receives are buffered for delayed processing to give processing priority to the VoIP data. If the buffer space is overrun, lower priority IP datagrams are discarded even though the router initially received them. This example describes configuring and assigning a network statistic monitor that monitors thresholds set for IP data received by a router but discarded from the buffer. It also configures and assigns an Email Action to notify you if the monitor fails.

To configure a Network Statistics Monitor:

1 From the **Admin** panel, select **Monitor Library**. The Monitor Library dialog appears.
2 If not already selected, select the **Active** tab.
3 In the Active Monitor Library, click **New**. The Select Active Monitor Type dialog appears.
4 Select **Network Statistics Monitor** from the list, and then click **OK**.
5 Type a **Name** for the monitor, such as `Cisco Router Buffer Overflow Monitor`.
6 Type a **Description** for the monitor. This description displays next to the monitor name in the Active Monitor Library.
7 In the **Thresholds to monitor** section of the dialog, select **IP received discarded**.
8 Click **OK** to save changes.

After configuring the *IP received discarded* monitor, you need to assign it to the device(s) that you want to check using the monitor. In the next steps of this example, you will assign the monitor to a single device, then using the Action Builder, configure and assign an Email Action to notify you when the monitor goes down.

Tip: You can also assign the monitor to multiple devices at one time via Bulk Field Change. For more information, see *Assigning a monitor to multiple devices* (on page 242).

To assign the IP Received Discarded monitor, and configure and assign an Email Action:

1 Go to the properties for the device to which you want to assign the monitor.

   a) From either the Device View or Map View, right-click the device. The right-click menu appears.

   b) Select **Properties**. The Device Properties dialog appears.

2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.

3 Click **Add**. The Active Monitor Properties dialog appears.

4 Select the **Cisco Router Buffer Overflow Monitor**, then click **Next**.

5 Set the monitor polling properties, then click **Next**.

6 Select **Apply individual actions**, then click **Add**. The Action Builder appears.

7 Select **Create a new action**, then click **Next**.

8 Select the **Email Action**, then click **Next**.

9 Under **Execute the action on the following state change**, select **Down**; this option specifies that WhatsUp Gold issues a state change after the monitor has detected that the router has received IP data, but the buffer has been overrun with too much data. Click **Finish**. The New Email Action dialog appears.

10 Type a **Name** for the monitor, such as `Cisco Router Buffer Overflow Monitor`.

11 Optionally, edit the description.

12 In the **SMTP Server** box, enter the IP address or Host (DNS) name of your email server (SMTP mail host).

13 Type the **Port** on which the SMTP Server is installed. The default SMTP port is 25.

14 Optionally, change the **Timeout** from the default of 5 seconds.

15 In the **Mail To** box, enter the email addresses which will receive the notification. You can enter two addresses, separated by commas (with no spaces). The address should not contain brackets, spaces, quotation marks, or parentheses.

16 Optionally, edit the address in the **Mail from** box. The address appearing here appears as the notification sender.

17 Select **SMTP server requires authentication** if your SMTP server uses authentication. This enables the Username and Password options.

18 Type a **Username** and **Password** for authentication, if necessary.

19 Select **Use an encrypted connection (SSL/TLS)** if your SMTP server requires data encryption over a TLS connection.

20 Click **Mail Content** to enter the notification content.

21 In **Subject**, enter `%ActiveMonitor.Name has failed (%Device.HostName)`. This message indicates the device type, its down state, and the hostname of the device on which the monitor has failed.

22 In **Message body**, enter

```
This %ActiveMonitor.Name has failed on %Device.Address.

Please check or restart the %Device.HostName.

-----------------------------------------
```

```
This mail was sent on %System.Date at %System.Time
Ipswitch WhatsUp Gold
```

This message indicates that the device, such as a router, has reached the threshold where IP data has overrun the buffer and should be checked or restarted.

Tip: Optionally, you can add a link to the **Device Status** or **Mobile Device Status** report for the device to which the monitor is assigned.

23 Click **OK** to save changes.

24 On the Active Monitor Properties dialog, click **Finish**.

Adding and editing a PowerShell active monitor

Windows PowerShell is a scripting language and command-line shell that system administrators can use to manage Windows operating systems. For more information on PowerShell, please visit the *Microsoft web site* (http://www.whatsupgold.com/MSPowerShell).

The PowerShell active monitor provides a platform for performing a wide variety of monitoring tasks through direct access to script component libraries, including the .NET Framework. For more information, see *PowerShell active monitor script examples* (on page 215).

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new PowerShell active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **PowerShell Active Monitor**, then click **OK**. The Add PowerShell Active Monitor dialog appears.
5. Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Timeout (Seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

Note: Although the default timeout is 60 seconds, you are discouraged from using a timeout longer than 10 seconds. Use the shortest timeout possible.

§ **Script text**. Enter your monitor code here.

6 Click **OK** to save changes.

7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing PowerShell active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit PowerShell Active Monitor dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

§ **Timeout (Seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: Although the default timeout is 60 seconds, you are discouraged from using a timeout longer than 10 seconds. Use the shortest timeout possible.

§ **Script text**. Enter your monitor code here.

5 Click **OK** to save changes.

Example - PowerShell active monitor scripts

PowerShell active monitor scripts have two instantiated objects available to support successful execution:

§ **Context**. An implementation of the IScriptContext interface. This object provides access to runtime variables and also provides mechanism for returning results to the client. A few useful methods are listed below:

§ object GetProperty(string propertyName) - allows retrieval of context variable values by name.

§ void SetResult(int resultCode) - allows the script to set a value to indicate success, usually 0 = success and 1 = failure.

§ **Logger**. An implementation of the ILog interface. This object provides the same methods available to C# applications. A few useful methods are listed below:

§ void Error(string message) - Creates an error-specific log entry that includes the message.

§ void Information(string message) - Creates an information-specific log entry that includes the message.

§ void WriteLine(string message) - Creates a generic log entry that includes the message.

Context Variables

The following context variables are available for use in PowerShell active monitor scripts:

- DeviceID
- DisplayName
- Address
- NetworkName
- Timeout
- CredWindows:DomainAndUserid
- CredWindows:Password
- CredSnmpV1:ReadCommunity
- CredSnmpV1:WriteCommunity
- CredSnmpV2:ReadCommunity
- CredSnmpV2:WriteCommunity
- CredSnmpV3:AuthPassword
- CredSnmpV3:AuthProtocol (values: 1 = None, 2 = MD5, 3 = SHA)
- CredSnmpV3:EncryptProtocol (values: 1 = None, 2 = DES56, 3 = AES128, 4 = AES192, 5 = AES256, 6 = THREEDES)
- CredSnmpV3:EncryptPassword
- CredSnmpV3:Username
- CredSnmpV3:Context
- CredADO:Password
- CredADO:Username
- CredSSH:Username
- CredSSH:Password
- CredSSH:EnablePassword
- CredSSH:Port
- CredSSH:Timeout
- CredVMware:Username
- CredVMware:Password

Script Timeout

You can configure a script timeout value (in seconds). If the script has not finished executing before the timeout value expires, it aborts.

Minimum: 1

Maximum: 60

Default: 60

Example Script

```
#
# This example looks for a process named 'outlook' and reports if its
# responding
#

# Use the built-in cmdlet named 'Get-Process', also aliased as 'ps'
$processes = ps
$processName = "outlook"
$proc = $processes | where { $_.ProcessName -match $processName }

# Active monitors must call Context.SetResult() to report results
if ($proc -eq $Null)
{
    $NotRunningMessage = "Process '" + $processName + "' is not running."
    $Context.SetResult(1, $NotRunningMessage )
}
else
{
     if ($proc.Responding)
     {
          $RespondingMessage = "Process '" + $processName + "' is responding."
          $Context.SetResult(0, $RespondingMessage )
     }
     else
    {

        $NotRespondingMessage = "Process '" + $processName + "' is not responding."

        $Context.SetResult(1, $NotRunningMessage )

    }

}
```

Adding and editing a Printer Monitor

This monitor uses SNMP to collect data on SNMP-enabled network printers. If a failure criteria is met, any associated actions fire. For example, you can monitor for printer ink levels, for a paper jam, for low input media (paper), for a fuse that is over temperature, and more.

> **Important**: In order for the Printer active monitor to work, in addition to being SNMP-enabled, the printer you are attempting to monitor must also support the Standard Printer MIB.
>
> **Note**: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Printer active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Printer Monitor**, then click **OK**. The New Printer Monitor dialog appears.

5 Enter the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 Enter or select the appropriate information in the **Failure Criteria** section:

- **If the ink level in any of the cartridges falls below___%**. Enter a numerical value for the threshold. If the ink level of any printer ink cartridge falls below this percentage, the monitor is considered down. By default, this option is not selected.
- **If the printer registers any of the following alerts**. By default, the monitor watches for all of the listed printer alerts. If you do not want to monitor a particular alert, clear its selection in the list. If the printer registers one of the selected alerts, the monitor is considered down.

> **Note**: Your printer may not support all of the SNMP objects associated with the available monitor alert checks.

7 (Optional) Click **Advanced** to set the advanced options.

8 Click **OK** to save changes.

9 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Printer active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Printer Monitor dialog appears.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 Enter or select the appropriate information in the **Failure Criteria** section:

§ **If the ink level in any of the cartridges falls below___%**. Enter a numerical value for the threshold. If the ink level of any printer ink cartridge falls below this percentage, the monitor is considered down. By default, this option is not selected.

§ **If the printer registers any of the following alerts**. By default, the monitor watches for all of the listed printer alerts. If you do not want to monitor a particular alert, clear its selection in the list. If the printer registers one of the selected alerts, the monitor is considered down.

Note: Your printer may not support all of the SNMP objects associated with the available monitor alert checks.

6 (Optional) Click **Advanced** to set the advanced options.

7 Click **OK** to save changes.

Adding and editing a Process Monitor

This monitor uses SNMP or WMI to monitor the status of device processes and issues state changes as needed. The Process Monitor can detect whether a process is running on your system. For example, you can use this monitor to verify that anti-spyware or antivirus software is running of a device. If the monitor does not find the specified program running, an associated action will notify you of this potentially harmful vulnerability.

For more information, see the example *Using the Process Monitor to Check for Antivirus Software*.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Process active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Process Monitor**, then click **OK**. The Add Process Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Protocol to Use**. Select either SNMP or WMI.
- **Advanced**. (Optional) Click to set the advanced options.
- **Process Name**. Enter name of the process or browse (**...**) to open the Select Device dialog. From here, you enter the information necessary to connect to the device from which you select a process for the monitor.

6 Completed the information for the **Threshold to Monitor** section:

- **Down if the process is**. Select this option to instruct the monitor to verify that the selected process is either not loaded, or is running, on a device, and issue a down state change accordingly.

7 Click **OK** to save changes.

8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Process active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit Process Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Protocol to Use**. Select either SNMP or WMI.
- **Advanced**. (Optional) Click to set the advanced options.
- **Process Name**. Enter name of the process or browse (**...**) to open the Select Device dialog. From here, you enter the information necessary to connect to the device from which you select a process for the monitor.

5 Completed the information for the **Threshold to Monitor** section:

- **Down if the process is**. Select this option to instruct the monitor to verify that the selected process is either not loaded, or is running, on a device, and issue a down state change accordingly.

6 Click **OK** to save changes.

Example: Using the Process Monitor to check for antivirus software

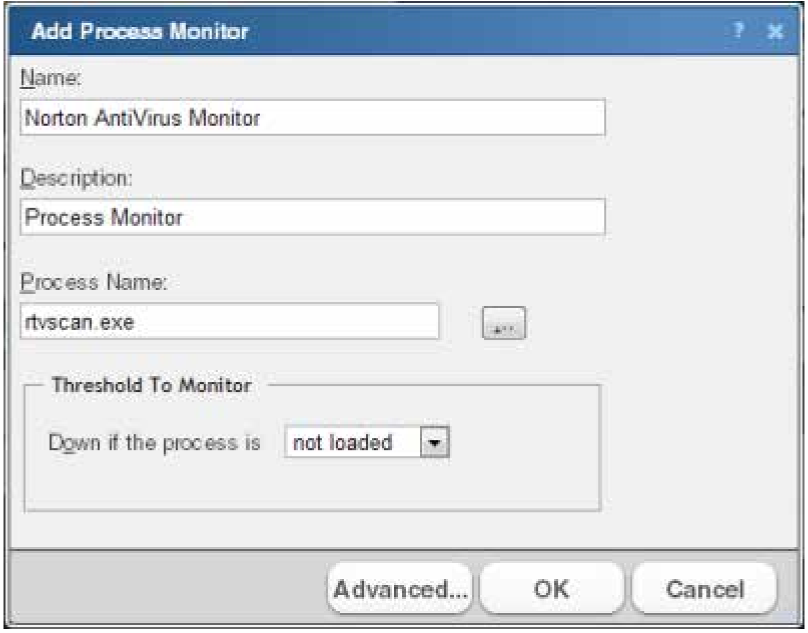
You can use the Process Monitor to verify that antivirus or anti-spyware software is a running on a device. If the monitor does not find the specified program running, an associated action notifies you of this potentially harmful vulnerability.

For this example, you will configure and assign a Process Monitor that checks to see if Norton AntiVirus™ is running on a device. You will also configure and assign an Email Action to notify you if the monitor fails.

To configure the Process Monitor:

1 In the Active Monitor Library, click **New**. The Select Active Monitor Type dialog appears.

2 Select **Process Monitor** from the list, then click **OK**. The Add Process Monitor dialog appears.



Add Process Monitor

Name: Norton AntiVirus Monitor

Description: Process Monitor

Process Name: rtvscan.exe

Threshold To Monitor

Down if the process is: not loaded

3 Enter a **Name** for the monitor, such as `Norton AntiVirus Monitor`.

4 Enter a **Description** for the monitor. This description is displayed next to the monitor name in the Active Monitor Library.

5 Type or browse (**...**) to the **Process name** that the monitor will check. To monitor Norton AntiVirus software, enter `rtvscan.exe`.

6 Under the **Thresholds to monitor** section of the dialog, select **Down if the process is** and **not loaded**. If the monitor does not find the `rtvscan.exe` process running on the device to which the monitor is assigned, the monitor is considered down.

Tip: Click **Advanced** to set the SNMP timeout and number of retries, and to decide if the monitor is used in Discovery.

7 Click **OK** to save changes.

After configuring the Norton AntiVirus Monitor, you need to assign it to the device(s) that you want to check are running the monitor. In the next steps of this example, you assign the monitor to a single device, and then, using the Action Builder, configure and assign an Email Action to notify you when the monitor goes down.

Tip: You can also assign the monitor to multiple devices at one time via Bulk Field Change. For more information, see *Assigning a monitor to multiple devices* (on page 242).

To assign the Norton AntiVirus Monitor, and configure and assign an Email Action:

1 Go to the properties for the device to which you want to assign the monitor.

§ From either the Device View or Map View, right-click the device. The right-click menu appears.

§ Select **Properties**. The Device Properties dialog appears.

2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.

3 Click **Add**. The Active Monitor Properties dialog appears.

4 Select the **Norton AntiVirus Monitor**, then click **Next**.

5 Set the monitor polling properties, then click **Next**.

6 Select **Apply individual actions**, then click **Add**. The Action Builder appears.

7 Select **Create a new action**, then click **Next**.

8 Select the **Email Action**, then click **Next**.

9 Under **Execute the action on the following state change**, select **20 minutes (Down at least 20 min).** This option specifies that WhatsUp Gold issues a state change after the monitor has been unable to find `rtvscan.exe` on the device for 20 minutes.

10 Click **Finish**. The New Email Action dialog appears.

Note: On the console, ensure that the Mail Destination tab is selected.

11 Enter a **Name** for the monitor, such as `Norton AntiVirus Email Notification`.

12 In **SMTP Mail Server**, enter the IP address or Host (DNS) name of your email server (SMTP mail host).

13 Enter the **Port** on which the SMTP Server is installed. The default SMTP port is 25.

14 Optionally, change the **Timeout** from the default of 5 seconds.

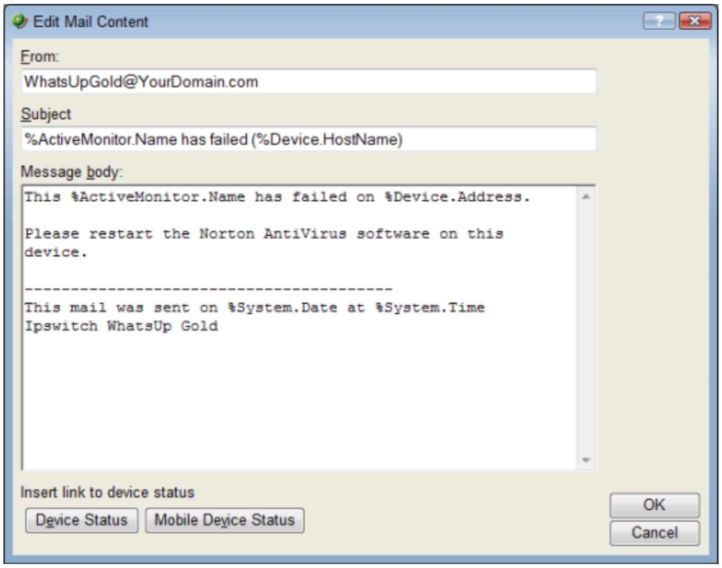
15 In **Mail To**, enter the email addresses to which you want send the notification. You can enter two addresses, separated by commas (with no spaces). The address should not contain brackets, spaces, quotation marks, or parentheses.

16 Select **SMTP server requires authentication** if your SMTP server uses authentication. This enables the **Username** and **Password** boxes.

17 Enter a **Username** and **Password** to be used with authentication.

18 Select **Use an encrypted connection (SSL/TLS)** if your SMTP server requires data encryption over a TLS connection.

19 Click **Mail Content** to enter the notification content.



From:
WhatsUpGold@YourDomain.com

Subject
%ActiveMonitor.Name has failed (%Device.HostName)

Message body:

```
This %ActiveMonitor.Name has failed on %Device.Address.

Please restart the Norton AntiVirus software on this
device.

----------------------------------------
This mail was sent on %System.Date at %System.Time
Ipswitch WhatsUp Gold
```

20 In **From**, enter the email address that will appear in the From field of the email that is sent from WhatsUp Gold.

21 In **Subject**, enter `%ActiveMonitor.Name has failed (%Device.HostName)`. This message indicates the monitor's name, its failed state, and the hostname of the device on which the monitor has failed.

22 In **Message body**, enter

```
This %ActiveMonitor.Name has failed on %Device.Address.

Please restart the Norton AntiVirus software on this device.

---------------------------------------

This mail was sent on %System.Date at %System.Time
Ipswitch WhatsUp Gold
```

This message indicates that the Norton AntiVirus software has stopped on the specified device and that it should be restarted.

Tip: Optionally, you can add a link to the **Device Status** or **Mobile Device Status** report for the device to which the monitor is assigned.

23 Click **OK** to save changes.

24 On the Active Monitor Properties dialog, click **Finish**.

Adding and editing a SQL Query active monitor

This monitor lets you check that certain conditions exist in a Microsoft SQL, MySQL, or ORACLE database, based on a database query. You can define the criteria you want to exist in the database and as long as the specified conditions are present, the SQL Query monitor is in an up state. If the database data changes outside the boundaries of the query criteria, the monitor triggers to a down state.

After the monitor is configured on this dialog, you must assign the monitor to a device through the **Device Properties > Active Monitors** dialog.

Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: To use the SQL Query monitor to monitor a MySQL database, you must first download and install the MySQL .NET Connector on the WhatsUp Gold machine. Note that only MySQL version 5.2.5 .NET Connector is supported due to compatibility issues. The connector is located on the WhatsUp Gold website (*http://www.whatsupgold.com/MySQL525Connector* (http://www.whatsupgold.com/MySQL525connector)). This link downloads the `mysql-connector-net-5.2.5.zip`file. After the file downloads, extract the `MySQL.Data.msi` and run the MySQL Connector setup utility by double-clicking on the **MySQL.Data.msi** icon. On the Choose Setup Type dialog, select **Typical**, then click **Install**. The MySQL .NET Connector is installed in the following location: `C:\Program Files\MySQL\MySQL Connector Net 5.2.5\`. After the .NET Connector has been installed, restart the WhatsUp Gold machine.

Note: The SQL Query monitor supports Windows and ADO authentication. Make sure that credentials are setup in the Credentials Library for the database for which you want to query. The credentials system stores Windows and ADO database credential information in your WhatsUp Gold database to be used when a database connection is required. For more information, see Using credentials.

Note: When connecting to a remote SQL instance, WhatsUp Gold only supports the TCP/IP network library.

To add a new SQL Query active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **SQL Query Monitor**, then click **OK**. The New SQL Query Monitor dialog appears.
5. Enter or select the appropriate information:

   - **Name**. Enter a unique name for the monitor. This name displays in the Active Monitor Library.

   - **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor name in the Active Monitor Library.

   Server Properties

   - **Server Type**. Select *Microsoft SQL Server*, *MySQL*, or *ORACLE* as the database server type.

Note: MySQL database is supported and listed as a server type option only if the MySQL 5.2.5 Connector is installed.

   - **Connection Timeout (sec)**. Enter the amount of time WhatsUp Gold waits for the server to respond before terminating the connection and returning the timeout error. Minimum allowed value is 1 second whereas maximum allowed value is 120. The default value is 15 seconds.

Note: The connection timeout setting configured by the user is used for polling only; the query builder does not use it. Instead, the query builder assumes a default of 15 seconds for the connection timeout.

- **Server Address**. Enter `ServerName\Instance` format for Microsoft SQL Server (for example, WUGServer\SQLEXPRESS), `ServerName` for MySQL (for example, WUGServer), or `ServerName/ServiceName` for Oracle (for example, WUGServer/Oracle).

Note: When using an Oracle server type, the SQL query monitor does not make use of the tsnnames.ora file on the client (i.e. WhatsUp Gold system).

- **Port (optional)**. Enter the database server port number if other than the standard database port number.

- **SQL Query to Run**. Enter a query you want to run against a database to monitor and check for certain database conditions. Only SELECT queries are allowed.

Important: Make sure that you include the full database name in your query. For query help, click **Build**. The SQL Query Builder will assist you in developing proper query syntax.

Important: The SQL query you enter must return a single numeric value. Specifically, a single record that has just one column. If the query returns more than one record, the monitor will fail to store the data. If the query returns a single record but there are multiple columns in the record returned, then the monitor will pick the first column as the value to store and this first column has to be numeric, otherwise the monitor will fail to store the data.

- **Build**. Click to open the SQL Query Builder dialog for assistance building queries.
- **Verify**. Click to check that the query is valid. If there is a syntax error with the SQL query, a message appears with tips about the syntax issue.

Monitor is up if

Important: All database rows must match the criteria settings in the **Monitor is up if** section for the monitor to be considered up. If multiple threshold criteria is used in the **Content of each retrieved row matches the following criteria**, all thresholds must match the criteria in each row.

- **Number of rows returned is**. Select this option to determine the success or failure of the monitor scan based on rows returned by the SQL query.
  For the following options, select the appropriate variables to determine the success or failure of the monitor scan:
  - **less than**
  - **less than or equal to**
  - **greater than**
  - **greater than or equal to**

- **equal to**
- **not equal to**

Enter a numeric value for number of rows in the box to the right of the conditions list.

- **Content of each retrieved row matches the following criteria**. Select to set criteria that each database row must match to determine the success or failure of the monitor scan.
  - **Add**. Click to open the New Row Content Threshold dialog. This dialog lets you set the database column values and conditions that must be matched for each table row.
  - **Edit**. Click to modify existing row criteria.
  - **Delete**. Click to remove existing row criteria.

As you specify the desired monitor criteria settings, this description updates to verbally illustrate the monitor you have configured.

6 Click **OK** to save changes.

To edit an existing SQL Query active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit SQL Query Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the monitor. This name displays in the Active Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor name in the Active Monitor Library.

Server Properties

- **Server Type**. Select *Microsoft SQL Server*, *MySQL*, or *ORACLE* as the database server type.

Note: MySQL database is supported and listed as a server type option only if the MySQL 5.2.5 Connector is installed.

- **Connection Timeout (sec)**. Enter the amount of time WhatsUp Gold waits for the server to respond before terminating the connection and returning the timeout error. Minimum allowed value is 1 second whereas maximum allowed value is 120. The default value is 15 seconds.

Note: The connection timeout setting configured by the user is used for polling only; the query builder does not use it. Instead, the query builder assumes a default of 15 seconds for the connection timeout.

- **Server Address**. Enter `ServerName\Instance` format for Microsoft SQL Server (for example, WUGServer\SQLEXPRESS), `ServerName` for MySQL (for example, WUGServer), or `ServerName/ServiceName` for Oracle (for example, WUGServer/Oracle).

Note: When using an Oracle server type, the SQL query monitor does not make use of the tsnnames.ora file on the client (i.e. WhatsUp Gold system).

- **Port (optional)**. Enter the database server port number if other than the standard database port number.
- **SQL Query to Run**. Enter a query you want to run against a database to monitor and check for certain database conditions. Only SELECT queries are allowed.

✓ **Important**: Make sure that you include the full database name in your query. For query help, click **Build**. The SQL Query Builder will assist you in developing proper query syntax.

✓ **Important**: The SQL query you enter must return a single numeric value. Specifically, a single record that has just one column. If the query returns more than one record, the monitor will fail to store the data. If the query returns a single record but there are multiple columns in the record returned, then the monitor will pick the first column as the value to store and this first column has to be numeric, otherwise the monitor will fail to store the data.

- **Build**. Click to open the SQL Query Builder dialog for assistance building queries.
- **Verify**. Click to check that the query is valid. If there is a syntax error with the SQL query, a message appears with tips about the syntax issue.

Monitor is up if

✓ **Important**: All database rows must match the criteria settings in the **Monitor is up if** section for the monitor to be considered up. If multiple threshold criteria is used in the **Content of each retrieved row matches the following criteria**, all thresholds must match the criteria in each row.

- **Number of rows returned is**. Select this option to determine the success or failure of the monitor scan based on rows returned by the SQL query.
  For the following options, select the appropriate variables to determine the success or failure of the monitor scan:
  - **less than**
  - **less than or equal to**
  - **greater than**
  - **greater than or equal to**
  - **equal to**
  - **not equal to**

Enter a numeric value for number of rows in the box to the right of the conditions list.

- **Content of each retrieved row matches the following criteria**. Select to set criteria that each database row must match to determine the success or failure of the monitor scan.
    - **Add**. Click to open the New Row Content Threshold dialog. This dialog lets you set the database column values and conditions that must be matched for each table row.
    - **Edit**. Click to modify existing row criteria.
    - **Delete**. Click to remove existing row criteria.

As you specify the desired monitor criteria settings, this description updates to verbally illustrate the monitor you have configured.

5 Click **OK** to save changes.

SQL Query Builder

This dialog assists in developing proper query syntax for SQL Query active monitors.

To use the SQL Query Builder:

1 From the Select a ADO/Windows Credential dialog, select the ADO or Windows credential you would like to use to build the query from the list or click browse (**...**) to select from the Credentials Library.

2 Click **OK**. The SQL Query Builder dialog appears.

3 Select the database you want to use to build the query in the **Database (Catalog)** box.

4 Select the database table you want to use to build the query in the **Table/View** box.

5 Select the database columns you want to use to build the query in the **Columns** box.

- **Select All**. Select this option to select all of the columns in the database table.
- **Deselect All**. Select this option to clear the selection of the columns in the database table.

Note: As you specify the database query selections, the **SQL Query** box updates to verbally illustrate the query you have configured.

6 Click **OK** to save changes.

Adding and editing a SQL Server 2000 monitor

The SQL Server 2000 monitor provides real-time information about the state and health of Microsoft SQL Server applications on your network. This monitor supports monitoring of Microsoft SQL Server 2000, and MSDE 2000 or later versions, which can be installed on any machine in your network.

Note: Although the SQL Server monitor is designed for Microsoft SQL Server 2000, some of the objects may also work with SQL Server 2005 or later.

To create custom parameters to monitor, the SQL Server host must be WMI-enabled.

WhatsUp Gold can monitor and report the status of the standard services associated with TCP/IP servers, such as SMTP, POP3, and IMAP, FTP, HTTP. If any of these services fail, users are unable to get mail, transfer files, or use the web. It is a good practice to set up monitoring on these services so you are the first to know if they fail. The SQL Server 2000 monitor extends monitoring to parameters reported by Microsoft SQL Server (and Microsoft MSDE), allowing you to get an early warning of a degradation in performance. For example, you can monitor system parameters on your SQL Server database server to see if performance is within an expected range, and if not, you can intervene before the SQL Server fails. In other words, you can detect a looming problem before it causes an application or service failure.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new SQL Server 2000 active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **SQL Server 2000 Monitor**, then click **OK**. The New SQL Server 2000 Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **SQL Server Instance Name.** Enter the name of the database you want to monitor.
- **Thresholds to monitor**. For more information about specific thresholds, see SQL Server Parameters.
- **Services to monitor**. For more information about specific services, see *SQL Server Services* (on page 231).

6 (Optional) Select **Use in rescan** to add the monitor to the Active Monitors list. From that list, you can select to scan for that service on all applications found during discovery.

7 Click **OK** to save changes.

8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing SQL Server 2000 active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit SQL Server 2000 Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **SQL Server Instance Name.** Enter the name of the database you want to monitor.
- **Thresholds to monitor**. For more information about specific thresholds, see SQL Server Parameters.
- **Services to monitor**. For more information about specific services, see *SQL Server Services* (on page 231).

5 (Optional) Select **Use in rescan** to add the monitor to the Active Monitors list. From that list, you can select to scan for that service on all applications found during discovery.

6 Click **OK** to save changes.

Getting Started with SQL Server Monitors

1 Determine which SQL parameters to monitor.

> **Note**: To use some parameters, configure your System Data Source (ODBC) name for the SQL Server. This is done in the Windows Data Sources (ODBC) administrator.

2 Determine which SQL services to monitor.

3 Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions. For example, if you create a single monitor to check disk usage, you can name it `SQLDisk` and it will be reported in logs with this name.

4 Configure an SQL Server Monitor with your selected parameters and/or services.

5 Add the SQL Monitor to the device that represents your SQL server.

6 Set up an action to tell you when the monitor goes down or comes back up.

> **Note**: The monitor is reported down if any of the parameters or services in that monitor are down.

SQL Server Parameters

You can set thresholds on the following parameters:

Select this parameter:	If you want to:
CPU	Monitor the CPU state on the SQL host.
Memory	Monitor free memory on the SQL host.
Disk	Monitor disk usage on the SQL host by the SQL server.
Disk space	Monitor free disk space on the SQL host.
System	Monitor system processes on the SQL host.
Buffers	Monitors SQL page buffers.
Cache	Monitors cache usage on the SQL server.
Locks	Monitors wait locks on the SQL server.
Transactions	Monitors the transactions on the SQL server.

Users	Monitors the users on the SQL server.
Alerts	Monitors SQL alerts and severity of alerts.
Custom Thresholds	Browse and select from the large number of additional parameters that SQL reports.

SQL Server Services

You can monitor the following critical SQL services to determine whether the service is available (Up) or is disabled (Down).

Select this process:	To monitor this function:
MSSQLSERVER	This is the database engine. It controls processes all SQL functions and manages all files that comprise the databases on the server.
SQLSERVERAGENT	This service works with the SQL Server service to create and manage local server jobs, alerts and operators, or items from multiple servers.
Microsoft Search	A full-text indexing and search engine.
Distributed Transaction Coordinator	The MS DTC service allows for several sources of data to be processed in one transaction. It also coordinates the proper completion of all transactions to make sure all updates and errors are processed and ended correctly.
SQL Server Analysis Services	Implements a highly scalable service for data storage, processing, and security.
SQL Server Reporting Services	Used to create/manage tabular, matrix, graphical, and free-form reports.
SQL Server Integration Services	A platform for building high performance data integration solutions.
SQL Server FullText Search	Issues full-text queries against plain character-based data in SQL Server tables.
SQL Server Browser	Listens for incoming requests for SQL Server resources and provides information about SQL Server instances installed on the computer.
SQL Server Active Directory Helper	View replication objects, such as a publication, and, if allowed, subscribe to that publication.
SQL Server VSS Writer	Added functionality for backup and restore of SQL Server 2005.

Example: SQL Server Monitor

The following example describes how to use the WhatsUp Gold web interface to monitor CPU utilization on a SQL Server 2000 device:

1. In the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library appears.
2. Select the **Active** tab. The Active Monitor Library appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **SQL Server 2000 Monitor**, then click **OK**. The New SQL Server 2000 Monitor dialog appears.
5. Enter `SQLCPU` in the Name box.
6. Enter the name of your database in the **SQL Server instance name** box.

7 Verify that **CPU** is the only parameter selected in the Thresholds to monitor section.

8 Select the **CPU parameter**, then click **Configure**. The CPU Threshold dialog appears.

9 Enter a **CPU percentage threshold** into the **Processor utilization must not be above** box.

10 Click **OK** to return to the New SQL Server 2000 Monitor dialog.

11 Click **OK** to return to the Active Monitor Library dialog.

12 Add the monitor to your SQL server device.

- In the device list, select the device that represents the SQL server. Right-click the device, then click **Properties**. Click Active Monitors.
- Click **Add**. The Active Monitor wizard appears.
- Select the SQLCPU monitor and continue with the wizard to configure actions for the monitor. For more information on setting up an action, see *Configuring an action* (on page 306).

Note: After you complete the wizard, the monitor immediately begins to monitor the SQL Server 2000 device.

Adding and editing a Temperature Monitor

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

The Temperature monitor checks select Cisco switches/routers, Dell servers, HP ProCurve switches/routers, and Ravica temperature probes to see that they return a value that signals they are in an up state. The monitor first checks to see if a device is a Cisco, Dell, HP, or Ravica device, then checks any enabled temperature monitor devices. If a temperature probe is disabled, the monitor ignores it; if a temperature probe does not return a value of 1 - Normal (for Cisco switches/routers), 3 - OK (for Dell server devices), 4 - Good (for HP ProCurve switches and routers), 2 - OK (for HP ProLiant servers), or 2 - normal (for Ravica temperature probes) the monitor is considered down.

This monitor is pre-configured and exists in the Active Monitor Library upon installation of WhatsUp Gold. Unlike many pre-configured active monitors, the Temperature Monitor's default configuration cannot be modified. However, you can modify the monitor name and description, as well as the SNMP timeout and number of retries used while attempting to connect to devices.

To add a new Temperature active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **Temperature Monitor**, then click **OK**. The New Temperature Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 (Optional) Click **Advanced** to set the advanced options.
7 Click **OK** to save changes.
8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing Temperature active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Select the monitor you would like to edit, then click **Edit**. The Edit Temperature Monitor dialog appears.
4 Enter the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 (Optional) Click **Advanced** to set the advanced options.
6 Click **OK** to save changes.

Adding and editing a VoIP Monitor

The VoIP Active Monitor lets you set the acceptable Mean Option Score (MOS) threshold for an IP SLA device. If the threshold is exceeded, an alert can be sent specifically to notify the appropriate network manager about the issue. For more information, see Using the WhatsUp Gold VoIP Monitor on the WhatsUp Gold web site.

Note: The WhatsUp Gold VoIP Monitor must be activated to use the VoIP Active Monitor.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new VoIP active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Active** tab. The Active Monitor list appears.
3 Click **New**. The Select Active Monitor Type dialog appears.
4 Select **VoIP Monitor**, then click **OK**. The VoIP Settings dialog appears.
5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Acceptable MOS threshold**. Use the slide bar to adjust the acceptable MOS (Mean Opinion Score) threshold.
- **Check MOS values of all jitters configured on the device**. Select this option to include all of the device RTT entries to check MOS performance thresholds. For example, if the following tags define the source and destination devices:
  - SLA 1 (Atlanta to Augusta Sat Office)
  - SLA 200 (Atlanta to Lexington)
  - SLA 300 (Atlanta to Florida Sat Office)
    then all entries are monitored for the acceptable MOS threshold compliance.
- **Only check MOS if tag contains**. Select this option to limit the device RTT entries that use this MOS performance threshold. Enter all, or a portion, of the tag used to identify the source and destination devices. For example, if the following tags define the source and destination devices:
  - SLA 1 (Atlanta to Augusta Sat Office)
  - SLA 200 (Atlanta to Lexington)
  - SLA 300 (Atlanta to Florida Sat Office)
    then if you include `Sat Office` in this box, only the source/destination devices with `Sat Office` as part of the tag entry is monitored for the acceptable MOS threshold compliance.

6 (Optional) Click **Advanced** to set the advanced options.

7 Click **OK** to save changes.

8 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing VoIP active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**. The Edit VoIP Monitor dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Acceptable MOS threshold**. Use the slide bar to adjust the acceptable MOS (Mean Opinion Score) threshold.
- **Check MOS values of all jitters configured on the device**. Select this option to include all of the device RTT entries to check MOS performance thresholds. For example, if the following tags define the source and destination devices:
  - SLA 1 (Atlanta to Augusta Sat Office)

    - SLA 200 (Atlanta to Lexington)
    - SLA 300 (Atlanta to Florida Sat Office)
      then all entries are monitored for the acceptable MOS threshold compliance.
  - **Only check MOS if tag contains**. Select this option to limit the device RTT entries that use this MOS performance threshold. Enter all, or a portion, of the tag used to identify the source and destination devices. For example, if the following tags define the source and destination devices:
    - SLA 1 (Atlanta to Augusta Sat Office)
    - SLA 200 (Atlanta to Lexington)
    - SLA 300 (Atlanta to Florida Sat Office)
      then if you include `Sat Office` in this box, only the source/destination devices with `Sat Office` as part of the tag entry is monitored for the acceptable MOS threshold compliance.

5. (Optional) Click **Advanced** to set the advanced options.
6. Click **OK** to save changes.

Adding and editing a WMI Formatted active monitor

The WMI Formatted active monitor watches for specific values on WMI enabled devices. Windows Management Instrumentation (WMI) is a Microsoft Windows standard for retrieving information from computer systems running Windows. Monitored metrics include systems resources (like CPU, disk and memory utilization) as well as specific process performance counters (like MS Exchange Mailbox and Transport server). Most Microsoft server and desktop operating systems and applications have built-in WMI support.

While similar to the WMI active monitor that uses raw data, the WMI Formatted active monitor uses calculated counter data.

Note: WMI formatted counters return data that is rounded as an integer and may be less precise than the raw data returned by the WMI active monitor.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: This monitor requires Windows credentials.

To add a new WMI Formatted active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Click **New**. The Select Active Monitor Type dialog appears.
4. Select **WMI Formatted Monitor**, then click **OK**. The Add WMI Formatted Monitor dialog appears.
5. Enter the appropriate information:
   - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.

- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

6 Click browse (**...**) to select a performance counter and instance for the monitor.

> **Note**: When WhatsUp Gold is running on Windows 2000, performance counters are not supported and do not display.

- **Check type**. Select the type of check you want the WhatsUp Gold WMI monitor to make on the performance counter selected above.
  - **Constant Value**. Monitors the performance counter/instance for a specific value. If the value changes, the monitor triggers a device state change.
  - **Range of Values**. Monitors the performance counter/instance to make sure the returned value falls within a range of values. If the value falls outside of the range, the monitor triggers a device state change.
  - **Rate of Change**. Monitors the performance counter/instance to make sure the change in value matches the rate you enter in the check values section. If the rate changes, the monitor triggers a device state change.
- **Constant Value**. The value for the designated check type.
- **Rate of Change**. The state of the device when the check value is met.

7 (Optional) Click **Advanced** to set the rescan usage information.

8 Click **OK** to save changes.

9 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing WMI Formatted active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Select the monitor you would like to edit, then click **Edit**.

4 Enter the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.

5 Click browse (**...**) to select a performance counter and instance for the monitor.

> **Note**: When WhatsUp Gold is running on Windows 2000, performance counters are not supported and do not display.

- **Check type**. Select the type of check you want the WhatsUp Gold WMI monitor to make on the performance counter selected above.
  - **Constant Value**. Monitors the performance counter/instance for a specific value. If the value changes, the monitor triggers a device state change.

  - **Range of Values**. Monitors the performance counter/instance to make sure the returned value falls within a range of values. If the value falls outside of the range, the monitor triggers a device state change.
  - **Rate of Change**. Monitors the performance counter/instance to make sure the change in value matches the rate you enter in the check values section. If the rate changes, the monitor triggers a device state change.
- **Constant Value**. The value for the designated check type.
- **Rate of Change**. The state of the device when the check value is met.

6 (Optional) Click **Advanced** to set the rescan usage information.

7 Click **OK** to save changes.

Adding and Editing a WMI Monitor

The WMI active monitor watches for specific values on WMI enabled devices. Windows Management Instrumentation (WMI) is a Microsoft Windows standard for retrieving information from computer systems running Windows. Monitored metrics include systems resources (like CPU, disk and memory utilization) as well as specific process performance counters (like MS Exchange Mailbox and Transport server). Most Microsoft server and desktop operating systems and applications have built-in WMI support.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: This monitor requires Windows credentials.

To add a new WMI active monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Active** tab. The Active Monitor list appears.

3 Click **New**. The Select Active Monitor Type dialog appears.

4 Select **WMI Monitor**, then click **OK**. The Add WMI Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
- **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
- **Performance counter/Instance**. Click browse (**...**) to select a performance counter and instance for the monitor.

Note: When WhatsUp Gold is run on Windows 2000, the performance counters are not supported and are not displayed.

- **Check type**. Select the type of check you want the WhatsUp Gold WMI monitor to make on the performance counter selected above.

    - **Constant Value**. Monitors the performance counter/instance for a specific value. If that value changes, the monitor triggers a device state change.
    - **Range of Values**. Monitors the performance counter/instance to make sure the returned value falls within a range of values. If the value falls outside of the range, the monitor triggers a device state change.
    - **Rate of Change**. Monitors the performance counter/instance to make sure the change in value matches the rate you enter in the check values section. If that rate changes, the monitor triggers a device state change.
  - **Constant Value**. The value for the designated check type.
  - **Rate of Change**. The state of the device when the check value is met.

6. (Optional) Click **Advanced** to set the Advanced Monitor Properties.
7. Click **OK** to save changes.
8. After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 240).

To edit an existing WMI active monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Active** tab. The Active Monitor list appears.
3. Select the monitor you would like to edit, then click **Edit**. The Edit WMI Monitor dialog appears.
4. Enter or select the appropriate information:
  - **Name**. Enter a unique name for the active monitor. This name displays in the Active Monitor Library.
  - **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Active Monitor Library.
  - **Performance counter/Instance**. Click browse (**...**) to select a performance counter and instance for the monitor.

> **Note**: When WhatsUp Gold is run on Windows 2000, the performance counters are not supported and are not displayed.

  - **Check type**. Select the type of check you want the WhatsUp Gold WMI monitor to make on the performance counter selected above.
    - **Constant Value**. Monitors the performance counter/instance for a specific value. If that value changes, the monitor triggers a device state change.
    - **Range of Values**. Monitors the performance counter/instance to make sure the returned value falls within a range of values. If the value falls outside of the range, the monitor triggers a device state change.
    - **Rate of Change**. Monitors the performance counter/instance to make sure the change in value matches the rate you enter in the check values section. If that rate changes, the monitor triggers a device state change.
  - **Constant Value**. The value for the designated check type.
  - **Rate of Change**. The state of the device when the check value is met.

5 (Optional) Click **Advanced** to set the Advanced Monitor Properties.

6 Click **OK** to save changes.

Troubleshooting

Having problems with your WMI monitor returning *false negatives* (on page 566)?

Using WMI monitors

This topic describes the overall process for configuring a WMI monitor, assigning it to a device, and getting feedback from the monitor.

1 Determine which WMI object you want to monitor.

2 Decide whether to create a single monitor with multiple WMI objects, several monitors with one object, or some combination.

To start, it may be simpler to create one monitor for each WMI object that you want to monitor. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions. For example, a single monitor to check errors on logon, named LogonErrors, is reported in logs with this name. If LogonErrors is reported down, you know it's a specific problem.

3 Configure a WMI Monitor with your objects.

4 Add the WMI Monitor to the device that represents your application host or server.

5 Set up an action to inform you when the monitor goes down or comes back up.

Note: The monitor is reported down if any of the objects that you select to monitor are down.

Example: WMI monitor

Imagine that a device on your network has been illegally logged into through a brute force attack (an attack where an intruder runs a script to try random usernames and passwords on a range of IP addresses on your network). These types of attacks are extremely dangerous if the device in peril is on your domain or is storing sensitive information.

You can use a custom WMI Active Monitor to check the appropriate performance counters on a Windows device and notify you when this type of attack occurs, so you can do something about it before a potential intruder gains access to your network.

To configure this type of active monitor:

1 Using the WhatsUp Gold web interface, create the WMI monitor.

a) From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

b) Click the **Active** tab inside the dialog.

c) Click **New**. The Select Active Monitor Type dialog appears.

d) Select **WMI Monitor** and click **OK**. The Add WMI Monitor dialog appears.

e) In the **Name** box, enter "ErrorsLogon" to identify that this monitor checks for logon errors.

f) Click browse (**...**) to access the Performance Counters dialog.

g) Enter the computer name or IP address of the computer in which you want to connect.

h) Select a credential from a list of Windows credentials (pulled from the Credentials Library), then click **OK** to connect to the computer.

i) Select **Server** from the **Performance object** list.

j) Under **Performance Counters**, select the **ErrorsLogon**.

k) Click **OK** to add the Performance counter to the New WMI Monitor dialog.

l) Select **Rate of Change** from the the **Check type** list.

m) In the **Rate of Change** box, enter the number of logon errors you feel is acceptable. This is the number of failed logon attempts between polls.

n) In the **If the value is above the rate, then the monitor is** box, select **Down**.

o) Click **OK** to add the active monitor to the library.

2 Enter the credentials for logging on to the device to which you will add this monitor.

a) In the Device Properties dialog for the device, select **Credentials**.

b) Select **Windows**, then click **Edit.**

c) Click browse (**...**) to access the Credentials Library.

d) Create a Windows credential using the administration login and password for the device you want to create the monitor for. When you have configured the credential, click **Close**.

e) On the Credentials page, select the new **Windows credential**, then click **OK**.

3 Add the **ErrorsLogon** monitor to the device.

a) In your device list, find the device. Double-click the device to display its properties, then click **Active Monitors**.

b) Click **Add**. The Active Monitor wizard appears.

c) Select the ErrorsLogon monitor, and continue working through the wizard to configure any actions for the monitor.
For more information on setting up an action, see *Configuring an Action* (on page 306).

Consider creating several levels of the active monitor, each with a higher threshold than the other, and with more severe actions associated with it.

For example, create a monitor with 30 as the threshold that simply sends you an email, letting you know that at least 31 attempts have been made. Next, create another monitor that uses 60 as the threshold. This monitor may have an SMS action associated with it that sends a text message to you when at least 61 attempts are made. For the most severe level you could create a 100 threshold and have the action send messages to several people who could block the IP or take the device off the network while the attack is addressed.

Assigning active monitors

After you configure an active monitor in the Active Monitor Library, you must add it to the individual devices for which you want to monitor services.

> **Note**: When you assign an active monitor to a device, an instance of the monitor is added to the device. Changes that you make to the monitor configuration via the Active Monitor Library affect all instances of the monitor. For example, if you assign a monitor to four separate devices and then make changes to the monitor from the Active Monitor Library, all four instances of the monitor adopt the changes.

To assign an active monitor to a device:

> **Note**: If you are assigning an active monitor to a device that uses WMI or SNMP credentials, before assigning an active monitor, make sure that the device has the proper credentials assigned. For more information, see *Using Credentials* (on page 68).

There are a number of ways to assign Active Monitors to devices:

To manually assign an active monitor to the device:

1. In the Device Properties Active Monitor dialog, click **Add**. The Active Monitor Properties dialog appears.
2. Select the active monitor type you want to assign to the device, then click **Next**.
3. Set the polling properties for the monitor, then click **Next**.
4. Set up *actions* (on page 346) for the monitor state changes.
5. Click **Finish** to add the monitor to the device.

To use Bulk Field Change **to add an active monitor to multiple devices:**

1. Select the devices in the device list, then right-click on one of the selected items.
2. From the right-click menu, click **Bulk Field Change > Active Monitor**.
3. Select the active monitor type you want to add.
4. Click **OK**.

Assigning a monitor from Device Properties

To assign an active monitor to a device from its properties:

1. Go to the properties for the device to which you want to assign the monitor.
    a) From either the Details View or Map View, right-click the device. The right-click menu appears.
    b) Select **Properties**. The Device Properties dialog appears.
2. Click **Active Monitors**. The Active Monitors dialog appears.
3. Click **Add**. The Active Monitor Properties dialog appears.
4. Select the active monitor type you want to assign to the device, then click **Next**.
5. Set the monitor polling properties, then click **Next**.
6. Set up the actions for the monitor state changes, then click **Finish**. The active monitor is assigned to the device.

Assigning a monitor to multiple devices

To assign an active monitor to multiple devices through Bulk Field Change:

1. From Details View, select multiple devices or a group to which you want to assign an active monitor, then right-click the selected devices or group. The right-click menu appears.
2. Click **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog appears.
3. Select the active monitor type that you want to assign, then click **OK**. The active monitor is assigned to the selected devices.

Removing and deleting active monitors

Because active monitors are assigned to devices on an individual basis, active monitors can only be removed from devices, and must be deleted from the Active Monitor Library. You also have the option to disable a monitor on the device-level, rather than completely removing it from a device. If you want to stop monitoring a particular device, but would like to keep the device-specific historical data associated with the active monitor, you should disable the monitor rather than removing it from the device.

Disabling an active monitor

To disable an active monitor from monitoring a device:

1. In the Details or Map View, right-click the device from which you want to disable polling for the active monitor. The right-click menu appears.
2. Select **Properties**. The Device Properties dialog appears.
3. Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
4. Select the monitor you want to disable, then click **Edit**. The Active Monitor Properties dialog appears.
5. Clear **Enable polling for this active monitor**, then click **Next**.
6. On the following dialog, click **Finish**.

When you return to the Device Properties - Active Monitors dialog, you will see that the monitor is disabled for the device.

Removing an active monitor

To remove an active monitor from a device:

1. From Device or Map View, right-click the device from which you want to remove the active monitor, then click **Properties**. The Device Properties dialog appears.
2. Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
3. Select the monitor you want to remove.
4. Click **Remove**. A warning dialog appears that states all data for that instance of the monitor is deleted when the monitor is removed.
5. Click **Yes** to remove the monitor.

To remove an active monitor from multiple devices:

1. Select the appropriate devices in Device View or Map View, then right-click on one of the selected items. The right-click menu appears.
2. Click **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog appears.
3. Under **Operation**, select **Remove**.

4 Under **Active Monitor type**, select the active monitor that you want to remove.

5 Click **OK** to remove the monitor from the selected devices.

About critical active monitors

Critical active monitors allow you to define a specific polling order for a device's active monitors; you can make one monitor dependent on another monitor on the same device, such as making an HTTP monitor dependent on the Ping monitor, so that you are not flooded with multiple alerts on the same device if network connectivity is lost.

In a critical monitor polling path, critical monitors are polled first. If you specify more than one critical monitor, you also specify the order in which they are polled. Critical monitors are "up" dependent on one another; if critical monitors return successful results, non-critical monitors are polled. If any of the critical monitors go down, all monitors behind it in the critical polling order are no longer polled and are placed in an unknown state for the duration of the polling cycle. If at the start of the next polling cycle, the critical monitor returns successful results, polling of successive critical monitors and non-critical monitors resumes.

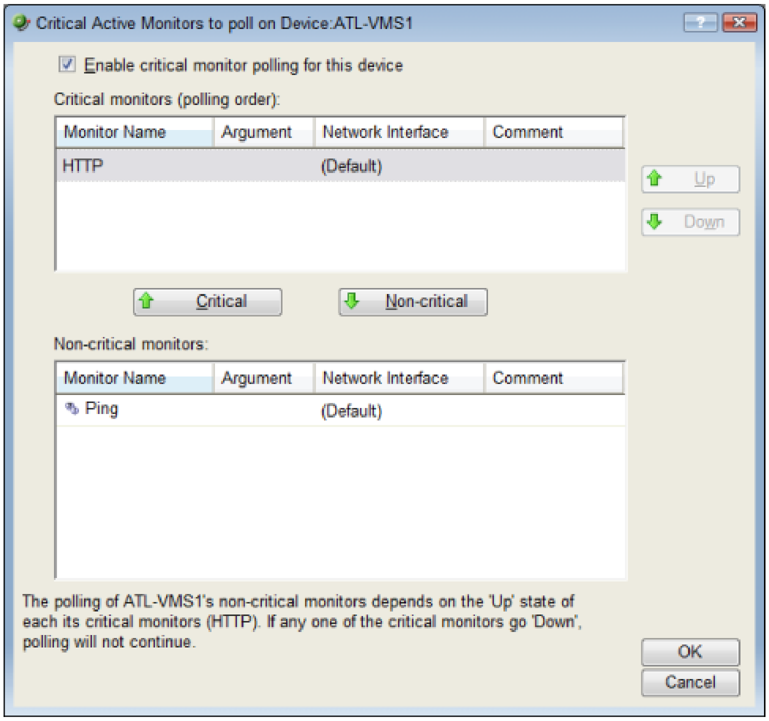
Note: Up and Down device dependencies take precedence over critical monitor polling; if WhatsUp Gold detects device dependencies, the configured dependencies are respected.

When critical monitoring is enabled, and you specify a critical polling order, you now receive only one alert when a device loses its network connectivity.

Note: When a monitor is placed in the unknown state, assigned actions are not fired. Likewise, when a monitor comes out of the unknown state into an up state, assigned actions are not fired.

Only monitors that you specify as critical follow a specific polling order; non-critical monitors are not polled in any specific order. Additionally, if multiple non-critical monitors fail, all associated actions fire.

Critical active monitors can be viewed and configured from the *Device Properties - Active Monitors* (on page 120) dialog.


Critical Active Monitors to poll on Device:ATL-VMS1
☑ Enable critical monitor polling for this device
Critical monitors (polling order):
Up
Down
Critical
Non-critical
Non-critical monitors:
OK
Cancel

Monitor Name	Argument	Network Interface	Comment
HTTP		(Default)	

Monitor Name	Argument	Network Interface	Comment
Ping		(Default)	

The polling of ATL-VMS1's non-critical monitors depends on the 'Up' state of each its critical monitors (HTTP). If any one of the critical monitors go 'Down', polling will not continue.

Note: Independent poll frequency for all monitors is ignored when a monitor is specified as critical.

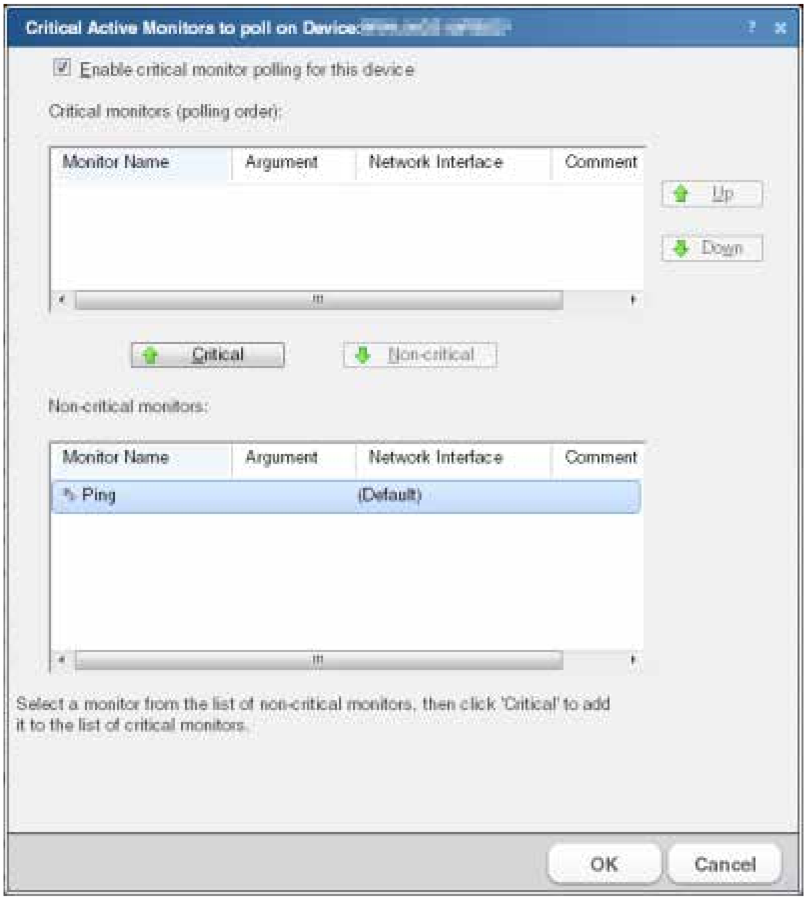
Configuring a critical polling path

To configure a critical polling path for device active monitors:

1 Right-click the device for which you want to configure a critical polling path in the Details or Map View, then click **Properties**. The Device Properties dialog appears.

2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.

3 Select an active monitor, then click **Critical**. The Critical Active Monitor properties appear.



Critical Active Monitors to poll on Device: [redacted]

☑ Enable critical monitor polling for this device

Critical monitors (polling order):

Monitor Name	Argument	Network Interface	Comment

Non-critical monitors:

Monitor Name	Argument	Network Interface	Comment
Ping		(Default)	

Select a monitor from the list of non-critical monitors, then click 'Critical' to add it to the list of critical monitors.

4 Select **Enable critical monitor polling for this device**.

5 Under the **Critical monitors** list, use the **Up** and **Down** buttons to place critical monitors in the order that you want the monitors polled. The first monitor is the first polled in the critical polling path. If the first monitor goes down, all monitors below it are not polled until the first monitor returns to an up state. If you select only one critical monitor, this is the first and only critical monitor in the critical polling path; all non-critical monitors are not polled unless the critical monitor is in the up state. Additionally, if a critical monitor fails, all subsequent critical and non-critical monitors are forced into an unknown state until the critical monitor returns to an up state.

Tip: The paragraph at the bottom of the dialog describes the critical monitor path as it is configured.

6 Under the **Non-critical monitors** list, select the monitor(s) that you would like polled first in the critical polling path, then click **Critical**.

Tip: To remove a monitor from the **Critical monitors** list, select the monitor in the **Critical monitors (polling order)** list, then click **Non-critical**.

7 Click **OK** to save changes.

Group and Device active monitor reports

The following reports display information for devices and device groups that have active monitors configured and enabled. Access these reports from the WhatsUp Gold web interface's Reports tab.

- State Change Acknowledgement
- Active Monitor Availability
- Active Monitor Outages
- Device Health
- State Change Timeline
- State Summary
- Device Status

Passive Monitor Library

In This Chapter

Passive monitors overview

Passive monitors are the WhatsUp Gold feature responsible for listening for device events. As active monitors actively query or poll devices for data, passive monitors passively listen for device events. Because passive monitors do not poll devices, they use less network bandwidth than active monitors.

Passive monitors are useful because they gather information that goes beyond simple Up or Down service and device states by listening for a variety of events. For example, if you want to know when someone with improper credentials tries to access one of your SNMP-enabled devices, you can assign the default AuthenticationFailure passive monitor. The monitor listens for an authentication failure trap on the SNMP device, and logs these events to the SNMP Trap Log. If you assign an action to the monitor, every time the authentication failure trap is received, you are notified as soon as it happens.

Although passive monitors are useful, you should not rely on them solely to monitor a device or service—passive monitors should be used in conjunction with active monitors. When used together, active and passive monitors make up a powerful and crucial component of 360-degree network management.

Passive monitor types are specific configurations of SNMP traps, Windows Log Events, and Syslog Events. After the monitor types are configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog.

Using the Passive Monitor Library, you can:

- Click **New** to create a new passive monitor.
- Select a monitor type in the list, then click **Edit** to change the settings.
- Select a monitor type in the list, then click **Copy** to create a new monitor type based on the selected type.
- Select a monitor type, then click **Delete** to remove it from the list.

Successful passive monitors

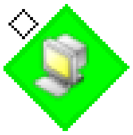
Creating a successful passive monitor requires that you take several steps:

> **Important**: Before you attempt to create a passive monitor, you should know the specific traps (and coinciding MIBs) for which you want WhatsUp Gold to listen—this makes the process much easier.

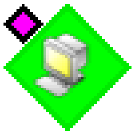
1. Turn on traps on the device from which you want to receive logs, entries, and/or alerts.
2. Point the traps on that device to the WhatsUp Gold machine.
3. Enable the WhatsUp Gold *Passive Monitor Listeners* (on page 249).
4. Create a passive monitor for each of the traps for which you want WhatsUp Gold to listen.
5. Assign the passive monitor to the device on which you want to listen for traps.

Additionally, after you create a passive monitor, you can configure alerts to notify you when a particular trap is received.

Passive Monitors Icon



When a passive monitor is configured on a device, the device icon displays a diamond shape on the upper left side.



This shape changes color when an unacknowledged state change occurs on the monitor. After the device has been acknowledged, the icon returns to the above appearance.

Using the Passive Monitor Library

The Passive Monitor Library stores all passive monitor types that have been created for WhatsUp Gold. The library includes a variety of pre-configured SNMP passive monitors, as well as a generic "Any" passive monitor for SNMP, Syslog, and Windows Event Log types. The Any passive monitor listens and receives *all* traps and events that occur on the device to which it is assigned.

Though you can create three types of passive monitors, SNMP passive monitors are the type most widely used.

SNMP Trap passive monitors in the library

The SNMP Trap monitors listed in the Passive Monitor Library are based on one of three things:

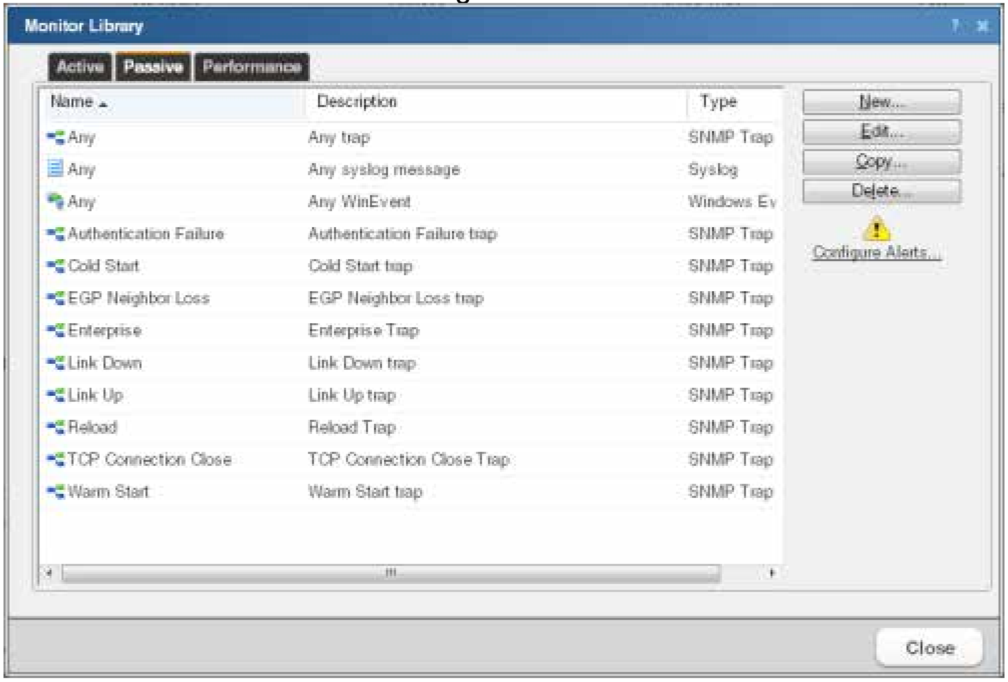
§ **Passive monitors already in the database**. By default, the passive monitor database comes with a few of the most Common SNMP traps already in it.

- **Passive monitors automatically created by WhatsUp Gold Trap Definition Import Tool**. Use the Trap Definition Import Tool to create SNMP Traps from MIB files stored in the `\Program Files\Ipswitch\WhatsUp\Data\Mibs` folder.
- **Passive monitors that you define yourself.** This can be done either by copying and pasting actual trap information directly from your existing logs, or by browsing the MIB for OID values that you are interested in, and adding the **Generic type (Major)** and **Specific type (Minor)** information if required.

To access and use the Passive Monitor Library:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Passive** tab inside the dialog.



Name	Description	Type
Any	Any trap	SNMP Trap
Any	Any syslog message	Syslog
Any	Any WinEvent	Windows Ev
Authentication Failure	Authentication Failure trap	SNMP Trap
Cold Start	Cold Start trap	SNMP Trap
EGP Neighbor Loss	EGP Neighbor Loss trap	SNMP Trap
Enterprise	Enterprise Trap	SNMP Trap
Link Down	Link Down trap	SNMP Trap
Link Up	Link Up trap	SNMP Trap
Reload	Reload Trap	SNMP Trap
TCP Connection Close	TCP Connection Close Trap	SNMP Trap
Warm Start	Warm Start trap	SNMP Trap

Use the Passive Monitor Library dialog to configure new or existing passive monitor types:

- Click **New** to create a new passive monitor type.
- Select a monitor type in the list, then click **Edit** to change the settings.
- Select a monitor type in the list, then click **Copy** to create a new monitor type based on the selected type.
- Select a monitor type, then click **Delete** to remove it from the list.

Understanding Passive Monitor Listeners

A Passive Monitor Listener is the component in passive monitors that listens for events to occur. When an event occurs, the listener notifies WhatsUp Gold and associated actions are fired.

WhatsUp Gold in installed with three Passive Monitor Listeners:

- **SNMP Trap Listener**. This listens for SNMP traps, or unsolicited SNMP messages, that are sent from a device to indicate a change in status.

- **Syslog Trap Listener**. This listens for Syslog messages forwarded from devices regarding a specific record and/or text within a record.
- **Windows Event Log Listener**. This listens for any WinEvent; for example a service start or stop, or logon failures.

Important: Before you can configure passive monitors, you must configure the coinciding Passive Monitor Listener(s) on the WhatsUp Gold console via Program Options. For more information, see Enabling the SNMP Trap listener, Enabling the Syslog listener, and Enabling the Windows Event Log listener.

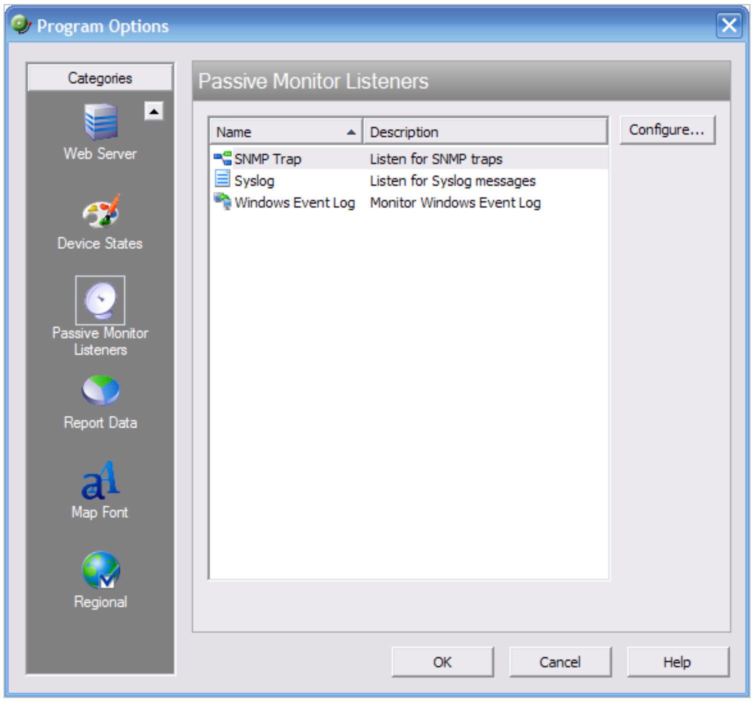
Configuring the SNMP Trap Listener

To configure the SNMP Trap Listener:

1 From the WhatsUp Gold console main menu, click **Configure > Program Options**. The Program Options dialog appears.

Note: If the Windows SNMP Trap Service (**Control Panel** > **Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.



Program Options

Passive Monitor Listeners

Name	Description
SNMP Trap	Listen for SNMP traps
Syslog	Listen for Syslog messages
Windows Event Log	Monitor Windows Event Log

3 Select the SNMP Trap listener, then click **Configure**. The SNMP Listener Configuration dialog appears.

4 Enter or select the appropriate information in the following fields:

- **Listen for messages on port**. Select this option if you want WhatsUp Gold to listen for SNMP traps. The standard SNMP trap port is 162, but you can change this port to a non-standard port number.

Note: When you change the port number, the change takes place as soon as you save the change; you do not have to re-start WhatsUp Gold for the change to take effect.

- **Accept unsolicited SNMP traps**. Select this option to receive and log all incoming SNMP traps, including those not assigned to devices as passive monitors. By default, SNMP traps assigned to devices as passive monitors are logged and can trigger actions. Incoming traps received as unsolicited traps are logged to the System SNMP Trap Log.

Caution: When this option is selected, every SNMP trap that is received by WhatsUp Gold is logged to the database. Enabling this option can result in a large database that impacts performance; we strongly advise that you leave this option disabled, except when you are troubleshooting.

Note: To configure SNMP traps initially, we recommend enabling the **Any** SNMP trap on the source device; you can then see all incoming traps sent from that device in the Device SNMP Trap Log. After you configure the trap successfully, you should disable the **Any** trap, as it may also log large amounts of data.

- **Forward traps**. Select this option to forward traps to the IP address(es) you specify in **Forward traps to**.
- **Forward unsolicited traps**. Select this option to forward all traps, including unsolicited traps.
- **Forward traps to**. Click Add to add in IP address and port to which to forward traps.

Note: You can forward traps to multiple IP addresses.

Tip: You can **Edit** and/or **Remove** IP addresses from this list.

5 Click **OK** to save changes.

Configuring the Syslog Listener

WhatsUp Gold has an internal SNMP trap handler, which when enabled, listens for and accepts SNMP traps. WhatsUp Gold records the trap in the device's **SNMP Trap Log**.

To configure WhatsUp Gold to receive traps:

1 On the devices that are to be monitored, set the SNMP agent to send traps to WhatsUp Gold. Trap manager addresses must be set on each physical device. This cannot be done from WhatsUp Gold.

2 Set up the MIB entries for traps by placing the MIB text file in the `C:\Program Files\Ipswitch\WhatsUp\Data\Mibs` directory.

3 Enable the SNMP Trap Handler.

To configure the Syslog Passive Monitor Listener:

1 From the WhatsUp Gold console main menu, click **Configure > Program Options**. The Program Options dialog appears.

Note: If the Windows SNMP Trap Service (**Control Panel** > **Services**) is running on the WhatsUp Gold console system, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listener Configure display in a list.

3 Click **Syslog**, then click **Configure**. The Syslog Listener Configuration dialog appears.

4 Enter or select the appropriate information in the following fields:

§ **Listen for messages on port**. Select this option if you want WhatsUp Gold to listen for Syslog messages.The Syslog Listener runs on port 514 by default, but can be changed if necessary.

§ **Accept unsolicited passive monitors**. If option this is cleared, ONLY Syslog entries which are specifically added to devices as passive monitors are logged to the System Syslog report. If you select this option, ALL incoming Syslog messages are detected and logged to the System Syslog report.

Note: Regardless of this filter setting, only Syslog messages that are solicited are logged to the devices' Syslog reports and are able to trigger actions.

5 Click **OK** to save changes.

Configuring the Windows Event Log Listener

To configure the Windows Event Log Listener:

1 From the WhatsUp Gold console main menu, click **Configure > Program Options**. The Program Options dialog appears.

Note: If the Windows SNMP Trap Service (**Control Panel** > **Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.

3 Select the Windows Event Log Listener, then click **Configure**. The Windows Event Log Listener Configuration dialog appears.

4 Enter or select the appropriate information in the following fields:

§ **Start Server**. Select this option if you would like WhatsUp Gold to listen for Windows Event logs.

§ **Do not generate payload**. Select this option to only add the event time and message to the Windows Event Log; the payload is withheld from the entry.

§ **Check connections interval**. Select this option to have WhatsUp Gold check for and close inactive connections at the interval you specify. The default interval is 60 seconds.

5 Click **OK** to save changes.

Configuring passive monitors

You can configure passive monitors two ways:

1 Automatically using the Trap Definition Import Tool.

2 Manually using the Passive Monitor Library.

The Trap Definition Import Tool allows you to search for the specific SNMP trap for which you want WhatsUp Gold to listen, and then import that trap into the Passive Monitor Library. After you import the trap, you can make specifications to the passive monitor in the Passive Monitor Library using the Rules Expression Editor dialog. For example, if you want WhatsUp Gold to monitor when a specific IP address causes an authentication failure on your SNMP-enabled device, you would create a rule that tells WhatsUp Gold to log an event only when that particular IP address attempts to access the SNMP-enabled device.

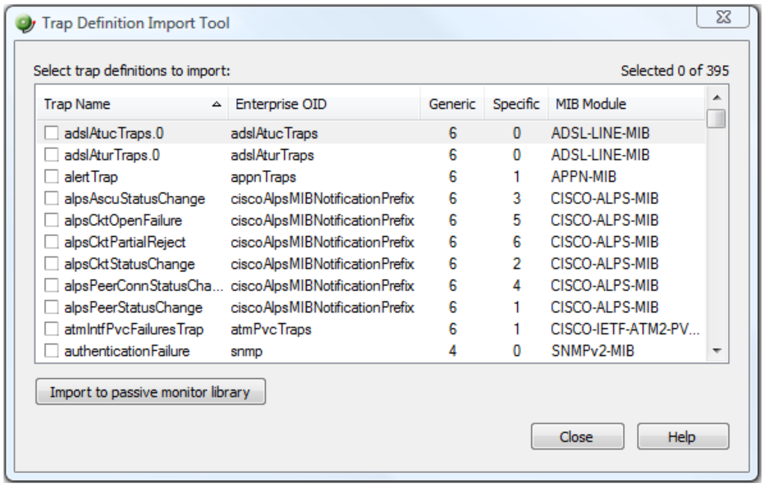
While using the Trap Definition Import Tool or any of the pre-configured passive monitors are two easy ways to configure SNMP Trap passive monitors, you still have the option to manually configure all passive monitor types via the Passive Monitor Library.

Using the Trap Definition Import Tool

The Trap Definition Import tool is used to import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your WhatsUp Gold MIB folder (`\Program Files\Ipswitch\WhatsUp\Data\Mibs`).

To import SNMP trap definitions into the Passive Monitor Library:

1 In the WhatsUp Gold console, click **Tools > Import Trap Definitions**. The Trap Definition Import Tool dialog appears.



Select trap definitions to import:

Selected 0 of 395

Trap Name	Enterprise OID	Generic	Specific	MIB Module
□ adslAtucTraps.0	adslAtucTraps	6	0	ADSL-LINE-MIB
□ adslAturTraps.0	adslAturTraps	6	0	ADSL-LINE-MIB
□ alertTrap	appnTraps	6	1	APPN-MIB
□ alpsAscuStatusChange	ciscoAlpsMIBNotificationPrefix	6	3	CISCO-ALPS-MIB
□ alpsCktOpenFailure	ciscoAlpsMIBNotificationPrefix	6	5	CISCO-ALPS-MIB
□ alpsCktPartialReject	ciscoAlpsMIBNotificationPrefix	6	6	CISCO-ALPS-MIB
□ alpsCktStatusChange	ciscoAlpsMIBNotificationPrefix	6	2	CISCO-ALPS-MIB
□ alpsPeerConnStatusCha...	ciscoAlpsMIBNotificationPrefix	6	4	CISCO-ALPS-MIB
□ alpsPeerStatusChange	ciscoAlpsMIBNotificationPrefix	6	1	CISCO-ALPS-MIB
□ atmIntfPvcFailuresTrap	atmPvcTraps	6	1	CISCO-IETF-ATM2-PV...
□ authenticationFailure	snmp	4	0	SNMPv2-MIB

2 Select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog appears and provides a message about the import results.

Note: Traps that already exist in the database are not imported.

Tip: Use the dialog's scroll bar to scan available traps.

Using the Passive Monitor Library

You can use the Passive Monitor Library to manually create new instances of a passive monitor type, or to edit the configuration of monitors you import using the Trap Definition Import Tool.

Adding and editing an SNMP Trap Passive monitor

To add or edit an SNMP trap passive monitor:

1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.

2 Click the **Passive** tab. The Passive Monitor list appears.

3 Click **New** and select **SNMP Trap** from the list to create a new SNMP trap passive monitor.
- or -
Select the SNMP trap passive monitor you want to change from the list of current monitors , and then click **Edit**.

4 Complete the information for the following boxes.

§ **Name**. Enter a name for the monitor. This name displays in the Passive Monitor Library.

§ **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Passive Monitor Library.

§ **Enterprise/OID**. Use **Browse** to select the desired object identifier (OID) from the Enterprise section of the MIB. This is the SNMP enterprise identifier in the trap, which is used for unique identification of traps for a particular application. If you specify the OID in this box, then an incoming trap matches this rule only if the trap enterprise box begins with the OID that you have specified. If you are unsure of the OID to use, or you do not need to be specific, you can leave this box blank and it is ignored.

Note: This option is only available if **Generic Type** is set to **6-EnterpriseSpecific**.

§ **Generic Type (Major)**. Each trap has a generic type number. This number is part of the rule that determines the matching criteria for an incoming trap. For more information, see Common SNMP Traps.

Note: The definitions of 0 through 6 are not WhatsUp Gold definitions, but come from the SNMP specifications.

§ **Specific Type (Minor)**. This can have an integer value from 0 to 4294967296. To use this option, **Generic Type** must be always enterprise-specific. If you want to ignore this box, select **Any**.

§ **Payload**. Click **Add** to view the Expression Editor where you can create an expression, test it, and compare it to potential payloads. After creating an expression, click **OK** to insert that string into the list under **Match On**.

5 Click the **Add** button to view the Expression Editor where you can create an expression, test it, and compare it against potential payloads you can receive. After creating the expression, click **OK** to insert that string into the **Match on** box.

Note: If you have multiple payload "match on" expressions, they are linked by "OR" logic—not "AND" logic. If you have two expressions, one set to "AB" and the other to "BA", it matches against a trap containing any of the following: "AB" or "BA" or "ABBA".

6 Click **OK** to add the monitor to the Passive Monitor Library.

After configuring a passive monitor in the Passive Monitor Library, *add the monitor to devices* (on page 257).

Adding and Editing a Syslog Monitor

To add or edit a Syslog monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Passive** tab. The Passive Monitor list appears.
3 Click **New** and select **Syslog** from the list to create a new Syslog monitor. Click **OK**.
- or -
Select the Syslog monitor you want to change from the list of current monitors, and then click **Edit**.
4 Enter or select the appropriate information in the following boxes.

§ **Name**. Enter a name for the monitor. This name displays in the Passive Monitor Library.

§ **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Passive Monitor Library.

§ **Match On**. You can click the **Add** button to access the *expression editor* (on page 170), where you can create your expression, test it, and compare it against potential payloads you can receive. After creating the expression, click **OK** to insert that string into the **Match on** box.

Note: If you have multiple payload "match on" expressions, they are linked by "OR" logic - not "AND" logic. Example: If you have two expressions, one set to "AB" and the other to "BA", it will match against a trap containing any of the following: "AB" or "BA" or "ABBA".

5 Click **OK** to list this event in the Passive Monitor Library as a Syslog Passive Monitor.

After configuring a passive monitor in the Passive Monitor Library, *add the monitor to devices* (on page 257).

For an example of why you might create a Syslog Event, see *Sample of a Syslog Monitor Event* (on page 255).

xv) Sample of a Syslog Monitor (Event)

Investigating Messages to Monitor:

The user is having trouble with a particular service on a remote system, but is not sure how to catch the problem. He does know the name of the service which is causing the problem (which is “TROUBLE”), but he does not know the content of the messages it logs. The service runs on a UNIX system.

He creates a Syslog message event called "Trouble Daemon Events." He sets it to match any facility and any severity and puts the following in the string to match: TROUBLE

This matches all messages coming from the service named TROUBLE, which is the one he is investigating.

He then applies this passive monitor to any device where the TROUBLE service is running. Since we are just investigating, no actions are created for this monitor. Instead, the end result is to review the Syslog Log at the end of the month and look for TROUBLE messages that might be used to create more specific passive monitors.

Adding and Editing a Windows Event Log Monitor

When assigning a Windows Event Log passive monitor to a device, make sure the device has credentials assigned to it before creating the passive monitor. To use multiple Windows Event Log passive monitors, assign a unique Windows Event Log passive monitor for each device.

The upgrade process to WhatsUp Gold from previous versions automatically migrates Windows Event Log passive monitor credentials into the Credentials Library. If you experience upgrade problems with Windows Event Log passive monitors, look in the Credentials Library for the Windows (WMI) credentials that work for the device. If the device credentials do not exist, create new credentials for the device.

To add or edit a Windows Event Log monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Passive** tab. The Passive Monitor list appears.

3 Click **New** and select **Windows Event Log** to create a new Windows Event Log monitor. Click **OK**.
- or -
Select the Windows Event Log monitor you want to change from the list of current monitors, and then click **Edit**.

4 Complete the information for the following boxes.

§ **Name**. Enter a name for the monitor. This name displays in the Passive Monitor Library.

§ **Description**. Enter a short description for the monitor. This description displays next to the monitor in the Passive Monitor Library.

§ **Condition**. Enter a list of conditions to match. Only log entries matching these expressions are converted to events. Conditions are processed sequentially from top to bottom. As each condition is evaluated, its results are applied to the next condition until all conditions are evaluated. For complex sets of conditions involving both ANDs and ORs, this serial logic may produce different results than intended. As a best practice, we recommend keeping conditions simple by opting for multiple Passive Monitors over complex sets of conditions. When complex conditions are unavoidable, we recommend grouping all OR conditions together at the beginning of the set of conditions, followed by the ANDs.

§ Click **Edit** to add or edit a condition or **Clear** to remove a condition from the box.

§ **Match On**. You can click the **Add** button to access the *expression editor* (on page 170), where you can create your expression, test it, and compare it against potential payloads you can receive. After creating the expression, click **OK** to insert that string into the **Match On** list.

Note: If you have multiple payload **Match On** expressions, they are linked by OR logic, not AND logic. For example, if you have two expressions, one set to "AB" and the other to "BA", it is matched against any log entry that includes either of the two strings.

5 Click **OK** to save changes.

After configuring a passive monitor in the Passive Monitor Library, *add the monitor to devices* (on page 257).

Using the Any Passive Monitor

The Any passive monitor receives *all* type-specific (SNMP, Syslog, Windows Event Log) traps and events sent from the device to which it is assigned. This monitor can be useful when you are trying to pinpoint the specific trap and coinciding MIB for which you want to WhatsUp Gold to listen and monitor. As the monitor gathers traps and events, this data is added to the respective log (SNMP Trap Log, Syslog Entries, Windows Event Log). You can scan the report entries to find the specific trap that you would like to monitor, and create a passive monitor for that specific trap.

If, after running the monitor for some time, you do not notice the trap for which you are looking, the MIB may not be loaded in the WhatsUp Gold MIB directory. If this is the case, import the MIB. For more information, see Using the SNMP MIB Manager.

Important: Because of the volume of data gathered when this monitor is enabled, we strongly advise that this monitor only be used for troubleshooting purposes. If this monitor is enabled for more than short periods of time, you run the risk of flooding your database and compromising the performance of WhatsUp Gold.

As the monitor has been pre-configured for you, to use it, you are required only to assign it to the device for which you researching traps and events. For more information, see *Assigning passive monitors* (on page 257).

It is important that you remember to remove the monitor when you have completed troubleshooting because of the monitor's potential to fill up the WhatsUp Gold database.

Assigning passive monitors

After you configure a passive monitor in the Passive Monitor Library, you must add it to the individual devices for which you want to monitor services.

Note: If you are assigning a Windows Event Log passive monitor type to a device, make sure that the device has credentials assigned before creating a passive monitor for it. For more information, see *Using Credentials* (on page 68).
If want to use multiple Windows Event Log passive monitors, you must assign a unique Windows Event Log passive monitor for each device.

Note: The upgrade process to WhatsUp Gold from previous versions, automatically migrates Windows Event Log passive monitor credentials into the Credentials Library. If you experience upgrade problems with Windows Event Log passive monitors, look in the credentials library for the Windows (WMI) credentials that will work for the device. If the device credentials do not exist, create new credentials for the device. For more information, see *Using Credentials* (on page 68).

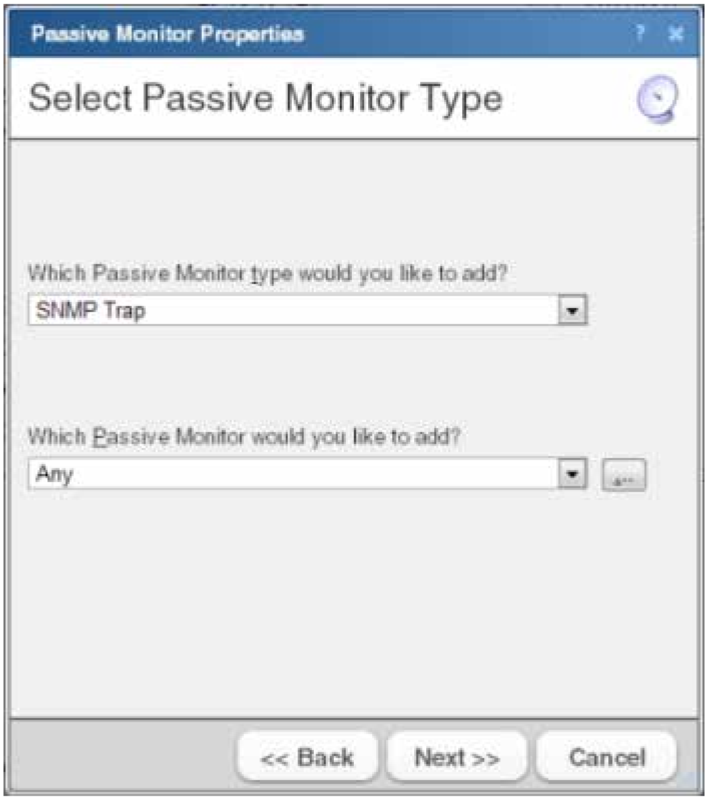
Note: When you assign a passive monitor to a device, an instance of the monitor is added to the device. Changes that you make to the monitor's configuration via the Passive Monitor Library affect all instances of the monitor. For example, if you assign a monitor to four separate devices and then make changes to the monitor from the Passive Monitor Library, all four instances of the monitor adopt the changes.

To assign a passive monitor to a device:

1 From the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Passive Monitors**. The Device Properties Passive Monitor dialog appears.

3 Click **Add**. The Passive Monitor Properties dialog appears.



Passive Monitor Properties

Select Passive Monitor Type

Which Passive Monitor type would you like to add?

SNMP Trap

Which Passive Monitor would you like to add?

Any

4 Select the passive monitor type and passive monitor you want to assign, then click **Next**. The Setup Actions for Passive Monitors dialog appears.

5 Click **Add** to setup a new action for the passive monitor. The Select or Create Action dialog appears.

6 Click either:

Select an action from the Action Library

- or -

Create a new action

Follow the remaining Wizard dialog pages for the selection you made.

7 Click **Finish** to add the passive monitor to the device.

> **Note**: You can view the monitor logs by selecting an option on the Logs tab.

Group and device passive monitor reports

The following reports display information for devices or device groups that have passive monitors configured and enabled. Access these reports from the WhatsUp Gold web interface's Reports tab.

- SNMP Trap Log
- Syslog Entries
- Windows Event Log
- Passive Monitor Error Log

Using Performance Monitors

In This Chapter

Performance monitors overview

Performance monitors are the WhatsUp Gold feature responsible for gathering data about the performance components of the devices running on your network; for example, CPU and memory utilization. The data is then used to create reports that trend utilization and availability of these device components.

WhatsUp Gold performance monitors gather data from the following components:

- CPU utilization
- Disk utilization
- Interface utilization
- Interface traffic
- Memory utilization
- Ping availability
- Ping response time

Additionally, you can create custom performance monitors to track specific performance monitors for Active Script, APC UPS, PowerShell Scripting, Printer, SNMP, SQL Query, SSH, WMI Formatted, and WMI performance counters.

Performance Monitors are configured in the *Performance Monitor Library* (on page 261) and are added to individual devices througha the Device Properties dialog. From the Device Properties Performance Monitor dialog, you can add:

- Pre-configured (standard) Performance Monitors
- Device-specific (custom) Performance Monitors

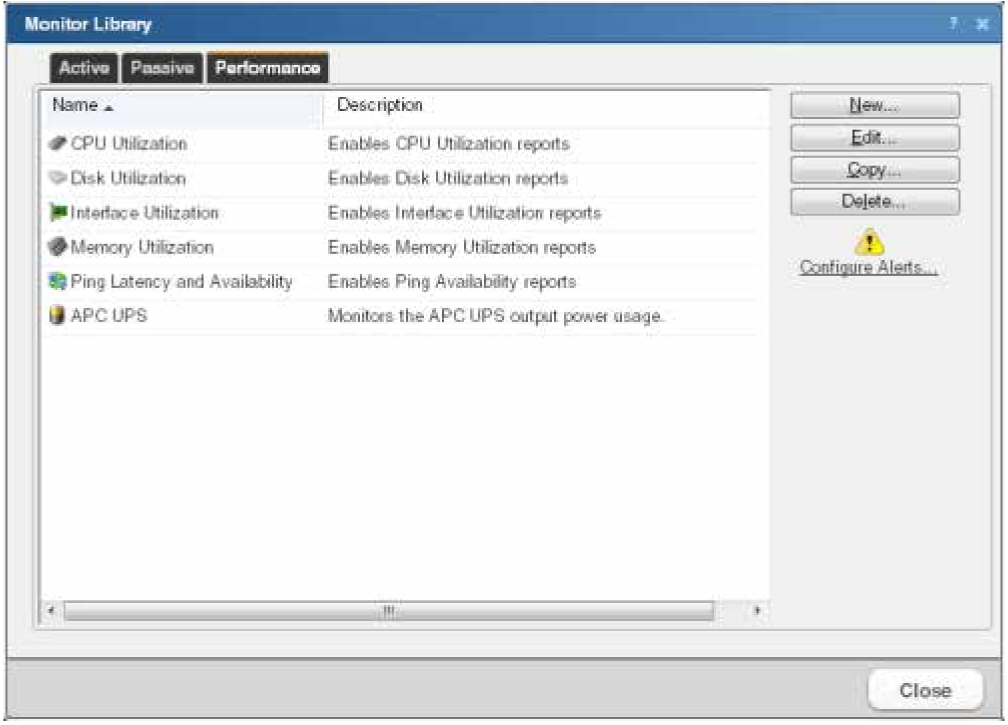
> **Note**: Printer monitors are specific to individual printer devices; as such, the Printer Performance Monitor can only be added as an individual performance monitor in the Device Properties Performance Monitor dialog.

Using the Performance Monitor Library

The Performance Monitor Library stores and displays the performance monitors that have been created for WhatsUp Gold. Performance monitors gather information about specific WMI and SNMP values from network devices. There are several default performance monitors available in the library and you can also add new performance monitors. Performance monitors can be applied to devices from the Device Properties dialog for that device.

To access the Performance Monitor Library:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.



Name	Description
CPU Utilization	Enables CPU Utilization reports
Disk Utilization	Enables Disk Utilization reports
Interface Utilization	Enables Interface Utilization reports
Memory Utilization	Enables Memory Utilization reports
Ping Latency and Availability	Enables Ping Availability reports
APC UPS	Monitors the APC UPS output power usage.

2 If it is not already selected, click the **Performance** tab.

3 Use the Performance Monitor Library dialog to configure new or existing performance monitor types:

- Click **New** to configure a custom performance monitor.
- Select an existing performance monitor, then click **Edit** to modify its configuration.

- Click **Copy** to create a duplicate of a monitor. You can use the Copy option to create new monitors based on existing monitors.

Note: The five default global monitors cannot be edited, copied or deleted: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

- Select an existing performance monitor, then click **Delete** to remove it from the list.

Caution: When you delete a performance monitor from the Performance Monitor Library, any instance of that monitor is also deleted, and all related report data is also lost.

- Click **Configure Alerts** to view the Alert Center Threshold Library.

For more information on Performance Monitors, see *Enabling performance monitors* (on page 373).

Working with Performance Monitors

The Performance Monitor Library is a central storehouse of all global performance monitors configured for your network. *Performance monitors* (on page 380) gather information about specific WMI and SNMP values from the network devices.

Note: Default monitors in the library cannot be edited or removed: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

You can use the Performance Monitor Library to configure and manage performance monitors.

Use the Performance Monitor Library dialog to configure new or existing performance monitor types:

- Click **New** to configure a custom performance monitor.
- Select an existing performance monitor, then click **Edit** to modify its configuration.

Note: The five default global monitors cannot be edited or deleted: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

- Select an existing performance monitor, then click **Delete** to remove it from the list.

Caution: When you delete a performance monitor from the Performance Monitor Library, any instance of that monitor is also deleted, and all related report data is lost.

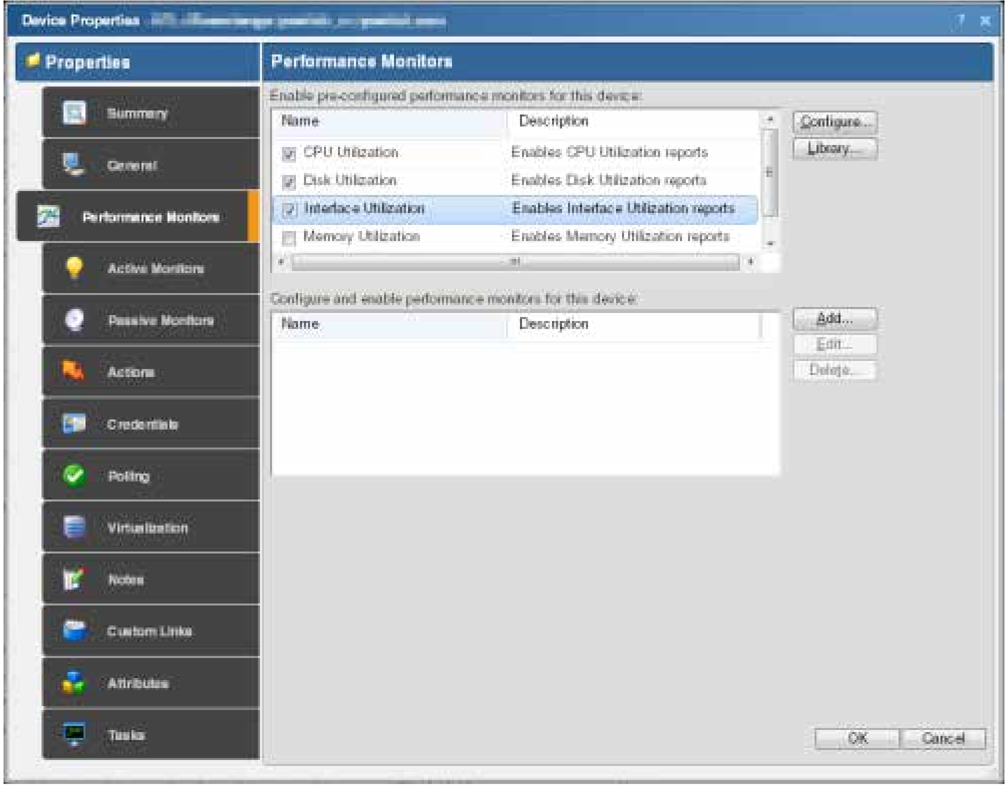
Tip: Click **Configure Alerts** to view the Alert Center Threshold Library.

Caution: When custom Performance Monitors are changed, the changes affect each instance of that particular monitor across device groups.

To configure Performance Monitors for the devices to which they are assigned:

1 From the Device Properties page, right-click a device you want to configure. The right-click menu appears.

2 Click **Properties**. The Device Properties dialog appears.



Device Properties [redacted]

Performance Monitors

Enable pre-configured performance monitors for this device:

Name	Description
☑ CPU Utilization	Enables CPU Utilization reports
☑ Disk Utilization	Enables Disk Utilization reports
☑ Interface Utilization	Enables Interface Utilization reports
□ Memory Utilization	Enables Memory Utilization reports

Configure and enable performance monitors for this device:

Name	Description

3 Select the monitor from the list and click **Configure** to enable a pre-configured monitor for this device.
- or -
Click **Add** and create a device-specific monitor.
- or -
Double-click an existing monitor to change its configuration.
- or -
Select a performance monitor type, then click **Delete** to remove it from the list.

4 Click **OK** to save changes.

Adding and editing an Active Script Performance Monitor

Warning: Modifying the configuration of any of the VoIP Active Script Performance monitors is not recommended; doing so prevents the VoIP setup utility from detecting pre-existing VoIP configuration.

For more information on the Active Script Performance Monitor, see *Scripting Performance Monitors* (on page 529).

This script performance monitor has a context object used to poll for specific information about the device in context.

We have provided several code samples to help you in creating useful Active Script Performance Monitors for your devices.

To add a new Active Script performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Script Type**. Select either JSCRIPT or VBSCRIPT.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: Though the maximum timeout allowed is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

§ **Reference variables**. Add, edit, or remove SNMP and WMI reference variables using the respective buttons on the right of the dialog.

> **Note**: The use of reference variables in the Active Script performance monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed. Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to use a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms you would normally have manage to access SNMP or WMI counters on a remote device.
>
> By using the `Context.GetReferenceVariable`(variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script. For more information, see Using the context object with performance monitors.

§ **Script text**. Enter your monitor code here.

5 Click **OK** to save changes.

6 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

> **Note**: The first time that you poll a WMI reference variable that requires two polls in order to calculate an average (such as "Processor\% Processor Time"), it returns "Null."

Troubleshooting

Having problems with your WMI monitor returning *false negatives* (on page 566)?

To edit an existing Active Script performance monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Performance** tab. The Performance Monitor list appears.
3. Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**.
4. Enter or select the appropriate information:

   § **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

   § **Description**. Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

   § **Script Type**. Select either JSCRIPT or VBSCRIPT.

   § **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: Though the maximum timeout allowed is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

   § **Reference variables**. Add, edit, or remove SNMP and WMI reference variables using the respective buttons on the right of the dialog.

> **Note**: The use of reference variables in the Active Script performance monitor is optional. If you do use them, you must use `Context.GetReferenceVariable,` for reference variables to be polled and their data graphed. Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to use a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms you would normally have to manage in order to access SNMP or WMI counters on a remote device.
>
> By using the `Context.GetReferenceVariable`(variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script. For more information, see Using the context object with performance monitors.

   § **Script text**. Enter your monitor code here.

5 Click **OK** to save changes.

Adding and Editing an APC UPS Performance Monitor

The APC UPS performance monitor collects statistical output power usage information and graphs APC UPS power utilization over time. This monitor detects when UPS devices are close to maximum performance level, and what time of day networking devices connected to UPS devices are using the most power—both indicating the need to equally distribute the load across several UPS devices.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add an APC UPS performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Select **APC UPS Performance Monitor**, then click **OK**. The Add APC UPS Performance Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

6 Click **OK** to save changes.

7 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing APC UPS performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**. The Edit APC UPS Performance Monitor dialog appears.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

5 Click **OK** to save changes.

Adding and editing a PowerShell Scripting performance monitor

Windows PowerShell is a scripting language and command-line shell that system administrators can use to manage Windows operating systems. For more information on PowerShell, please visit the *Microsoft web site* (http://www.whatsupgold.com/MSPowerShell).

The PowerShell Scripting performance monitor allows the experienced user to perform a wide variety of monitoring tasks through direct access to script component libraries, including the .NET Framework. The Windows PowerShell scripting language can be used in conjunction with WhatsUp Gold to help you monitor, control, manage, and automate Windows operating system activities. For example, you might implement a script to look for a process and report the current number of threads in the process. Or, you might implement a script to look for idle time levels and log the results. For more information and examples of PowerShell performance monitors, see *PowerShell performance monitor script examples* (on page 269).

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new PowerShell performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Select **PowerShell Scripting Monitor**, then click **OK**. The Add PowerShell Performance Monitor dialog appears.

5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

Note: Although the default timeout is 60 seconds, you are highly discouraged from using a timeout longer than 10 seconds. Please use the shortest timeout possible.

§ **Reference variables**. Add, edit, or remove SNMP and WMI reference variables using the respective buttons.

Note: The use of reference variables in the PowerShell performance monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed. Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to use a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms you would normally have to manage in order to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable`(variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script. For more information, see Using the context object with performance monitors.

§ **Script text**. Enter your code here.

6 Click **OK** to save changes.

7 Click **OK** to exit the Performance Monitor Library.

8 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing PowerShell performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

Note: Although the default timeout is 60 seconds, you are highly discouraged from using a timeout longer than 10 seconds. Please use the shortest timeout possible.

§ **Reference variables**. Add, edit, or remove SNMP and WMI reference variables using the respective buttons.

Note: The use of reference variables in the PowerShell performance monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed. Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms you would normally have manage to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable`(variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script. For more information, see Using the context object with performance monitors.

§ **Script text**. Enter your code here.

5 Click **OK** to save changes.

6 Click **OK** to exit the Performance Monitor Library.

Example - PowerShell performance monitor scripts

The PowerShell performance monitor scripts have two instantiated objects available to support successful execution:

§ **Context**. An implementation of the IScriptContext interface. This object provides access to runtime variables and also provides mechanism for returning results to the client. A few methods are listed below:

§ object GetReferenceVariable(string variableName) - allows retrieval of previously configured reference variable values by name.

§ object GetProperty(string propertyName) - allows retrieval of context variable values by name.

§ void SetResult(int resultCode) - allows the script to set a value to indicate success, usually 0 = success and 1 = failure.

§ **Logger**. An implementation of the ILog interface. This object provides the same methods available to C# applications. A few useful methods are listed below:

§ void Error(string message) - Creates an error-specific log entry that includes the message.

§ void Information(string message) - Creates an information-specific log entry that includes the message.

§ void WriteLine(string message) - Creates a generic log entry that includes the message.

Context Variables

The following context variables are available for use in PowerShell performance monitor scripts:

§ DeviceID

§ DisplayName

§ Address

- NetworkName
- Timeout
- CredWindows:DomainAndUserid
- CredWindows:Password
- CredSnmpV1:ReadCommunity
- CredSnmpV1:WriteCommunity
- CredSnmpV2:ReadCommunity
- CredSnmpV2:WriteCommunity
- CredSnmpV3:AuthPassword
- CredSnmpV3:AuthProtocol (values: 1 = None, 2 = MD5, 3 = SHA)
- CredSnmpV3:EncryptProtocol (values: 1 = None, 2 = DES56, 3 = AES128, 4 = AES192, 5 = AES256, 6 = THREEDES)
- CredSnmpV3:EncryptPassword
- CredSnmpV3:Username
- CredSnmpV3:Context
- CredADO:Password
- CredADO:Username
- CredSSH:Username
- CredSSH:Password
- CredSSH:EnablePassword
- CredSSH:Port
- CredSSH:Timeout
- CredVMware:Username
- CredVMware:Password

Script Timeout

You can configure a script timeout value (in seconds). If the script has not finished executing before the timeout value expires, it aborts.

Minimum: 1

Maximum: 60

Default: 60

Example Script #1

```
#

# This example looks for a process named 'outlook' and reports its

# current number of threads.

#
```

```
# Use the built-in cmdlet named 'Get-Process', also aliased as 'ps'

$processes = ps

$processName = "outlook"

$proc = $processes | where { $_.ProcessName -match $processName }


# Performance monitors must call Context.SetValue() to report results

$Context.SetValue($proc.Threads.Count)
```

Example Script #2

```
#

# This example uses a reference variable to look for idle time

# levels and logs the results

#


# Use available context variables

$resultText = "Address: " + $Context.GetProperty("Address");


# Access the reference variable

$monitorValue = $Context.GetReferenceVariable("IdleTime")


# Log if necessary

$resultText = $resultText + ", Idle time: " + $monitorValue.ToString()

$Logger.WriteLine($resultText)


# Always set the performance value

$Context.SetValue($monitorValue);
```

Adding and editing a Printer performance monitor

This monitor uses SNMP to collect data on SNMP-enabled network printers. If a failure criteria is met, any associated actions fire. For example, you can monitor for printer ink levels, for a paper jam, for low input media (paper), for a fuse that is over temperature, and more.

Note: In order for the Printer performance monitor to work, in addition to being SNMP-enabled, the printer you are attempting to monitor must also support the Standard Printer MIB.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To add a new Printer performance monitor:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **Printer Performance Monitor**, then click **OK**. The New Printer Performance Monitor dialog appears.

5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Ink/Toner Cartridge**. Select the ink/toner cartridge from which you want to collect ink/toner level data.

Note: You must set up a Printer performance monitor for each color ink/toner cartridge you want to monitor.

§ **Collection interval**. Select the collection interval (in minutes) for how often you want data to be collected for the selected toner cartridge. This number represents the number of minutes between each collection.

Note: Your printer may not support all of the SNMP objects associated with the available monitor alert checks.

6 (Optional) Click **Advanced** to select advanced options.

7 Click **OK** to save changes.

8 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing Printer performance monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2. Click the **Performance** tab. The Performance Monitor list appears.
3. Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**. The Edit Printer Performance Monitor dialog appears.
4. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
   - **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
   - **Ink/Toner Cartridge**. Select the ink/toner cartridge from which you want to collect ink/toner level data.

> **Note**: You must set up a Printer performance monitor for each color ink/toner cartridge you want to monitor.

   - **Collection interval**. Select the collection interval (in minutes) for how often you want data to be collected for the selected toner cartridge. This number represents the number of minutes between each collection.

> **Note**: Your printer may not support all of the SNMP objects associated with the available monitor alert checks.

5. (Optional) Click **Advanced** to select advanced options.
6. Click **OK** to save changes.

Adding and editing an SNMP Performance Monitor

The Simple Network Management Protocol (SNMP) performance monitor allows you to access SNMP supported devices and plot the performance output on a graph.

To add a new SNMP performance monitor:

1. From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.
2. Click the **Performance** tab. The Performance Monitor list appears.
3. Click **New**. The Select Performance Monitor Type dialog appears.
4. Enter the appropriate information:
   - **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
   - **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
5. Enter the **OID** and **Instance** or click browse (**...**) to access the SNMP MIB Browser.
6. Click **OK** to save changes.

7 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing SNMP performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

5 Enter the **OID** and **Instance** or click browse (**...**) to access the SNMP MIB Browser.

6 Click **OK** to save changes.

Adding and editing a SQL Query performance monitor

This monitor allows you to check for certain conditions in a Microsoft SQL, MySQL, or ORACLE database, based on a database query.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: To use the SQL Query monitor to monitor a MySQL database, you must first download and install the MySQL .NET Connector on the WhatsUp Gold machine. Note that only MySQL version 5.2.5 .NET Connector is supported due to compatibility issues. The connector is located on the WhatsUp Gold website (*http://www.whatsupgold.com/MySQL525Connector* (http://www.whatsupgold.com/MySQL525connector)). This link downloads the `mysql-connector-net-5.2.5.zip` file. After the file downloads, extract the `MySQL.Data.msi` and run the MySQL Connector setup utility by double-clicking on the **MySQL.Data.msi** icon. On the Choose Setup Type dialog, select **Typical**, then click **Install**. The MySQL .NET Connector is installed in the following location: `C:\Program Files\MySQL\MySQL Connector Net 5.2.5\`. After the .NET Connector has been installed, restart the WhatsUp Gold machine.

Note: The SQL Query monitor supports Windows and ADO authentication. Make sure that credentials are setup in the Credentials Library for the database for which you want to query. The Credentials system stores Windows and ADO database credential information in your WhatsUp Gold database to be used when a database connection is required. For more information, see Using Credentials.

Note: When connecting to a remote SQL instance, WhatsUp Gold only supports the TCP/IP network library.

To add a new SQL Query performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Select **SQL Query Performance Monitor**, then click **OK**. The New SQL Query Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

6 Enter or select the appropriate information for the **Server Properties** section:

§ **Server Type**. Select *Microsoft SQL Server*, *MySQL*, or *ORACLE* as the database server type.

> **Note**: MySQL database is supported and listed as a server type option only if the MySQL 5.2.5 Connector is installed.

§ **Connection Timeout (sec)**. Used by the SQL Query monitor to determine how long to wait for the server to respond before terminating the connection and returning the timeout error. Minimum allowed value is 1 second whereas maximum allowed value is 120. The default value is 15 seconds.

> **Note**: The connection timeout setting configured by the user is used for polling only; the query builder does not use it. Instead, the query builder assumes a default of 15 seconds for the connection timeout.

§ **Server Address**. `ServerName\Instance` format for Microsoft SQL Server (for example, WUGServer\SQLEXPRESS), `ServerName` for MySQL (for example, WUGServer), or `ServerName/ServiceName` for Oracle (for example, WUGServer/Oracle).

> **Note**: When using an Oracle server type, the SQL query monitor does not make use of the `tsnnames.ora` file on the client (i.e. WhatsUp Gold system).

§ **Port (optional)**. The database server port number if other than the standard database port number.

§ **SQL Query to Run**. A query you want to run against a database to monitor and check for certain database conditions. Only select queries are allowed.

> **Important**: Make sure that you include the full database name in your query. For query help, click **Build**. The SQL Query Builder will assist you in developing proper query syntax.

Important: The SQL query you enter must return a single numeric value. Specifically, a single record that has just one column. If the query returns more than one record, the monitor will fail to store the data. If the query returns a single records but there are multiple columns in the record returned, then the monitor will pick the first column as the value to store and this first column has to be numeric, otherwise the monitor will fail to store the data.

§ **Build**. Click to open the *SQL Query Builder* (on page 277) dialog for assistance building queries.

§ **Verify**. Click to check that the query is valid. If there is a syntax error with the SQL query, a message appears with tips about the syntax issue.

7 Click **OK** to save changes.

8 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing SQL Query performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**. The Edit SQL Query Performance Monitor dialog appears.

4 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

5 Enter or select the appropriate information for the **Server Properties** section:

§ **Server Type**. Select *Microsoft SQL Server*, *MySQL*, or *ORACLE* as the database server type.

Note: MySQL database is supported and listed as a server type option only if the MySQL 5.2.5 Connector is installed.

§ **Connection Timeout (sec)**. Used by the SQL Query monitor to determine how long to wait for the server to respond before terminating the connection and returning the timeout error. Minimum allowed value is 1 second whereas maximum allowed value is 120. The default value is 15 seconds.

Note: The connection timeout setting configured by the user is used for polling only; the query builder does not use it. Instead, the query builder assumes a default of 15 seconds for the connection timeout.

§ **Server Address**. `ServerName\Instance` format for Microsoft SQL Server (for example, WUGServer\SQLEXPRESS), `ServerName` for MySQL (for example, WUGServer), or `ServerName/ServiceName` for Oracle (for example, WUGServer/Oracle).

> **Note**: SQL query monitors do not make use of `tsnnames.ora` file on the client (i.e. WhatsUp Gold system).

- **Port (optional)**. The database server port number if other than the standard database port number.
- **SQL Query to Run**. A query you want to run against a database to monitor and check for certain database conditions. Only select queries are allowed.

> **Important**: Ensure that you include the full database name in your query.

- **Build**. Click to open the *SQL Query Builder* (on page 277) dialog for assistance building queries.
- **Verify**. Click to check that the query is valid. If there is a syntax error with the SQL query, a message appears with tips about the syntax issue.

6 Click **OK** to save changes.

SQL Query Builder

This dialog assists in developing proper query syntax for SQL Query performance monitors.

To use the SQL Query Builder:

1 From the Select a ADO/Windows Credential dialog, select the ADO or Windows credential you would like to use to build the query from the list or click browse (**...**) to select from the Credentials Library.

2 Click **OK**. The SQL Query Builder dialog appears.

3 Select the database you want to use to build the query in the **Database (catalog)** box.

4 Select the database table you want to use to build the query in the **Table/View** box.

5 Select the database column you want to use to build the query in the **Columns** box.

> **Note**: As you specify the database query selections, the **SQL Query** box updates to verbally illustrate the query you have configured.

6 Click **OK** to save changes.

Adding and editing an SSH Performance Monitor

The Secure Shell (SSH) monitor connects to a remote device using SSH to execute commands or scripts. The success or failure of the monitor is dependant upon values returned by the commands or scripts that can be interpreted by WhatsUp Gold as up or down.

To add a new SSH performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Select **SSH Performance Monitor**, then click **OK**. The New SSH Performance Monitor dialog appears.

5 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Command to run**. Enter the command you want to run and execute on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a Perl script.

✓ **Important**: The command or script must return a single numeric value.

Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

§ **SSH Credential**. Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select **Use the device SSH credential**, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, click browse (**...**) to open the WhatsUp Gold Credentials Library and configure a set of credentials.

6 Click **OK** to save changes.

7 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing SSH performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**. The Edit SSH Performance Monitor dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Command to run**. Enter the command you want to run and execute on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a Perl script.

✓ **Important**: The command or script must return a single numeric value.

Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- § **SSH Credential**. Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select **Use the device SSH credential**, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, click browse (**...**) to open the WhatsUp Gold Credentials Library and configure a set of credentials.

5 Click **OK** to save changes.

Adding and Editing a WMI Formatted Performance Monitor

The WMI Formatted Counter performance monitor allows you to obtain performance data on devices using the Windows Management Instrumentation (WMI) technology. WMI is a Microsoft Windows standard for retrieving information from computer systems running Windows and is installed by default on most Windows operating systems.

While similar to the WMI performance monitor that uses raw data, the WMI Formatted Counter performance monitor uses calculated counter data.

Note: WMI formatted counters return data that is rounded as an integer and may be less precise than the raw data returned by the WMI performance monitor.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: This monitor requires Windows credentials.

To add a new WMI Formatted Counter performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Select **WMI Formatted Counter Monitor**, then click **OK**. The Add WMI Formatted Monitor dialog appears.

5 Enter or select the appropriate information:

- § **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- § **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
- § **Performance counter/Instance**. Click browse (**...**) to select a performance counter for the monitor.

6 Click **OK** to save changes.

7 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing WMI Formatted Counter performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.
2 Click the **Performance** tab. The Performance Monitor list appears.
3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**. The Edit WMI Formatted Monitor dialog appears.
4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
- **Performance counter/Instance**. Click browse (**...**) to select a performance counter for the monitor.

5 Click **OK** to save changes.

Adding and editing a WMI Performance Monitor

The WMI performance monitor watches for specific values on Windows Management Instrumentation (WMI) enabled devices. WMI is a Microsoft Windows standard for retrieving information from computer systems running Windows and is installed by default on most Windows operating systems.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: This monitor requires Windows credentials.

To add a new WMI performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.
2 Click the **Performance** tab. The Performance Monitor list appears.
3 Click **New**. The Select Performance Monitor Type dialog appears.
4 Select **WMI Performance Monitor**, then click **OK**. The Add WMI Performance Monitor dialog appears.
5 Enter the appropriate information:

- **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

6 Click browse (**...**). The Select Performance Counter dialog appears.
7 Enter the **Name** or **IP address** of the computer to which you are trying to connect or click browse (**...**) to select a device, then click **OK**.

8 Select the **Credential** used to connect to the device. You can also click browse (**...**) to access the Credentials Library to create a new credential.

9 Click **OK**. The Add WMI Performance Monitor dialog appears.

10 Use the navigation tree in the left panel to select the specific **Performance Counter** you want to monitor. You can view more information about the property/value at the bottom of the dialog.

11 In the right pane, select the specific **Performance Instance** of the selected counter you want to monitor.

12 Click **OK** to add the appropriate values to the **Performance counter** and **Instance** boxes on the Add WMI Performance Monitor dialog.

13 Click **OK** to save changes.

14 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 281).

To edit an existing WMI performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Select the performance monitor you would like to edit from the list of current monitors, then click **Edit**. The Edit WMI Performance Monitor dialog appears.

4 Enter the appropriate information:

- **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

5 Click browse (**...**). The Select Performance Counter dialog appears.

6 Enter the **Name** or **IP address** of the computer to which you are trying to connect or click browse (**...**) to select a device, then click **OK**.

7 Select the **Credential** used to connect to the device. You can also click browse (**...**) to access the Credentials Library to create a new credential.

8 Click **OK**. The Add WMI Performance Monitor dialog appears.

9 Use the navigation tree in the left panel to select the specific **Performance Counter** you want to monitor. You can view more information about the property/value at the bottom of the dialog.

10 In the right pane, select the specific **Performance Instance** of the selected counter you want to monitor.

11 Click **OK** to add the appropriate values to the **Performance counter** and **Instance** boxes on the Add WMI Performance Monitor dialog.

12 Click **OK** to save changes.

Enabling global performance monitors

In order for a performance monitor to gather performance data from a device, it must be enabled on that device. You can *enable a monitor on a single device* (on page 282) through the Device Properties dialog, or *enable a monitor on multiple devices* (on page 282) through the Bulk Field Change feature.

Enabling a global performance monitor on a single device

To enable a global performance monitor for a single device:

1. In Device or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
2. Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
3. Under **Enable pre-configured performance monitors for this device**, select the global monitor you would like to enable.
4. Click **Configure** to complete the settings for the selected performance monitor.

> **Important**: To enable a CPU, disk, interface, or memory global performance monitor, you must first select an SNMP credential for the device from the Credentials Library. For more information, see *Using credentials* (on page 68).

5. Click **OK** to save the changes.

Enabling a global performance monitor on multiple devices

To enable multiple a performance monitor on multiple devices:

1. In Details or Map View, select the devices or group for which you would like to enable the monitor, then right-click.
2. Click **Bulk Field Change > Performance Monitors**. The Bulk Field Change: Performance Monitors dialog appears.
3. Under **Collect data for**, select the desired option for the appropriate performance monitor. After you have selected the monitor for which you want to collect data, you also have the option to modify the monitor **Data collection interval**.
4. Click **OK** to save changes.

Configuring the CPU monitor collection settings

To configure the CPU utilization monitor collection settings for a device:

1. On the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
2. Click **Performance Monitors**. The Performance Monitors list appears.
3. Select **CPU Utilization**, then click **Configure**. The Configure CPU Utilization dialog appears.
4. Enter or select the appropriate information:
    - **Collect data for**. Select the CPU(s) for which you want to gather data. You can choose to track all CPUs or a specific CPU. If you select All CPUs, all CPUs in the list are automatically selected.
    - **Data collection interval**. Enter how often (in minutes) you want data to be collected for the selected CPUs. This number represents the number of minutes between each collection.

> **Tip**: Click **Advanced** to specify the timeout and number of retries, and how WhatsUp Gold is to determine uniqueness when the monitor is tracking more than one CPU.

5 Click **OK** to save changes.

Configuring the disk monitor collection settings

To configure the disk utilization monitor collection settings for a device:

1 On the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors list appears.

3 Select **Disk Utilization**, then click **Configure**. The Configure Disk Utilization dialog appears.

4 Enter or select the appropriate information:

§ **Collect data for**. Select the disk(s) for which you want to gather data. You can choose to track all disks, one disk, or a combination of disks. If you select **All disks**, all disks in the list are automatically selected.

§ **Data collection interval**. Enter how often (in minutes) you want data to be collected for the selected disks. This number represents the number of minutes between each collection.

Tip: Click **Advanced** to specify the timeout and number of retries, and how WhatsUp Gold is to determine uniqueness when the monitor is tracking more than one disk.

5 Click **OK** to save changes.

Configuring the interface monitor collection settings

To configure the interface utilization monitor collection settings for a device:

1 From the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors list appears.

3 Select **Interface Utilization**, then click **Configure**. The Configure Interface Utilization dialog appears.

4 Enter or select the appropriate information:

§ **Collect data for**. Select the interface(s) for which you want to gather data. You can select all interfaces, active interfaces, specific interfaces, or custom active interfaces. If you select custom active interface, you can specify to track high speed interfaces, interfaces whose name contain a certain variable, or interfaces that match a certain type. Additionally, if you chose to track a specific interface, you can override the interface **Speed**.

Important: Be aware when you use the **Collect errors and discards data for selected interfaces** feature, it has potential to increase the database size quickly because there is potential for a significant amount of errors and discards data. You can set WhatsUp Health thresholds in the Alert Center to stay informed when the database size exceeds specified thresholds. For more information, see Configuring system thresholds.

Tip:To disable the errors and discards data collection, you can disable for the individual device (**Device Properties > Performance Monitor**) or disable for multiple devices with the bulk field change option:
1. Select multiple devices that have the Interface Utilization performance monitor enabled, right-click, then select **Bulk Field Change > Performance Monitors**. The Bulk Field Change dialog appears.
2. In the Interface section of the dialog, under the **Collect errors and discards data for enabled interfaces** list, click **Yes**.
For more information, see *Editing multiple devices with the Bulk Field Change feature* (on page 113).

§ **Collect errors and discards data for all selected interfaces**. Select this option to collect the following device interface data:

§ ifInErrors. Lists the number of inbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.14.

§ ifOutErrors. Lists the number of outbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.20.

§ ifInDiscards. List the number of inbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.13.

§ ifOutDiscards. List the number of outbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.19.

Note: All of the above OIDs point to values of type "counter," and therefore their raw value by itself is not meaningful. The difference between the values obtained from two consecutive polls provides meaningful data.

§ **Speed**. Click to specify the speed for the currently selected interface.

§ **Data collection interval**. Enter how often (in minutes) you want data to be collected for the selected interfaces. This number represents the number of minutes between each collection.

Tip: Click **Advanced** to specify the timeout and number of retries, how WhatsUp Gold is to determine uniqueness when the monitor is tracking more than one disk, and which interface traffic counters to poll.

5 Click **OK** to save changes.

Configuring the memory monitor collection settings

To configure the memory utilization monitor collection settings for a device:

1 On the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors list appears.

3 Select **Memory Utilization**, then click **Configure**. The Configure Memory Utilization dialog appears.

4 Enter or select the appropriate information:

§ **Collect data for**. Select the memory item(s) for which you want to gather data. You can choose to track all memory items, or specific memory items. If you select **All memory items**, all memory items in the list are automatically selected.

§ **Data collection interval**. Enter how often (in minutes) you want data to be collected for the selected CPUs. This number represents the number of minutes between each collection.

Tip: Click **Advanced** to specify the timeout and number of retries, and how WhatsUp Gold determines uniqueness when the monitor is tracking more than one memory item.

5 Click **OK** to save changes.

Configuring the ping monitor collection settings

To configure the ping latency and availability monitor collection settings for a device:

1 On the Device or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors list appears.

3 Select **Ping Latency and Availability**, then click **Configure**. The Configure Ping Latency and Availability dialog appears.

4 Enter or select the appropriate information:

§ **Collect data for**. Select the interface(s) for which you want to gather data. You can choose to track the default interface, all interfaces, or a specific interface. If you select **All interfaces**, all interfaces in the list are automatically selected.

§ **Data collection interval**. Enter how often (in minutes) you want data to be collected for the selected CPUs. This number represents the number of minutes between each collection.

Tip: Click **Advanced** to specify the timeout and number of iterations.

5 Click **OK** to save changes.

Enabling SNMP on Windows devices

Before you can collect performance data on a Windows computer using SNMP, you must first install and enable the Microsoft SNMP Agent on the device itself. For more information, see *Using SNMP* (on page 501).

To install SNMP Monitoring :

1 From the Windows Control Panel, do one of the following:

- Click **Add or Remove Programs.**
  - or -
- Click **Programs**.

2 Do one of the following:

- Click **Add/Remove Windows Components**.
  - or -
- Click **Turn Windows features on or off**.

3 Do one of the following:

- From the Components list, select **Management and Monitoring Tools**, then click **Details** to view the list of Subcomponents.
  - or -
- Locate **Simple Network Management Protocol (SNMP)** in the list.

4 Make sure Simple Network Management Protocol is selected.

5 Click **OK**.

6 Click **Next** to install the components.

7 After the install wizard is complete, click **Finish** to close the window.

To enable SNMP Monitoring:

1 Click the **Start** and enter `services.msc`.

2 In the Services (Local) list, double-click **SNMP Service** to view the Properties.

3 On the **Agent** tab, enter the **Contact** name for the person responsible for the upkeep and administration of the computer, then enter the **Location** of the computer. These items are returned during some SNMP queries.

4 On the **Security** tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like WhatsUp Gold to read information about the computer. This community string will be later used to *create credentials* (on page 68) for connecting to this device.

5 On the **General** tab, click **Start** to start the service (if necessary).

6 Click **OK** to close the dialog.

You can test the device by connecting to it through SNMP View.

Creating custom performance monitors

In addition to the five default performance monitors, WhatsUp Gold gives you the option to create custom performance monitors to track specific Active Script, APC UPS, PowerShell, Printer, SNMP, SQL Query, SSH, WMI Formatted, and WMI performance counters.

Creating device-specific Active Script performance monitors

Warning: Modifying the configuration of any of the VoIP Active Script Performance monitors is not recommended; doing so prevents the VoIP setup utility from detecting pre-existing VoIP configuration.

For more information on the Active Script Performance Monitor, see *Scripting Performance Monitors* (on page 529).

This script performance monitor has a context object used to poll for specific information about the device in context.

We have provided several code samples to help you in creating useful Active Script Performance Monitors for your devices.

To create a device-specific Active Script performance monitor:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **Active Script Performance Monitor**, then click **OK**. The Add Active Script Performance Monitor dialog appears.

5 Enter the appropriate information for the following fields:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Script Type**. Enter either JSCRIPT or VBSCRIPT.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

Note: Though the maximum timeout allowed is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

§ **Reference variables**. Add, edit, or remove SNMP and WMI reference variables using the respective buttons on the right of the dialog.

Note: The use of reference variables in the Active Script Performance Monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed. Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to use a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms you would normally have to manage in order to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable`(variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script.

Note: You can add up to 10 reference variables.

- **Script text**. Enter your monitor code here.

6 Click **OK** to save changes.

To configure an SNMP Active Script performance monitor:

1 On the Add Active Script Performance Monitor dialog, click **Add** to add a new variable to the **Reference variables** field. The Add New Reference Variable dialog appears.

Note: You can add up to 10 reference variables.

Reference variables simplify your scripting code and enable you to write scripts efficiently without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They take care of the underlying SNMP or WMI mechanisms that you would normally have to deal with to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable` (variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses a device's credentials to connect to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script.

Important: The use of reference variables in the Active Script performance monitor is optional. If you use them, you must use `Context.GetReferenceVariable,` for reference variables to be polled and their data graphed.

2 Enter the appropriate information:

- **Variable name**. Enter a unique name for the variable.
- **Description**. (Optional) Enter additional information about the variable.

3 Select **SNMP** from the **Object Type** list.

4 (Optional) Enter the **Timeout** and **Retries** count for connection to the device.

5 Click browse (**...**). The Select Computer dialog appears.

6 Enter the **Name** or **IP address** of the computer to which you are trying to connect.

7 Select the **SNMP Credential** used to connect to the device. You can also click browse (**...**) to access the Credentials Library to create a new credential.

8 (Optional) Adjust the **Timeout** and **Retries** count for the computer to which you are trying to connect.

9 Click **OK**. The SNMP MIB Browser appears.

10 Use the navigation tree in the left panel to select the specific MIB you want to monitor. You can view more information about the property/value at the bottom of the dialog.

11 Click **OK** to add the OID to the **Performance counter** and **Instance** fields in the Add New Reference Variable dialog.

12 Verify the configuration and click **OK** to add the variable to the **Reference variables list** in the Add Active Script Performance Monitor dialog.

13 Write or paste your monitor code in the **Script text** field.

14 Click **OK** to save changes.

Tip: The SNMP API is useful for writing Active Script performance monitors using SNMP.

To configure a WMI Active Script performance monitor:

1 On the Add Active Script Performance Monitor dialog, click **Add** to add a new variable to the **Reference Variables** list.

Note: You can add up to 10 reference variables.

Reference variables simplify your scripting code and enable you to write scripts efficiently without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They take care of the underlying SNMP or WMI mechanisms that you would normally have to deal with to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable` (variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses a device's credentials to connect to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script.

Important: The use of reference variables in the Active Script performance monitor is optional. If you use them, you must use `Context.GetReferenceVariable,` for reference variables to be polled and their data graphed.

2 Enter the appropriate information:

- **Variable name**. Enter a unique name for the variable.
- **Description**. (Optional) Enter additional information about the variable.

3 Select **WMI** from the **Object Type** list.

4 Click browse (**...**). The Select Performance Counter dialog appears.

5 Click browse (**...**) to select counters from the computer. The Select Computer dialog appears.

6 Enter the **Name** or **IP address** of the computer in which you want to connect.

7 Select the **Windows Credential** used to connect to the device. You can also click browse (**...**) to access the Credentials Library to create a new credential.

8 Click **OK** to connect to the computer.

9 Use the performance counter tree to navigate to the **Performance Counter** you want to monitor.

10 After you select the performance counter, select the specific **Performance Instance** you want to monitor.

11 Click **OK** to add the variable to the **Performance counter** field in the Add New Reference Variable dialog.

12 Click **OK** to add the variable to the **Reference variable** list on the Add Active Script Performance Monitor dialog.

13 Write or paste your monitor code into the **Script text** field.

14 Click **OK** to save changes.

Important: The first time that you poll a WMI reference variable that requires two polls in order to calculate an average (such as "Processor\% Processor Time"), it returns "Null."

Creating device-specific APC UPS performance monitors

The APC UPS performance monitor collects statistical output power usage information and graphs APC UPS power utilization over time. This monitor detects when UPS devices are close to maximum performance level, and what time of day networking devices connected to UPS devices are using the most power—both indicating the need to equally distribute the load across several UPS devices.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To create a device-specific APC UPS performance monitor:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **APC UPS Performance Monitor**, then click **OK**. The Add APC UPS Performance Monitor dialog appears.

5 Enter or select the appropriate information for the following boxes:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

§ **Collection interval (min)**. How often you want data to be collected for the selected APC UPS. This number represents the number of minutes between each collection.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

§ **Retries**. The number of times you want to attempt to make the connection to the selected device.

6 Click **OK** to save changes.

Creating device-specific PowerShell Scripting performance monitors

Windows PowerShell is a scripting language and command-line shell that system administrators can use to manage Windows operating systems. For more information on PowerShell, please visit the *Microsoft web site* (http://www.whatsupgold.com/MSPowerShell).

The PowerShell Scripting performance monitor allows the experienced user to perform a wide variety of monitoring tasks through direct access to script component libraries, including the .NET Framework. The Windows PowerShell scripting language can be used in conjunction with WhatsUp Gold to help you monitor, control, manage, and automate Windows operating system activities. For example, you might implement a script to look for a process and report the current number of threads in the process. Or, you might implement a script to look for idle time levels and log the results. For more information and examples of

PowerShell performance monitors, see *Example - PowerShell performance monitor scripts* (on page 269).

> **Note**: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To create a device-specific PowerShell Scripting performance monitor:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **PowerShell Scripting Monitor**, then click **OK**. The Add PowerShell Performance Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
- **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: Although the default timeout is 60 seconds, you are highly discouraged from using a timeout longer than 10 seconds. Please use the shortest timeout possible.

- **Collection interval (min)**. The amount of time between performance polls.
- **Reference variables**. Add, edit, or remove SNMP and WMI reference variables using the respective buttons.
- **Script text**. Enter your code here.

6 Click **OK** to save changes.

7 Click **OK** to exit the Device Properties dialog.

Example - PowerShell performance monitor scripts

The PowerShell performance monitor scripts have two instantiated objects available to support successful execution:

- **Context**. An implementation of the IScriptContext interface. This object provides access to runtime variables and also provides mechanism for returning results to the client. A few methods are listed below:
- object GetReferenceVariable(string variableName) - allows retrieval of previously configured reference variable values by name.
- object GetProperty(string propertyName) - allows retrieval of context variable values by name.

- void SetResult(int resultCode) - allows the script to set a value to indicate success, usually 0 = success and 1 = failure.
- **Logger**. An implementation of the ILog interface. This object provides the same methods available to C# applications. A few useful methods are listed below:
- void Error(string message) - Creates an error-specific log entry that includes the message.
- void Information(string message) - Creates an information-specific log entry that includes the message.
- void WriteLine(string message) - Creates a generic log entry that includes the message.

Context Variables

The following context variables are available for use in PowerShell performance monitor scripts:

- DeviceID
- DisplayName
- Address
- NetworkName
- Timeout
- CredWindows:DomainAndUserid
- CredWindows:Password
- CredSnmpV1:ReadCommunity
- CredSnmpV1:WriteCommunity
- CredSnmpV2:ReadCommunity
- CredSnmpV2:WriteCommunity
- CredSnmpV3:AuthPassword
- CredSnmpV3:AuthProtocol (values: 1 = None, 2 = MD5, 3 = SHA)
- CredSnmpV3:EncryptProtocol (values: 1 = None, 2 = DES56, 3 = AES128, 4 = AES192, 5 = AES256, 6 = THREEDES)
- CredSnmpV3:EncryptPassword
- CredSnmpV3:Username
- CredSnmpV3:Context
- CredADO:Password
- CredADO:Username
- CredSSH:Username
- CredSSH:Password
- CredSSH:EnablePassword
- CredSSH:Port
- CredSSH:Timeout
- CredVMware:Username

- CredVMware:Password

Script Timeout

You can configure a script timeout value (in seconds). If the script has not finished executing before the timeout value expires, it aborts.

Minimum: 1

Maximum: 60

Default: 60

Example Script #1

```
#

# This example looks for a process named 'outlook' and reports its

# current number of threads.

#


# Use the built-in cmdlet named 'Get-Process', also aliased as 'ps'

$processes = ps

$processName = "outlook"

$proc = $processes | where { $_.ProcessName -match $processName }


# Performance monitors must call Context.SetValue() to report results

$Context.SetValue($proc.Threads.Count)
```

Example Script #2

```
#

# This example uses a reference variable to look for idle time

# levels and logs the results

#


# Use available context variables
```

```
$resultText = "Address: " + $Context.GetProperty("Address");


# Access the reference variable

$monitorValue = $Context.GetReferenceVariable("IdleTime")


# Log if necessary

$resultText = $resultText + ", Idle time: " + $monitorValue.ToString()

$Logger.WriteLine($resultText)


# Always set the performance value

$Context.SetValue($monitorValue);
```

Creating device-specific SNMP performance monitors

The Simple Network Management Protocol (SNMP) performance monitor allows you to access SNMP supported devices and plot the performance output on a graph.

To create a device-specific SNMP performance monitor:

1. From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.
2. Click **Performance Monitors**. The Performance Monitors information appears.
3. Click **Add**. The Select Performance Monitor Type dialog appears.
4. Select **SNMP Performance Monitor**, then click **OK**. The Add SNMP Performance Monitor dialog appears.
5. Enter the appropriate information:
   - **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
   - **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
6. Click browse (**...**). The SNMP MIB Browser dialog appears.
7. Click browse (**...**) to select the IP address of the device to which you want to connect. The MIB Browser dialog appears.
8. Enter a **Computer Name** or **IP Address** or click browse (**...**) to select a device, then click **OK**.
9. Select the **Credential** used to connect to the device. You can also click browse (**...**) to access the Credentials Library to create a new credential.
10. (Optional) Adjust the **Timeout** and **Retries** count for the computer to which you are trying to connect.
11. Click **OK**. The SNMP MIB Browser appears.

12 Use the navigation tree in the left panel to select the specific **MIB** you want to monitor. You can view more information about the property/value at the bottom of the dialog.

13 In the right panel, select the specific **Property** for the MIB you want to monitor.

14 Click **OK** to add the OID to the **Performance counter** and **Instance** boxes of the Add SNMP Performance Monitor dialog.

15 Click **OK** to save changes.

Creating device-specific Printer performance monitors

This monitor uses SNMP to collect data on SNMP-enabled network printers. If a failure criteria is met, any associated actions fire. For example, you can monitor for printer ink levels, for a paper jam, for low input media (paper), for a fuse that is over temperature, and more.

> **Note**: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

To create a device-specific Printer performance monitor:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **Printer Performance Monitor**, then click **OK**. The New Printer Performance Monitor dialog appears.

5 Enter or select the appropriate information:

- § **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- § **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
- § **Ink/Toner Cartridge** Select the ink/toner cartridge from which you want to collect ink/toner level data.

> **Note**: You must set up a Printer performance monitor for each color ink/toner cartridge you want to monitor.

- § **Collection interval**. Enter the collection interval (in minutes) for how often you want data to be collected for the selected toner cartridge. This number represents the number of minutes between each collection.**Note**: Your printer may not support all of the SNMP objects associated with the available monitor alert checks.

6 (Optional) Click **Advanced** to select advanced options.

7 Click **OK** to save changes.

Creating device-specific SQL Query performance monitors

This monitor allows you to check for certain conditions in a Microsoft SQL, MySQL, or ORACLE database, based on a database query.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: To use the SQL Query monitor to monitor a MySQL database, you must first download and install the MySQL .NET Connector on the WhatsUp Gold machine. Note that only MySQL version 5.2.5 .NET Connector is supported due to compatibility issues. The connector is located on the WhatsUp Gold website (*http://www.whatsupgold.com/MySQL525Connector* (http://www.whatsupgold.com/MySQL525connector)). This link downloads the `mysql-connector-net-5.2.5.zip` file. After the file downloads, extract the `MySQL.Data.msi` and run the MySQL Connector setup utility by double-clicking on the **MySQL.Data.msi** icon. On the Choose Setup Type dialog, select **Typical**, then click **Install**. The MySQL .NET Connector is installed in the following location: `C:\Program Files\MySQL\MySQL Connector Net 5.2.5\`. After the .NET Connector has been installed, restart the WhatsUp Gold machine.

Note: The SQL Query monitor supports Windows and ADO authentication. Make sure that credentials are setup in the Credentials Library for the database for which you want to query. The credentials system stores Windows and ADO database credential information in your WhatsUp Gold database to be used when a database connection is required. For more information, see Using Credentials.

Note: When connecting to a remote SQL instance, WhatsUp Gold only supports the TCP/IP network library.

To create a device-specific SQL Query performance monitor:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **SQL Query Performance Monitor**, then click **OK**. The New SQL Query Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

6 Enter or select the appropriate information for the **Server Properties** section:

- **Server Type**. Select *Microsoft SQL Server*, *MySQL*, or *ORACLE* as the database server type.

> **Note**: MySQL database is supported and listed as a server type option only if the MySQL 5.2.5 Connector is installed.

- **Connection Timeout (sec)**. Used by the SQL Query monitor to determine how long to wait for the server to respond before terminating the connection and returning the timeout error. Minimum allowed value is 1 second whereas maximum allowed value is 120. The default value is 15 seconds.

> **Note**: The connection timeout setting configured by the user is used for polling only; the query builder does not use it. Instead, the query builder assumes a default of 15 seconds for the connection timeout.

- **Server Address**. Enter `ServerName\Instance` format for Microsoft SQL Server (for example, WUGServer\SQLEXPRESS), `ServerName` for MySQL (for example, WUGServer), or `ServerName/ServiceName` for Oracle (for example, WUGServer/Oracle).

> **Note**: When using an Oracle server type, the SQL query monitor does not make use of the `tsnnames.ora` file on the client (i.e. WhatsUp Gold system).

- **Port (optional)**. Enter the database server port number if other than the standard database port number.
- **SQL Query to Run**. Enter a query you want to run against a database to monitor and check for certain database conditions. Only select queries are allowed.

> **Important**: Make sure that you include the full database name in your query. For query help, click **Build**. The SQL Query Builder will assist you in developing proper query syntax.
>
> **Important**: The SQL query you enter must return a single numeric value. Specifically, a single record that has just one column. If the query returns more than one record, the monitor will fail to store the data. If the query returns a single records but there are multiple columns in the record returned, then the monitor will pick the first column as the value to store and this first column has to be numeric, otherwise the monitor will fail to store the data.

- **Build**. Click to open the *SQL Query Builder* (on page 277) dialog for assistance building queries.
- **Verify**. Click to check that the query is valid. If there is a syntax error with the SQL query, a message appears with tips about the syntax issue.

7 Click **OK** to save changes.

SQL Query Builder

This dialog assists in developing proper query syntax for SQL Query performance monitors.

To use the SQL Query Builder:

1. From the Select a ADO/Windows Credential dialog, select the ADO or Windows credential you would like to use to build the query from the list or click browse (**...**) to select from the Credentials Library.
2. Click **OK**. The SQL Query Builder dialog appears.
3. Select the database you want to use to build the query in the **Database (catalog)** box.
4. Select the database table you want to use to build the query in the **Table/View** box.
5. Select the database column you want to use to build the query in the **Columns** box.

Note: As you specify the database query selections, the **SQL Query** box updates to verbally illustrate the query you have configured.

6. Click **OK** to save changes.

Creating device-specific SSH performance monitors

The Secure Shell (SSH) performance monitor allows you to securely access Unix-like devices and plot the performance output on a graph.

To create a device-specific SSH performance monitor:

1. From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.
2. Click **Performance Monitors**. The Performance Monitors information appears.
3. Click **Add**. The Select Performance Monitor Type dialog appears.
4. Select **SSH Performance Monitor**, then click **OK**. The New SSH Performance Monitor dialog appears.
5. Enter the appropriate information:
   - **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
   - **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
   - **Command to run**. Enter the command that is to be executed on the remote device. This command can be anything that the device can interpret and run; for example, a basic Unix command or Perl script.

Important: The command or script must return a single numeric value.

Note: If you create a script to run on the remote device, the script must be developed, tested and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

   - **SSH credential** . Select the credential that WhatsUp Gold will use to connect to the remote device. If you select **Use the device SSH credential**, WhatsUp Gold uses the

SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (**...**) to the WhatsUp Gold Credentials Library to configure a set of credentials.

- **Collection Interval**. Enter the collection interval (in minutes) you want data to be collected. This number represents the number of minutes between each collection.

6 Click **OK** to save changes.

Creating device-specific WMI Formatted Counter performance monitors

The WMI Formatted Counter performance monitor allows you to obtain performance data on devices using the Windows Management Instrumentation (WMI) technology. WMI is a Microsoft Windows standard for retrieving information from computer systems running Windows and is installed by default on most Windows operating systems.

While similar to the WMI performance monitor that uses raw data, the WMI Formatted Counter performance monitor uses calculated counter data.

Note: WMI formatted counters return data that is rounded as an integer and may be less precise than the raw data returned by the WMI performance monitor.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

✓ **Important**: This monitor requires Windows credentials.

To create device-specific WMI Formatted Counter performance monitors:

1 From the WhatsUp Gold web interface, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Performance Monitors**. The Performance Monitors information appears.

3 Click **Add**. The Select Performance Monitor Type dialog appears.

4 Select **WMI Formatted Counter Monitor**, then click **OK**. The Add WMI Formatted Performance Monitor dialog appears.

5 Enter or select the appropriate information:

- **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.
- **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.
- **Performance counter/Instance**. Click browse (**...**) to select a performance counter for the monitor.
- **Collection interval (minutes)**. Enter how often you want data to be collected. This number represents the number of minutes between each collection.
- **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

6 Click **OK** to save changes.

Creating device-specific WMI performance monitors

The WMI performance monitor watches for specific values on Windows Management Instrumentation (WMI) enabled devices. WMI is a Microsoft Windows standard for retrieving information from computer systems running Windows and is installed by default on most Windows operating systems.

Note: This feature is available with WhatsUp Gold Premium Edition only. To update your license, visit the *WhatsUp Customer Portal* (http://www.whatsupgold.com/wugCustPortal).

Important: This monitor requires Windows credentials.

To create a device-specific WMI performance monitor:

1 From the WhatsUp Gold web interface, go to **Admin > Monitor Library**. The Monitor Library dialog appears.

2 Click the **Performance** tab. The Performance Monitor list appears.

3 Click **New**. The Select Performance Monitor Type dialog appears.

4 Select **WMI Performance Monitor** from the list, then click **OK**. The Add WMI Performance Monitor dialog appears.

5 Enter the appropriate information:

§ **Name**. Enter a unique name for the performance monitor. This name displays in the Performance Monitor Library.

§ **Description**. (Optional) Enter additional information about the monitor. This description displays next to the monitor in the Performance Monitor Library.

6 Click browse (**...**). The Performance Counter dialog appears.

7 Enter the **Name** or **IP address** of the computer to which you are trying to connect or click browse (**...**) to select a device, then click **OK**.

8 Select the **Credential** used to connect to the device. You can also click browse (**...**) to access the Credentials Library to create a new credential.

9 Click **OK**. The Add WMI Performance Monitor dialog appears.

10 Use the navigation tree in the left panel to select the specific **Performance Counter** you want to monitor. You can view more information about the property/value at the bottom of the dialog.

11 In the right pane, select the specific **Performance Instance** of the selected counter you want to monitor.

12 Click **OK** to add the appropriate values to the **Performance counter** and **Instance** boxes on the Add WMI Performance Monitor dialog.

13 Click **OK** to save changes.

Example: monitoring router bandwidth

You can configure WhatsUp Gold to gather bandwidth usage on your SNMP enabled devices (routers, switches, etc.) and then track that usage through performance logs. For bandwidth monitoring, the Interface Utilization monitor is the most useful as it illustrates percent utilization and throughput.

The Interface Utilization monitor gathers statistics on the volume of bytes traveling to and from the active interfaces on a device. You can collect data on all interfaces, active interfaces, or specific interfaces. This monitor is configured and enabled through **Device Properties > Performance Monitors**.

> **Note**: Before you can configure the monitor for a device, you must enable SNMP and assign the proper credentials via the *Credentials Library* (on page 458). The Performance Monitoring system uses these credentials to connect to the device during the configuration process, and during normal performance gathering. For more information, see *Enabling SNMP on Windows devices* (on page 285).

Configuring the monitor

The Interface Utilization Performance Monitor is one of the default performance monitors installed with WhatsUp Gold, and needs no global configuration to configure the monitor for a single device.

To configure the Bandwidth Monitor:

1. In either the Details or Map View, right-click on a device, then click **Properties** from the right-click menu.
2. Select **Performance Monitors** on the Device Properties dialog.
3. Select the Interface Utilization monitor from the list.
4. Click **Configure** to set up the monitor for the device. WhatsUp Gold scans the device and discovers the interfaces on the device.

   When the scan completes, the Configure Interface Data Collection dialog appears. If the credentials for the device are not configured properly, the scan fails (return to the Credentials Library to fix it). If the device is not SNMP-enabled, the scan fails.
5. Select the interfaces you want to collect data for. From the **Collect data for** list, select **All**, **Active**, **Specific**, or **Custom active**. If you select **Specific**, select just the interfaces you want to monitor in the list below. By default, active interfaces are measured.
6. On the Configure Interface Data Collection dialog, enter a time interval (in minutes) for how long you want the application to wait between polls in the **Data collection interval** box. The default is 10 minutes. See Program Options - Report Data for more information on data collection and roll-up.
7. Select **Collect errors and discards data for selected interfaces** to record this data.
8. (Optional) click **Advanced** to change the retry and timeout settings for the SNMP connection to the device. Click **OK** to save the changes to the Advanced Settings.
9. Click **OK** to save the Interface Utilization configuration.

Viewing data

WhatsUp Gold takes several polling cycles to produce meaningful graphs (with a 10 minute poll interval, this may mean a few hours). After enough data is gathered, several reports display this data.

- **By Device**. Click the Monitoring tab, click the Interface or Interface Errors & Discards monitor report, and then select a device.
- **By Group**. Click the Monitoring tab, click the Interface or Interface Errors & Discards monitor report, and then select a group.
- **System Wide**. Use the Top 10 Dashboard to view the top performers in terms of bandwidth utilization across your network.

Example: troubleshooting a slow network connection

The real-time reporting provided by performance monitors can provide both the raw data and the data trend analysis that can help you isolate network problems. For example, we recently experienced a problem with a network connection between two of our Ipswitch office sites. This example shows how we used Performance Monitors to troubleshoot the slow network connection.

Scenario:

A developer working in Augusta, GA on an Atlanta-based project complained of a slow network connection between the Augusta and Atlanta offices. He stated it took 40 minutes to check in files to the source library over the T1 connection.

The Atlanta office network administrator reacted by completing the following steps:

1. On the WhatsUp Gold web interface, he accessed the Monitoring tab to select the Ping Response Time report.
2. From the Ping Response Time report, he checked the connection from the Atlanta WhatsUp Gold application to the Augusta primary server. The report showed an increased response time beginning at 11:45 a.m.

This connection was previously configured with the appropriate Performance Monitors and had accumulated data for several weeks. This data enabled the administrator to accurately narrow down the possible cause of the problem to the primary server connection. He was then able to troubleshoot that specific connection and take steps to fix the slowness issue.

To set up this type of monitor for a connection, configure the Ping Latency and Availability monitor on a device located on the other end of the connection. For more information, see *Learning about network monitors* (on page 391).

Using the Active Script Performance Monitor

Active Script Performance Monitors let you write VBScript and JScript to easily poll one or more SNMP or WMI values, perform math or other operations on those values, and graph a single output value. You should only use the Active Script Performance Monitor when you need to perform calculations on the polled values. A variety of Active Script resources are available on the *Active Scripts resources page.* (http://www.whatsupgold.com/script_library)

Note: Please be aware that Ipswitch does not support the custom scripts that you create; only the ability to use them in the Active Script Monitor.

For more information, see *Extending WhatsUp Gold with scripting* (on page 512).

Using Actions

In This Chapter

Actions overview

WhatsUp Gold actions are designed to perform a task as a device or monitor state change occurs.

As you configure an action, you choose the task it is to perform. Actions can try to correct the problem, notify someone of the state change, or launch an external application. Also, when you configure an action, you choose whether to assign it to a device, or to an active or passive monitor.

When assigned to an active monitor, actions fire according to the state changes it issues. For example, you can configure an Email Action to send an email alert when the active monitor for a Web server issues a down state change.

You can configure actions on a single device or monitor, or define an Action Policy to use across multiple devices or monitors.

Managing Action Strategies

As you configure and assign actions, you should take several things into consideration.

§ Assigning an external notification action (email, SMS, beeper) to a large list of devices greatly increases the chance of numerous notifications being sent at one time.

For example, an email action assigned to a router and each of the devices that depend on that router for their Internet connectivity, would send email notifications not only from the router, but also from every single connected device, should the router go down.

In a situation like this, it considers using dependencies allowing you to restrict email notifications to only the router and the critical devices to which it is connected. For more information, see *Dependencies overview* (on page 106).

§ An action can be assigned to a device or to an active or passive monitor.

If you want to be notified if and when any or all of the monitors on a device go down, assign the action to the device. If you are concerned with specific monitors on a device, assign the action to the monitor itself. If you assign to both the device and a specific monitor, both actions fire when the monitor goes down.

§ Action policies are easier to manage than lists of actions built on a device.

Whenever possible, use action policies in lieu of configuring multiple actions for one device.

§ If the existing WhatsUp Gold device states do not fit your monitoring needs, you can modify them, or configure new ones.

Consider adding device states for longer periods of downtime, such as creating a **Down at least 60 mins** state, and sending an escalated message to show that the device is still down after an hour.

§ Web Alarms are only useful if someone is able to hear the notifications.

While Web Alarms are useful in many situations, they are not the most efficient way to monitor devices and services overnight.

§ Visual notifications are usually ample enough for most of the devices on your network.

Unless the device is vital to the daily-operation of your network or business, the color and shape of each device state easily informs you of current network device status.

§ You can check on the status of firing alerts via Running Actions. From here, you can cancel single alerts, or all currently firing alerts.

About the Action Library

The Action Library displays all actions currently configured for use in WhatsUp Gold.

WhatsUp Gold includes five pre-configured actions. These actions display in the Action Library. As you create new actions, they are added to the Action Library.

To access the Action Library from the WhatsUp Gold web interface, go to **Admin > Action Library**.

Use the Action Library to configure new or existing action types:

§ Click **New** to configure a new action type.

§ Select an action type, then click **Edit** to change its configuration.

Note: If the action you are editing was previously created in the Alert Center, any changes that you make here are made to the version of the action in the Alert Center Notification Library.

- Select an action type, then click **Copy** to make a duplicate of the selected action type.
- Select an action type, then click **Delete** to remove it from the library.

Caution: When you delete an action from the Action Library, all instances of that action are also deleted, and all related report data is lost.

Selecting an action type

Select the type of action you want to create for this device. The list menu lists all possible actions that can occur through the WhatsUp Gold action system.

- **Active Script Action**. Write code to perform a customized action.
- **Beeper Action**. Activate a beeper with this type of action.
- **Email Action**. Send an Email to a specific address.
- **Log to Text File**. Write a message to a text file.
- **Pager Action**. Send a message to a pager.
- **PowerShell Action**. Develop custom actions through direct access to scriptable component libraries, including the .NET Framework.
- **Program Action**. Execute an external application.
- **Service Restart Action**. Start or stop a Windows service.
- **SMS Action**. Send a text message to a specific target.
- **SMS Direct**. Send a text message to a wireless phone or other wireless device.
- **SNMP Set**. Use SNMP to set the value of an attribute of a managed object.
- **Sound Action**. Play a specific sound.
- **SSH Action**. Connect to remote devices via SSH to execute commands or scripts.
- **Syslog Action**. Write a message to a log in the Syslog system.
- **Text to Speech Action**. Plays a voice message on your computer.
- **VMware Action**. Use the VMware API to perform an action on a virtual machine.
- **Web Alarm Action**. Activate a Web Alarm in the WhatsUp Gold Web Interface
- **Windows Event Log Action**. Write an event in the Windows Event Log.
- **Winpopup Action**. Send a Winpopup to a user or specific computer.

All action types are executed based on a state change specified in the next dialog.

Configuring an action

There are two aspects of fully configuring an action. First, you create the action itself in the Action Library dialog or through the Action Builder wizard. The setup consists of:

§ Defining the target of the action (for example, a pager or email address)

§ Entering the notification variables or program arguments (that specify what information to report in the action message, or to pass to another program).

Next, you assign the action or action policy to a device or active monitor and to link it to a state change (action policies are already linked to a state change during the policy definition). For more information see:

§ *Assigning an action to a device* (on page 346)

§ *Assigning an action to an active monitor* (on page 346)

§ Creating a custom action policy

After the actions have been completely configured, WhatsUp Gold launches the action as soon as the proper state change is reached.

Adding and editing an Active Script Action

This action allows you to write either VBScript or JScript code to perform a customized action. If the script returns an error code, the action failed.

Note: This script action has a context object you can use to get specific information about the context of the action.

Note: We have provided several code samples for you to create useful script actions for your devices.

Note: All script features in WhatsUp Gold utilize the *SNMP API* (on page 544).

To add a new Active Script action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Active Script Action**, then click **OK**. The New Active Script Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: Though the maximum timeout is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

- **Script type**. Select the scripting language that you want to use to write this active script (either VBScript or JScript).
- **Script text**. Enter your action code here.

> **Note**: We do not recommend that you use percent variables in script text, because they may resolve to text containing special characters (' ' (quotes), " " (double-quotes), % (percent), new line characters, and the like) that may break your script.

5 Click **OK** to save changes.

> **Tip**: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Active Script action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: Though the maximum timeout is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

- **Script type**. Select the scripting language that you want to use to write this active script (either VBScript or JScript).
- **Script text**. Enter your action code here.

> **Note**: It is not recommend that you use percent variables in script text, because they may resolve to text containing special characters (' ' (quotes), " " (double-quotes), % (percent), new line characters, and the like) that may break your script.

4 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing a Beeper Action

The Beeper action activates a beeper when a device reaches a certain state change. The settings below are used to automatically build a dial string for use by the modem sending the beeper action.

Tip: The Beeper Action can identify network devices through a specific device attribute.

To add a new Beeper action:

1. From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.
2. Click **New**. The Select Action Type dialog appears.
3. Select **Beeper Action**, then click **OK**. The New Beeper Action dialog appears.
4. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the action. This name displays in the Action Library.
   - **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
   - **Beeper number**. Enter the phone number to dial. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers, for example: (617) 555-5555.
   - **Pause after answer (sec)**. Enter a number of seconds the modem should pause before sending the signal codes once a connection is made.
   - **End transmission**. By default, # is the correct symbol for the end transmission command. Some international systems require other or additional symbols.
   - **Modem setup**. Select Primary or one of the alternate setups. Click **Port Settings** to further define your selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your beeper notifications. There could also be times you want to change your settings to meet a specific service provider requirements for a specific notification (for example, a lower baud rate). To do this, set up an alternate Modem Setup and associate this to the notification instead of using your Primary setting.

Note: Changing the port settings for the desired modem setup affects all uses of that setting.

   - **Up code**. Specifies the characters sent to the beeper to indicate that the device is up after being down (the default value is 0*).
   - **Down Code**. Specifies the code sent to indicate the device is down (the default value is 1*).

- **On passive monitor code**. Specifies the code sent to indicate that an active monitor has been received for the device. (Default value is 2*) You can use the asterisk (*) character to separate codes from a subsequent message.
- **Recurring action code**. The percent variables for the action. The default action code is: %System.NumberofUpDevices*%System.NumberofDownDevices

5 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Beeper action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Beeper number**. Enter the phone number to dial. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers, for example: (617) 555-5555.
- **Pause after answer (sec)**. Enter a number of seconds the modem should pause before sending the signal codes once a connection is made.
- **End transmission**. By default, # is the correct symbol for the end transmission command. Some international systems require other or additional symbols.
- **Modem setup**. Select Primary or one of the alternate setups. Click **Port Settings** to further define your selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your beeper notifications. There could also be times you want to change your settings to meet a specific service provider requirements for a specific notification (for example, a lower baud rate). To do this, set up an alternate Modem Setup and associate this to the notification instead of using your Primary setting.

Note: Changing the port settings for the desired modem setup affects all uses of that setting.

- **Up code**. Specifies the characters sent to the beeper to indicate that the device is up after being down (the default value is 0*).
- **Down Code**. Specifies the code sent to indicate the device is down (the default value is 1*).
- **On passive monitor code**. Specifies the code sent to indicate that an active monitor has been received for the device. (Default value is 2*) You can use the asterisk (*) character to separate codes from a subsequent message.

- **Recurring action code**. The percent variables for the action. The default action code is: %System.NumberofUpDevices*%System.NumberofDownDevices

4 Click **OK** to save changes.

> **Tip**: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing an Email Action

The E-mail action sends an SMTP mail message to a specific e-mail account. An E-mail action can also be used as an e-mail notification in the WhatsUp Gold Alert Center. While you can configure this action on both the console and web interface, you can only configure the Alert Center notification message on the web. For more information, see Configuring an Alert Center e-mail notification.

To add a new E-mail action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **E-mail Action**, then click **OK**. The New Email Action dialog appears.

4 Enter the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

5 Complete the information on the **Configuration** tab. This tab contains options pertaining to the action e-mail destination.

- **SMTP Server**. Enter the IP address or Host (DNS) name of your e-mail server (SMTP mail host).
- **Port**. Enter the port number on which the SMTP server is installed.
- **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.
- **Mail To**. Enter the e-mail addresses to which you want to send the alert. E-mail addresses must be fully qualified. You can enter two addresses, separated by commas (but no spaces). The address should not contain brackets, braces, quotes, or parentheses.
- **Mail From**. Enter the e-mail address you want to appear in the From field of the e-mail that is sent by the E-mail action.
- **SMTP server requires authentication**. Check this option if your SMTP server uses authentication. This enables the Username and Password fields.

  The Email action supports three authentication types:

  - CRAM-MD5

    - login
    - plain

  The authentication type is not configurable. It is negotiated with the SMTP server automatically.

  - **Username**. Enter the username for SMTP authentication.
  - **Password**. Enter the password of the username for authentication.
  - **Use an encrypted connection (SSL/TLS)**. Check this option if your SMTP server requires the data to be encrypted over a TLS connection (formerly known as SSL).

6. Complete the information on the **Mail Content** tab. This tab contains options pertaining to the action e-mail message content.
   - **Subject**. Enter a text message or edit the default message. You can use percent variable codes to display specific information in the subject.
   - **Message body**. Enter a text message or edit the default message. You can use percent variable codes to display specific information in the message body.

> **Tip**: You can add a link to either or both the Device Status and Mobile Device Status reports by clicking the appropriate button.

7. Complete the information on the **Alert Center Settings** tab. This tab contains options pertaining to the message sent from WhatsUp Gold Alert Center.
   - **Alert Center email subject**. Enter a subject for the message. This text appears as the subject in the e-mail that is sent by the Alert Center notification. This subject can include percent variables.

> **Tip**: To include Alert Center percent variables, right click inside the box.

   - **Alert Center Link.** Select **Include hyperlink to Alert Center in the email content** to include a link to the Alert Center home page in the email message sent by the Alert Center notification.
     - Select to use either **HTTP** or **HTTPS** in the link address.
     - Select to either **Use dynamic address** or **Use static hostname or IP address**. If you select to use the dynamic address, WhatsUp Gold automatically generates the URL using the current IP address or hostname at the time the action runs.
     - When static hostname or IP address is selected, specify the **Hostname** or **IP address** to include in the link address.
     - Specify the **Port** to include in the link address.

> **Important**: The address you enter here must be the exact address of the Alert Center home page to which you want to connect. Verify the address and enter its exact contents in the above options.

8. Click **OK** to save changes.

To edit an existing E-mail action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

4 Complete the information on the **Configuration** tab. This tab contains options pertaining to the action e-mail destination.

§ **SMTP Server**. Enter the IP address or Host (DNS) name of your e-mail server (SMTP mail host).

§ **Port**. Enter the port number on which the SMTP server is installed.

§ **Timeout (sec)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

§ **Mail To**. Enter the e-mail addresses to which you want to send the alert. E-mail addresses must be fully qualified. You can enter two addresses, separated by commas (but no spaces). The address should not contain brackets, braces, quotes, or parentheses.

§ **Mail From**. Enter the e-mail address you want to appear in the **From** box of the e-mail that is sent by the E-mail action.

§ **SMTP server requires authentication**. Check this option if your SMTP server uses authentication. This enables the **Username** and **Password** boxes.

The Email action supports three authentication types:

§ CRAM-MD5

§ login

§ plain

The authentication type is not configurable. It is negotiated with the SMTP server automatically.

§ **Username**. Enter the username for SMTP authentication.

§ **Password**. Enter the password of the username for authentication.

§ **Use an encrypted connection (SSL/TLS)**. Check this option if your SMTP server requires the data to be encrypted over a TLS connection (formerly known as SSL).

5 Complete the information on the **Mail Content** tab. This tab contains options pertaining to the action e-mail message content.

§ **Subject**. Enter a text message or edit the default message. You can use percent variable codes to display specific information in the subject.

§ **Message body**. Enter a text message or edit the default message. You can use percent variable codes to display specific information in the message body.

> **Tip**: You can add a link to either or both the Device Status and Mobile Device Status reports by clicking the appropriate button.

6 Complete the information on the **Alert Center Settings** tab. This tab contains options pertaining to the message sent from WhatsUp Gold Alert Center.

- § **Alert Center email subject**. Enter a subject for the message. This text appears as the subject in the e-mail that is sent by the Alert Center notification. This subject can include percent variables.

> **Tip**: To include Alert Center percent variables, right click inside the box.

- § **Alert Center Link.** Select **Include hyperlink to Alert Center in the email content** to include a link to the Alert Center home page in the email message sent by the Alert Center notification.
  - § Select to use either **HTTP** or **HTTPS** in the link address.
  - § Select to either **Use dynamic address** or **Use static hostname or IP address**. If you select to use the dynamic address, WhatsUp Gold automatically generates the URL using the current IP address or hostname at the time the action runs.
  - § When static hostname or IP address is selected, specify the **Hostname** or **IP address** to include in the link address.
  - § Specify the **Port** to include in the link address.

> **Important**: The address you enter here must be the exact address of the Alert Center home page to which you want to connect. Verify the address and enter its exact contents in the above options.

7 Click **OK** to save changes.

Adding and editing a Log to Text File Action

The Log to Text action logs custom messages to specified text files.

To add a new Log to Text File action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Log to Text File**, then click **OK**. The New Log To Text File Action dialog appears.

4 Enter or select the appropriate information:

- § **Name**. Enter a unique name for the action. This name displays in the Action Library.
- § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- § **Log file**. Enter the full path to the location where the log file will bee written.
- § **Log file write mode**. Select **Append** to have log messages appended to the Log file. Select **Overwrite** to have log messages overwrite existing log messages.

- **Log Message**. Enter the message that will be written to the log file. This message supports percent variables. The default log message is:

  ```
  %Device.ActiveMonitorDownNames is %Device.State on %Device.Type:
  %Device.HostName (%Device.Address).

  Details:

  Monitors that are down include: %Device.ActiveMonitorDownNames

  Monitors that are up include: %Device.ActiveMonitorUpNames

  Notes on this device (from device property page):

  %Device.Notes

  ----------------------------------------
  ```

  This message was logged on %System.Date at %System.Time

```
Ipswitch WhatsUp Gold
```

5 Click **OK** to save changes.

To edit an existing Log to Text action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Log file**. Enter the full path to the location where the log file will be written.
- **Log file write mode**. Select **Append** to have log messages appended to the Log file. Select **Overwrite** to have log messages overwrite existing log messages.
- **Log Message**. Enter the message that will be written to the log file. This message supports percent variables. The default log message is:

  ```
  %Device.ActiveMonitorDownNames is %Device.State on %Device.Type:
  %Device.HostName (%Device.Address).

  Details:

  Monitors that are down include: %Device.ActiveMonitorDownNames

  Monitors that are up include: %Device.ActiveMonitorUpNames

  Notes on this device (from device property page):

  %Device.Notes

  ----------------------------------------
  ```

  This message was logged on %System.Date at %System.Time

  ```
  Ipswitch WhatsUp Gold
  ```

Tip: Right-click in the **Log Message** box to select the percent variables you would like to use in the action.

4 Click **OK** to save changes.

Adding and editing a Pager Action

The Pager action sends a user-specified message to a pager.

To add a new Pager action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Pager Action**, then click **OK**. The New Pager Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Terminal number**. Enter the pager number to dial. Your service provider can provide you with this number.

§ **Terminal password**. If required, enter the pager password here. This is a password that is required to log in to some paging services.

§ **Modem Setup**. Select either Primary, or one of the Alternate setups.

§ **Protocol**. Select the type of protocol used by your pager service.

§ **Pager ID**. Enter the pager identification number.

§ **Message**. Enter a text message plus any of the percent variable codes used to deliver WhatsUp Gold information with the page.

5 (Optional) Click **Port Settings** to further define your modem setup selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your pager notifications. There could also be times you want to change your settings to meet a specific service provider's requirements for a specific notification (for example: a lower baud rate). To do this, you can set up an alternate Modem Setup and associate this to the notification instead of using your Primary setting.

Note: Changing the port settings for the desired modem setup affects ALL uses of that setting.

6 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Pager action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Terminal number**. Enter the pager number to dial. Your service provider can provide you with this number.

§ **Terminal password**. If required, enter the pager password here. This is a password that is required to log in to some paging services.

§ **Modem Setup**. Select either Primary, or one of the Alternate setups.

§ **Protocol**. Select the type of protocol used by your pager service.

§ **Pager ID**. Enter the pager identification number.

§ **Message**. Enter a text message plus any of the percent variable codes used to deliver WhatsUp Gold information with the page.

4 (Optional) Click **Port Settings** to further define your modem setup selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your pager notifications. There could also be times you want to change your settings to meet a specific service provider's requirements for a specific notification (for example: a lower baud rate). To do this, you can set up an alternate Modem Setup and associate this to the notification instead of using your Primary setting.

Note: Changing the port settings for the desired modem setup affects ALL uses of that setting.

5 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing a PowerShell action

Windows PowerShell is a scripting language and command-line shell that system administrators can use to manage Windows operating systems. For more information on PowerShell, please visit the *Microsoft web site* (http://www.whatsupgold.com/MSPowerShell).

The PowerShell action delivers a robust and flexible environment to the experienced user for developing custom actions through direct access to script component libraries, including the .NET Framework. For more information, see *PowerShell action script examples* (on page 319).

To add a new PowerShell action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **PowerShell**, then click **OK**. The New PowerShell Script Action dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: You are highly discouraged from using a timeout longer than 10 seconds. Please use the shortest timeout possible.

- **Script Text.** Enter your action code.

> **Important**: When using percent variables as part of string literals in your PowerShell scripts, please use double quotation marks (" ") instead of single quotation marks (' ') to enclose the string literal. For example: $Message = "%Device.DisplayName changed state".

5 Click **OK** to save changes.

6 Click **OK** to exit the Action Library.

To edit an existing PowerShell action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**. The Edit PowerShell Script Action dialog appears.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.

> **Note**: You are highly discouraged from using a timeout longer than 10 seconds. Please use the shortest timeout possible.

- **Script Text.** Enter your action code.

4 Click **OK** to save changes.

5 Click **OK** to exit the Action Library.

Example - PowerShell action scripts

The PowerShell action scripts have two instantiated objects available to support successful execution:

- **Context**. An implementation of the IScriptContext interface. This object provides access to runtime variables and also provides mechanism for returning results to the client. A few useful methods are listed below:
- object GetProperty(string propertyName) - allows retrieval of context variable values by name.
- void SetResult(int resultCode, string resultText) - allows the script to set a value to indicate success, usually 0 = success and 1 = failure. The second argument allows the script to provide a text string as output.
- **Logger**. An implementation of the ILog interface. This object provides the same methods available to C# applications. A few useful methods are listed below:
- void Error(string message) - Creates an Error-specific log entry that includes the message.
- void Information(string message) - Creates an information-specific log entry that includes the message.
- void WriteLine(string message) - Creates a generic log entry that includes the message.

Context Variables

The following context variables are available for use in PowerShell action scripts:

- DeviceID
- DisplayName
- Address
- NetworkName
- Timeout
- TriggerCondition
- ActionName
- ActionTypeID

Percent Variables

Please see Percent Variables for a list of percent variables that are available for use in PowerShell action scripts.

✓ **Important**: When using percent variables as part of string literals in your PowerShell scripts, please use double quotation marks (" ") instead of single quotation marks (' ') to enclose the string literal. For example: $Message = "%Device.DisplayName changed state".

Script Timeout

The user can configure a script timeout value (in seconds). If the script has not finished executing before the timeout value expires it will be aborted.

Minimum: 1

Maximum: 60

Default: 10

Example Scripts

Example 1:

```
#

# This example plays a sound file

#



# Point to an existing wav file

$wavFile = "C:\temp\Sound1.wav"



# Create a .NET SoundPlayer object

$sound = new-Object System.Media.SoundPlayer;

$sound.SoundLocation=$wavFile;



# Play the file

$sound.Play();



# Report the action results. The text will also be logged

$Context.SetResult($result, "Sound action completed")
```

Example 2:

```
#

# This example sends an email
```

```
#


# Change this value to the recipient

$to = "target_email"


# Change this value to the sender

$from = "source_email"


# This line creates a .NET object for the message

$message = New-Object system.Net.Mail.MailMessage $from, $to


$message.Subject = "Notification from " +
$Context.GetProperty("DisplayName")

$message.Body = "Address is down: " + $Context.GetProperty("Address")


# Name the mail server

$server = "alpha.ipswitch.com"


# Create a .NET object to represent the mail client

$client = New-Object System.Net.Mail.SmtpClient $server

$client.UseDefaultCredentials = $true

$result = 1


# Send the message.  If no exception is thrown, consider it a success

try {

      $client.Send($message);

      $result = 0
}

catch {

      $result = 1

}


# Report the action results. The text will also be logged

$Context.SetResult($result, "Email Action Completed")
```

Adding and editing a Program Action

Program actions can be defined to launch an external application when a state change occurs.

To add a new Program action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Program Action**, then click **OK**. The New Program Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Program file name**. Enter the file path where the working files for the application are stored.

§ **Working path**. Enter the file path where the working files for the application are stored. The working path is located on the server where WhatsUp Gold is running.

§ **Program arguments**. Enter any percent variables you want to pass to the specified program.

5 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Program action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Program file name**. Enter the file path where the working files for the application are stored.
- **Working path**. Enter the file path where the working files for the application are stored. The working path is located on the server where WhatsUp Gold is running.
- **Program arguments**. Enter any percent variables you want to pass to the specified program.

4 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing a Service Restart Action

After you configure this action, you can start or stop a Windows service when another device or monitor experiences a state change. In order for the Service Restart Action to work:

- Both the WhatsUp Gold computer and the target device (where the Windows service is to restart) must have identical user accounts.
- The Ipswitch WhatsUp Engine service needs to log on as a user account that belongs to the administrators group and that exists on the target machine.

To set up the service restart action:

1 Go to **Windows Control Panel > Administrative Tools > Services**.

2 Right click **Ipswitch WhatsUp Engine**, then select **Properties**.

3 Click the **Log On** tab, select **Log on as: This account**, then enter the user name and password.

Important: If the service that is to be stopped or started by the action is running on a Windows XP machine, then the machine requires the following settings.

- **Set Local Security settings**. Click **Local Security Settings > Local Policies > Security Options > Network Access: Sharing and security model for local accounts > Classic - local users authenticate as themselves.**

4 In the WhatsUp Gold Action Library, in the Service Restart Action dialog, complete the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Host**. Enter the desired host from your network neighborhood.
- **User name (domain\username)**. Enter a user login to use with this monitor. In order to monitor the service on another machine, the WinEvent monitor has to be configured with the correct user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, then

the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user. No user name and password is needed for local services (services on the machine where WhatsUp Gold is running).

- **Password**. Enter the password for the login used above.

  To monitor Windows services on a XP machine with an account that has empty password, the XP Local Security Settings might have to be modified:

  From **Administrative tools > Local Security Settings**, select **Security Settings > Local Policies > Security Options**. Next, right click on **Account**: **Limit local account use of blank passwords to console logon only**, then click **Properties**, and select **Disable**.

- **Service**. Click browse (**...**) to select the desired service associated with your host.
- **Command**. Select either Start or Stop, depending on whether you want the associated alert to start or stop the service you have selected.

5 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Service Restart action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Host**. Enter the desired host from your network neighborhood.
- **User name (domain\username)**. Enter a user login to use with this monitor. In order to monitor the service on another machine, the WinEvent monitor has to be configured with the correct user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, then the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user. No user name and password is needed for local services (services on the machine where WhatsUp Gold is running).
- **Password**. Enter the password for the login used above.

  To monitor Windows services on a XP machine with an account that has empty password, the XP Local Security Settings might have to be modified:

  From **Administrative tools > Local Security Settings**, select **Security Settings > Local Policies > Security Options**. Next, right click on **Account**: **Limit local account use of blank passwords to console logon only**, then click **Properties**, and select **Disable**.

- **Service**. Click browse (**...**) to select the desired service associated with your host.
- **Command**. Select either Start or Stop, depending on whether you want the associated alert to start or stop the service you have selected.

4 Click **OK** to save changes.

> **Tip**: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing a SMS Action

The SMS Action sends a Short Message Service (SMS) notification to a pager or cell phone using an email gateway or dial-up modem. An SMS Action can also be used as an SMS notification in the WhatsUp Gold Alert Center.

To add a new SMS action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **SMS Action**, then click **OK**. The New SMS Action dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Country**. Select the country for the SMS provider.
- **Provider**. Select the desired provider. If the provider list is incomplete and/or incorrect, you can click browse (**...**) to add, edit, or delete providers in this list.
- **Mode**. Either *Email* or *Dialup*, depending on how the provider was created in the system.
- **Email to**. If the connection setting is *Email*, enter the email address of the SMS device.
- **Phone Number**. If the connection setting is *Dialup*, enter the phone number to call with the message. You can enter multiple phone numbers, separated by a comma. There is a 2,000 character limit in this field. Also, non-numeric characters such as "-" and "." are ignored.

5 The New/Edit SMS Action dialog contains two tabs. Select a tab to configure message settings.

The **Message** tab contains options pertaining to the message sent as the result of an active or passive monitor.

Enter a text message plus any desired percent variable codes. Keep in mind that if you use percent variables, this will greatly increase the character count.

> **Note**: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

Tip: Click **Mobile Device Status** to insert a link to the device status in the message.

The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

Enter a text message plus any desired percent variable codes. Keep in mind that if you using percent variables greatly increases the character count.

Tip: To enter Alert Center percent variables, right click inside the **Message** box.

Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

6 Click **OK** to save changes.

To edit an existing SMS action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Country**. Select the country for the SMS provider.

§ **Provider**. Select the desired provider. If the provider list is incomplete and/or incorrect, you can click browse (**...**) to add, edit, or delete providers in this list.

§ **Mode**. Either *Email* or *Dialup*, depending on how the provider was created in the system.

§ **Email to**. If the connection setting is *Email*, enter the email address of the SMS device.

4 **Phone Number**. If the connection setting is *Dialup*, enter the phone number to call with the message. You can enter multiple phone numbers, separated by a comma. There is a 2,000 character limit in this field. Also, non-numeric characters such as "-" and "." are ignored.

5 The New/Edit SMS Action dialog contains two tabs. Select a tab to configure message settings.

The **Message** tab contains options pertaining to the message sent as the result of an active or passive monitor.

Enter a text message plus any desired percent variable codes. Keep in mind that if you use percent variables, this will greatly increase the character count.

Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

Tip: Click **Mobile Device Status** to insert a link to the device status in the message.

The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

Enter a text message plus any desired percent variable codes. Keep in mind that if you using percent variables greatly increases the character count.

Tip: To enter Alert Center percent variables, right click inside the **Message** box.

Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

6 Click **OK** to save changes.

Adding and editing a SMS Direct Action

SMS Direct messages are similar to SMS messages, except a phone line is not required. Instead, messages are sent directly to a cell phone, or other texting capable device, via a GSM modem. If the receiving phone is not active or is out of range when a SMS message is sent, messages are received when the phone is turned on. SMS messages are listed in the WhatsUp Gold Action log.

You need the following items to use the SMS Direct Action:

§ GSM modem to connect to the WhatsUp machine

§ SIM card for the GSM modem

§ Cell service/signal in the room in which the WhatsUp machine and GSM modem reside

To add a new SMS Direct action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **SMS Direct**, then click **OK**. The New SMS Direct Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Phone number**. Enter the cell phone number(s) of the intended SMS message recipients.

Note: All non-numeric characters such as "-" and ".", are ignored.

Note: There is a 2,000 character limit in this box.

§ **COM Port**. Select the COM port you want to use with this notification.

Note: The list displays all ports associated with the GSM modem, including virtual and hard-wired, serial ports. You must select the port that is assigned to the modem in the Windows Device Manager.

§ **Message**. Enter a text message, plus any desired percent variable codes. Using percent variables greatly increases character count.

Note: If the message exceeds 140 characters, the message may be broken into up to three parts and is sent as separate messages ("1 of 3", "1 of 2", etc.), each message containing up to 140 characters, for a total of up to 420 characters. Spaces are included in the character count.

The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

Enter a text message plus any desired percent variable codes. Keep in mind that if you using percent variables greatly increases the character count.

Tip: To enter Alert Center percent variables, right click inside the **Message** box.

Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

5 Click **OK** to save changes.

To edit an existing SMS Direct action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Phone number**. Enter the cell phone number(s) of the intended SMS message recipients. You can enter multiple phone numbers, separated by a comma. For example: 555-555-5555, 55 555 55 55 55, (555) 555 5555

Note: All non-numeric characters, other than the comma, such as "-" and ".", are ignored.

Note: There is a 2,000 character limit in this box.

§ **COM Port**. Select the COM port you want to use with this notification.

Note: The list displays all ports associated with the GSM modem, including virtual and hard-wired, serial ports. You must select the port that is assigned to the modem in the Windows Device Manager.

The New/Edit SMS Direct Action dialog contains two tabs. Select a tab to configure message settings.

The **Message** tab contains options pertaining to the message sent as the result of an active or passive monitor.

Enter a text message, plus any desired percent variable codes. If you use percent variables, the character count is greatly increased.

Note: If the message exceeds 140 characters, the message may be broken into up to three parts and is sent as separate messages ("1 of 3", "1 of 2", etc.), each message containing up to 140 characters, for a total of up to 420 characters. Spaces are included in the character count.

The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

Enter a text message plus any desired percent variable codes. Keep in mind that if you using percent variables greatly increases the character count.

Tip: To enter Alert Center percent variables, right click inside the **Message** box.

Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

4 Click **OK** to save changes.

Adding and editing a SNMP Set Action

This action sends an SNMP Set to a device in order to change a specific SNMP action. You can configure SNMP Set actions to perform a number of tasks, including rebooting a device, changing the state of a network remotely, disabling or enabling a device feature, etc.

The SNMP Set action can use any SNMP credential defined in the WhatsUp Gold Credential Library and supports all types of writable objects (strings, integers, timeticks, etc.).

If the action operation fails, errors are reported to the Action log.

To add a new SNMP Set action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **SNMP Set**, then click **OK**. The New SNMP Set Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **IP address or host name**. Enter the IP address or host name of the device to which the action to send the SNMP Set.
- **SNMP v1/v2/v3 credentials**. Select the SNMP credential that the action is to use. This list is populated with credentials currently configured in the Credentials Library.
- **Object identifier**. Enter the object identifier (OID) that the action is to use or click browse (**...**) to select the OID.
- **Instance**. Enter the instance that coincides with the OID that the action is to use or click browse (**...**) to select the instance.
- **Value type**. Select the type of written object the action is to use.
- **Value to set**. Enter a value for the type you selected.

Note: The action only allows you to set one value at a time.

5 (Optional) Click **Advanced** to change the SNMP timeout and retry settings.

6 Click **OK** to save changes.

To edit an existing SNMP Set action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **IP address or host name**. Enter the IP address or host name of the device to which the action to send the SNMP Set.
- **SNMP v1/v2/v3 credentials**. Select the SNMP credential that the action is to use. This list is populated with credentials currently configured in the Credentials Library.
- **Object identifier**. Enter the object identifier (OID) that the action is to use or click browse (**...**) to select the OID.
- **Instance**. Enter the instance that coincides with the OID that the action is to use or click browse (**...**) to select the instance.
- **Value type**. Select the type of written object the action is to use.
- **Value to set**. Enter a value for the type you selected.

Note: The action only allows you to set one value at a time.

4 (Optional) Click **Advanced** to change the SNMP timeout and retry settings.

5 Click **OK** to save changes.

Adding and editing a Sound Action

A sound file can be assigned to an action by creating a sound action.

Note: The Desktop Actions application must be running for the Sound action to work. For more information, see *About the Task Tray and Desktop Actions applications* (on page 21).

If you want to bring the text-to-speech action sound to a Windows 2003 or Windows 2008 server class remote desktop (RDP) system, you need to enable audio mapping for the remote system Terminal Services Configuration. To do this:
1. In Windows, click **Start > Run**, in the Run dialog type `TSCC.msc`, then click **OK**.
2. In the Connections folder, double-click **RDP-tcp**. The RDP-TCP Properties dialog appears.
3. Select the **Client Settings** tab, then click to clear the **Audio Mapping** check box. When enabled, the text-to-speech action sound only plays on the remote desktop system.

To add a new Sound action:

1. From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.
2. Click **New**. The Select Action Type dialog appears.
3. Select **Sound Action**, then click **OK**. The New Sound Action dialog appears.
4. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the action. This name displays in the Action Library.
   - **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
   - **Sound file name**. Enter the full path to the sound file. The sound file name is located on the server where WhatsUp Gold is running.
   - **Continuous play**. Select this option to have the sound play continuously until the Cancel Sound button is clicked on the main WhatsUp Gold toolbar.
5. Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Sound action:

1. From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.
2. Select the action you would like to edit, then click **Edit**.
3. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the action. This name displays in the Action Library.
   - **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
   - **Sound file name**. Enter the full path to the sound file. The sound file name is located on the server where WhatsUp Gold is running.

- **Continuous play**. Select this option to have the sound play continuously until the Cancel Sound button is clicked on the main WhatsUp Gold toolbar.

4 Click **OK** to save changes.

> **Tip**: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing a SSH Action

The SSH action connects to remote devices via SSH to execute commands or scripts.

To add a new SSH action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **SSH Action**, then click **OK**. The New SSH Action dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **IP address**. Enter the IP address of the device to which you want to connect using SSH.

> **Note**: You can enter `%Device.Address` into the **IP Address** field; however, an SSH action that does not specify a specific IP address in this field is not available in the Recurring Actions wizard.

- **Command to run**. Enter the command to be run and executed on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.

> **Note**: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- **SSH credential**. Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device for which the IP address is listed above. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.

5 Click **OK** to save changes.

To edit an existing SSH action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **IP address**. Enter the IP address of the device to which you want to connect using SSH.

Note: You can enter `%Device.Address` into the **IP Address** box; however, an SSH action that does not specify a specific IP address in this box is not available in the Recurring Actions wizard.

§ **Command to run**. Enter the command to be run and executed on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.

Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

§ **SSH credential**. Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device for which the IP address is listed above. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.

4 Click **OK** to save changes.

Adding and editing a Syslog Action

When a device does not respond to polling, you can send a Syslog message to a host that is running a Syslog server.

To add a new Syslog action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Syslog Action**, then click **OK**. The New Syslog Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Syslog Server**. Enter the IP address or hostname of the machine that is running the Syslog server.

§ **Port**. Enter the UDP port that the Syslog listener is listening on. The default port is 514.

- **Message**. Enter a text message to send to the Syslog server. This message may include notification variables. The Syslog message box limits input to 511 characters. If notification variables are used, then the message that actually gets sent is limited to 1023 bytes, in order to comply with the Syslog protocol. Non-visible ASCII characters such as tabs and line feeds are replaced by space characters.

5 Click **OK** to save changes.

> **Note**: If you attempt to run another application on the same system that also listens on the same Syslog port as WhatsUp Gold, the error message *Unable to Open Socket* displays.
>
> **Note**: The WhatsUp Gold Syslog listener runs on Port 514 by default. This port can be configured in the WhatsUp Gold console at **Configure > Program Options > Passive Monitor Listeners > Syslog**.
>
> **Tip**: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Syslog action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Syslog Server**. Enter the IP address or hostname of the machine that is running the Syslog server.
- **Port**. Enter the UDP port that the Syslog listener is listening on. The default port is 514.
- **Message**. Enter a text message to send to the Syslog server. This message may include notification variables. The Syslog message box limits input to 511 characters. If notification variables are used, then the message that actually gets sent is limited to 1023 bytes, in order to comply with the Syslog protocol. Non-visible ASCII characters such as tabs and line feeds are replaced by space characters.

4 Click **OK** to save changes.

> **Note**: If you attempt to run another application on the same system that also listens on the same Syslog port as WhatsUp Gold, the error message *Unable to Open Socket* displays.
>
> **Note**: The WhatsUp Gold Syslog listener runs on Port 514 by default. This port can be configured in the WhatsUp Gold console at **Configure > Program Options > Passive Monitor Listeners > Syslog**.
>
> **Tip**: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and editing a Text-To-Speech Action

This action plays a text-to-speech message on your computer.

Note: The Desktop Actions application must be running for the Text to Speech action to work.

If you want to bring the text-to-speech action sound to a Windows 2003 or Windows 2008 server class remote desktop (RDP) system, you need to enable audio mapping for the remote system's Terminal Services Configuration. To do this:
1. In Windows, click **Start > Run**, in the Run dialog type `TSCC.msc`, then click **OK**.
2. In the **Connections** folder, double-click **RDP-tcp**. The RDP-TCP Properties dialog appears.
3. Select the **Client Settings** tab, then click to clear the **Audio Mapping** check box. When enabled, the text-to-speech action sound only plays on the remote desktop system.

To add a Text to Speech action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Text to Speech Action**, then click **OK**. The New Text to Speech Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Speak Rate**. Select how fast the voice speaks the message.

§ **Volume**. Select the volume of the message.

§ **Message**. Enter any text message you want audibly repeated. You can use your own text in addition to percent variables.

5 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

To edit an existing Text to Speech action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**. The Edit Text to Speech Action dialog appears.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Speak Rate**. Select how fast the voice speaks the message.

- **Volume**. Select the volume of the message.
- **Message**. Enter any text message you want audibly repeated. You can use your own text in addition to percent variables.

4 Click **OK** to save changes.

Tip: To check the status of an action, or to cancel an action, in the WhatsUp Gold console go to **Tools > Running Actions**.

Adding and Editing a VMware Action

VMWare actions perform operations such as starting, stopping, or taking a snapshot of virtual machines running on a VMware host or being managed by a VMware vCenter server.

To add a new VMware action:

1. From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.
2. Click **New**. The Select Action Type dialog appears.
3. Select **VMWare**, then click **OK**. The Add VMWare Action dialog appears.
4. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the action. This name displays in the Action Library.
   - **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
   - **VMware server IP address**. Enter the IP address of the VMware host or vCenter server managing the virtual machine.
   - **VMware credentials**. Select the VMware credentials from the Credentials Library for the VMware host or vCenter server managing the virtual machine. Click browse (**...**) to manage credentials in the credentials library.
   - **VMware name**. Select the Virtual machine VMware name for the virtual machine on which you want the action performed. You can enter the VMware name, or select from the list of virtual machines associated with the VMware host or vCenter server. Click browse (**...**) to access the list of virtual machines associated with the VMware host.
   - **Operation**. Select the operation you want the action to perform from the list.

     The following operations can be performed on a virtual machine:
     - **Power On**. Powers up the virtual machine and boots the guest operating system if the guest operating system is installed.
     - **Power Off**. Powers down the virtual machine. The virtual machine does not attempt to gracefully shut down the guest operating system.
     - **Reset**. Powers down the virtual machine and restarts it.
     - **Shutdown**. Shuts down the guest operating system. If the guest operating system automatically powers off its host, then the virtual machine also powers off.
     - **Suspend**. Pauses the virtual machine activity; all transactions are frozen.

- § **Restart**. Shuts down and restarts the guest operating system; does not power off the virtual machine.
- § **Take snapshot**. Saves the current state of the virtual machine to the virtual disk of the guest system.

5 Click **OK** to save changes.

To edit an existing VMWare action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- § **Name**. Enter a unique name for the action. This name displays in the Action Library.
- § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- § **VMware server IP address**. Enter the IP address of the VMware host or vCenter server managing the virtual machine.
- § **VMware credentials**. Select the VMware credentials from the Credentials Library for the VMware host or vCenter server managing the virtual machine. Click browse (**...**) to manage credentials in the credentials library.
- § **VMware name**. Select the Virtual machine VMware name for the virtual machine on which you want the action performed. You can enter the VMware name, or select from the list of virtual machines associated with the VMware host or vCenter server. Click browse (**...**) to access the list of virtual machines associated with the VMware host.
- § **Operation**. Select the operation you want the action to perform from the list box.

  The following operations can be performed on a virtual machine:

  - § **Power On**. Powers up the virtual machine and boots the guest operating system if the guest operating system is installed.
  - § **Power Off**. Powers down the virtual machine. The virtual machine does not attempt to gracefully shut down the guest operating system.
  - § **Reset**. Powers down the virtual machine and restarts it.
  - § **Shutdown**. Shuts down the guest operating system. If the guest operating system automatically powers off its host, then the virtual machine also powers off.
  - § **Suspend**. Pauses the virtual machine activity; all transactions are frozen.
  - § **Restart**. Shuts down and restarts the guest operating system; does not power off the virtual machine.
  - § **Take snapshot**. Saves the current state of the virtual machine to the virtual disk of the guest system.

4 Click **OK** to save changes.

Adding and Editing a Web Alarm Action

The Web Alarm action sounds an alarm by playing sound file on the WhatsUp Gold console. For more information on how Web Alarms work, see the Working with Web Alarms topic.

Note: In previous versions of WhatsUp Gold, the Web Alarm action was included in the Implicit Action Policy. This is no longer true in WhatsUp Gold v14 and later.

To add a new Web Alarm action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Web Alarm**, then click **OK**. The New Web Alarm Action dialog appears.

4 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Message**. Enter a short message to send to the visual cue part of the Web Alarm in the web interface. You can use percent variable codes to display specific information in the message body.
- **Play Sound**. Select this option to play the sound file whenever a web alarm action fires. Clear this option to only have the visual cue appear in the Web Interface.
- **Sound file name**. Select a sound file that is installed in your `\Program Files\Ipswitch\WhatsUp\HTML\Nm.UI\WebSounds` directory. Custom sounds added to this directory appear in the drop-down list.

5 Click **OK** to save changes.

Note: For Web Alarms to work properly, your browser must support embedded sound files.

To edit an existing Web Alarms action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Message**. Enter a short message to send to the visual cue part of the Web Alarm in the web interface. You can use percent variable codes to display specific information in the message body.
- **Play Sound**. Select this option to play the sound file whenever a web alarm action fires. Clear this option to only have the visual cue appear in the Web Interface.
- **Sound file name**. Select a sound file that is installed in your `\Program Files\Ipswitch\WhatsUp\HTML\Nm.UI\WebSounds` directory. Custom sounds added to this directory appear in the drop-down list.

4 Click **OK** to save changes.

Note: For Web Alarms to work properly, your browser must support embedded sound files.

The Web Alarm popup window

When a Web alarm Action fires and you are logged into the WhatsUp Gold web interface, the Web Alarm popup appears in your browser. From here, you can:

- Dismiss one or all of the alarms
- Mute alarms to stop the alarm from sounding
- Access detailed information by double-clicking the device to bring up the Device Status Dashboard

Note: You cannot disable Web Alarms from the Web Alarm popup.

Note: If there are web alarms in the list with different sounds configured for each, the oldest web alarm's sound takes priority. To hear a new or different sound for a web alarm, dismiss the previous web alarm from the list.

Note: In order for a WhatsUp Gold user to view the Web Alarm popup and hear the alarm that sounds, a user must have the **Manage Devices** user right enabled. For more information, see About user rights.

Enabling and disabling Web Alarms

While you can mute and dismiss web alarms from the Web Alarms popup window, you cannot disable, or turn them off, from there. Instead, you must enable and disable web alarms in the WhatsUp Gold web interface. To do this:

1. Click your username in the upper right of the web interface. The Preferences dialog appears.
2. Select the **Enable web alarms** check box.
3. (Optional) Enter an interval into the **Check every (seconds)** box to adjust the web alarms check interval. This interval indicates the number of seconds WhatsUp Gold waits before checking for new Web Alarms. By default, Web Alarms are enabled on the web interface and are checked every 120 seconds.

Accessing Web Alarms on the web interface

There are two places users can access Web Alarms from the WhatsUp Gold web interface:

- **The Web Alarm window**. Click **Devices > Web Alarms**. The Web Alarms dialog appears.
- **The Web Alarms dashboard report**. This is an optional dashboard report you can add to a view on the Home Dashboard. This report displays recent Web Alarms.

You can also create a dynamic group to provide easy access to your current network Web Alarms. For more information on Dynamic Groups in WhatsUp Gold, please see Configuring Dynamic Groups.

Adding and Editing a Windows Event Log Action

The Windows Event Log action allows you to configure log messages to post to the Windows Event Viewer.

To add a Windows Event Log action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **Windows Event Log**, then click **OK**. The New Windows Event Log Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Source**. The origin of messages logged to the Windows Event Viewer. The default source is the Ipswitch WhatsUp Log Action.

§ **Event ID**. Enter an event ID for the messages that are logged to the Windows Event Viewer. The default event ID is 1000, the WhatsUp engine event ID.

§ **Level**. Select a level for messages logged to the Windows Event Viewer. You can select Error, Warning, or Information. The default level is Error.

§ **Log Message**. Enter a log message that displays in the Windows Event Viewer. This message supports percent variables. The default log message is: %Device.ActiveMonitorDownNames is %Device.State on %Device.Type: %Device.HostName (%Device.Address).

```
Details:

Monitors that are down include: %Device.ActiveMonitorDownNames

Monitors that are up include: %Device.ActiveMonitorUpNames

Notes on this device (from device property page):

%Device.Notes

----------------------------------------

This message was logged on %System.Date at %System.Time

Ipswitch WhatsUp Gold
```

Tip: Right-click in the **Log Message** box to select the percent variables you would like to use in the action.

5 Click **OK** to save changes.

To edit an existing Windows Event Log action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Source**. The origin of messages logged to the Windows Event Viewer. The default source is the Ipswitch WhatsUp Log Action.

§ **Event ID**. Enter an event ID for the messages that are logged to the Windows Event Viewer. The default event ID is 1000, the WhatsUp engine event ID.

§ **Level**. Select a level for messages logged to the Windows Event Viewer. You can select Error, Warning, or Information. The default level is Error.

§ **Log Message**. Enter a log message that displays in the Windows Event Viewer. This message supports percent variables. The default log message is: %Device.ActiveMonitorDownNames is %Device.State on %Device.Type: %Device.HostName (%Device.Address).

```
Details:
Monitors that are down include: %Device.ActiveMonitorDownNames
Monitors that are up include: %Device.ActiveMonitorUpNames
Notes on this device (from device property page):
%Device.Notes
----------------------------------------
This message was logged on %System.Date at %System.Time
Ipswitch WhatsUp Gold
```

Tip: Right-click in the **Log Message** box to select the percent variables you would like to use in the action.

4 Click **OK** to save changes.

Using the WinPopup Action

The WinPopup action displays a user-specified message in a pop-up window on a Windows NT system.

Note: WinPopup actions are not supported on Windows Vista or later operating systems.

To add a WinPopup action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.

2 Click **New**. The Select Action Type dialog appears.

3 Select **WinPopup Action**, then click **OK**. The New WinPopup Action dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Destination**. Specify the Windows NT host or domain that you want to receive this notification.
- **Message**. Enter a text message using *percent variables* (on page 342) if needed.
- **Refresh**. Click to refresh the **Destination** list. This populates the list with all of the targets you can choose in which to send a Winpopup action.

5 Click **OK** to save changes.

To edit an existing WinPopup action:

1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.

2 Select the action you would like to edit, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the action. This name displays in the Action Library.
- **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- **Destination**. Specify the Windows NT host or domain that you want to receive this notification.
- **Message**. Enter a text message using *percent variables* (on page 342) if needed.
- **Refresh**. Click to refresh the **Destination** list. This populates the list with all of the targets you can choose in which to send a Winpopup action.

4 Click **OK** to save changes.

About Percent Variables

Percent variables allow you to customize the message notification sent from an action.

These variables can be used in all of the WhatsUp Gold actions, though we do not recommend that you use them in the Active Script action, as they may cause the action's code to break.

Percent Variables

You can customize an action's message by adding any of the percent variables in the following table.

Note: We do not recommend that you use percent variables in script text (active script action), because they may resolve to text containing special characters ('' (quotes), "" (double-quotes), % (percent), new line characters, and the like) that may break your script.

Important: Active monitor variables are only used when an action is associated directly with an active monitor, and not the device as a whole.

✓ **Important**: When using percent variables as part of string literals in your PowerShell scripts, please use double quotation marks (" ") instead of single quotation marks (' ') to enclose the string literal. For example: $Message = "%Device.DisplayName changed state".

Active Monitor Variables	**Description**
`%ActiveMonitor.Argument`	SNMP instance number. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
`%ActiveMonitor.Comment`	The human readable name that coincides with the network switch. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
`%ActiveMonitor.Name`	The name of the active monitor that fired an action. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
`%ActiveMonitor.NetworkInterfaceAddress`	IP address for the network interface. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
`%ActiveMonitor.Payload`	The payload returned by a WMI, Exchange, SQL, SNMP or Active Script active monitor. This is only used when an action is associated directly with an active monitor and not the devices as a whole. For Active Script Active Monitors, the payload is the text that is passed to the `SetResult()` method in the script.
`%ActiveMonitor.State`	The Current status of the monitor, such as "Down at least 5 min." This is only used when an action is associated directly with an active monitor, and not the device as a whole.

Device Variables	**Description**
`%Device.ActiveMonitorDownNames`	List of down services using the abbreviated name if available.
`%Device.ActiveMonitorUpNames`	Full service names of all UP monitored services on a device.
`%Device.Address`	IP address (from device properties).
`%Device.Attribute.[Attribute Name]`	Returns an attribute from the SNMP information available for the device, such as the Contact name. To specify the attribute, append the category name (listed below) to the end of the variable. For example: `%Device.Attribute.Contact`, returns the contact name. Default categories: · *****. Returns all attributes · **Info1**. Upgrade path from v8

	· **Info2**. Upgrade path from v8 · **Contact.** Contact information from SNMP · **Location.** Location information from SNMP · **Description.** Description information from SNMP · **Custom.** If you have created a custom attribute you can use the name of that custom attribute in the percent variable. Example: %Device.Attribute.Phone %Device.Attribute.RackPosition To avoid an error, always place a space or line break after the attribute name.
`%Device.DatabaseID`	Returns the database ID of a device.
`%Device.DisplayName`	Display Name (from General of device properties)
`%Device.HostName`	Host Name (from General of device properties)
`%Device.Notes`	Notes. (Notes are from the device properties Notes)
`%Device.SNMPOid`	SNMP Object identifier.
`%Device.State`	The state's description (such as "Down at least 2 min" or "Up at least 5 min")
`%Device.Status`	This shows the name of the active monitor, preceded by the device state id. For example, 10|DNS. Device State ID values: 0 = Not Started, 1 = Paused, 2 = Canceled, 3 = Running, 4 = Complete, 5 = Resolving Hostname, 6 = Looking for Type, 7 = Scanning for SNMP Credentials, 8 = Scanning for Windows Credentials, 9 = Device Detail Scan, 10 = Scanning Custom Monitors, 12 = Scanning Custom Monitors, 13 = Device VMWare Host Scan, 14 = Scanning SSH Credentials, 15 = Layer 2 Scan, 16 = Computing Layer 2 Topology, 17 = Wireless Scan, 18 = Scanning Network Interfaces, 19 = Checking for Duplicate Devices, 21 = Scanning for Known Addresses
`%Device.Type`	Device Type (from General of device properties)

Passive Monitor Variables	**Description**
`%PassiveMonitor.DisplayName`	The name of the monitor as it appears in the Passive Monitor Library.
`%PassiveMonitor.LoggedText`	Detailed Event description. (SNMP traps - Returns the full SNMP trap text.) (Windows Log Entries - Returns information contained in the Windows Event Log entries.) (Syslog Entries - Returns the text contained in the Syslog message.)
`%PassiveMonitor.Payload.*`	Payload generated by a passive monitor.

`%PassiveMonitor.Payload.EventType`	The type of passive monitor (Syslog, Windows Event, or SNMP Trap)
`%PassiveMonitor.Payload.LogicalSource`	Shows the device's logical IP address.
`%PassiveMonitor.Payload.PhysicalSource`	Shows the device's physical IP address.

System Variables	Description
`%System.Date`	The current system date. Configure the date format in Regional Options (from Program Options)
`%System.DisplayNamesDownDevices`	Display names of devices with down monitors
`%System.DisplayNamesDownMonitors`	Shows the name of a device and each monitor that is down on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping
`%System.DisplayNamesUpDevices`	Display names of up devices
`%System.DisplayNamesUpMonitors`	Shows the name of a device and each monitor that is up on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping
`%System.InstallDir`	Displays the directory on which WhatsUp Gold is installed
`%System.NumberofDownDevices`	Number of down devices on your network
`%System.NumberOfDownMonitors`	Shows the number of down monitors on your network
`%System.NumberofUpDevices`	Number of up devices on your network
`%System.NumberOfUpMonitors`	Shows the number of up monitors on your network
`%System.Time`	The current system time. The format is hh:mm:ss

Testing an action

After you create an action, you can test it to make sure it works properly. You must access WhatsUp Gold through the console to access the Test option.

To test an action:

1. From the WhatsUp Gold console, click **Configure**, then click **Action Library**. The Action Library appears.
2. In the Action Library, select the action you want to test.
3. Click **Test**.
4. Review the action in the Action Progress dialog. Click **Details** to view more information about the progress of the action.

Assigning an action

After you configure an action in the Action Library, you must add it to the individual devices and monitors for which you want to receive notifications or related tasks performed.

You can assign one or more individual actions to a device, or an instance of an active or passive monitor assigned to a single device.

Note: When you assign an action to a device or monitor, an instance of that action is added to the device or monitor. Changes that you make to the action's configuration via the Action Library affect all instances of that action. For example, if you assign an action to four separate devices and then make changes from the Action Library, all four instances of that action adopt the changes.

Assigning an action to a device

To assign an action to a device:

1. In the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
2. Click **Actions**. The Device Properties - Actions dialog appears; the **Apply individual actions** option is selected by default.
3. Click **Add**. The Action Builder appears; you can choose to add an action from the Action Library, or create a new action.
4. Follow the directions in the Action Builder wizard.
5. At the end of the wizard, click **Finish** to add the action to the monitor.
6. On the Device Properties dialog, click **OK** to save changes.

Assigning an action to an active monitor

As you configure active monitors for a device, you have the opportunity to assign actions; however, it is not required that you assign them at that time. If you decide to assign an action to the monitor at a later time, you can do so through the device Properties.

To assign an action to an active monitor:

1. In the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
2. Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
3. Select the monitor to which you would like to assign an action, then click **Edit**. The Set Polling Properties dialog appears.
4. Make any adjustments to polling selections, then click **Next**. The Setup Actions for Monitor State Change dialog appears. The **Apply individual actions** option is selected by default.
5. Click **Add**. The Action Builder appears; you can choose to add an action from the Action Library, or create a new action.
6. Follow the directions in the Action Builder wizard.
7. At the end of the wizard, click **Finish** to add the action to the monitor.
8. On the Device Properties dialog, click **OK** to save changes.

Assigning an action to a passive monitor

As you configure passive monitors for a device, you have the opportunity to assign actions; however, it is not require that you assign them at that time. If you decide to assign an action to the monitor at a later time, you can do so through the device Properties.

To assign an action to a passive monitor:

1 In the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.

2 Click **Passive Monitors**. The Device Properties -Passive Monitors dialog appears.

3 Select the monitor to which you would like to assign an action, then click **Edit**. The monitor properties dialog appears.

4 Click **Add**. The Action Builder appears.

5 Select the action you would like to assign to the monitor.

6 (Optional) Create a **Blackout Schedule**.

7 Click **OK** to add the action to the monitor.

Removing an action

Because actions are assigned to devices and monitors on an individual basis, actions can only be removed on the device- and monitor-level, and must be deleted from the Action Library. Additionally, if you have assigned action policies to your devices, you can remove the action from the policy itself.

When you remove an action from a device or monitor, the action still exists in the Active Monitor Library and is available for use with other devices and monitors. When you delete an action, you remove it from the database, and from all devices and monitors to which it is assigned; further, all log data related to the action is lost. Therefore, we recommend that you only delete an action when you are absolutely positive that you will not use it in the future, and feel that the related log data is not useful to your monitoring records.

Removing an action from a device

To remove an action from a device:

1 From Details or Map View, right-click the device from which you want to remove the active monitor, then click **Properties**. The Device Properties dialog appears.

2 Click **Actions**. The Device Properties - Actions dialog appears.

3 Select the action you want to remove, then click **Remove**. A dialog appears and asks you if you are sure you want to remove the action.

4 Click **OK** to remove the action.

Removing an action from an active monitor

To remove an action from an active monitor:

1 From the Device or Map View, right-click the device from which you want to remove the action, then click **Properties**. The Device Properties dialog appears.

2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.

3 Select the monitor from which you want to remove the associated action, then click **Edit**. The Active Monitor Properties dialog appears.

4 Click **Next**. The Actions associated with the active monitor are listed.

5 Select the action you want to remove, then click **Remove**. A dialog appears and asks you if you are sure you want to remove the action.

6 Click **Yes** to remove the action, then click **Finish**.

Removing an action from a passive monitor

To remove an action from a passive monitor:

1 From the Details or Map View, right-click the device from which you want to remove the action, then click **Properties**. The Device Properties dialog appears.

2 Click **Passive Monitors**. The Device Properties - Passive Monitors dialog appears.

3 Select the monitor from which you want to remove the associated action, then click **Edit**. The Passive Monitor Properties dialog appears.

4 Under **Actions for this passive monitor**, select the action that you would like to remove, then click **Remove**. A dialog appears and asks you if you are sure you want to remove the action.

5 Click **OK** to remove the action.

Creating a Blackout Period

You can create a Blackout Period to have WhatsUp Gold suspend specific actions during a scheduled period of time. Use this feature to keep from sending a notification to someone who is on vacation, or to keep from sounding a Web Alarm when there is no one near-by to hear the alert.

Note: Polling dependencies & blackouts only apply to the collection of device active monitors.

To create a Blackout period:

1 On the device from which you want to create a Blackout Period, right-click, then click **Properties**. The Device Properties dialog appears.

2 Click **Actions**. The Device Properties - Actions dialog appears.

3 Select the action for which you want to create the Blackout Period, then click **Edit**. The monitor properties dialog appears.

4 Click **Edit**. The Action Builder appears.

5 Click **Blackout Period**. The Weekly Blackout Schedule dialog appears.

6 Set the times for which you want the blackout to occur.

Note: The schedule that you set is repeated weekly.

7 Click **OK**.

Action Policies

Action policies allow you to group or sequence multiple actions together for use on any device or monitor.

If you make changes to actions in a policy, the changes are applied to all of the devices and monitors that use that particular policy.

For more information, see:

- Adding and editing Action Policies
- Configuring an implicit Action Policy

Reports

In This Section

Working with monitor reports

In This Chapter

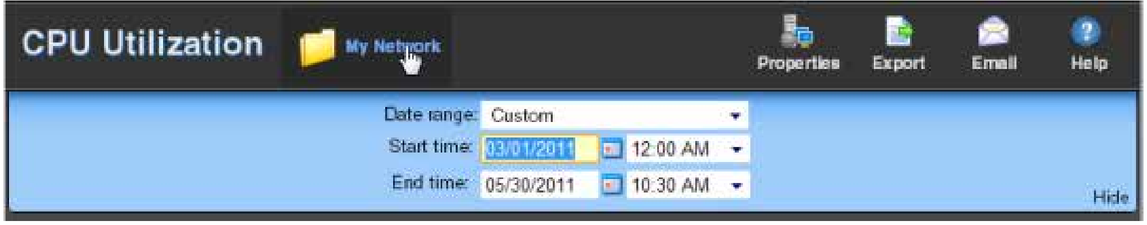
Viewing device reports

Device monitor reports display information related to specific devices. For example, you can view reports for a specific Cisco router with Interface Utilization performance monitors.

To view a report for a specific device:

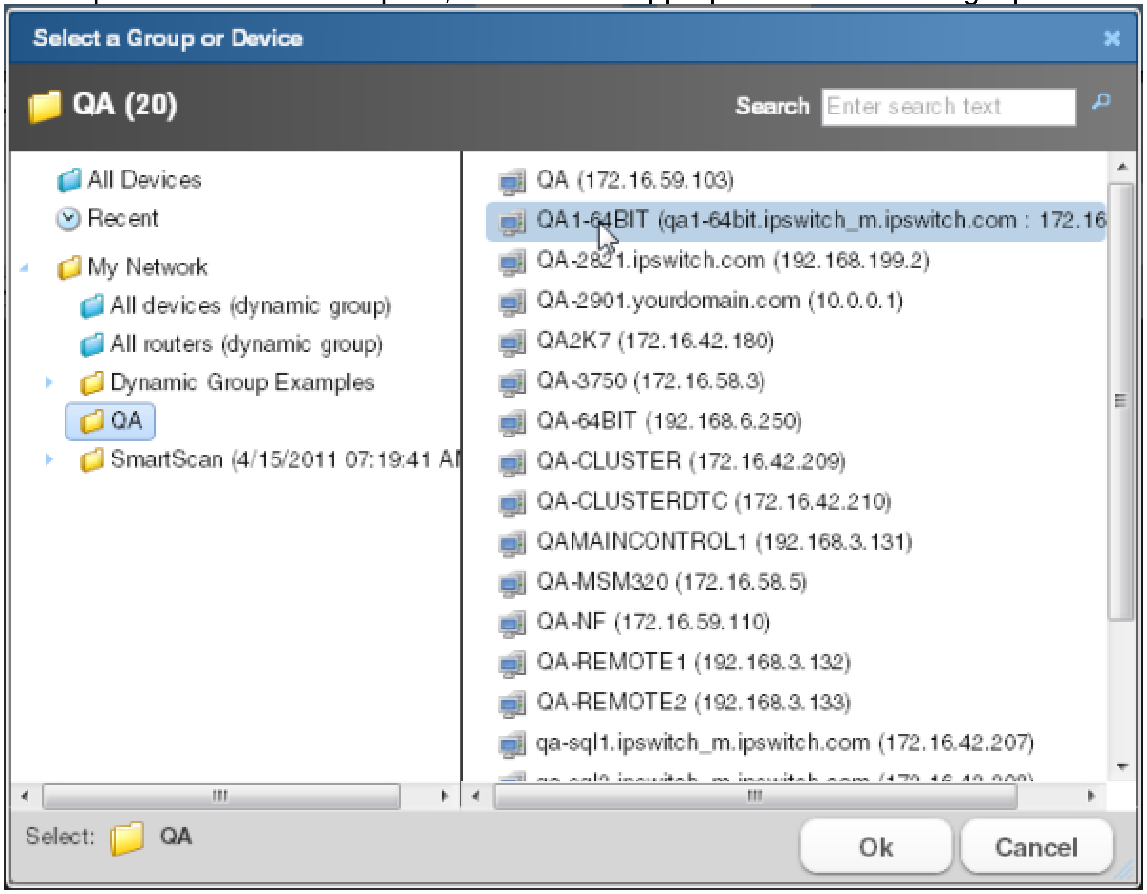
1 Click the **Reports** tab, then select the report you want to view.

2 In the page title bar, click the device context. The Select a Group or Device dialog appears.



Date range: Custom
Start time: 03/01/2011 12:00 AM
End time: 05/30/2011 10:30 AM

3 Click a parent folder in the left pane, and select the appropriate device in the right pane.

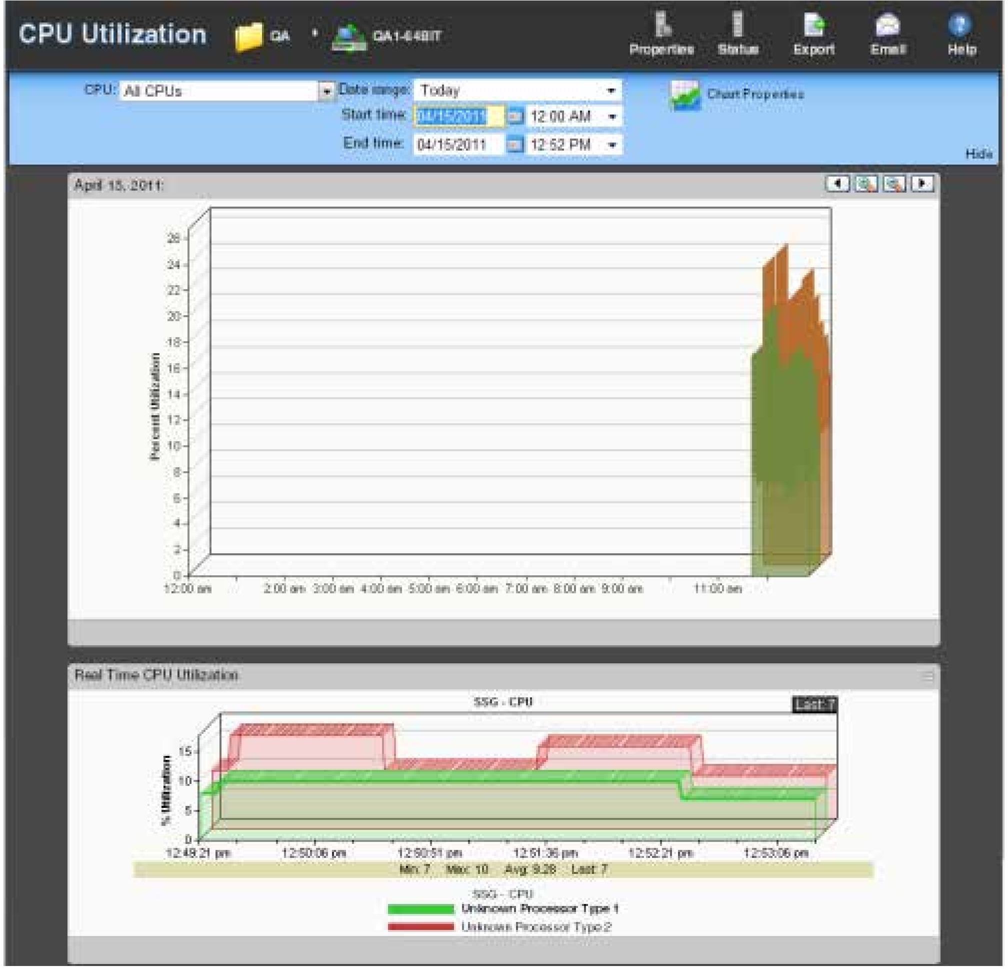


All Devices
Recent
My Network
All devices (dynamic group)
All routers (dynamic group)
Dynamic Group Examples
QA
SmartScan (4/15/2011 07:19:41 AI

QA (172.16.59.103)
QA1-64BIT (qa1-64bit.ipswitch_m.ipswitch.com : 172.16
QA-2821.ipswitch.com (192.168.199.2)
QA-2901.yourdomain.com (10.0.0.1)
QA2K7 (172.16.42.180)
QA-3750 (172.16.58.3)
QA-64BIT (192.168.6.250)
QA-CLUSTER (172.16.42.209)
QA-CLUSTERDTC (172.16.42.210)
QAMAINCONTROL1 (192.168.3.131)
QA-MSM320 (172.16.58.5)
QA-NF (172.16.59.110)
QA-REMOTE1 (192.168.3.132)
QA-REMOTE2 (192.168.3.133)
qa-sql1.ipswitch_m.ipswitch.com (172.16.42.207)

Select: QA

4 Click **OK** to make your selection. The selected device displays as the new context and the monitor report displays information for the selected device.



CPU: All CPUs

Date range: Today

Start time: 04/15/2011 12:00 AM

End time: 04/15/2011 12:52 PM

- Click the current device context to open the device picker and select a device or group from a list of devices and groups on your network.
- Click other reports on the navigation bar to view other reports for the same device.
- Use the report **Date/Time Picker**, located in the middle of the page, to easily change the time period for the report you are viewing.
- Select **Export** to export your data using the following options: Export to Text, Export to Excel, or Export to PDF.
- Select **Email** to email and schedule reports. For more information, see *Scheduling reports* (on page 376).

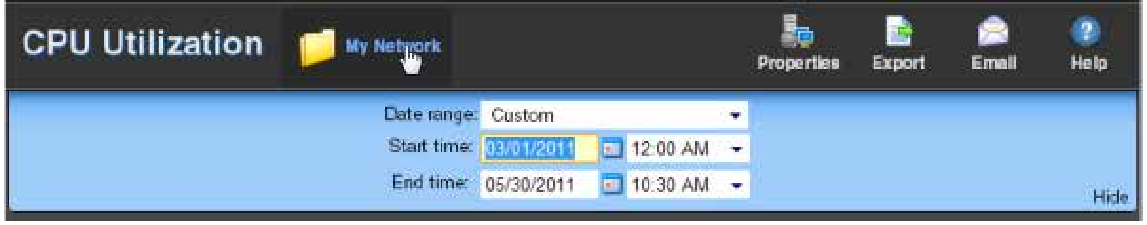
Viewing group reports

Group monitor reports display information related to specific groups. For example, you can view reports for Cisco devices with Interface Utilization performance monitors.

To view a report for a specific device group:

1 Click the **Reports** tab, then select the report you want to view.

2 In the page title bar, click the device context. The Select a Group or Device dialog appears.

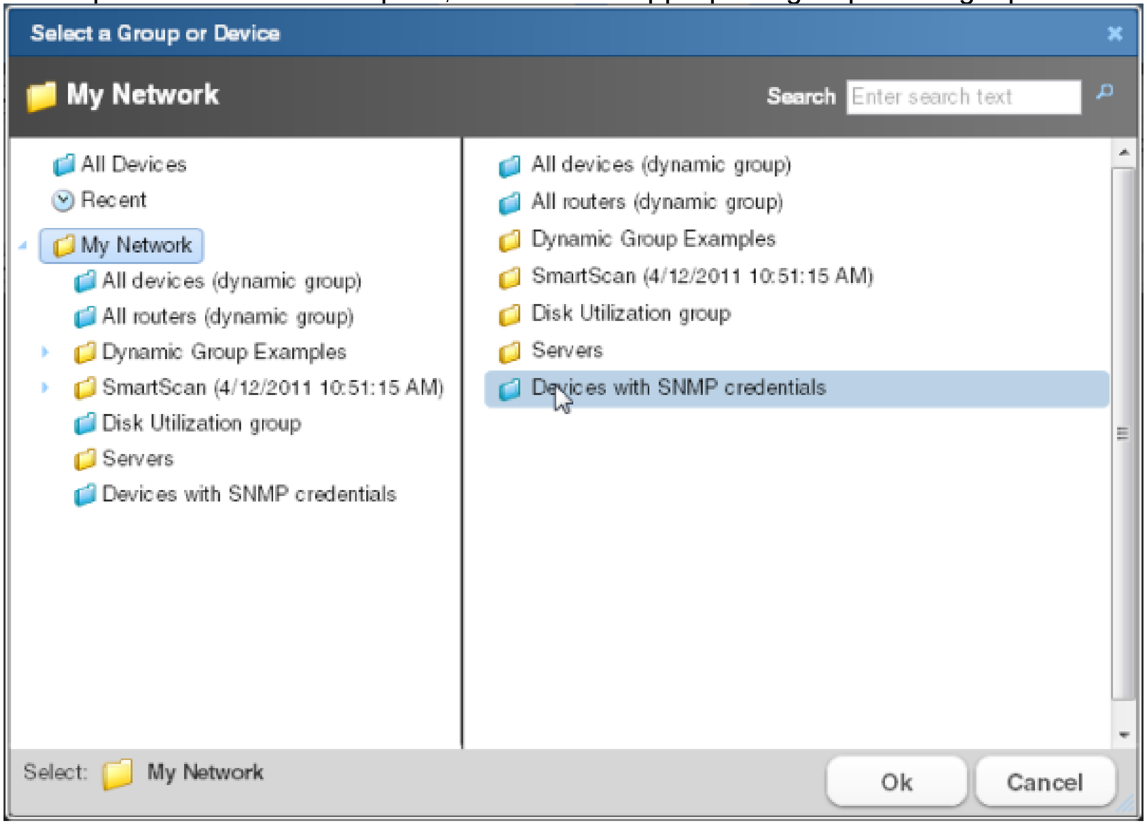


Date range: Custom

Start time: 03/01/2011 12:00 AM

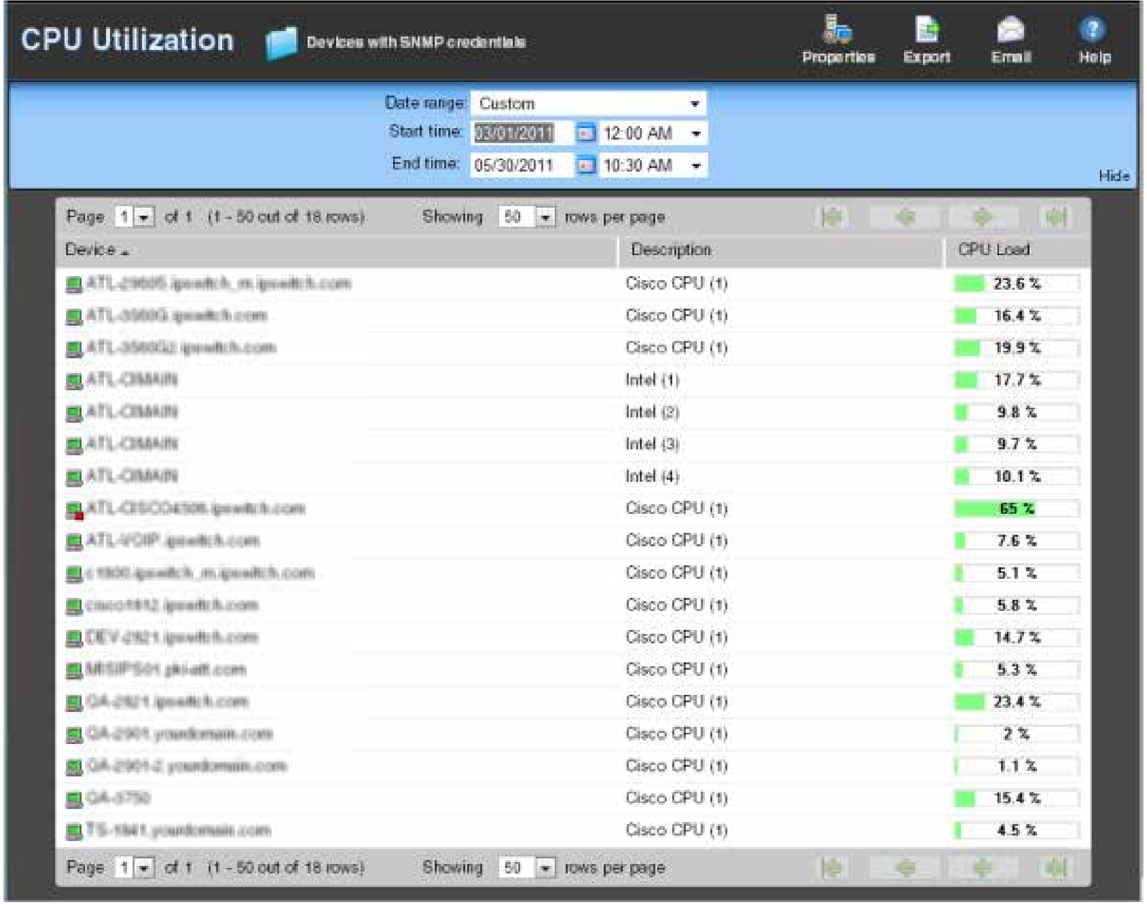
End time: 05/30/2011 10:30 AM

3 Click a parent folder in the left pane, and select the appropriate group in the right pane.


Select a Group or Device
My Network
Search
Enter search text
All Devices
Recent
My Network
All devices (dynamic group)
All routers (dynamic group)
Dynamic Group Examples
SmartScan (4/12/2011 10:51:15 AM)
Disk Utilization group
Servers
Devices with SNMP credentials
All devices (dynamic group)
All routers (dynamic group)
Dynamic Group Examples
SmartScan (4/12/2011 10:51:15 AM)
Disk Utilization group
Servers
Devices with SNMP credentials
Ok
Cancel

Select: My Network

4 Click **OK** to make your selection. The selected group displays as the new context and the monitor report displays information for the selected group.



Date range: Custom
Start time: 03/01/2011 12:00 AM
End time: 05/30/2011 10:30 AM

Page 1 of 1 (1 - 50 out of 18 rows) Showing 50 rows per page

Device	Description	CPU Load
ATL-2960S.ipswitch_m.ipswitch.com	Cisco CPU (1)	23.6 %
ATL-3560G.ipswitch.com	Cisco CPU (1)	16.4 %
ATL-3560G2.ipswitch.com	Cisco CPU (1)	19.9 %
ATL-CIMAIN	Intel (1)	17.7 %
ATL-CIMAIN	Intel (2)	9.8 %
ATL-CIMAIN	Intel (3)	9.7 %
ATL-CIMAIN	Intel (4)	10.1 %
ATL-CISCO4506.ipswitch.com	Cisco CPU (1)	65 %
ATL-VOIP.ipswitch.com	Cisco CPU (1)	7.6 %
c1800.ipswitch_m.ipswitch.com	Cisco CPU (1)	5.1 %
cisco1812.ipswitch.com	Cisco CPU (1)	5.8 %
DEV-2821.ipswitch.com	Cisco CPU (1)	14.7 %
MISIPS01.pki-att.com	Cisco CPU (1)	5.3 %
QA-2821.ipswitch.com	Cisco CPU (1)	23.4 %
QA-2901.yourdomain.com	Cisco CPU (1)	2 %
QA-2901-2.yourdomain.com	Cisco CPU (1)	1.1 %
QA-3750	Cisco CPU (1)	15.4 %
TS-1841.yourdomain.com	Cisco CPU (1)	4.5 %

Page 1 of 1 (1 - 50 out of 18 rows) Showing 50 rows per page

- Click the current device context to open the device picker and select a device or group from a list of devices and groups on your network.
- Click other reports on the navigation bar to view other reports for the same group.
- Use the report **Date/Time Picker**, located in the middle of the page, to easily change the time period for the report you are viewing. In the **Date range** list, you can specify business hours. This allows you to view the network activity only for the hours you specify.
- Select **Export** o export your data using the following options: Export to Text, Export to Excel, or Export to PDF.
- Select **Email** to email and schedule reports. For more information, see *Scheduling reports* (on page 376).

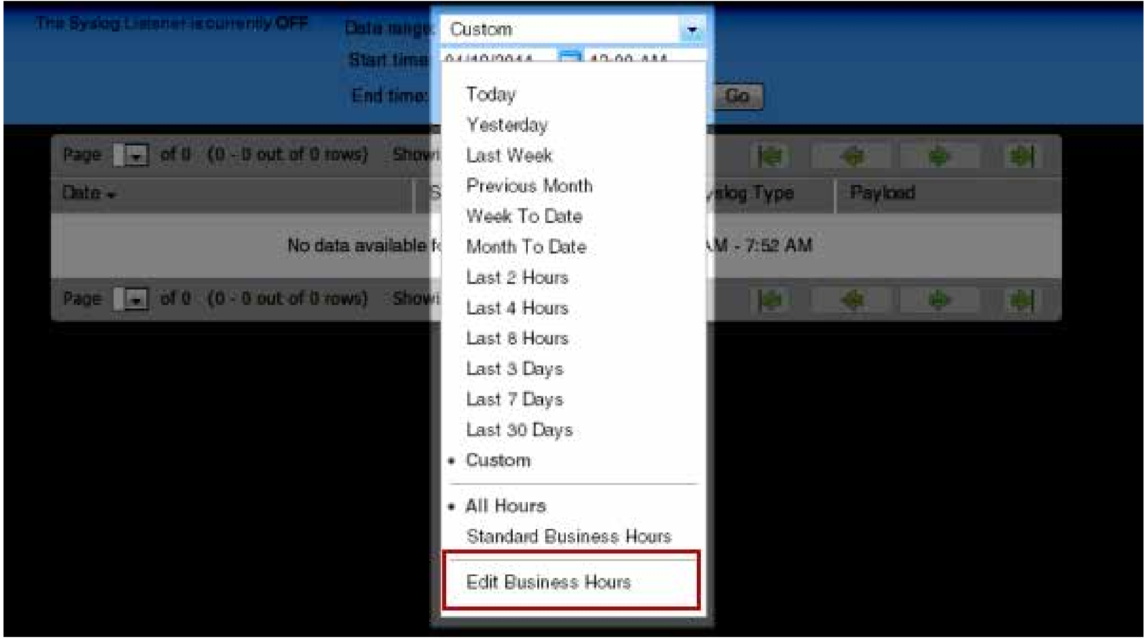
Using Business Hours settings in monitor reports

You can select **Standard Business Hours** for many WhatsUp Gold and Flow Monitor reports using the **Date range** list. Selecting this option limits report views to standard business operation hours, which default to Monday - Friday from 9:00 am - 5:00 pm. You can add, edit, and delete business hour report times in the Business Hours dialog.

Note: The Business Hours setting is available for group reports only.

To change/edit Standard Business Hours:

1 In any report, click the **Date Range** list.
Select **Edit Business Hours**. The Business Hours dialog appears.



2 Click **Add Hours** to add a new set of business hours for report time ranges. Type a name for the new business hours setting, and then click **OK**.

- or -

Select a name in the list to edit an existing business hours setting, and then click **OK**.

3 Select the **Link days** option if you want to use the same start and end time for each scheduled day.

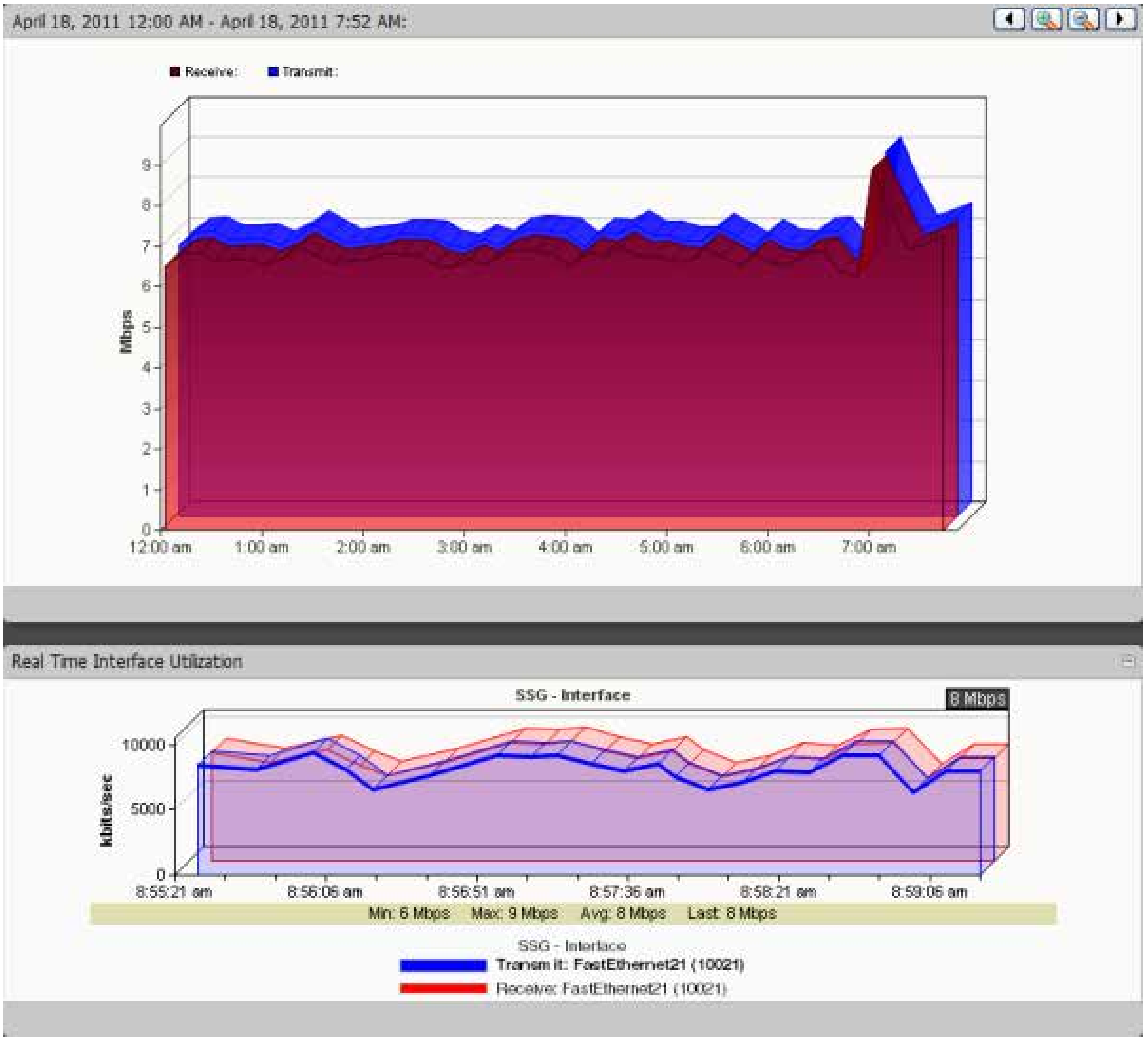
4 Select the days you want to include in the business hours setting, then use the slider bar to adjust the start and end times for the report.

5 Click **OK** to save changes.

Note: You must have the appropriate account rights to view and make changes to business hours.

Viewing real-time data in monitor reports

For all reports where real-time data is available, a second graph is available below the historical data graph. This second graph displays poll data for the report in real-time, updating every second.



About report refresh intervals

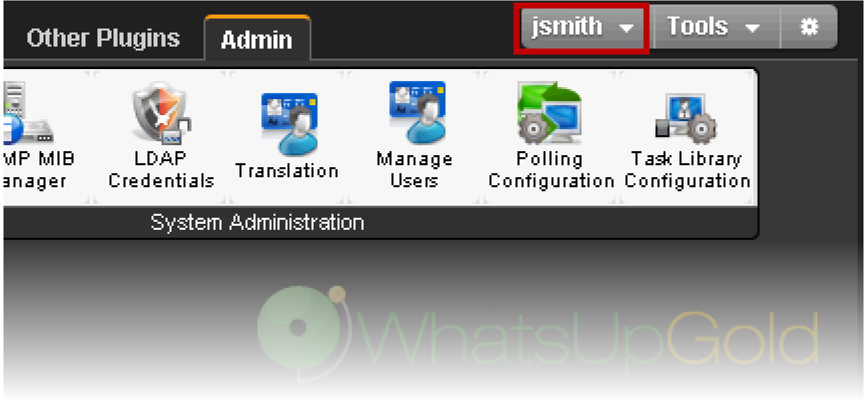
Reports are refreshed at an interval specified in the User Preferences dialog called the report refresh interval. The default report refresh interval is 120 seconds.

Note: The report refresh interval is user specific and is only applied to the user account logged in when the change is made.

To change the report refresh interval:

1 Click the **Admin** tab, then click **Preferences**.
- or -
Click the **[username]** link, where [username] is your account log in name, in the upper

right of the application, then click **User Settings > WhatsUp Gold > Preferences for [username]**.



2 Enter a new time (in seconds) for the report refresh interval in the **Full report** box. This setting controls how frequently the monitor reports update.

3 Click **OK** to save changes.

Changing the date range

Use the time and date menus in the control bar to select the time period you want to view the data for. You can select a pre-configured time period from the **Date Range** list, or select **Custom** and enter the start and end time manually. If no data exists for that time period, the following message displays: **No data available for the selected date range**.

To change the date range for a report or log:

- Click the calendar icon next to the date box to select the specific date from the calendar.
- Click the left and right arrows on the calendar to browse through the months.
- In the Date range list, click **Today** to navigate back to the current date. When you click a date, the calendar closes and the box is populated with the selected date.

Note: The date and time format on this report or log matches the format specified in the WhatsUp Gold console (**Configure > Program Options > Regional**).

You can also use the report *zoom tool* (on page 358) to select a date and time for monitor reports.

To control the date/time picker display:

- Hide the control bar by clicking the **Hide** link in the control bar. The selected date/time range displays instead and allows more rows of the report or log to display.
- To redisplay the date/time picker, click anywhere in the control bar summary.

Using the Zoom tool

Use the zoom tool to navigate through a monitor report. The zoom tool is associated with charts and changes the displayed date and time interval of a report as you page right and left, or zoom in and out.

Click:	To:
▶ **Page right**	Move the report date forward. For example, clicking the Page right button changes the date from today to tomorrow. The page right button appears in monitor reports.
🔍 **Zoom in**	Decrease the amount of time displayed in the report. For example, click the Zoom in button decreases the display time from 24 hours to 12 hours.
🔍 **Zoom out**	Increase the amount of time displayed in the report. For example, clicking the Zoom out button increases the display time from 12 hours to 24 hours.
◀ **Page left**	Move the report date backward. For example, clicking the Page left button changes the date from today to yesterday. The page left button appears in monitor reports.
▲ **Page up**	Go back one page of data. The page up button appears in logs.
▼ **Page down**	Go forward one page of data. The page down button appears in logs.

Using paging options

At both the bottom and the top of a report or log table are paging controls that allow you to move through large amounts of data.

Use the **Page** list to select the specific page to view. Next, use the **Showing ___ rows per page** list to specify the number of rows to display in the report. You can choose to display 25, 50, 100, 250, or 500 rows. The default maximum is 50 rows.

The paging buttons allow you to move from page to page, or go to the first or last page:

Click:	To view:
⇤	§ The first page of values
←	§ The previous page of values
→	§ The next page of values
⇥	§ The last page of values

Changing preferences

Use this dialog to change various web user preferences. Changes made in this dialog only change settings for the *current* user web account. To access the Preferences dialog, go to **Admin > Preferences.**

General

- **Change your password**. Select this option to change your account password.
- **Show Getting Started Pane**. Select this option to display the Getting Started pane. The Getting Started pane includes links to resources to help you resolve issues and learn more about WhatsUp Gold.

Note: If you have an evaluator license, this box displays as **Show Evaluator Pane.** This option is not selectable with an evaluator license.

Refresh intervals

- **Dashboard report**. Enter a time (in seconds) for how often dashboard reports should refresh.
- **Full report**. Enter a time (in seconds) for how often *monitor reports* (on page 370) should refresh.
- **Devices list**. Enter a time (in seconds) for how often the content Devices tab should refresh.

Reports

- **Default records per page for long reports**. Enter a number to control the maximum number of rows reports and logs display. If a report contains a number of rows greater than the maximum number specified, you can use either the page controls to view the data. The default max records setting is 50.
- **Collapse legends on split second graph dashboard reports**. Select this option to hide the legends on split second graph dashboard reports until the mouse pointer moves over a graph. When multiple split second graph dashboard reports display in a dashboard view, selecting this option can help reduce the percentage of the screen area used by reports. This option affects split second graph dashboard reports only; legends are always displayed in popups.

Web Alarms

- **Enable web alarms**. Select this option to enable *Web alarms* (on page 114).

Note: Web alarms are enabled by default.

- **Check every**. If you enable Web alarms, enter a time (in seconds) for how often WhatsUp Gold should check for Web alarms.

Instant Info (popups)

- **Show popups on device list**. Select this option to enable popups on the device list. If this option is cleared, popups are not displayed when you hover device or group names in the device list.
- **Show popups on dashboard reports**. Select this option to enable popups on dashboard reports. If this option is cleared, popups are not displayed on dashboard reports.
- **Show popups on full reports**. Select this option to enable popups on monitor reports. If this option is cleared, popups are not displayed on monitor reports.

Note: By default, popups are enabled on both dashboard and reports.

Note: Popups are not available in WhatsUp Gold Standard Edition.

Using the WhatsUp Gold toolbar buttons

Click:	To:
Email	§ Email a report or log as a PDF attachment. § Schedule the report or log to be emailed at regular intervals.
Add Content	§ Add additional dashboard reports to the current dashboard view using the Add Content panel.
Edit View	§ Edit settings for the currently displayed dashboard view.
Properties	§ View and configure dynamic group properties. Note: This button only appears when you are viewing a device group other than the default *All Devices* dynamic group.
Status	§ Display the Device Status of the device currently in context. This icon does not appear when a group is in the current context.
Export	§ Export a report or log: § To a text file § To an Excel file § To a PDF file
Help	§ View help for the current page.

Note: Different sets of icons appear on different types of pages.

Configuring monitor report charts

To configure a chart in a report:

1. Click **Chart Properties** in the control bar. The Chart Properties dialog appears.
2. Make any changes to the following settings:
   - **Width**. Enter the chart width (in pixels).
   - **Height**. Enter the chart height (in pixels).
   - **Graph Type**. Select the type of chart to display:
     - Bar
     - Line
     - Area
     - Spline
     - Stepline

   For more information on graph types, see *Understanding the Graph Types* (on page 364).

Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

   - **Trend Type**. Select the type of trend to display. This line shows the average value of data for the duration of the graph.
     Options include:
     - None
     - Line
     - Curve
   - **Dimensions**. Select whether to display the chart as a 2D or 3D graph.
   - **Vertical Axis Scale**. Select how you want the vertical axis (the Y axis) for the graph to display:
     - **Auto Scale**. Select to adjust the axis based on the minimum and maximum values displayed. When Auto Scale is selected, small changes in the data may appear as a large data spike. Use Auto Scale to make changes in graph data more visible for graphs that are typically flat and do not have a lot of data variation.
     - **Fixed Scale.** Select to show the data on the scale you enter in the **Min** and **Max** boxes.
   - **Min**. Enter the minimum value to display in the graph. By default, this is zero, but for certain data sets a different minimum value may be more relevant.
   - **Max**. Enter the maximum value to display in the graph. By default, this is 100, but for certain data sets a different maximum value may be more relevant.

3 Click **OK** to save changes.

Resizing and sorting report columns

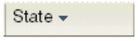
Both column sizing and sorting are maintained on a per user basis, and only for the report where the column changes are made.

Resizing

Report columns can be resized. Resize a report column by clicking on the edge of the report title box and moving it either left or right. When a report column is resized, the new size is saved and used each time the report is viewed.

Sorting

Most monitor report columns can be sorted. You can sort by left-clicking a column heading. The report column then automatically sorts itself either ascending or descending. The sort direction is indicated with an upward, or downward pointing arrow.



As in column sizing, column sorting settings are saved and are used each time the report is viewed.

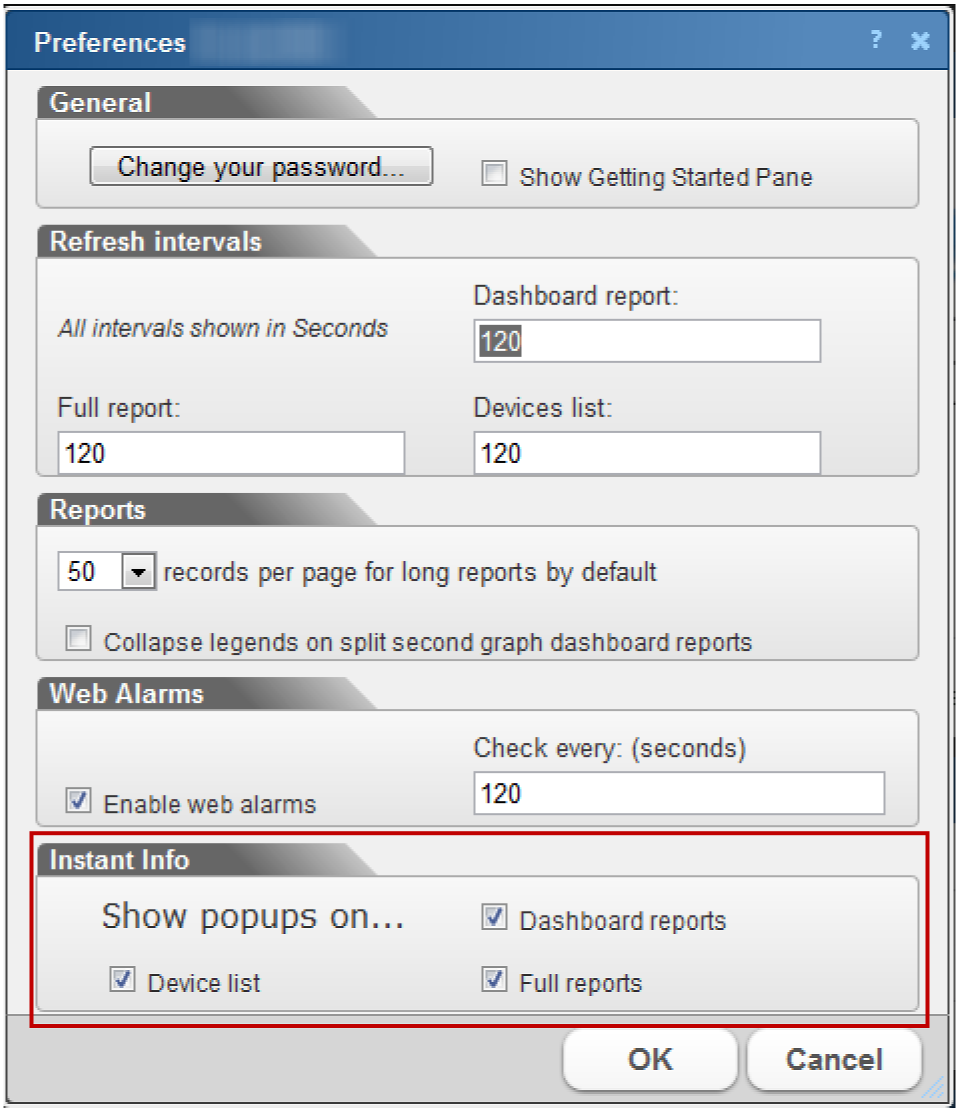
Disabling Instant Info popups

By default, Instant Info popups are available in both dashboard and full reports, but you can disable them if you prefer.

To disable Instant Info popups:

1 Click the **Logged in as [username]** link in the upper right corner of the page.
- or -
Click the **Admin** tab, then click **Preferences**. The Preferences dialog appears.

2 In the **Instant Info** section, clear the options for the areas where you do *not* want popups to appear.



Preferences

General

□ Show Getting Started Pane

Refresh intervals

All intervals shown in Seconds

Dashboard report: 120

Full report: 120

Devices list: 120

Reports

50 records per page for long reports by default

□ Collapse legends on split second graph dashboard reports

Web Alarms

☑ Enable web alarms

Check every: (seconds) 120

Instant Info

Show popups on...

☑ Dashboard reports

☑ Device list

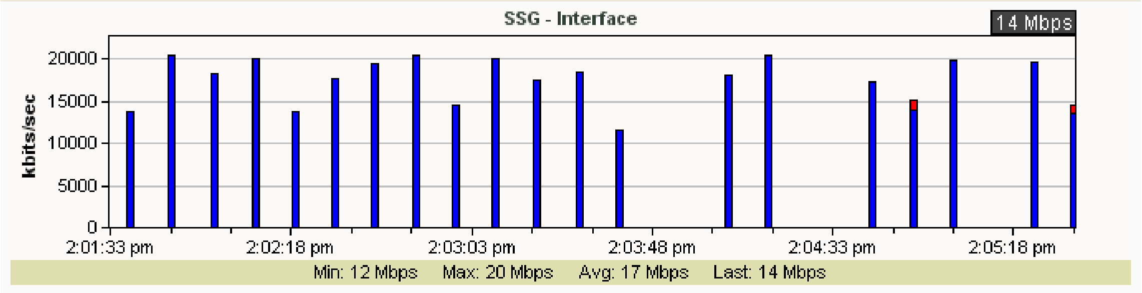
☑ Full reports

3 Click **OK** to save changes.

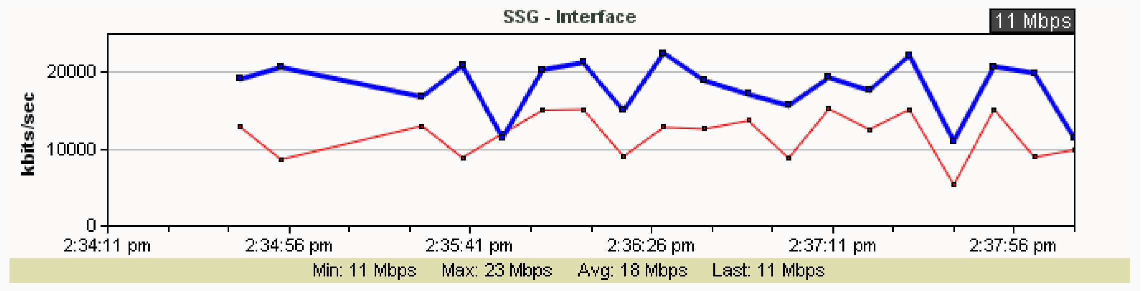
Understanding graph types

The following graph types are available for use with WhatsUp Gold dashboard reports, including the Split Second Graph dashboard reports. All graphs have 2D and 3D options.

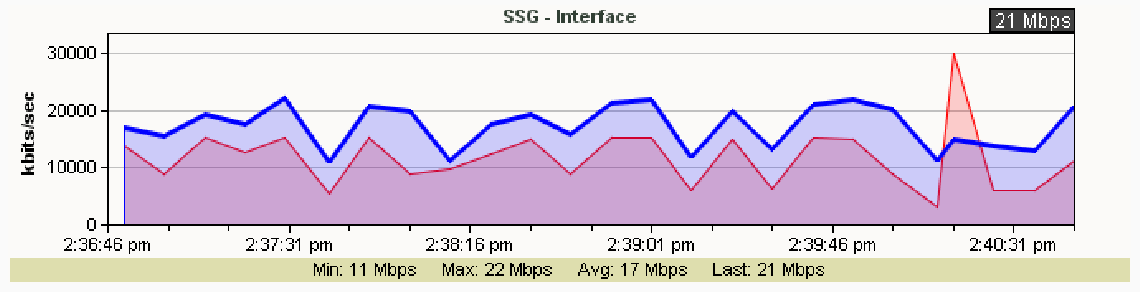
- **Bar.** A vertical bar is displayed for each data point.



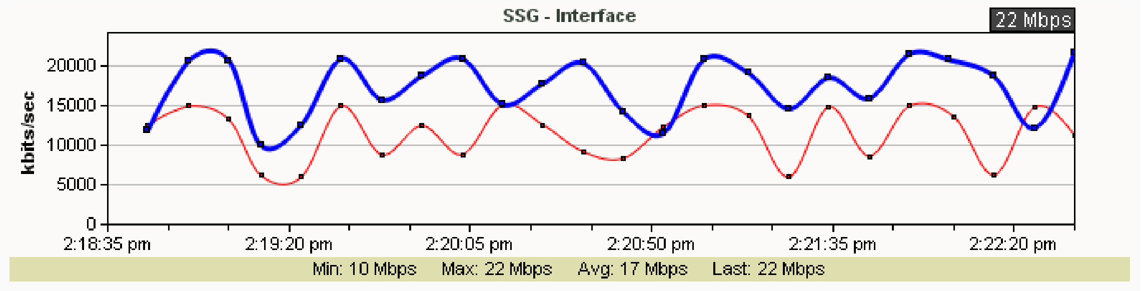
- **Line.** A segmented line connects each of the data points. These data points are represented as small squares. Line graphs are useful for viewing each individual data point or for viewing several counters on the same graph (when used with Split Second Graphs).



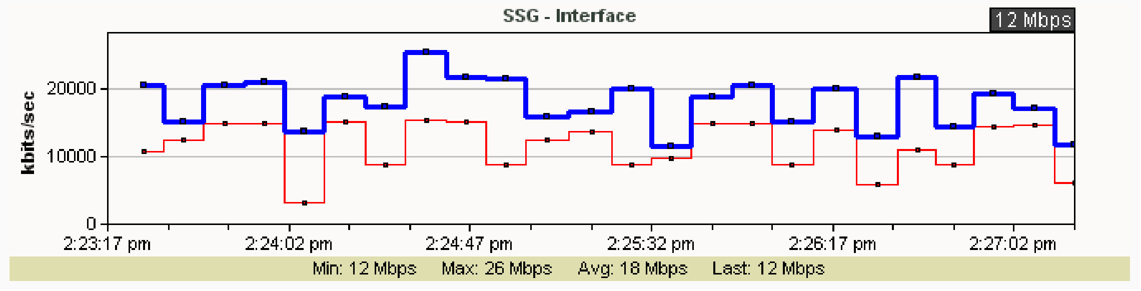
- **Area.** A solid line connects each data point. The area between the data point and the X-axis is filled with a semi-transparent back ground color. This graph type has the greatest visibility at a glance, but when used with Split Second Graphs, is only useful for viewing one to two performance counters at the most.



- **Spline.** This graph type is similar to the line graph type, but the line through the data points is drawn using a best-fit algorithm that interprets the area between data points.



- **Stepline.** This graph type uses horizontal and vertical lines to connect data points.



Using Favorites

In This Chapter

Understanding favorites

WhatsUp Gold favorites let you create your own customized toolbar by adding the WhatsUp Gold options you use most often to a single tab. You can edit and organize your favorites the way that best fits your needs. For more information, see *Adding favorites* (on page 366).

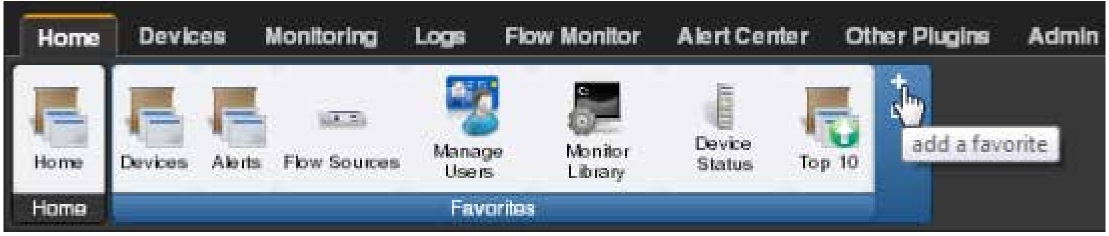
To access WhatsUp Gold Favorites, go to the **Dashboard > Favorites**.

Adding favorites

To add a link to your favorites group:

1 Click **Dashboard**.

2 Click the Add a Favorites plus sign (**+**) to the right of the Favorites group. The Add to Favorites dialog appears.



3 From the dialog, click the tab containing the option you want to add. The buttons available on that tab appear in the pane.

4 Click to select the check box to the left of each button you want to add to the Favorites group. A running total appears in the lower left of the pane as you select additional buttons to add. You can have up to 12 buttons in your Favorites group.

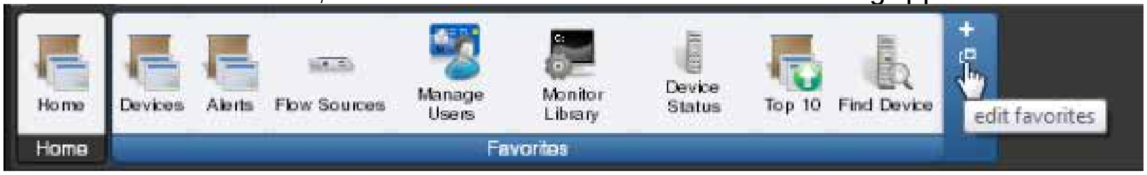
5 Continue clicking tabs and selecting buttons until you have added as many as you want to add.

6 Click **Add** to save your changes and add the selected buttons to your Favorites. The selected buttons appear in your Favorites group.

Editing favorites

To remove buttons from your Favorites group:

1 From the **Dashboard** tab, click **Edit Favorites**. The Edit Favorites dialog appears.



2 Click the **X** at the upper right of each button you want to remove from the toolbar.

3 When you have deleted all of the buttons from the Favorites group that you want to remove, click **Save**. The buttons are removed from your Favorites group.

> **Note**: If you delete all of the buttons from the Favorites group, the WhatsUp Gold default Favorites appear in the group when you save.

To change the order of your Favorites group:

1 From the **Dashboard** tab, click **Edit Favorites**. The Edit Favorites dialog appears.

2 From within the Edit Favorites dialog, click and drag the buttons to the order you prefer.

3 When the buttons are in the preferred order, click **Save**. The dialog closes and the toolbar updates with the new button order.

Using WhatsUp Gold monitor reports

In This Chapter

List of reports and logs

The following is a list of all reports and logs that are available in Ipswitch WhatsUp Gold.

Name of report	What information it conveys
Action Log (on page 429)	A record of all actions that WhatsUp Gold attempts to fire.
Activity Log (on page 440)	A history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the selected time period.
General Error Log (on page 430)	A record of error messages generated by WhatsUp Gold.
Home Dashboard	Your Home Dashboard for WhatsUp Gold. This dashboard contains four default views: Active Management, Getting Started, Passive Management, and Performance Management
Passive Monitor Error Log (on page 432)	A record of Passive Monitor errors reported by WhatsUp Gold.
Performance Monitor Error Log (on page 433)	A record of Performance Monitor errors reported by WhatsUp Gold for all devices or for a selected device.
Recurring Action Log (on page 442)	Results of Recurring Action executions.
Recurring / Scheduled Report Log (on page 441)	Results of Recurring and Scheduled Report executions.

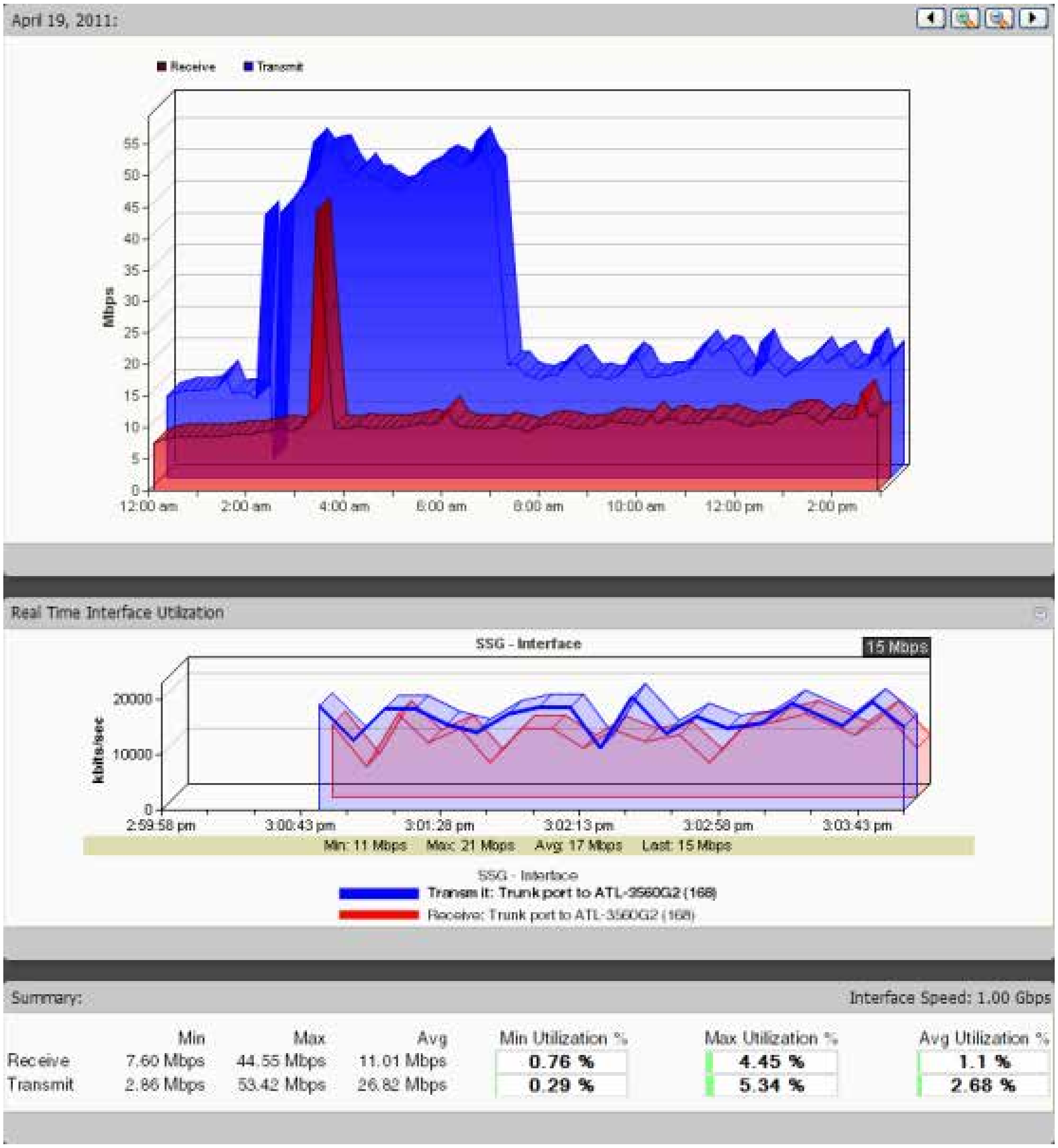
Remote Site Log	A record of messages generated by Remote Server connection attempts. Available in WhatsUp Gold MSP and WhatsUp Gold Distributed editions.
Remote Site Status	View the Remote Location State of devices and Active Monitors. Available only in the central installation of WhatsUp Gold MSP and WhatsUp Gold Distributed editions.
SNMP Trap Log (on page 435)	A history of SNMP traps ocurring during the selected time period for all devices or for a selected device. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.
Syslog (on page 436)	Syslog events logged during the selected time period. If the Syslog Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Syslog Entries log.
Web User Activity Log (on page 444)	Shows the history of user activity on the system.
Windows Event Log (on page 439)	Shows Windows events logged for all devices or for a selected device during the selected time period. If the Windows Event Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Windows Event Log.
WhatsVirtual Event Log	Provides a record of events generated from virtual devices. (The WhatsVirtual Event Log can be found under the Virtual tab.)
Actions Applied (on page 445)	The Group Actions Applied report shows how actions are applied to devices and Monitors in the current group. Each entry shows an action and the device, monitor and state that triggered it.
Active Monitor Availability	Compare the amount of time the active monitors on your devices have been available.
Active Monitor Outages (on page 409)	Compare the amount of time the active monitors on your devices have been down.
Blackout Summary Log (on page 446)	A detailed view of actions that were not fired during a blackout period.
CPU Utilization (on page 381)	CPU utilization statistics for devices by group or device.
Device Uptime (on page 410)	Shows the percentage of uptime, maintenance, unknown, down, and availability for devices by group.
Disk Utilization (on page 383)	Disk space utilization statistics for devices and by group.
Device Health (on page 412)	The current status of monitored devices in a group, or for a selected device, along with each monitor configured on each device. If a device is selected, the current status of the selected device and all monitors applied display. Each monitor shows its own device state, the current status of each item, how long the device has been in that status, and the time that status was first reported.
Interface Utilization (on page 391)	Interface utilization for devices by group or for a selected device

	(by percentage).
Interface Traffic (on page 394)	Interface traffic for devices by group or for a selected device (in bps).
Memory Utilization (on page 386)	Memory utilization statistics for devices by group or for a selected device.
Monitors Applied (on page 448)	A list of monitors applied to devices in the group currently in context.
Ping Availability (on page 396)	Ping availability statistics for devices by group or device.
Ping Response Time (on page 399)	Ping response times for devices by group or for an individual device.
Quarterly Availability Summary (on page 449)	Shows the availability summary for a group.
State Change Acknowledgement (on page 413)	When a device state changes, regardless of any action that has been placed on the device, WhatsUp Gold uses the Acknowledgement feature to make you aware that the state change occurred. This report can be used to view the devices in a group that require acknowledgement.
State Change Timeline (on page 415)	A timeline displaying when each monitor changed from one state to another during the selected time period. Information is displayed for selected devices and for groups.
State Summary (on page 451)	A summary of device states organized by device group.
Top 10 (on page 416)	A collection of Top 10 dashboard reports.
WhatsConfigured Task Log	A record of all log messages generated by WhatsConfigured. This report is filterable by device and task.
Custom Performance Monitors (on page 389)	View information on groups and devices collected by custom monitors.
Device Status	A detailed look at a specific device.

Learning about monitor reports

Monitor reports display performance and historical data collected during the operation of the application. You can use these reports to troubleshoot and monitor your network and devices.

You can view monitor information for a device:



April 19, 2011:

Real Time Interface Utilization

SSG - Interface

Min: 11 Mbps Max: 21 Mbps Avg: 17 Mbps Last: 15 Mbps

SSG - Interface

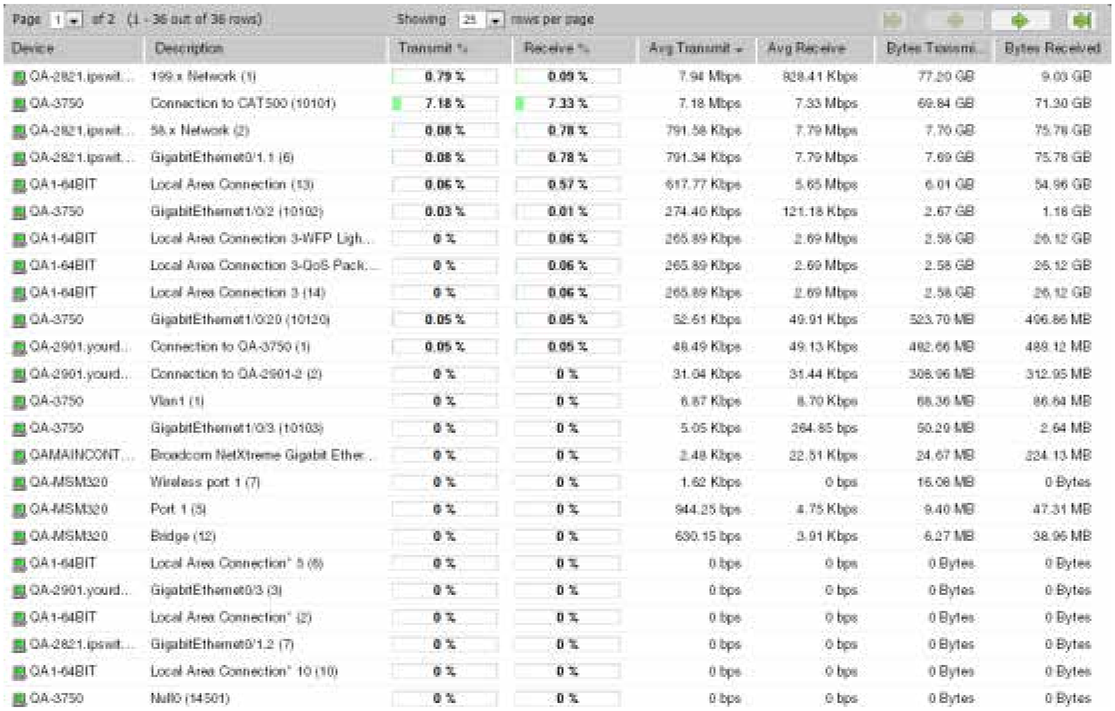
Transmit: Trunk port to ATL-3560G2 (168)

Receive: Trunk port to ATL-3560G2 (168)

Summary: Interface Speed: 1.00 Gbps

	Min	Max	Avg	Min Utilization %	Max Utilization %	Avg Utilization %
Receive	7.60 Mbps	44.55 Mbps	11.01 Mbps	0.76 %	4.45 %	1.1 %
Transmit	2.86 Mbps	53.42 Mbps	26.82 Mbps	0.29 %	5.34 %	2.68 %

You can view monitor information for a group:



Page 1 of 2 (1 - 36 out of 36 rows) Showing 25 rows per page

Device	Description	Transmit %	Receive %	Avg Transmit	Avg Receive	Bytes Transmi...	Bytes Received
QA-2821.ipswit...	199.x Network (1)	0.79 %	0.09 %	7.94 Mbps	828.41 Kbps	77.20 GB	9.03 GB
QA-3750	Connection to CAT500 (10101)	7.18 %	7.33 %	7.18 Mbps	7.33 Mbps	69.84 GB	71.30 GB
QA-2821.ipswit...	58.x Network (2)	0.08 %	0.78 %	791.58 Kbps	7.79 Mbps	7.70 GB	75.78 GB
QA-2821.ipswit...	GigabitEthernet0/1.1 (6)	0.08 %	0.78 %	791.34 Kbps	7.79 Mbps	7.69 GB	75.78 GB
QA1-64BIT	Local Area Connection (13)	0.06 %	0.57 %	617.77 Kbps	5.65 Mbps	6.01 GB	54.96 GB
QA-3750	GigabitEthernet1/0/2 (10102)	0.03 %	0.01 %	274.40 Kbps	121.18 Kbps	2.67 GB	1.18 GB
QA1-64BIT	Local Area Connection 3-WFP Ligh...	0 %	0.06 %	265.89 Kbps	2.69 Mbps	2.58 GB	26.12 GB
QA1-64BIT	Local Area Connection 3-QoS Pack...	0 %	0.06 %	265.89 Kbps	2.69 Mbps	2.58 GB	26.12 GB
QA1-64BIT	Local Area Connection 3 (14)	0 %	0.06 %	265.89 Kbps	2.69 Mbps	2.58 GB	26.12 GB
QA-3750	GigabitEthernet1/0/20 (10120)	0.05 %	0.05 %	52.61 Kbps	49.91 Kbps	523.70 MB	496.86 MB
QA-2901.yourd...	Connection to QA-3750 (1)	0.05 %	0.05 %	48.49 Kbps	49.13 Kbps	482.66 MB	489.12 MB
QA-2901.yourd...	Connection to QA-2901-2 (2)	0 %	0 %	31.04 Kbps	31.44 Kbps	308.96 MB	312.95 MB
QA-3750	Vlan1 (1)	0 %	0 %	6.87 Kbps	8.70 Kbps	68.36 MB	86.64 MB
QA-3750	GigabitEthernet1/0/3 (10103)	0 %	0 %	5.05 Kbps	264.85 bps	50.29 MB	2.64 MB
QAMAINCONT...	Broadcom NetXtreme Gigabit Ether...	0 %	0 %	2.48 Kbps	22.51 Kbps	24.67 MB	224.13 MB
QA-MSM320	Wireless port 1 (7)	0 %	0 %	1.62 Kbps	0 bps	16.08 MB	0 Bytes
QA-MSM320	Port 1 (3)	0 %	0 %	944.25 bps	4.75 Kbps	9.40 MB	47.31 MB
QA-MSM320	Bridge (12)	0 %	0 %	630.15 bps	3.91 Kbps	6.27 MB	38.96 MB
QA1-64BIT	Local Area Connection* 5 (8)	0 %	0 %	0 bps	0 bps	0 Bytes	0 Bytes
QA-2901.yourd...	GigabitEthernet0/3 (3)	0 %	0 %	0 bps	0 bps	0 Bytes	0 Bytes
QA1-64BIT	Local Area Connection* (2)	0 %	0 %	0 bps	0 bps	0 Bytes	0 Bytes
QA-2821.ipswit...	GigabitEthernet0/1.2 (7)	0 %	0 %	0 bps	0 bps	0 Bytes	0 Bytes
QA1-64BIT	Local Area Connection* 10 (10)	0 %	0 %	0 bps	0 bps	0 Bytes	0 Bytes
QA-3750	Null0 (14501)	0 %	0 %	0 bps	0 bps	0 Bytes	0 Bytes

Access monitor reports by clicking the **Reports** tab and then selecting the appropriate button for the type of report you want to view.

Monitor report categories

Monitor reports in WhatsUp Gold are grouped according to the type of information displayed within each report.

There are three categories of monitor reports:

§ **Performance**. Reports which display information about thresholds. Determine which resources on your network are under- or over-utilized using Performance monitor reports.

§ **Network**. Reports which display reports related to network statistics about traffic through your network. Network reports include such parameters as speed, response times, and success or failure in contacting devices.

§ **Device**. These reports display information about specific devices that you select to to monitor for parameters such as outages and uptime percentages.

Advantages of monitor reports

§ Larger than dashboard reports, monitor reports give you a broader data view, which is useful in pinpointing the time an event occurred or when viewing multiple graphed items. Many dashboard reports link to monitor reports, so that you can access this larger data view to troubleshoot.

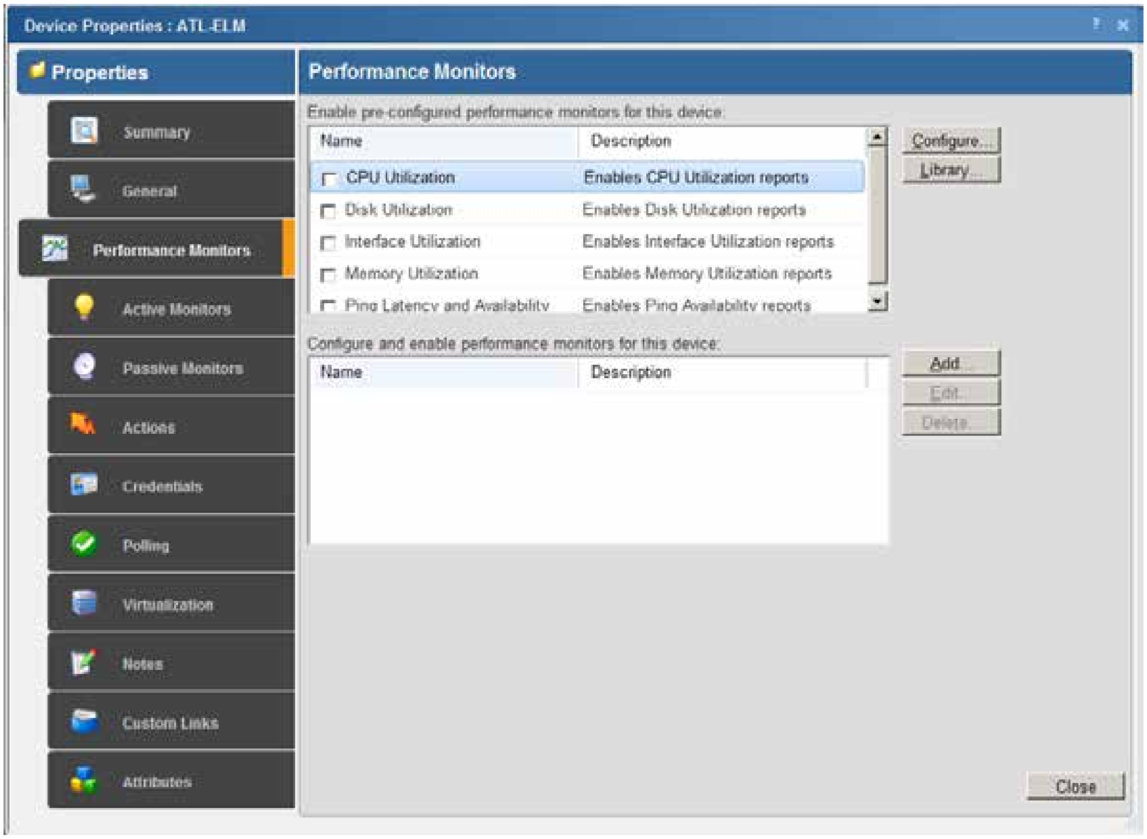
§ The date range on full reports can be zoomed in or out so that you can get a smaller or larger picture of what's going on with an aspect of the network.

- Click the options within the same tab in the navigation bar to quickly access other monitor reports. The currently selected group or device and date range is applied to the next monitor report you access.
- The data in monitor reports can be exported to a formatted text file, Microsoft Excel, or a PDF. You can also email reports as a PDF, or send on scheduled intervals.

Device Properties - Performance Monitors

Use the Device Properties dialog to configure and manage performance monitors for the selected device. For more information, see *Using Performance Monitors* (on page 119).

Note: For some performance monitors, credentials on the device must be configured. For example, the Windows credential is required for WMI performance monitors.



Enable pre-configured performance monitors for this device:

Name	Description
□ CPU Utilization	Enables CPU Utilization reports
□ Disk Utilization	Enables Disk Utilization reports
□ Interface Utilization	Enables Interface Utilization reports
□ Memory Utilization	Enables Memory Utilization reports
□ Ping Latency and Availability	Enables Ping Availability reports

Configure and enable performance monitors for this device:

Name	Description

- **Enable pre-configured performance monitors for this device**. Select options in this list to enable monitors. The following monitors are populated by entries in the *Performance Monitor Library* (on page 261), but cannot be edited or changed from their default settings. These monitors are ready to be added to devices.
- **CPU Utilization**. Monitors the CPU utilization on the selected device.
- **Disk Utilization**. Monitors the available disk space for the selected device.
- **Interface Utilization**. Monitors all interfaces on the selected device.
- **Memory Utilization**. Monitors memory utilization on the selected device.

- **Ping Latency and Availability**. Monitors how often and quickly the device responds to a ping check.

  If you select a specific performance monitor without configuring the monitor manually, the default collection type is automatically selected. The collection type refers to the item on the current device that is being monitored (This does not pertain to the custom WMI and SNMP monitors that may appear):

  - CPU - All
  - Disk - All
  - Interface - All, Default, or Specific
  - Memory - All
  - Ping - All

  For example, if you have multiple CPUs running on the device, WhatsUp Gold gathers statistics on all of them by default.

- **Configure**. Click to configure additional data stream options for the global performance monitor.

> **Note**: If an error occurs, a warning message appears directing you to the problem. If it is a timeout error, you are prompted to open the Advanced dialog to change the **Timeout** value. For any other error, you are returned to this dialog.

- **Library**. Click for options to create (**New**), **Edit**, **Copy**, or **Delete** performance monitor library items to use on all devices.
- **Configure and enable performance monitors for this device**. Use this section of the dialog to add customized Active Script, APC UPS, Printer, SQL Query, SNMP, SSH, WMI Formatted, or WMI performance monitors to only be used on this device. The monitors added here do not appear in the Performance Monitor Library, and cannot be used on other devices unless it is manually created for that device.
- Click **New** to configure a new monitor.
- Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.
- Select a performance monitor type, then click **Delete** to remove it from the list.

For information on the Active Script Performance Monitor, see *Adding and Editing an Active Script Performance Monitor* (on page 263).

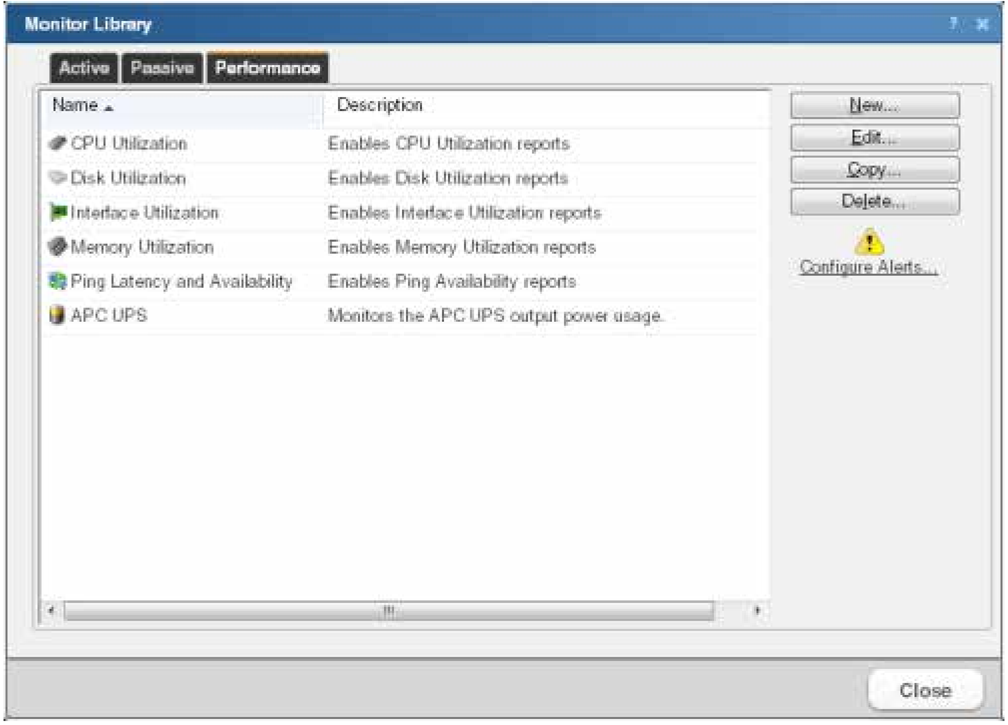
> **Note**: If you are attempting to monitor a Cisco device with either the CPU or Memory Performance Monitors, the Cisco device must support Cisco IOS 12.2(3.5) or later.

Using the Performance Monitor Library

The Performance Monitor Library stores and displays the performance monitors that have been created for WhatsUp Gold. Performance monitors gather information about specific WMI and SNMP values from network devices. There are several default performance monitors available in the library and you can also add new performance monitors. Performance monitors can be applied to devices from the Device Properties dialog for that device.

To access the Performance Monitor Library:

1 From the WhatsUp Gold web interface, go to **Admin > Monitors**. The Monitor Library dialog appears.



Name	Description
CPU Utilization	Enables CPU Utilization reports
Disk Utilization	Enables Disk Utilization reports
Interface Utilization	Enables Interface Utilization reports
Memory Utilization	Enables Memory Utilization reports
Ping Latency and Availability	Enables Ping Availability reports
APC UPS	Monitors the APC UPS output power usage.

2 If it is not already selected, click the **Performance** tab.

3 Use the Performance Monitor Library dialog to configure new or existing performance monitor types:

§ Click **New** to configure a custom performance monitor.

§ Select an existing performance monitor, then click **Edit** to modify its configuration.

§ Click **Copy** to create a duplicate of a monitor. You can use the Copy option to create new monitors based on existing monitors.

Note: The five default global monitors cannot be edited, copied or deleted: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

§ Select an existing performance monitor, then click **Delete** to remove it from the list.

Caution: When you delete a performance monitor from the Performance Monitor Library, any instance of that monitor is also deleted, and all related report data is also lost.

§ Click **Configure Alerts** to view the Alert Center Threshold Library.

For more information on Performance Monitors, see *Enabling performance monitors* (on page 373).

Scheduling reports

Tip: In some cases, exported reports show more detailed data than that of the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To send a log or monitor report as a scheduled report:

1 Open the monitor report you want to email.

2 Click **Email** in the WhatsUp Gold toolbar.

3 Select **Email / Schedule Report**. The **Email Report** dialog appears.

4 Enter the following information for the **Email Options** tab:

- **To**. The email address of the account which is to receive the report
- **From**. The address you want to appear as the sender of the report.
- **Subject.** The subject line you want to appear in the report email.
- **Include url in email**. Select to also include the report as a web link.
    - **Alternate host**. When **Include url in email** is selected, you can choose to alter the way the URL appears to the end user. This is a useful option if users outside of your network need to access the server using a different name or address than the default address of the WhatsUp Gold server.

5 Select **PDF Options**, if appropriate. See *Exporting reports and logs* (on page 377) more information.

6 Click the **Email Server** tab.

7 Enter the following information for the email server:

- **SMTP Server**. The name of the mail server.
- **SMTP Port number**. If necessary, change the SMTP port number. The default value is 25.
- **Timeout**. The amount of time to retry connecting to the SMTP server before giving up.
- **Use SMTP authentication**. Select this option if the SMTP server requires authentication.
    - **Username**. The username WhatsUp Gold should use to authenticate.
    - **Password**. The password WhatsUp Gold should use to authenticate.
- **Use an encrypted connection**. Select this option if the SMTP server requires an encrypted connection.

8 Click **Schedule**.

9 Enter a name for the report.

10 Select **Disable this schedule** if you want to prevent WhatsUp Gold from running and sending scheduled reports.

11 In the **Send email** section, make the following selections:

- **Interval**
- **Start Time**

12 Complete the settings in the box that display after you make your interval selection. These options change according to the Interval selection.

13 Click **OK** to save your scheduled report.

Exporting reports and logs

Tip: In some cases, exported reports show more detailed data than that of the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To export to text format:

1. Open the report you want to export.
2. Click **Export**.
3. Select **Export to Text**.
4. Clear or select the following options:
   - § **Include report title**
   - § **Include column names**
5. Select an option from the **Column delimiter** menu.
6. Select an option from the **Text qualifier** menu.
7. Click **OK** to export the report to a text file.

To export to Microsoft Excel format:

1. Open the report you want to export.
2. Click **Export**.
3. Select **Export to Excel**.
4. Clear or select the following options:
   - § **Include report title**
   - § **Include column names**
5. Click **OK** to export the report in Excel format.

To export to PDF format:

1. Open the report you want to export.
2. Click **Export**.
3. Select **Export to PDF**. The Export to PDF dialog appears.
4. Select the following options:
   - § **Page size**. Select a page size from the menu.
     - or -
   - § **Auto size**. Select this option to automatically adjust the page size to fit all content on the PDF.
     - § **Page orientation**. When a page size is selected, select **Portrait** or **Landscape** PDF.
   - § Select the **Live links** option if you want to include clickable URL links in the PDF report.

- Select **Current page** to export the currently viewed page, or select **All pages** to export all pages in the report.

5 Click **Export** to export the report to a PDF.

Emailing reports and logs

> **Tip**: In some cases, exported reports show more detailed data than that of the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To email a report as a PDF:

1 Open the report you want to email.

2 Click **Email**.

3 Click **Email / Schedule Report**. The **Email Report** dialog appears.

4 Click **Email Options**. Complete the following information:

- **To**. The email address of the account receiving the report
- **From**. The address that appears as the sender of the report
- **Subject.** The subject line appearing in the report email
- **Include url in email**. Select to also include the report as a web link
    - **Alternate host**. When **Include url in email** is selected, you can choose to alter the way the URL appears to the end user. This is a useful option if users outside of your network need to access the server using a different name or address than the default address of the WhatsUp Gold server.

5 Select the appropriate **PDF Options**. See *Exporting reports and logs* (on page 377) for more information.

6 Click **Email Server**.

7 Enter the following information for the email server:

- **SMTP Server**. The name of the mail server
- **SMTP Port number**. If necessary, change the SMTP port number. The default value is 25.
- **Timeout**. The length of time to retry connecting to the SMTP server before abandoning the attempt
- **Use SMTP authentication**. Select this option if the SMTP server requires authentication.
    - **Username**. The username WhatsUp Gold uses to authenticate to the mail server
    - **Password**. The password WhatsUp Gold uses to authenticate to the mail server
- **Use an encrypted connection**. Select this option if the SMTP server requires an encrypted connection.

8 Click **Send Email** to send a PDF email immediately, or click **Schedule** to complete the scheduled email settings. See *Scheduling reports* (on page 376) for more information.

Printing reports and logs

To print a report or log:

1 Open the report you want to print.

2 Right-click anywhere inside the report window, then select **Print**.
- or -
Click **File > Print** from the browser menu options.

Viewing scheduled reports

The Scheduled Reports option lets you view, edit, disable, delete, and send scheduled reports configured using the WhatsUp Gold web interface **Email > Email / Schedule Report**.

To view scheduled reports:

1 Click **Email**.

2 Click **Scheduled Reports**. The currently scheduled reports display in the Scheduled Reports dialog.

The Scheduled Reports dialog provides the following information about each report:

§ **Name**. Lists the name of the scheduled report.

§ **User**. Lists the user that set up the scheduled report.

§ **Schedule**. Lists the intervals that the report is scheduled to be emailed.

§ **Show scheduled reports from all users** (optional). When selected, you can view reports that other users have scheduled. This option is available to users with user rights for **Manage Scheduled Report** enabled. For more information, see About user rights.

Click one of the following options to manage scheduled reports:

§ **Edit**. Select a report you want to modify, then click **Edit**. The scheduled report opens in the Scheduled Report dialog where you can change the report settings.

§ **Disable**. Select a report you want to stop sending at scheduled intervals, then click **Disable**. To return a report to a scheduled interval, select the report, then click **Enable**.

§ **Delete**. Select a report you want to remove, then click **Delete**.

§ **Send Email**. Select a report, then click **Send Email**. The scheduled email report is sent to the intended recipients immediately.

Performance monitor reports

In This Chapter

Learning about performance monitor reports

Performance monitor reports deliver information about system thresholds for resources in your network.

Use performance monitor reports to view performance data (CPU, disk, interface, and memory utilization) for devices. These reports that track utilization and availability information for these device components. Performance monitors gather performance counter data from network devices that have SNMP or WMI enabled. For more information, see *Creating custom performance monitors* (on page 286).

In addition to the default performance monitor reports, you can create custom monitors which let you view specific performance information for Active Script, APC UPS, PowerShell, Printer, SNMP, SQL Query, SSH, WMI Formatted, and WMI performance counters.

Add and edit the following performance monitors through the Performance Monitor Library.

Apply performance monitors to individual devices through the Device Properties dialog. From the Device Properties Performance Monitor dialog, you can enable:

§ **Pre-configured performance monitors**. These are the default monitors that are stored in the Monitor Library.

§ **Individual (device-specific) performance monitors**. These are custom monitors that require configuration for specific devices.

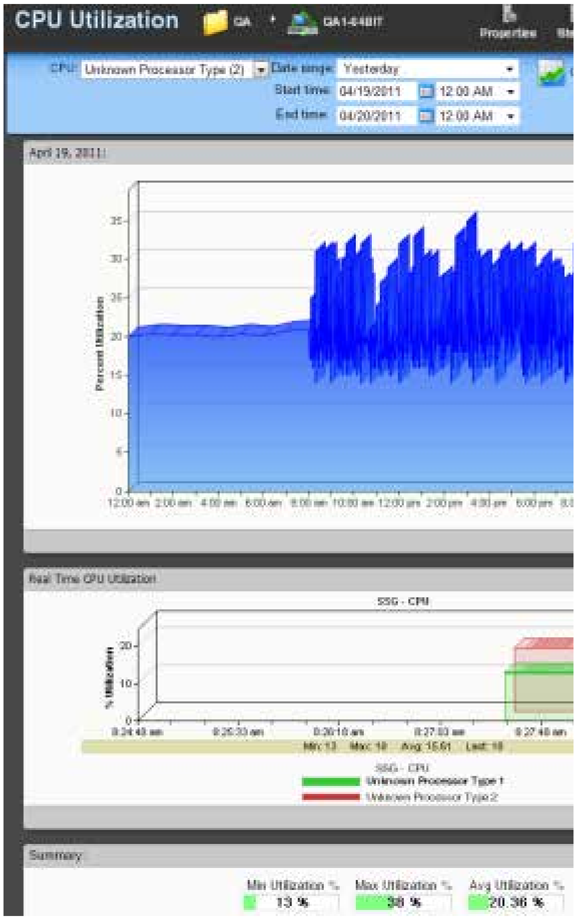
Note: Unlike the other performance monitors, because a printer monitor is specific to an individual printer device, you can only add the Printer Performance Monitor as an individual performance monitor in the Device Properties Performance Monitor dialog.

CPU Utilization

This performance monitor report displays CPU utilization percentages collected during the selected time period from the device displayed at the top of the report.

- Configure the data collection for a device by selecting a device from the Device list and selecting **Properties > Performance Monitors > CPU Utilization**.
- Configure the data collection for a group by selecting a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the CPU menu.

Device Report:



CPU Utilization QA • QA1-64BIT

CPU: Unknown Processor Type (2)

Date range: Yesterday

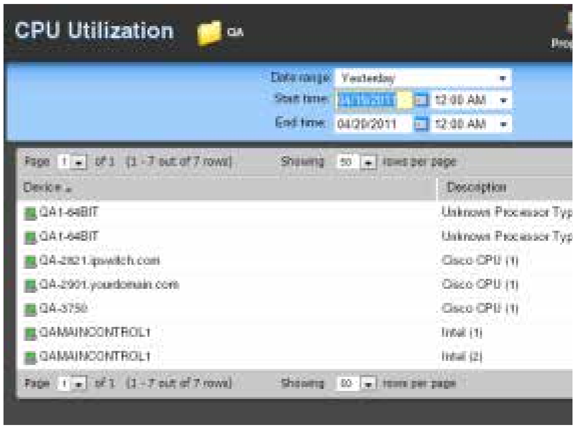
Start time: 04/19/2011 12:00 AM

End time: 04/20/2011 12:00 AM

Summary

Min Utilization %	Max Utilization %	Avg Utilization %
13 %	38 %	20.36 %

Group Report:



CPU Utilization QA

Date range: Yesterday

Start time: 04/19/2011 12:00 AM

End time: 04/20/2011 12:00 AM

Page 1 of 1 (1 - 7 out of 7 rows) Showing 50 rows per page

Device	Description
QA1-64BIT	Unknown Processor Typ
QA1-64BIT	Unknown Processor Typ
QA-2821.ipswitch.com	Cisco CPU (1)
QA-2901.yourdomain.com	Cisco CPU (1)
QA-3750	Cisco CPU (1)
QAMAINCONTROL1	Intel (1)
QAMAINCONTROL1	Intel (2)

Page 1 of 1 (1 - 7 out of 7 rows) Showing 50 rows per page

Monitor report body for group reports

The group report displays a list of all devices in the group and the current average CPU load for each CPU in each monitored device for that group. To view the CPU Utilization report for a specific device, click the CPU displayed in the Description column. WhatsUp Gold opens the CPU Utilization device report for that device.

Monitor report body for device reports

Below the control bar is a graph showing the CPU utilization for the selected time period for the device displayed in the title bar. Each point on the graph corresponds with an entry in the graph data table below.

If the currently viewed device contains multiple CPUs, you can select which CPU information to view by making a selection from the CPU menu in the control bar.

When multiple CPUs are present, the following selections are also available:

- The CPU menu lists all available CPUs in the device. You can select any CPU and view utilization information for that CPU.
- **All CPUs (average)**. The average utilization across all CPUs in the device.
- **All CPUs**. A combined graph displaying utilization for all CPUs.

Split Second Graph - Real-Time CPU Utilization for devices

When you view a device, a Split Second Graph displays under the real-time utilization data for CPUs. When you view a group, hover over the CPU description in the Description column to view the Split Second Graph for that device.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the average CPU utilization percentages collected during the time period:

- **Min Utilization %**. The minimum CPU utilization percentage experienced.
- **Max Utilization %.** The maximum CPU utilization percentage experienced.
- **Avg Utilization %.** The average CPU utilization percentage across all sample data for this time period.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Note: If you are viewing data for all CPUs on a device the summary section displays the lowest of the minimum CPU utilization percentages experienced across all CPUs, and the highest of the maximum CPU utilization percentages experienced across all CPUs. The average CPU utilization percentage is calculated across all sample data for all CPUs

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

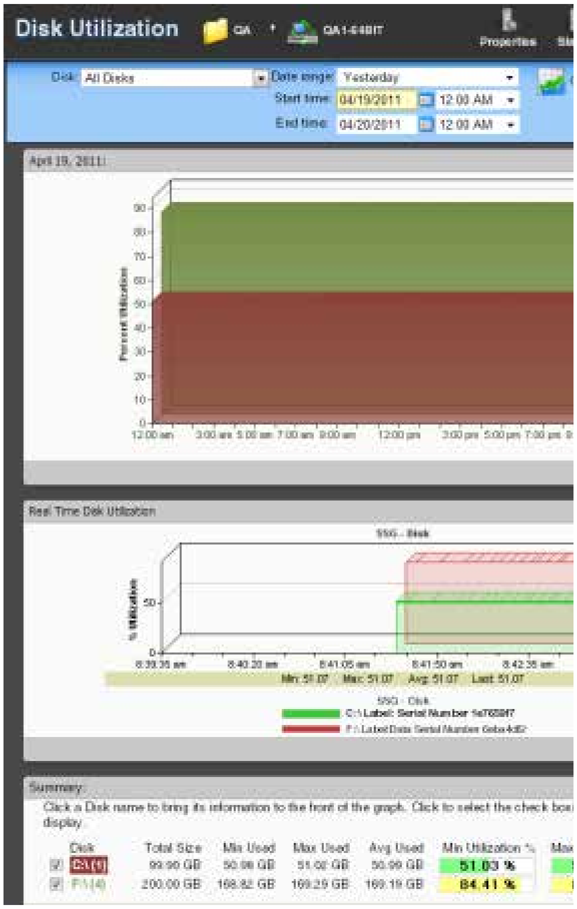
To view the properties of the current group or device, click **Properties** in the toolbar.

About the Disk Utilization report

This performance monitor report displays disk utilization percentages collected during the selected time period for the group or device displayed at the top of the report.

- Configure the data collection for a device by selecting a device from the Device list and selecting **Properties > Performance Monitors > Disk Utilization**.
- Configure the data collection for a group by selecting a group from the Device picker, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Disk** menu.

Device Report:



Disk Utilization QA QA1-64BIT

Disk: All Disks

Date range: Yesterday

Start time: 04/19/2011 12:00 AM

End time: 04/20/2011 12:00 AM

April 19, 2011:

Real Time Disk Utilization

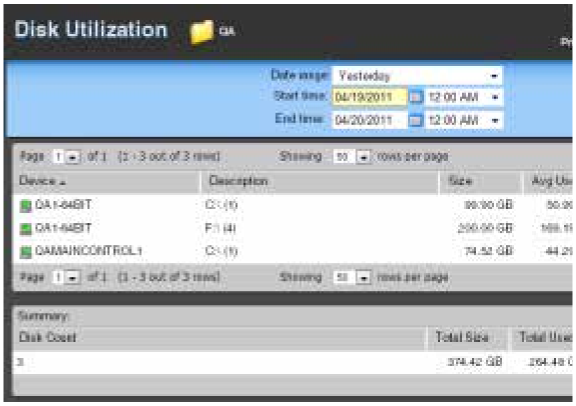
550 - Disk
% Utilization
50
0
8:39:35 am
8:40:20 am
8:41:05 am
8:41:50 am
8:42:35 am
Min: 51.07 Max: 51.07 Avg: 51.07 Last: 51.07
550 - Disk
C:\ Label: Serial Number 1a7f0897
F:\ Label:Data Serial Number 6eba4d62

Summary:

Click a Disk name to bring its information to the front of the graph. Click to select the check box display.

	Disk	Total Size	Min Used	Max Used	Avg Used	Min Utilization %	Max
☑	C:\ (1)	99.90 GB	50.98 GB	51.02 GB	50.99 GB	51.03 %	
☑	F:\ (4)	200.00 GB	168.82 GB	169.29 GB	169.19 GB	84.41 %	

Group Report:



Disk Utilization QA

Date range: Yesterday

Start time: 04/19/2011 12:00 AM

End time: 04/20/2011 12:00 AM

Page 1 of 1 (1 - 3 out of 3 rows) Showing 50 rows per page

Device	Description	Size	Avg Us
QA1-64BIT	C:\ (1)	99.90 GB	50.99
QA1-64BIT	F:\ (4)	200.00 GB	169.19
QAMAINCONTROL1	C:\ (1)	74.52 GB	44.29

Page 1 of 1 (1 - 3 out of 3 rows) Showing 50 rows per page

Summary:

Disk Count	Total Size	Total Use
3	374.42 GB	264.48

Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, be sure to change the **Determine uniqueness by option** in the Advanced Data Collection settings for this performance monitor to description. For more information on advanced data collection settings, see Configuring Data Collection Advanced Settings.

Monitor report body for group reports

The group report displays a list of all devices in the group and the current disk utilization for each disk in each monitored device. To view the Disk Utilization monitor report for a specific device, click the disk displayed in the Description column. WhatsUp Gold opens the Disk Utilization device report for that device.

Monitor report body for device reports

Below the control bar is a graph showing the disk utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

The group report displays a list of all devices in the group and the current disk utilization for the primary disk (if multiple disks are present in the device). To view the Disk Utilization monitor report for a specific device, click displayed in the Description column. WhatsUp Gold redirects you to the CPU Utilization device report for that device.

Below the date/time picker is a graph showing the disk utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

When multiple disks are present in the selected device, the following selections are also available from the **Disk** menu:

§ The Disks menu lists all available disks in the device. You can select any disk and view utilization information for that disk.

§ **All Disks**. A combined graph displaying utilization for all disks.

Split Second Graph - Real-Time Disk Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time disk utilization.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the average disk utilization percentages collected during the time period:

§ **Total Size**. The size of the disk being monitored.

§ **Min Used**. The minimum amount of disk space used.

§ **Max Used**. The maximum amount of disk space used.

§ **Avg Used**. The average amount of disk spaced in use during the time period.

§ **Min Utilization %**. The minimum disk utilization percentage experienced.

§ **Max Utilization %**. The maximum disk utilization percentage experienced.

§ **Avg Utilization %**. The average disk utilization percentage across all sample data for this time period.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Note: Linux holds 5% disk space in reserve that cannot be used for normal operations.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

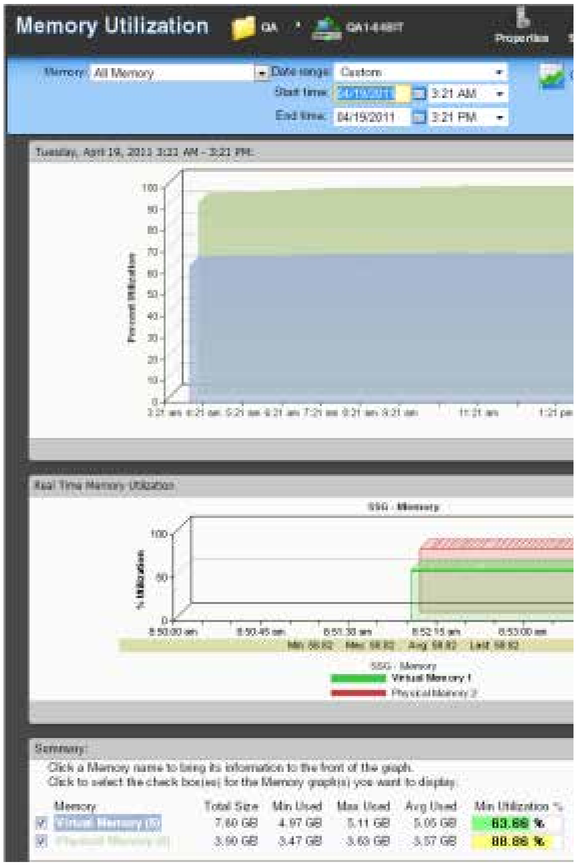
To view the properties of the current group or device, click **Properties** in the toolbar.

About the Memory Utilization report

This performance monitor report displays memory utilization collected during the selected time period from the device displayed at the top of the report.

- Configure the data collection for a device by right-clicking a device in the Device list and selecting **Properties > Performance Monitors > Memory Utilization**.
- Configure the data collection for a group by selecting a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Memory** menu.

Device Report:


Memory Utilization
QA
QA1-64BIT
Properties
100
90
80
70
60
50
40
30
20
10
0
Percent Utilization
3:21 am 4:21 am 5:21 am 6:21 am 7:21 am 8:21 am 9:21 am 11:21 am 1:21 pm
SSG - Memory
100
50
0
% Utilization
8:50:00 am 8:50:45 am 8:51:30 am 8:52:15 am 8:53:00 am
Min 58.82 Max 58.82 Avg 58.82 Last 58.82
SSG - Memory
Virtual Memory 1
Physical Memory 2

Memory: All Memory
Date range: Custom
Start time: 04/19/2011 3:21 AM
End time: 04/19/2011 3:21 PM

Tuesday, April 19, 2011 3:21 AM - 3:21 PM

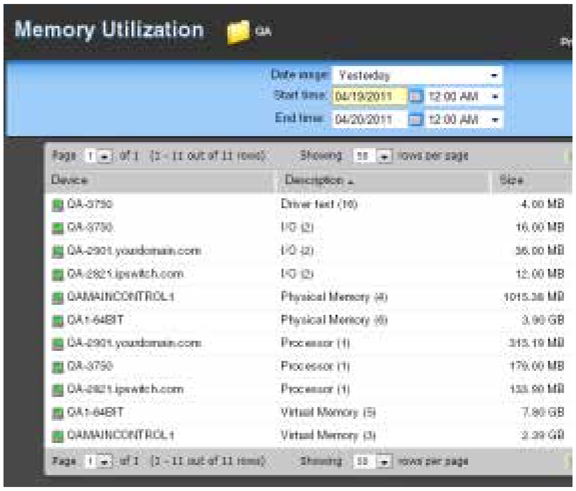
Real Time Memory Utilization

Summary:

Click a Memory name to bring its information to the front of the graph.
Click to select the check box(es) for the Memory graph(s) you want to display.

	Memory	Total Size	Min Used	Max Used	Avg Used	Min Utilization %
☑	Virtual Memory (5)	7.80 GB	4.97 GB	5.11 GB	5.05 GB	63.68 %
☑	Physical Memory (6)	3.90 GB	3.47 GB	3.63 GB	3.57 GB	88.86 %

Group Report:



Date range: Yesterday
Start time: 04/19/2011 12:00 AM
End time: 04/20/2011 12:00 AM

Page 1 of 1 (1 - 11 out of 11 rows) Showing 50 rows per page

Device	Description	Size
QA-3750	Driver text (10)	4.00 MB
QA-3750	I/O (2)	16.00 MB
QA-2901.yourdomain.com	I/O (2)	36.00 MB
QA-2821.ipswitch.com	I/O (2)	12.00 MB
QAMAINCONTROL1	Physical Memory (4)	1015.38 MB
QA1-64BIT	Physical Memory (6)	3.90 GB
QA-2901.yourdomain.com	Processor (1)	315.19 MB
QA-3750	Processor (1)	176.00 MB
QA-2821.ipswitch.com	Processor (1)	133.90 MB
QA1-64BIT	Virtual Memory (5)	7.80 GB
QAMAINCONTROL1	Virtual Memory (3)	2.39 GB

Page 1 of 1 (1 - 11 out of 11 rows) Showing 50 rows per page

Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, be sure to change the Determine uniqueness by option in the Advanced Data Collection settings for this performance monitor to description.

Monitor report body for group reports

The group report displays a list of all devices in the group and the current memory utilization for each memory type in each monitored device. To view the Memory Utilization monitor report for a specific device, click the memory type displayed in the Description column. WhatsUp Gold opens the CPU Utilization device report for that device.

Monitor report body for devices

Below the date/time picker is a graph showing the memory utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

When multiple memory types are present in the selected device, the following selections are available from the **Memory** menu:

- The Memory menu lists all available memory types in the device. You can select any type and view utilization information for that memory.
- **All Memory**. A combined graph displaying utilization for all memory types.

Split Second Graphs - Real-Time Memory Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time memory utilization data.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the average memory utilization collected during the time period:

- **Total Size**. The total amount of memory on the device being monitored.
- **Min Used**. The minimum amount of memory in use on the device.
- **Max Used**. The maximum amount of memory in use on the device.
- **Avg Used**. The average amount of memory in use on the device during the time period.
- **Min Utilization %**. The minimum disk utilization percentage experienced.
- **Max Utilization %**. The maximum disk utilization percentage experienced.
- **Avg Utilization %**. The average disk utilization percentage across all sample data for this time period.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.

- Change to another device monitor report by selecting a different report button.

Viewing Properties

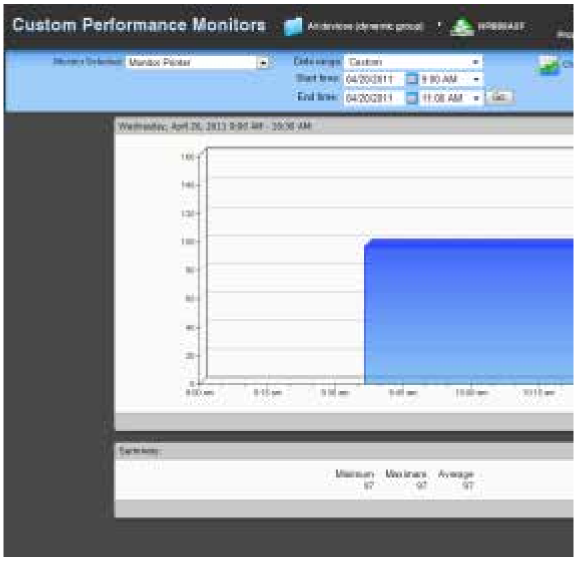
To view the properties of the current group or device, click **Properties** in the toolbar.

About the Custom performance monitor report

This performance monitor report graphs custom performance monitor values over a selected period of time.

- Configure the data collection for a device by selecting a device from the Device list and selecting **Properties > Performance Monitors**, then selecting the monitor you want to apply to the device.
- Configure the data collection for a group by selecting a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then selecting the monitor you want to apply to the group.

Device Report:



Custom Performance Monitors

All devices (dynamic group)

Monitor Selected: Monitor Printer

Date range: Custom

Start time: 04/20/2011 9:00 AM

End time: 04/20/2011 11:08 AM

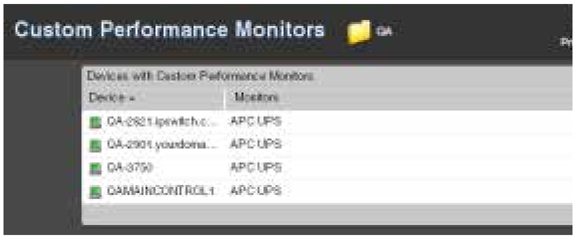
Go

Wednesday, April 20, 2011 9:00 AM - 10:30 AM

Summary:

Minimum	Maximum	Average
97	97	97

Group Report:



Custom Performance Monitors

QA

Devices with Custom Performance Monitors

Device	Monitors
QA-2821.ipswitch.c...	APC UPS
QA-2901.yourdoma...	APC UPS
QA-3750	APC UPS
QAMAINCONTROL1	APC UPS

Monitor report body for group reports

The group report displays a list of all devices in the group and the custom monitor applied to each device. To view the custom monitor data for each device, click the link to the right of the device name in the Monitors column.

Monitor report body for device reports

- Below the date/time picker, Monitor, and Chart size boxes is a graph showing the chosen monitor for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

Split Second Graph - Real Time

Under the main report graph is a Split Second Graph that displays real-time data for the WMI or SNMP custom performance monitor.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Note: Split Second Graphs are not available with Active Script performance monitors.

At the bottom of the graph, the report displays the average monitor percentages collected during the time period:

- **Minimum**. The minimum monitor percentage experienced.
- **Maximum**. The maximum percentage experienced.
- **Average**. The average monitor percentage across all sample data for this period.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Device Properties

To view the properties on the current device, click the **Device Properties** button in the application at the top of the page.

Network monitor reports

Learning about network monitors

The Network monitor group provides data about network traffic. This group includes the following monitor reports:

Interface. Displays the percent utilization or traffic for a selected interface on a device, or for all interfaces for a group of devices.

Ping Availability. Displays ping availability data collected during the selected time period for the device or group displayed in the page title bar.

Ping Response Time. Displays ping response time data collected during the selected period from the device or group displayed in the page title bar.

Interface Discards. Displays the percentage of interface utilization discards for inbound and outbound packet data for a device interface, or group of device interfaces, during a selected time period.

Interface Errors. Displays a line graph showing the percentage of interface utilization errors for inbound and outbound packet data for a specific device interface, or group of device interfaces, during a selected time period.

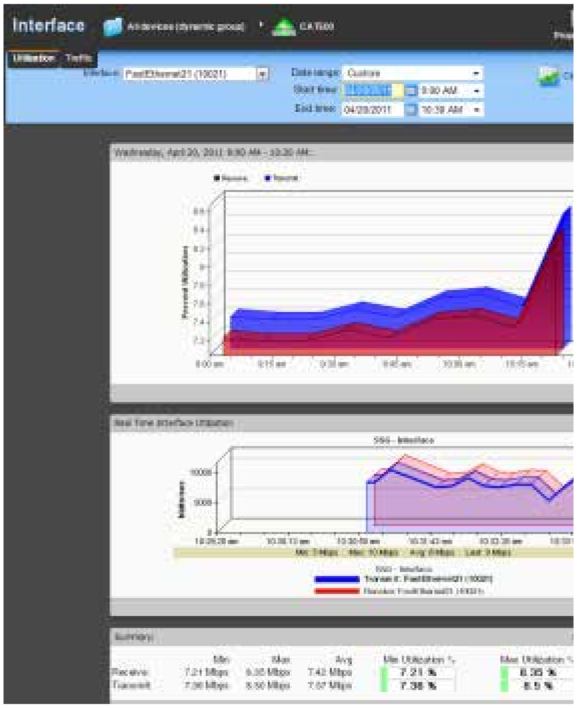
About the Interface Utilization report

This monitor report displays the percent utilization for device interfaces.

§ Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.

§ Configure the data collection for a group by right-clicking a group in the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Interfaces** menu.

Device Report:



Interface: FastEthernet21 (10021)

Date range: Custom

Start time: 04/20/2011 9:00 AM

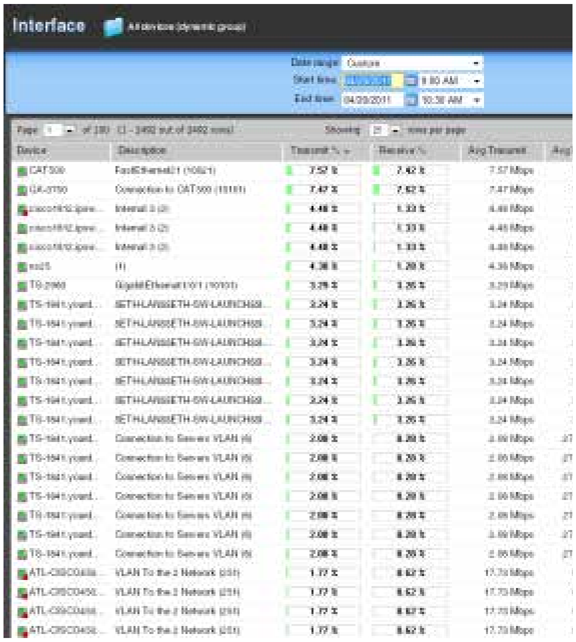
End time: 04/20/2011 10:30 AM

Wednesday, April 20, 2011 9:00 AM - 10:30 AM

Min: 3 Mbps | Max: 10 Mbps | Avg: 8 Mbps | Last: 9 Mbps

	Min	Max	Avg	Min Utilization %	Max Utilization %
Receive	7.21 Mbps	8.35 Mbps	7.42 Mbps	7.21 %	8.35 %
Transmit	7.38 Mbps	8.50 Mbps	7.57 Mbps	7.38 %	8.5 %

Group Report:



Date range: Custom

Start time: 04/20/2011 9:00 AM

End time: 04/20/2011 10:30 AM

Page 1 of 100 (1 - 2492 out of 2492 rows) Showing 25 rows per page

Device	Description	Transmit %	Receive %	Avg Transmit	Avg
CAT500	FastEthernet21 (10021)	7.57 %	7.42 %	7.57 Mbps	
GX-3750	Connection to CAT500 (10101)	7.47 %	7.62 %	7.47 Mbps	
cisco1812.ipsw...	Internal 3 (2)	4.48 %	1.33 %	4.48 Mbps	
cisco1812.ipsw...	Internal 3 (2)	4.48 %	1.33 %	4.48 Mbps	
cisco1812.ipsw...	Internal 3 (2)	4.48 %	1.33 %	4.48 Mbps	
ss25	(1)	4.36 %	1.28 %	4.36 Mbps	
TS-2960	GigabitEthernet1/0/1 (10101)	3.29 %	3.26 %	3.29 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	SETH-LANSSETH-SW-LAUNCHSS...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.yoard...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
ATL-CISCO456...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	
ATL-CISCO456...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	
ATL-CISCO456...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	
ATL-CISCO456...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	

Monitor report body for device reports

When a device is selected, the percent utilization for the currently selected interface displays. Each point on the graph corresponds with an entry in the graph data table below. In Octets are graphed with a red line, while Out Octets are graphed using blue.

When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graphs - Real-Time Interface Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time interface utilization data.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the Summary report displays the average interface utilization collected during the time period:

- **Min**. The minimum bits per second rate recorded for the interface.
- **Max**. The maximum bits per second rate recorded for the interface.
- **Avg**. The average bits per second rate recorded for the interface during the time period.
- **Min Utilization %**. The minimum interface utilization percentage recorded.
- **Max Utilization %**. The maximum interface utilization percentage recorded.
- **Avg Utilization %**. The average interface utilization percentage across all sample data for this time period.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Monitor report body for groups

Below the date/time picker is a table showing interface utilization across the current group for the selected time period.

- **Device**. The name and IP address of the device.
- **Description**. The label for the interface being shown.
- **Transmit %**. The percentage of available bandwidth used by this interface in transmitting data.
- **Receive %**. The percentage of available bandwidth used by this interface in receiving data.
- **Avg. Transmit**. The average number of bytes transmitted through the interface.
- **Avg. Receive**. The average number of bytes received through the interface.
- **Bytes Transmitted**. The total number of bytes transmitted through the interface.
- **Bytes Received**. The total number of bytes received by the interface.

Split Second Graphs in group reports

To see a real-time graph for the utilization of a device, hover over the interface description in the Description column.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.

Change to another device monitor report by selecting a different report button.

Viewing Properties

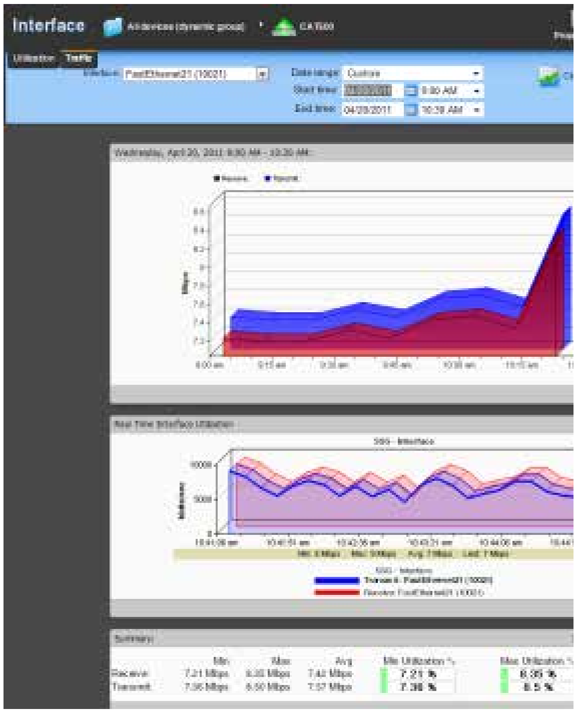
To view the properties of the current group or device, click **Properties** in the toolbar.

About the Interface Traffic report

This monitor report displays the traffic in automatically selected units for device interfaces.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.
- Configure the data collection for a group by right-clicking a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Interfaces** menu.

Device Report:



Interface: FastEthernet21 (10021)

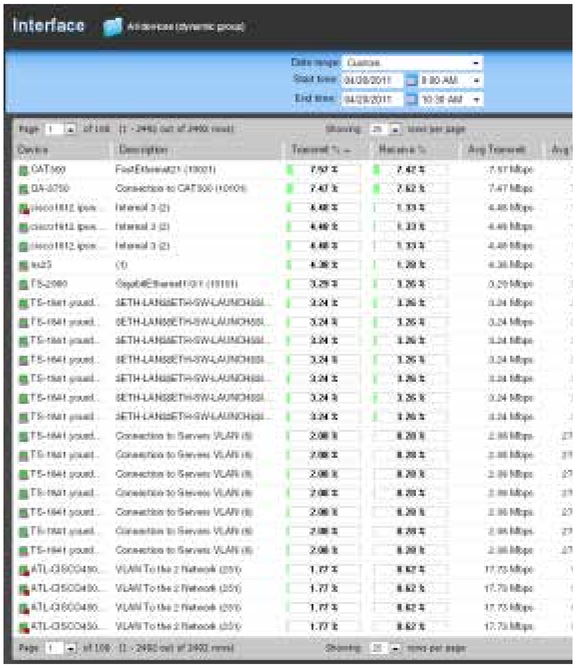
Date range: Custom

Start time: 04/20/2011 8:30 AM

End time: 04/20/2011 10:30 AM

	Min	Max	Avg	Min Utilization %	Max Utilization %
Receive	7.21 Mbps	8.35 Mbps	7.42 Mbps	7.21 %	8.35 %
Transmit	7.36 Mbps	8.50 Mbps	7.57 Mbps	7.38 %	8.5 %

Group Report:



Date range: Custom

Start time: 04/20/2011 8:30 AM

End time: 04/20/2011 10:30 AM

Page 1 of 100 (1 - 2492 out of 2492 rows) Showing: 25 rows per page

Device	Description	Transmit %	Receive %	Avg Transmit	Avg
CAT500	FastEthernet21 (10021)	7.57 %	7.42 %	7.57 Mbps	
DA-3750	Connection to CAT500 (10109)	7.47 %	7.62 %	7.47 Mbps	
cisco1812.ipsw...	Internal 3 (2)	4.48 %	1.33 %	4.48 Mbps	
cisco1812.ipsw...	Internal 3 (2)	4.48 %	1.33 %	4.48 Mbps	
cisco1812.ipsw...	Internal 3 (2)	4.48 %	1.33 %	4.48 Mbps	
lsx23	(1)	4.36 %	1.28 %	4.36 Mbps	
TS-2980	GigabitEthernet1/0/1 (10101)	3.29 %	3.26 %	3.29 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	SETH-LANS&ETH-SW-LAUNCH&&...	3.24 %	3.26 %	3.24 Mbps	
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
TS-1841.ipswd...	Connection to Servers VLAN (6)	2.08 %	8.20 %	2.08 Mbps	27
ATL-CISCO450...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	
ATL-CISCO450...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	
ATL-CISCO450...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	
ATL-CISCO450...	VLAN To the 2 Network (251)	1.77 %	8.62 %	17.73 Mbps	

Page 1 of 100 (1 - 2492 out of 2492 rows) Showing: 25 rows per page

Monitor report body for device reports

When a device is selected, the traffic for the currently selected interface displays. Each point on the graph corresponds with an entry in the graph data table below. In Octets are graphed with a red line, while Out Octets are graphed using blue.

When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Note: The units displayed in this report vary depending on the amount of traffic moving through the selected interface. Both transmitted and received traffic are considered when selecting the units to display. If there is a large difference between the transmitted and received traffic, the most relevant unit for the smaller amount of traffic is selected and applied to both.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graphs - Real-Time Interface Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time interface traffic data.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the Summary report displays the average interface utilization collected during the time period:

- **Min**. The minimum bits per second rate recorded for the interface.
- **Max**. The maximum bits per second rate recorded for the interface.
- **Avg**. The average bits per second rate recorded for the interface during the time period.
- **Min Utilization %**. The minimum interface utilization percentage recorded.
- **Max Utilization %**. The maximum interface utilization percentage recorded.
- **Avg Utilization %**. The average interface utilization percentage across all sample data for this time period.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Monitor report body for groups

Below the date/time picker is a table showing interface utilization across the current group for the selected time period.

- **Device**. The name and IP address of the device.
- **Description**. The label for the interface being shown.
- **Transmit %**. The percentage of available bandwidth used by this interface in transmitting data.
- **Receive %**. The percentage of available bandwidth used by this interface in receiving data.
- **Avg. Transmit**. The average number of bytes transmitted through the interface.
- **Avg. Receive**. The average number of bytes received through the interface.
- **Bytes Transmitted**. The total number of bytes transmitted through the interface.
- **Bytes Received**. The total number of bytes received by the interface.

Split Second Graphs in group reports

To see a real-time graph for the utilization of a device, hover over the interface description in the Description column.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.

Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

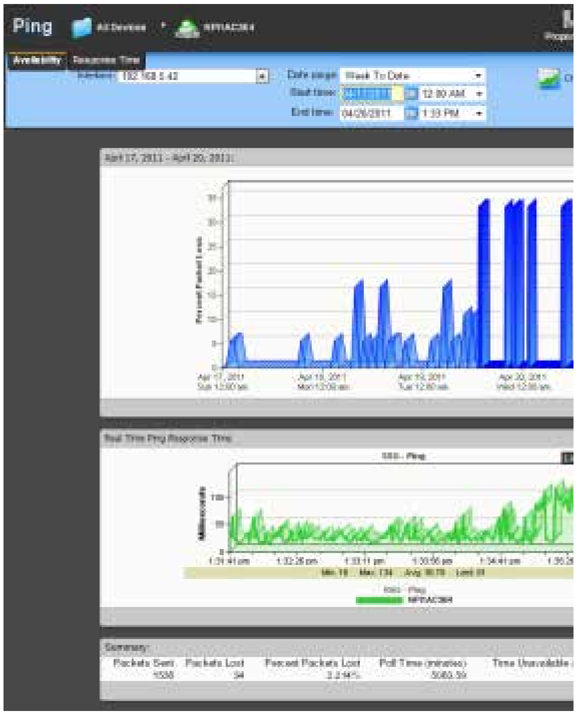
About the Ping Availability report

This performance report displays ping availability data collected during the selected time period for the device or group displayed at the top of the report.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Ping Latency and Availability > Configure**.

- Configure the data collection for a group by right-clicking a group in the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Ping** menu.

Device Report:



Ping · All Devices › NPIAC384

Availability | Response Time

Interface: 192.168.3.42

Date range: Week To Date

Start time: [illegible] 12:00 AM

End time: 04/26/2011 1:33 PM

April 17, 2011 - April 20, 2011

Percent Packet Loss
35
30
25
20
15
10
5
0
Apr 17, 2011 Sun 12:00 am
Apr 18, 2011 Mon 12:00 am
Apr 19, 2011 Tue 12:00 am
Apr 20, 2011 Wed 12:00 am

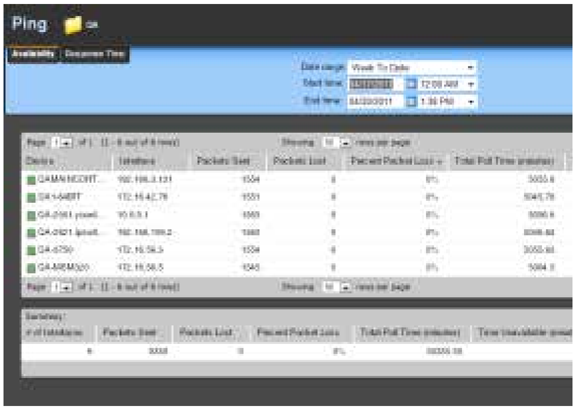
Real Time Ping Response Time

SSG - Ping
Milliseconds
100
50
0
1:31:41 pm
1:32:26 pm
1:33:11 pm
1:33:56 pm
1:34:41 pm
1:35:2
Min: 18 Max: 134 Avg: 50.70 Last: 51
SSG - Ping
NPIAC384

Summary:

Packets Sent	Packets Lost	Percent Packets Lost	Poll Time (minutes)	Time Unavailable
1538	34	2.214%	5080.59	

Group Report:



Ping · QA

Availability | Response Time

Date range: Week To Date

Start time: [illegible] 12:00 AM

End time: 04/20/2011 1:36 PM

Page 1 of 1 (1 - 6 out of 6 rows) Showing 10 rows per page

Device	Interface	Packets Sent	Packets Lost	Percent Packet Loss	Total Poll Time (minutes)
QAMAINCORT...	192.168.3.121	1554	0	0%	5055.6
QA1-64BIT	172.16.42.78	1551	0	0%	5045.78
QA-2961 yosemi...	10.0.0.1	1560	0	0%	5090.6
QA-2821 lpoal...	192.168.199.2	1560	0	0%	5095.44
QA-6750	172.16.56.3	1554	0	0%	5050.44
QA-MEM320	172.16.56.5	1545	0	0%	5084.3

Page 1 of 1 (1 - 6 out of 6 rows) Showing 10 rows per page

Summary:

# of Interfaces	Packets Sent	Packets Lost	Percent Packet Loss	Total Poll Time (minutes)	Time Unavailable
6	9308	0	0%	30335.38	

Monitor report body for device reports

Below the date/time picker is a graph showing device ping availability for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graph - Real Time Ping Availability for devices

Under the main report graph is a Split Second Graph that displays real-time ping availability data.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays general ping availability information for the device collected during the selected time period:

- **Packets Sent**. The total number of packets sent from the device during the selected time period.
- **Packets Lost**. The total number of packets lost from the device during the selected time period.
- **Percent Packets Lost**. The percentage of packets lost from the device during the selected time period.
- **Poll Time (minutes)**. Amount of total time (in minutes) that passed during the time period selected.
- **Time Unavailable (minutes)**. Amount of total time (in minutes) that the device was unavailable in the group.
- **Percent Available**. The total availability percentage for the device.

Monitor report body for groups

Below the date/time picker is a table showing ping availability across the current group for the selected time period.

- **Device**. The network device.
- **Interface**. The network interface.
- **Packets Sent**. The total number of packets sent throughout the current group during the selected time period.
- **Packets Lost**. The total number of packets lost throughout the current group during the selected time period.
- **Percent Packet Loss**. A percentage of packet loss throughout the current group for the selected time period.
- **Total Poll Time (minutes)**. Amount of total time (in minutes) that passed during the time period selected..
- **Time Unavailable (minutes)**. Amount of total time (in minutes) that a device was unavailable in the group.
- **Percent Available**. The total availability percentage averaged over all samples during the selected time period.

The Device Data table displays the same information as above, but on a per device basis.

Note: The Percent Available is a weighted average of availability for all data entries. It is not a simple average of percent availability for each entry. The value for the total availability percentage is reached by: multiplying the availability percentage with the amount of time that passed between polls to get a sum for each entry. Add those sums and divide by the sum of all time periods between polls.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Note: Click the device name to access the Device Status report, and click the interface name in the Interface column to view the availability report for that interface.

Split Second Graphs in group reports

To see a real-time graph for the availability of a device, hover over the interface name in the **Interface** column.

Below the body text is a summary of the above information:

§ **# if Interfaces**. The total number of monitored network interfaces.

§ **Packets Sent**. The total number of packets sent over the selected time period by the monitored interfaces.

§ **Packets Lost**. The total number of packets lost over the selected time period by the monitored interfaces.

§ **Percent Packet Lost**. The percentage of packets lost over the selected time period by the monitored interfaces.

§ **Total Poll Time**. The total amount of time in minutes the monitored interfaces were polled.

§ **Time Unavailable**. The total amount of time the monitored interfaces were unavailable.

§ **Percent Available**. The percentage of the amount of time the monitored interfaces were available.

Navigation

§ Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.

§ Change to another device monitor report by selecting a different report button.

Viewing Properties

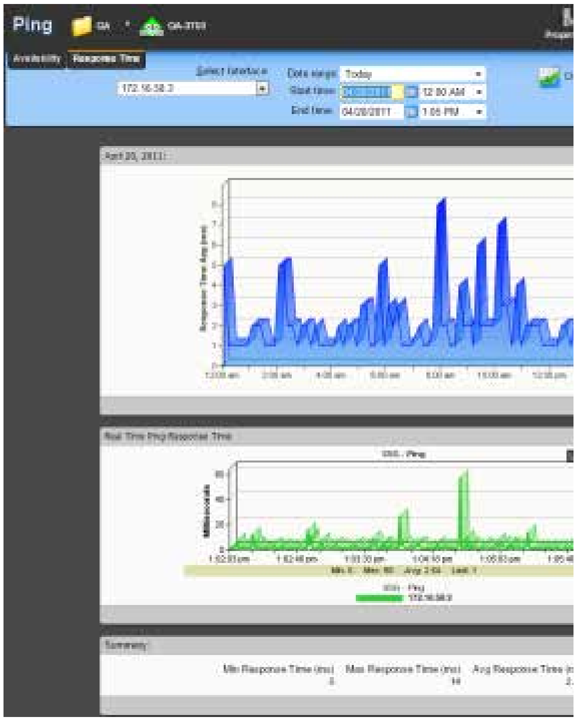
§ To view the properties of the current group or device, click **Properties** in the toolbar.

About the Ping Response Time report

This monitor report displays ping response time data collected during the selected period from the device or group displayed in the page title bar. This is the amount of time it takes a packet to be returned from the device after an ICMP (Internet Control Message Protocol) poll. It is enabled when the Ping performance monitor is applied to a device.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Ping Latency and Availability > Configure**.
- Configure the data collection for a group by right-clicking a group in the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Ping** menu.

Device Report:



Select Interface: 172.16.38.2

Date range: Today

Start time: 12:00 AM

End time: 04/20/2011 1:05 PM

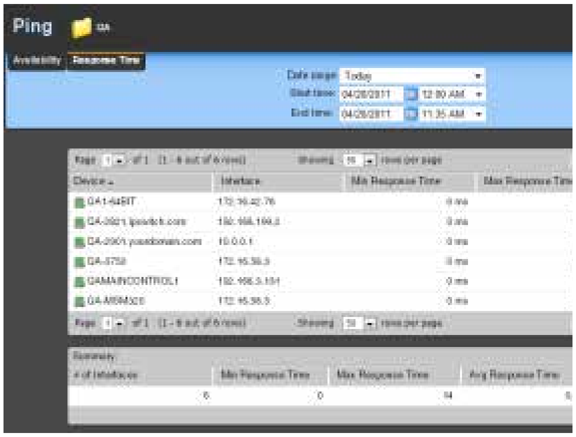
April 20, 2011:

Real Time Ping Response Time

Summary

Min Response Time (ms)	Max Response Time (ms)	Avg Response Time (m
0	14	2.

Group Report:



Date range: Today

Start time: 04/20/2011 12:00 AM

End time: 04/20/2011 11:35 AM

Page 1 of 1 (1 - 6 out of 6 rows) Showing 10 rows per page

Device	Interface	Min Response Time	Max Response Tim
QA1-64BIT	172.16.42.76	0 ms	
QA-2021.ipswitch.com	192.168.199.2	0 ms	
QA-2901.yourdomain.com	10.0.0.1	0 ms	
QA-3750	172.16.38.3	0 ms	
QAMAINCONTROL1	192.168.3.151	0 ms	
QA-M8M320	172.16.38.3	0 ms	

Page 1 of 1 (1 - 6 out of 6 rows) Showing 10 rows per page

Summary

# of Interfaces	Min Response Time	Max Response Time	Avg Response Time
6	0	14	5

Monitor report body for device reports

Below the date/time picker is a graph showing ping response times for the selected time period. Each point on the graph corresponds to an entry in the graph data table below.

When multiple interfaces are present in the selected device, change the selected interface using the **Select an Interface** menu.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graph - Real Time Ping Response Time for devices

Under the main report graph is a Split Second Graph that displays real-time ping response data.

Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.

Note: Split Second Graphs are not available in VMware host reports.

Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the summary for ping response time during the selected time period:

- **Min. Response Time**. The minimum amount of time (in milliseconds) that it took for the interface to respond to a ping over the selected time period.
- **Max Response Time**. The maximum amount of time (in milliseconds) that it took for the interface to respond to a ping over the selected time period.
- **Avg. Response Tim**e. The average amount of time (in milliseconds that it took for the interface to respond to a ping over the selected time period.

Monitor report body for groups

Below the list of devices in the current group, the Summary table shows the average response time for all interfaces in the group.

- **Device**. The device the ping monitor is active on.
- **Interface**. The specific interface the ping monitor is active on.
- **Min response time (ms)**. The minimum ping response time (in milliseconds) for the device during the selected time period
- **Max response time (ms)**. The maximum ping response time (in milliseconds) for the device during the selected time period.
- **Avg response time (ms)**. The average ping response time (in milliseconds) for the device across all sample data for this time period.

Split Second Graphs in group reports

To see a real-time graph for a device's ping response time, hover over a device interface in the Interface column.

Below the report body is an information summary:

- **# of Interfaces**. The number of monitored interfaces.
- **Min Response Time**. The minimum response time from the monitored interfaces over the selected time period.
- **Max Response Time**. The maximum response time from the monitored interfaces over the selected time period.
- **Avg Response Time**. The average response time from the monitored interfaces over the selected time period.

Note: Split Second Graphs are not available in VMware host reports.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Note: Click the device name to access the Device Status report, and click the interface.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the Interface Discards report

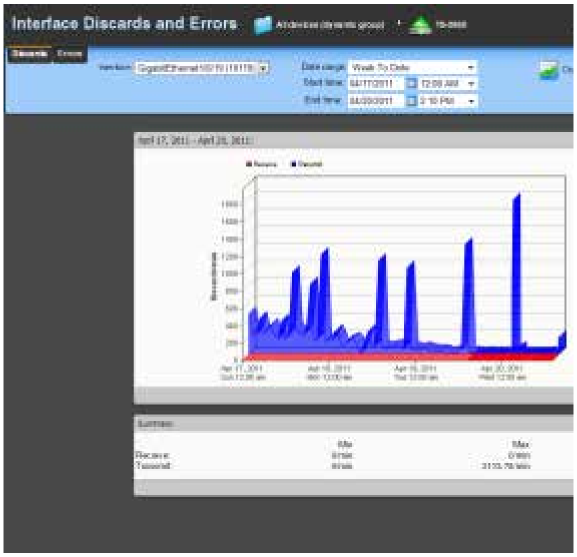
This network monitor report displays the percentage of interface utilization discards for inbound and outbound packet data for a device interface, or group of device interfaces, during a selected time period. This report allows you to monitor and troubleshoot interfaces experiencing packet discard problems.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties** > **Performance Monitors**, then selecting **Interface Utilization** > **Configure**.

Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, click **Advanced** and change the **Determine uniqueness by** list option to **Interface description**.

- Configure the data collection for a group by right-clicking a group from the Device list, selecting **Bulk Field Change** > **Performance Monitors**, and then making a selection from the **Interface** menu.

Device report:



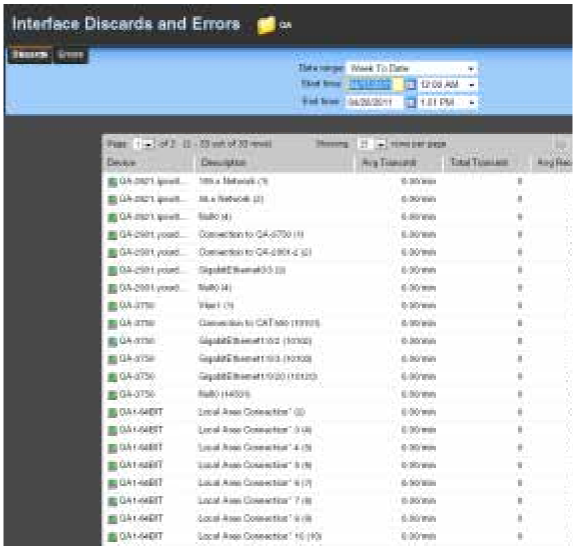
Interface Discards and Errors

Discards
Errors
All devices (dynamic group)
Interface: GigabitEthernet1/0/19 (10119)
Date range: Week To Date
Start time: 04/17/2011 12:00 AM
End time: 04/20/2011 2:10 PM
April 17, 2011 - April 20, 2011
Receive
Transmit
Discards/min
1600
1400
1200
1000
800
600
400
200
0
Apr 17, 2011 Sun 12:00 am
Apr 18, 2011 Mon 12:00 am
Apr 19, 2011 Tue 12:00 am
Apr 20, 2011 Wed 12:00 am

Summary

	Min	Max
Receive	0/min	0/min
Transmit	0/min	2133.78/min

Group report:



Interface Discards and Errors

Device	Description	Avg Transmit	Total Transmit	Avg Rec
QA-2821 ipswit...	16th a Network (1)	0.00/min	0	
QA-2821 ipswit...	3rd a Network (2)	0.00/min	0	
QA-2821 ipswit...	Null0 (4)	0.00/min	0	
QA-2901 ipswit...	Connection to QA-3750 (1)	0.00/min	0	
QA-2901 ipswit...	Connection to QA-2901-2 (2)	0.00/min	0	
QA-2901 ipswit...	GigabitEthernet0/3 (3)	0.00/min	0	
QA-2901 ipswit...	Null0 (4)	0.00/min	0	
QA-3750	Vlan1 (1)	0.00/min	0	
QA-3750	Connection to CAT500 (10101)	0.00/min	0	
QA-3750	GigabitEthernet1/0/2 (10102)	0.00/min	0	
QA-3750	GigabitEthernet1/0/3 (10103)	0.00/min	0	
QA-3750	GigabitEthernet1/0/20 (10120)	0.00/min	0	
QA-3750	Null0 (14501)	0.00/min	0	
QA1-64BIT	Local Area Connection* (2)	0.00/min	0	
QA1-64BIT	Local Area Connection* 3 (4)	0.00/min	0	
QA1-64BIT	Local Area Connection* 4 (5)	0.00/min	0	
QA1-64BIT	Local Area Connection* 5 (6)	0.00/min	0	
QA1-64BIT	Local Area Connection* 6 (7)	0.00/min	0	
QA1-64BIT	Local Area Connection* 7 (8)	0.00/min	0	
QA1-64BIT	Local Area Connection* 9 (9)	0.00/min	0	
QA1-64BIT	Local Area Connection* 10 (10)	0.00/min	0	

Monitor report body for device reports

Below the date/time picker is a graph showing interface utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below. ifInDiscards (Receive) are graphed as a red line, while ifOutDiscards (Transmit) are graphed as a blue line.When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Summary

Under the main report graph, the report displays a summary of data for the interface collected during the time period:

Receive

- **Min**. The minimum number of interface discard packets received (ifInDiscards) per minute.
- **Max**. The maximum number of interface discard packets received (ifInDiscards) per minute.
- **Avg**. The average number of interface discard packets received (ifInDiscards) per minute.

Transmit

- **Min**. The minimum number of interface discard packets transmitted (ifOutDiscards) per minute.
- **Max**. The maximum number of interface discard packets transmitted (ifOutDiscards) per minute.
- **Avg**. The average number of interface discard packets transmitted (ifOutDiscards) per minute.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Monitor report body for groups

Below the date/time picker is a table showing device interface packet discard information for the selected time period:

- **Device**. The network device name.
- **Description**. The network device interface decription.
- **Avg Transmit**. The avergage number of discarded packets transmitted from each interface per minute.
- **Total Transmit**. The total number of discarded packets transmitted for each interface.
- **Receive**. The average number of discarded packets received from each interface per minute.
- **Total Receive**. The total number of discarded packets received for each interface.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

- To view the properties of the current group or device, click **Properties** in the toolbar.

About the Interface Errors report

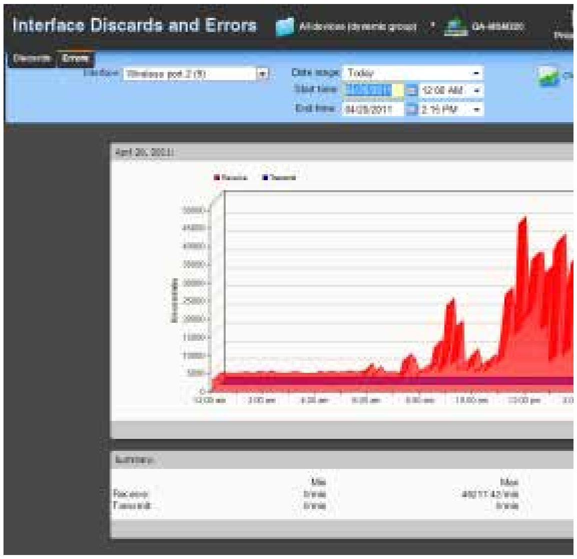
This network monitor report displays a line graph showing the percentage of interface utilization errors for inbound and outbound packet data for a specific device interface, or group of device interfaces, during a selected time period. This report allows you to monitor and troubleshoot interfaces experiencing packet error problems

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.

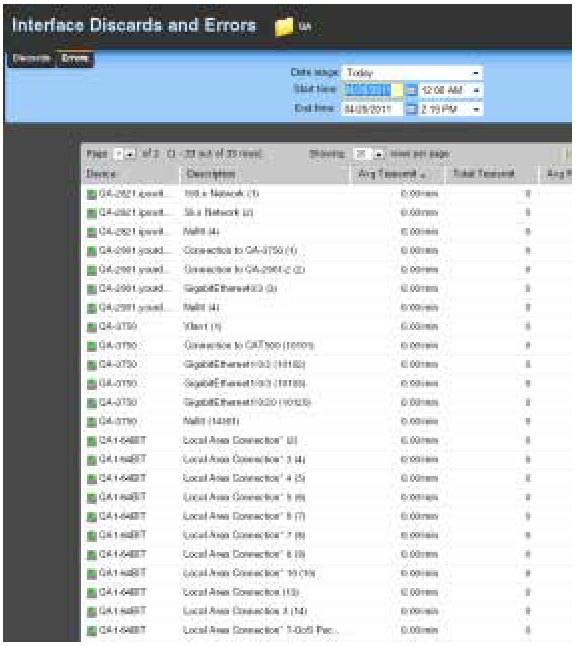
> **Note**: To ensure that your data collection is uninterrupted in the occurrence of a re-index, click **Advanced** and change the **Determine uniqueness by** list option to **Interface description**.

- Configure the data collection for a group by right-clicking a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Interface** menu.

Device report:



Group report:


Interface Discards and Errors
QA
Discards
Errors
Date range: Today
Start time: 12:00 AM
End time: 04/28/2011 2:15 PM
Page 1 of 2 (1 - 25 out of 33 rows)
Showing: 25 rows per page

Device	Description	Avg Transmit	Total Transmit
QA-2821 ipswit...	100.x Network (1)	0.00/min	0
QA-2821 ipswit...	5b.x Network (2)	0.00/min	0
QA-2821 ipswit...	Null0 (4)	0.00/min	0
QA-2901 youd...	Connection to QA-3750 (1)	0.00/min	0
QA-2901 youd...	Connection to QA-2901-2 (2)	0.00/min	0
QA-2901 youd...	GigabitEthernet0/3 (3)	0.00/min	0
QA-2901 youd...	Null0 (4)	0.00/min	0
QA-3750	Vlan1 (1)	0.00/min	0
QA-3750	Connection to CAT500 (10101)	0.00/min	0
QA-3750	GigabitEthernet1/0/2 (10102)	0.00/min	0
QA-3750	GigabitEthernet1/0/3 (10103)	0.00/min	0
QA-3750	GigabitEthernet1/0/20 (10120)	0.00/min	0
QA-3750	Null0 (14501)	0.00/min	0
QA1-64BIT	Local Area Connection* (2)	0.00/min	0
QA1-64BIT	Local Area Connection* 3 (4)	0.00/min	0
QA1-64BIT	Local Area Connection* 4 (5)	0.00/min	0
QA1-64BIT	Local Area Connection* 5 (6)	0.00/min	0
QA1-64BIT	Local Area Connection* 6 (7)	0.00/min	0
QA1-64BIT	Local Area Connection* 7 (8)	0.00/min	0
QA1-64BIT	Local Area Connection* 8 (9)	0.00/min	0
QA1-64BIT	Local Area Connection* 10 (10)	0.00/min	0
QA1-64BIT	Local Area Connection (13)	0.00/min	0
QA1-64BIT	Local Area Connection 3 (14)	0.00/min	0
QA1-64BIT	Local Area Connection* 7-QoS Pac...	0.00/min	0

Monitor report body for device reports

Below the date/time picker is a graph showing interface utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below. ifInErrors (Receive) are graphed as a red line, while ifOutErrors (Transmit) are graphed as a blue line.

When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Summary for device reports

Under the main report graph, the report displays a summary of data for the interface collected during the time period:

Receive

- **Min**. The minimum number of interface error packets received (ifInErrors) per minute.
- **Max**. The maximum number of interface error packets received (ifInErrors) per minute.
- **Avg**. The average number of interface error packets received (ifInErrors) per minute.

Transmit

- **Min**. The minimum number of interface error packets transmitted (ifOutErrors) per minute.
- **Max**. The maximum number of interface error packets transmitted (ifOutErrors) per minute.
- **Avg**. The average number of interface error packets transmitted (ifOutErrors) per minute.

Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.

You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Monitor report body for groups

Below the date/time picker is a table showing device interface packet error information for the selected time period:

- **Device**. The network device name.
- **Description**. The network device interface description.
- **Avg Transmit**. The average number of packets transmitted with errors from each interface per minute.
- **Total Transmit**. The total number of packets transmitted with errors for each interface.
- **Receive**. The average number of packets received with errors from each interface per minute.
- **Total Receive**. The total number of packets received with errors for each interface.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

§ To view the properties of the current group or device, click **Properties** in the toolbar.

Using Device monitor reports

Learning about Device monitors

The Device monitor group includes monitors which provide information about specific devices that you select to monitor. This group includes the following monitor reports:

§ **Active Monitor Availability**. Displays a graph that outlines the availability of the Active Monitors for a device or group of devices.

§ **Active Monitor Outages**. Displays a table showing the downtime of all active monitors in the currently selected group.

§ **Device Uptime**. Displays a table showing the uptime status for monitored devices in the selected group.

§ **Device Health**. Displays the current status of monitored devices in the selected group, along with each monitor applied to those devices.

§ **State Change Acknowledgement**. Displays a table of devices in the selected group that have changed state and have not received acknowledgement.

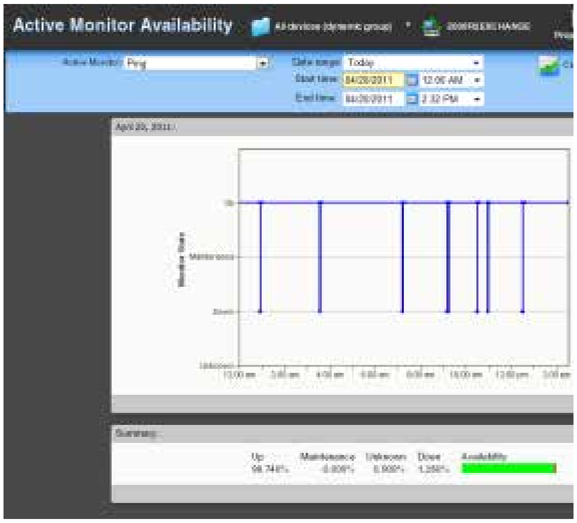
§ **State Change Timeline**. Displays a table showing when a monitor on a device, or all monitors on all devices in a group, changed from one state to another during a selected time period.

§ **Top 10**. Displays a dashboard containing lists of top 10 devices based on a variety of monitor reports.

About the Active Monitor Availability report

This device monitor report displays an area graph that outlines the availability of the Active Monitors for a device or group of devices.

Device report:



Active Monitor Availability — All devices (dynamic group) • 2008R2EXCHANGE

Active Monitor: Ping

Date range: Today

Start time: 04/20/2011 12:00 AM

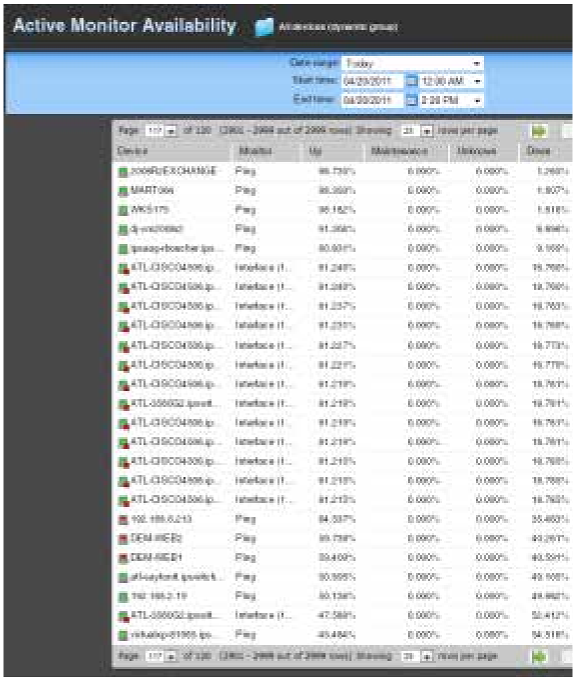
End time: 04/20/2011 2:32 PM

April 20, 2011:

Summary:

Up	Maintenance	Unknown	Down	Availability
98.740%	0.000%	0.000%	1.260%	🟩

Group report



Active Monitor Availability — All devices (dynamic group)

Date range: Today

Start time: 04/20/2011 12:00 AM

End time: 04/20/2011 2:28 PM

Page 117 of 120 (2901 - 2999 out of 2999 rows) Showing 25 rows per page

Device	Monitor	Up	Maintenance	Unknown	Down
2008R2EXCHANGE	Ping	98.740%	0.000%	0.000%	1.260%
MART064	Ping	98.393%	0.000%	0.000%	1.607%
WKS175	Ping	98.182%	0.000%	0.000%	1.818%
dj-vm2008r2	Ping	91.306%	0.000%	0.000%	8.694%
tpsaap-boacher.ips...	Ping	90.831%	0.000%	0.000%	9.169%
ATL-CISCO4506.ip...	Interface (I...	81.240%	0.000%	0.000%	18.760%
ATL-CISCO4506.ip...	Interface (I...	81.240%	0.000%	0.000%	18.760%
ATL-CISCO4506.ip...	Interface (I...	81.237%	0.000%	0.000%	18.763%
ATL-CISCO4506.ip...	Interface (I...	81.231%	0.000%	0.000%	18.769%
ATL-CISCO4506.ip...	Interface (I...	81.227%	0.000%	0.000%	18.773%
ATL-CISCO4506.ip...	Interface (I...	81.221%	0.000%	0.000%	18.779%
ATL-CISCO4506.ip...	Interface (I...	81.219%	0.000%	0.000%	18.781%
ATL-3560G2.ipswit...	Interface (I...	81.219%	0.000%	0.000%	18.781%
ATL-CISCO4506.ip...	Interface (I...	81.219%	0.000%	0.000%	18.781%
ATL-CISCO4506.ip...	Interface (I...	81.219%	0.000%	0.000%	18.781%
ATL-CISCO4506.ip...	Interface (I...	81.215%	0.000%	0.000%	18.785%
ATL-CISCO4506.ip...	Interface (I...	81.215%	0.000%	0.000%	18.785%
ATL-CISCO4506.ip...	Interface (I...	81.213%	0.000%	0.000%	18.787%
192.168.0.213	Ping	64.537%	0.000%	0.000%	35.463%
DEM-WEB2	Ping	59.733%	0.000%	0.000%	40.267%
DEM-WEB1	Ping	59.409%	0.000%	0.000%	40.591%
atl-cayford.ipswitch...	Ping	50.495%	0.000%	0.000%	49.505%
192.168.2.19	Ping	50.138%	0.000%	0.000%	49.862%
ATL-3560G2.ipswit...	Interface (I...	47.588%	0.000%	0.000%	52.412%
rivkalep-81965.ips...	Ping	45.484%	0.000%	0.000%	54.516%

Page 117 of 120 (2901 - 2999 out of 2999 rows) Showing 25 rows per page

Monitor report body for device reports

A graph at the top of the monitor report displays the state of the selected active monitor for the device.

Summary for device reports

At the bottom of the graph, the summary section displays:

- **Up**. The percentage for the amount of time the Active Monitors were up.
- **Maintenance**. The percentage for the amount of time the Active Monitors were in maintenance.
- **Unknown**. The percentage for the amount of time the Active Monitors status was unknown.
- **Down**. The percentage for the amount of time the Active Monitors were down.
- **Availability**. The overall availability for the Active Monitor by color for the selected time period.
- **Green**. Percentage of the time device was available.
- **Red**. Percentage of time the device was unavailable.
- **Orange**. Percentage of time the device was in maintenance mode.
- **Gray**. Percentage of time the device was in an unknown state. The state of a device is unknown when the monitors for that device are disabled or deleted, or if a device has an "up" dependency and the device it is dependent upon is down.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Monitor report body for group reports

This group report displays a summary of availability times for all Active Monitors within a device group. The following information is displayed within the report:

- **Device**. The network device. Click one of the device entries to view the Device Active Monitor Availability Report for that device.
- **Monitor**. The type of Active Monitor.
- **Up**. The percentage for the amount of time the Active Monitor was up.
- **Maintenance**. The percentage for the amount of time the Active Monitor was in maintenance.
- **Unknown**. The percentage for the amount of time the Active Monitor was in an unknown state.
- **Down**. The percentage for the amount of time the Active Monitor was down.
- **Availability**. The overall availability for the Active Monitor by color for the selected time period.
- **Green**. Percentage of the time device was available.
- **Red**. Percentage of time the device was unavailable.
- **Orange**. Percentage of time the device was in maintenance mode.
- **Gray**. Percentage of time the device was in an unknown state. The state of a device is unknown when the monitors for that device are disabled or deleted, or if a device has an "up" dependency and the device it is dependent upon is down.

Navigation

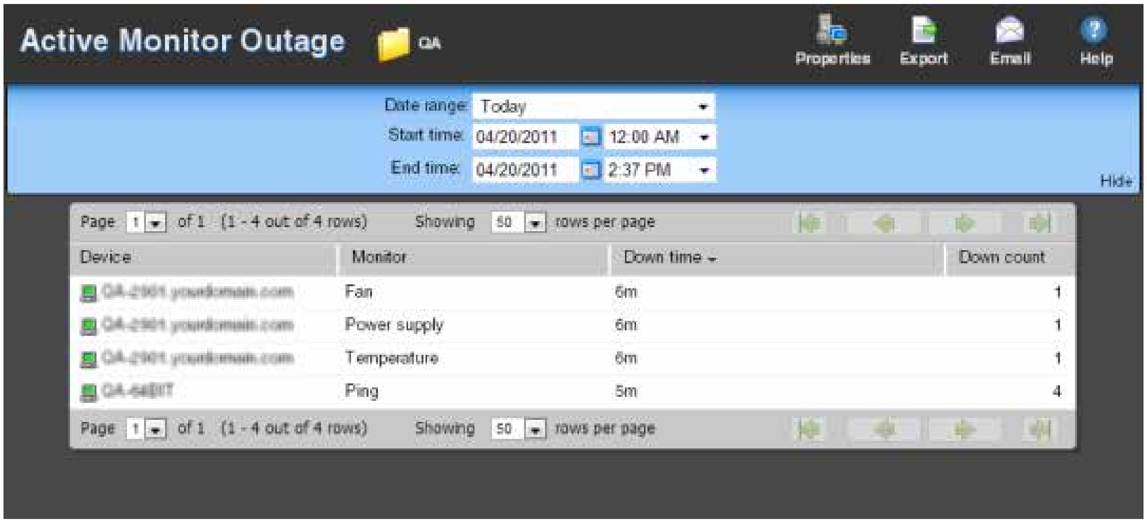
- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the Active Monitor Outages report

This device report shows the downtime of all active monitors in the currently selected group.



Date range: Today

Start time: 04/20/2011 12:00 AM

End time: 04/20/2011 2:37 PM

Page 1 of 1 (1 - 4 out of 4 rows) Showing 50 rows per page

Device	Monitor	Down time	Down count
[redacted]	Fan	6m	1
[redacted]	Power supply	6m	1
[redacted]	Temperature	6m	1
[redacted]	Ping	5m	4

Page 1 of 1 (1 - 4 out of 4 rows) Showing 50 rows per page

Monitor report body

- **Device**. Lists the device state icon, host name, and IP address.
- **Monitor**. Lists the active monitor as it appears in the Active Monitor Library.
- **Down time**. Specifies how long the active monitor has been in the down state.
- **Down count**. Specifies how many times the active monitor has gone into the down state during the down time.

Navigation

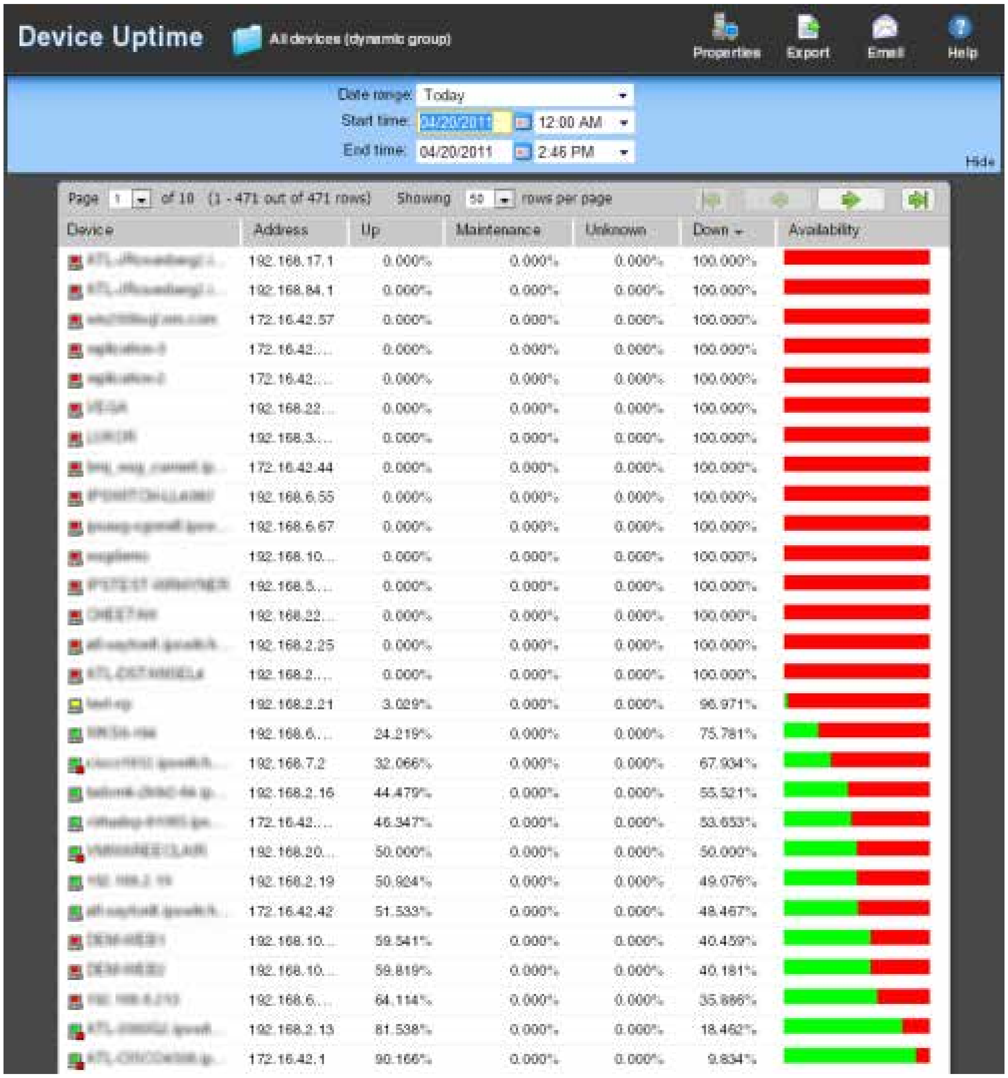
- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the Device Uptime report

This device report displays the uptime status for monitored devices in the selected group.



Date range: Today
Start time: 04/20/2011 12:00 AM
End time: 04/20/2011 2:46 PM

Page 1 of 10 (1 - 471 out of 471 rows) Showing 50 rows per page

Device	Address	Up	Maintenance	Unknown	Down	Availability
[redacted]	192.168.17.1	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.84.1	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	172.16.42.57	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	172.16.42....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	172.16.42....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.22....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.3....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	172.16.42.44	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.6.55	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.6.67	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.10....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.5....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.22....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.2.25	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.2....	0.000%	0.000%	0.000%	100.000%	🟥
[redacted]	192.168.2.21	3.029%	0.000%	0.000%	96.971%	🟩🟥
[redacted]	192.168.6....	24.219%	0.000%	0.000%	75.781%	🟩🟥
[redacted]	192.168.7.2	32.066%	0.000%	0.000%	67.934%	🟩🟥
[redacted]	192.168.2.16	44.479%	0.000%	0.000%	55.521%	🟩🟥
[redacted]	172.16.42....	46.347%	0.000%	0.000%	53.653%	🟩🟥
[redacted]	192.168.20....	50.000%	0.000%	0.000%	50.000%	🟩🟥
[redacted]	192.168.2.19	50.924%	0.000%	0.000%	49.076%	🟩🟥
[redacted]	172.16.42.42	51.533%	0.000%	0.000%	48.467%	🟩🟥
[redacted]	192.168.10....	59.541%	0.000%	0.000%	40.459%	🟩🟥
[redacted]	192.168.10....	59.819%	0.000%	0.000%	40.181%	🟩🟥
[redacted]	192.168.6....	64.114%	0.000%	0.000%	35.886%	🟩🟥
[redacted]	192.168.2.13	81.538%	0.000%	0.000%	18.462%	🟩🟥
[redacted]	172.16.42.1	90.166%	0.000%	0.000%	9.834%	🟩🟥

- For more information about what each icon state means, see Device State Legend.

Monitor report body

Below the date/time picker is a table showing the devices in the group collecting data for the time period chosen, and the uptime status information for the each device in the group:

- **Device**. The group device's display name (or IP address if a display name isn't specified in its Device Properties) and device state icon.
- **Address**. The device IP address monitor.

- **Up**. The percentage for the amount of time the device was up during the selected time period for all devices.
- **Maintenance**. The percentage for the amount of time the device was in maintenance during the selected time period for all devices.
- **Unknown**. The percentage for the amount of time the device status was in an unknown state during the selected time period for all devices.
- **Down**. The percentage for the amount of time the device was down during the selected time period for all devices.
- **Availability**. The overall availability for the device during the selected time period, by color. The percentage of the bar shaded red in the Availability column indicates the percentage of time the device was not available, while the percentage shaded green indicates the percentage of time the device was available.

Navigation

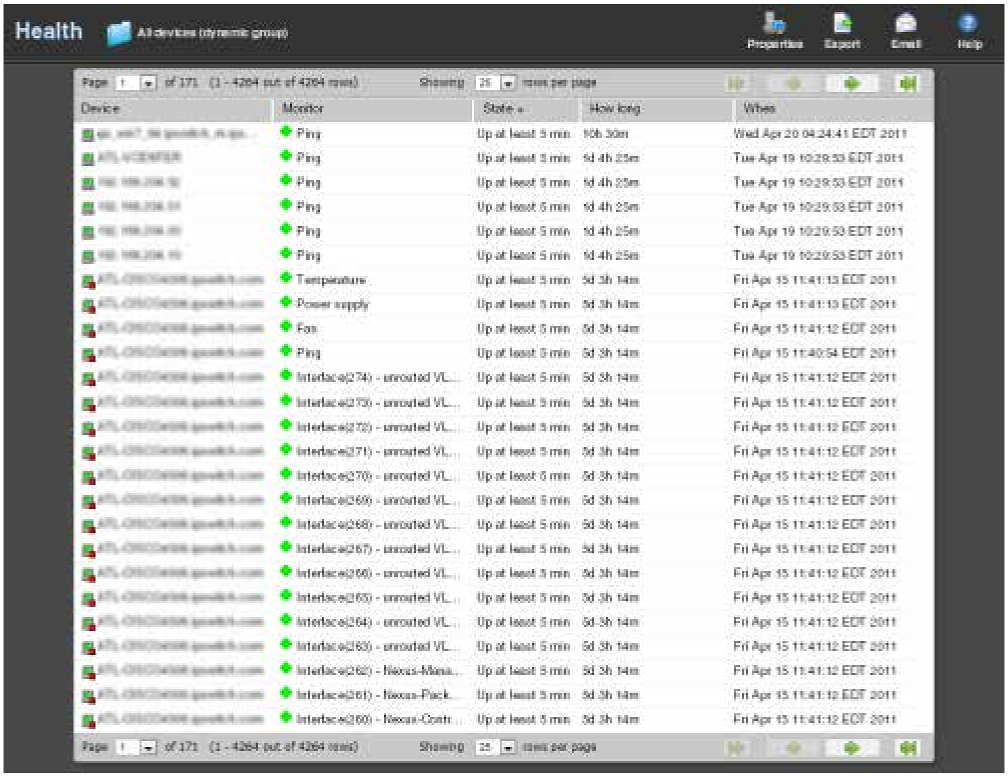
- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the Device Health report

This group report displays the current status of monitored devices in the selected group, along with each monitor configured to those devices.



Page 1 of 171 (1 - 4264 out of 4264 rows) Showing 25 rows per page

Device	Monitor	State ▲	How long	When
[redacted]	Ping	Up at least 5 min	10h 30m	Wed Apr 20 04:24:41 EDT 2011
[redacted]	Ping	Up at least 5 min	1d 4h 25m	Tue Apr 19 10:29:53 EDT 2011
[redacted]	Ping	Up at least 5 min	1d 4h 25m	Tue Apr 19 10:29:53 EDT 2011
[redacted]	Ping	Up at least 5 min	1d 4h 25m	Tue Apr 19 10:29:53 EDT 2011
[redacted]	Ping	Up at least 5 min	1d 4h 25m	Tue Apr 19 10:29:53 EDT 2011
[redacted]	Ping	Up at least 5 min	1d 4h 25m	Tue Apr 19 10:29:53 EDT 2011
[redacted]	Temperature	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:13 EDT 2011
[redacted]	Power supply	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:13 EDT 2011
[redacted]	Fan	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Ping	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:40:54 EDT 2011
[redacted]	Interface(274) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(273) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(272) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(271) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(270) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(269) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(268) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(267) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(266) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(265) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(264) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(263) - unrouted VL...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(262) - Nexus-Mana...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(261) - Nexus-Pack...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011
[redacted]	Interface(260) - Nexus-Contr...	Up at least 5 min	5d 3h 14m	Fri Apr 15 11:41:12 EDT 2011

Page 1 of 171 (1 - 4264 out of 4264 rows) Showing 25 rows per page

For more information about what each icon state means, see Device State Legend.

Monitor report body

Below the date/time picker is a table showing the total number of devices in the group collecting data for the time period chosen, and the status of the monitors configured for the devices in that group. The following information displays:

- **Device**. The network device.
- **Monitor**. The specific monitor.
- **State**. The state of the monitor at the time of the last poll.
- **How long**. The period of time that the monitor has been in the current state.
- **When**. The date and time the monitor went in to the current state.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

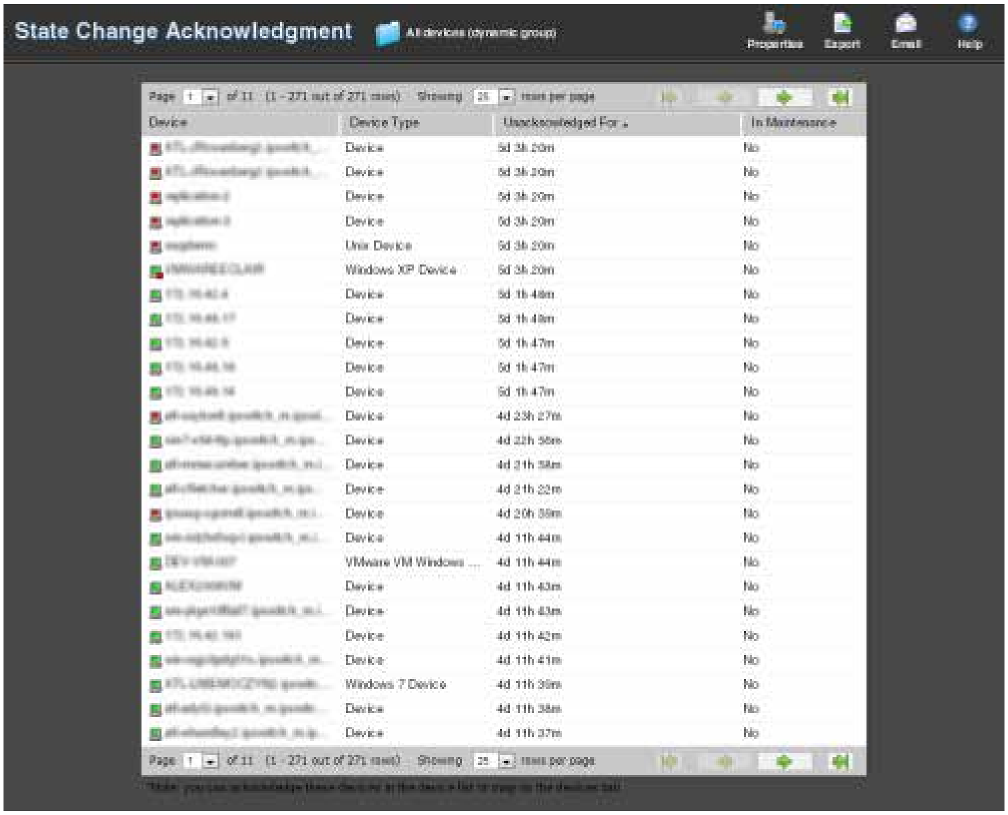
Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the State Change Acknowledgment report

When a device state changes, regardless of any action that has been placed on the device, WhatsUp Gold uses the Acknowledgement feature to make you aware that the state change occurred. In the device list, the name of the device appears in bold, and in the map view, the device name appears on a black background.

Once the device is in Acknowledgement mode, it will remain until you actively acknowledge it.



Page 1 of 11 (1 - 271 out of 271 rows) Showing 25 rows per page

Device	Device Type	Unacknowledged For	In Maintenance
🟥 [redacted]	Device	5d 3h 20m	No
🟥 [redacted]	Device	5d 3h 20m	No
🟥 [redacted]	Device	5d 3h 20m	No
🟥 [redacted]	Device	5d 3h 20m	No
🟥 [redacted]	Unix Device	5d 3h 20m	No
🟩 [redacted]	Windows XP Device	5d 3h 20m	No
🟩 [redacted]	Device	5d 1h 48m	No
🟩 [redacted]	Device	5d 1h 48m	No
🟩 [redacted]	Device	5d 1h 47m	No
🟩 [redacted]	Device	5d 1h 47m	No
🟩 [redacted]	Device	5d 1h 47m	No
🟥 [redacted]	Device	4d 23h 27m	No
🟩 [redacted]	Device	4d 22h 58m	No
🟩 [redacted]	Device	4d 21h 58m	No
🟩 [redacted]	Device	4d 21h 22m	No
🟥 [redacted]	Device	4d 20h 59m	No
🟩 [redacted]	Device	4d 11h 44m	No
🟩 [redacted]	VMware VM Windows ...	4d 11h 44m	No
🟩 [redacted]	Device	4d 11h 43m	No
🟩 [redacted]	Device	4d 11h 43m	No
🟩 [redacted]	Device	4d 11h 42m	No
🟩 [redacted]	Device	4d 11h 41m	No
🟩 [redacted]	Windows 7 Device	4d 11h 39m	No
🟩 [redacted]	Device	4d 11h 38m	No
🟩 [redacted]	Device	4d 11h 37m	No

Page 1 of 11 (1 - 271 out of 271 rows) Showing 25 rows per page

[illegible]

Note: Acknowledging a device state change does not keep that device from firing actions. To stop a device from firing actions, you must put the device into maintenance mode.

This group report shows the following information:

- **Device**. The current state and label of the device that has changed state.
- **Device Type**. The type of device.
- **Unacknowledged for**. The amount of time the device has remained unacknowledged on this report.
- **In Maintenance**. Indicates whether or not the device is in maintenance mode. The state is either yes or no.

Navigation

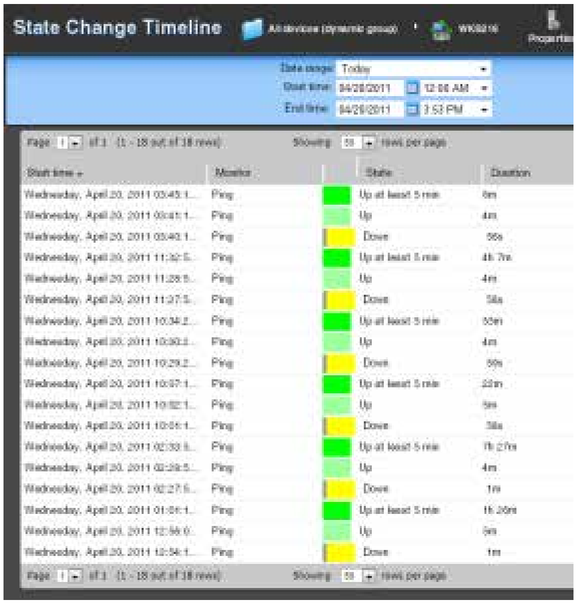
- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the State Change Timeline report

Device report:



State Change Timeline · All devices (dynamic group) • WKS216 · Properties

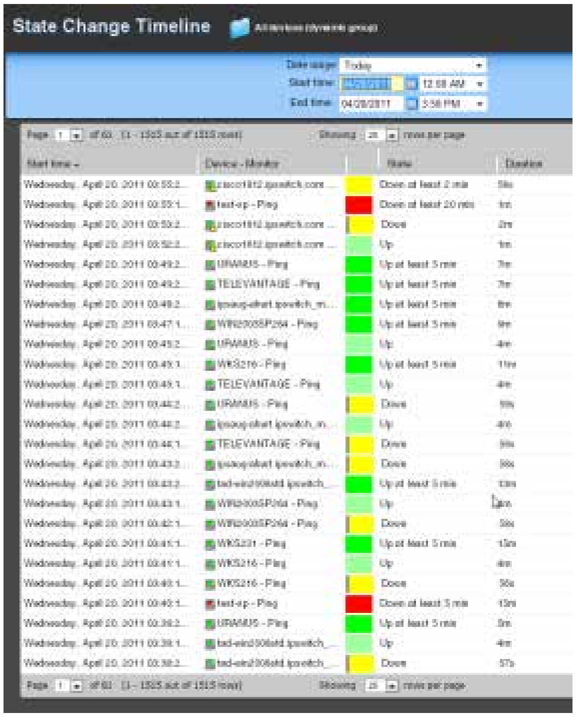
Date range: Today
Start time: 04/20/2011 12:00 AM
End time: 04/20/2011 3:53 PM

Page 1 of 1 (1 - 18 out of 18 rows) Showing 50 rows per page

Start time	Monitor		State	Duration
Wednesday, April 20, 2011 03:45:1...	Ping	🟩	Up at least 5 min	6m
Wednesday, April 20, 2011 03:41:1...	Ping	🟩	Up	4m
Wednesday, April 20, 2011 03:40:1...	Ping	🟨	Down	56s
Wednesday, April 20, 2011 11:32:5...	Ping	🟩	Up at least 5 min	4h 7m
Wednesday, April 20, 2011 11:28:5...	Ping	🟩	Up	4m
Wednesday, April 20, 2011 11:27:5...	Ping	🟨	Down	58s
Wednesday, April 20, 2011 10:34:2...	Ping	🟩	Up at least 5 min	53m
Wednesday, April 20, 2011 10:30:2...	Ping	🟩	Up	4m
Wednesday, April 20, 2011 10:29:2...	Ping	🟨	Down	59s
Wednesday, April 20, 2011 10:07:1...	Ping	🟩	Up at least 5 min	22m
Wednesday, April 20, 2011 10:02:1...	Ping	🟩	Up	5m
Wednesday, April 20, 2011 10:01:1...	Ping	🟨	Down	38s
Wednesday, April 20, 2011 02:33:5...	Ping	🟩	Up at least 5 min	7h 27m
Wednesday, April 20, 2011 02:29:5...	Ping	🟩	Up	4m
Wednesday, April 20, 2011 02:27:5...	Ping	🟨	Down	1m
Wednesday, April 20, 2011 01:01:1...	Ping	🟩	Up at least 5 min	1h 26m
Wednesday, April 20, 2011 12:56:0...	Ping	🟩	Up	5m
Wednesday, April 20, 2011 12:54:1...	Ping	🟨	Down	1m

Page 1 of 1 (1 - 18 out of 18 rows) Showing 50 rows per page

Group report:



State Change Timeline · All devices (dynamic group)

Date range: Today
Start time: 04/20/2011 12:00 AM
End time: 04/20/2011 3:56 PM

Page 1 of 61 (1 - 1525 out of 1515 rows) Showing 25 rows per page

Start time	Device - Monitor		State	Duration
Wednesday, April 20, 2011 03:55:2...	cisco1812.ipswitch.com ...	🟨	Down at least 2 min	58s
Wednesday, April 20, 2011 03:55:1...	test-up - Ping	🟥	Down at least 20 min	1m
Wednesday, April 20, 2011 03:53:2...	cisco1812.ipswitch.com ...	🟨	Down	2m
Wednesday, April 20, 2011 03:52:2...	cisco1812.ipswitch.com ...	🟩	Up	1m
Wednesday, April 20, 2011 03:49:2...	URANUS - Ping	🟩	Up at least 5 min	7m
Wednesday, April 20, 2011 03:49:2...	TELEVANTAGE - Ping	🟩	Up at least 5 min	7m
Wednesday, April 20, 2011 03:48:2...	ipsaug-elhart.ipswitch_m...	🟩	Up at least 5 min	8m
Wednesday, April 20, 2011 03:47:1...	WIN2003SP2x64 - Ping	🟩	Up at least 5 min	9m
Wednesday, April 20, 2011 03:45:2...	URANUS - Ping	🟩	Up	4m
Wednesday, April 20, 2011 03:45:1...	WKS216 - Ping	🟩	Up at least 5 min	11m
Wednesday, April 20, 2011 03:45:1...	TELEVANTAGE - Ping	🟩	Up	4m
Wednesday, April 20, 2011 03:44:2...	URANUS - Ping	🟨	Down	59s
Wednesday, April 20, 2011 03:44:2...	ipsaug-elhart.ipswitch_m...	🟩	Up	4m
Wednesday, April 20, 2011 03:44:1...	TELEVANTAGE - Ping	🟨	Down	59s
Wednesday, April 20, 2011 03:43:2...	ipsaug-elhart.ipswitch_m...	🟨	Down	58s
Wednesday, April 20, 2011 03:43:2...	tad-win2008std.ipswitch_...	🟩	Up at least 5 min	13m
Wednesday, April 20, 2011 03:43:1...	WIN2003SP2x64 - Ping	🟩	Up	4m
Wednesday, April 20, 2011 03:42:1...	WIN2003SP2x64 - Ping	🟨	Down	58s
Wednesday, April 20, 2011 03:41:1...	WKS231 - Ping	🟩	Up at least 5 min	13m
Wednesday, April 20, 2011 03:41:1...	WKS216 - Ping	🟩	Up	4m
Wednesday, April 20, 2011 03:40:1...	WKS216 - Ping	🟨	Down	58s
Wednesday, April 20, 2011 03:40:1...	test-up - Ping	🟥	Down at least 3 min	13m
Wednesday, April 20, 2011 03:38:2...	URANUS - Ping	🟩	Up at least 5 min	5m
Wednesday, April 20, 2011 03:38:1...	tad-win2008std.ipswitch_...	🟩	Up	4m
Wednesday, April 20, 2011 03:38:2...	tad-win2008std.ipswitch_...	🟨	Down	57s

Page 1 of 61 (1 - 1525 out of 1515 rows) Showing 25 rows per page

Monitor report body for devices

This device monitor report shows a timeline of when a monitor on a device, or all monitors on all devices in a group, changed from one state to another during a selected time period.

- **Start time.** The date and time of the state change.
- **Monitor**. The device name and the type of monitor that experienced the state change.
- **State**. The state of the condition at the time of the poll. The thin gray bar on a state indicator color block means that the device state change has not been acknowledged.
- **Duration**. The amount of time the state remained unchanged.
- **Message**. The actual result message returned to WhatsUp Gold at the time of the poll.

Monitor report body for groups

This group report shows a timeline of when each monitor on a device in the selected group changed from one state to another during the selected time period.

- **Start time**. The date and time of the state change.
- **Device-Monitor**. The device name and the type of monitor that experienced the state change.

- **State**. The state of the condition at the time of the poll. The thin gray bar on a state indicator color block means that the device state change has not been acknowledged.
- **Duration**. The amount of time the state remained unchanged.
- **Message**. The actual result message returned to WhatsUp Gold at the time of the poll.

Click a device name to access the Device Status Report for that device.

Click the current state to access the State Change Timeline for that device.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

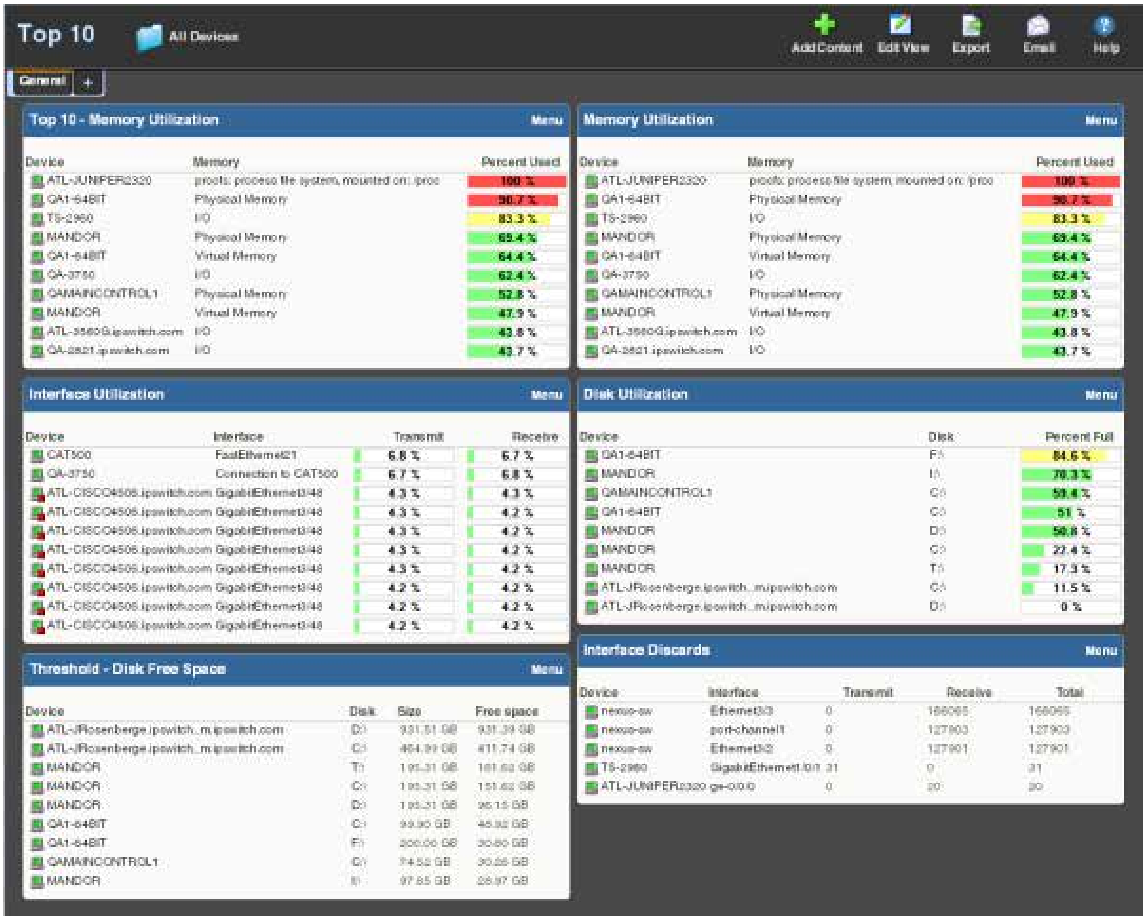
Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

About the Top 10 dashboard

The WhatsUp Gold Top 10 dashboard displays Top 10 reports for your network devices. The Top 10 dashboard shows devices, at a glance, that may be potential problems and to provide information on the current health of your network devices. It is pre-configured to include reports that display data on the top network devices by:

- Interface Errors
- Interface Discards
- Interface Utilization
- Interface Traffic
- Ping Response Time
- Disk Utilization
- CPU Utilization
- Memory Utilization



Top 10 - Memory Utilization

Device	Memory	Percent Used
ATL-JUNIPER2320	procfs: process file system, mounted on: /proc	100 %
QA1-64BIT	Physical Memory	90.7 %
TS-2960	I/O	83.3 %
MANDOR	Physical Memory	69.4 %
QA1-64BIT	Virtual Memory	64.4 %
QA-3750	I/O	62.4 %
QAMAINCONTROL1	Physical Memory	52.8 %
MANDOR	Virtual Memory	47.9 %
ATL-3560G.ipswitch.com	I/O	43.8 %
QA-2821.ipswitch.com	I/O	43.7 %

Memory Utilization

Device	Memory	Percent Used
ATL-JUNIPER2320	procfs: process file system, mounted on: /proc	100 %
QA1-64BIT	Physical Memory	90.7 %
TS-2960	I/O	83.3 %
MANDOR	Physical Memory	69.4 %
QA1-64BIT	Virtual Memory	64.4 %
QA-3750	I/O	62.4 %
QAMAINCONTROL1	Physical Memory	52.8 %
MANDOR	Virtual Memory	47.9 %
ATL-3560G.ipswitch.com	I/O	43.8 %
QA-2821.ipswitch.com	I/O	43.7 %

Interface Utilization

Device	Interface	Transmit	Receive
CAT500	FastEthernet21	6.8 %	6.7 %
QA-3750	Connection to CAT500	6.7 %	6.8 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.3 %	4.3 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.3 %	4.2 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.3 %	4.2 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.3 %	4.2 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.3 %	4.2 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.2 %	4.2 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.2 %	4.2 %
ATL-CISCO4506.ipswitch.com	GigabitEthernet3/48	4.2 %	4.2 %

Disk Utilization

Device	Disk	Percent Full
QA1-64BIT	F:\	84.6 %
MANDOR	I:\	70.3 %
QAMAINCONTROL1	C:\	59.4 %
QA1-64BIT	C:\	51 %
MANDOR	D:\	50.8 %
MANDOR	C:\	22.4 %
MANDOR	T:\	17.3 %
ATL-JRosenberge.ipswitch...m.ipswitch.com	C:\	11.5 %
ATL-JRosenberge.ipswitch...m.ipswitch.com	D:\	0 %

Threshold - Disk Free Space

Device	Disk	Size	Free space
ATL-JRosenberge.ipswitch...m.ipswitch.com	D:\	931.51 GB	931.39 GB
ATL-JRosenberge.ipswitch...m.ipswitch.com	C:\	464.99 GB	411.74 GB
MANDOR	T:\	195.31 GB	161.62 GB
MANDOR	C:\	195.31 GB	151.62 GB
MANDOR	D:\	195.31 GB	96.15 GB
QA1-64BIT	C:\	99.90 GB	46.92 GB
QA1-64BIT	F:\	200.00 GB	30.60 GB
QAMAINCONTROL1	C:\	74.52 GB	30.26 GB
MANDOR	I:\	97.65 GB	28.97 GB

Interface Discards

Device	Interface	Transmit	Receive	Total
nexus-sw	Ethernet3/3	0	166065	166065
nexus-sw	port-channel1	0	127903	127903
nexus-sw	Ethernet3/2	0	127901	127901
TS-2960	GigabitEthernet1/0/1	31	0	31
ATL-JUNIPER2320	ge-0/0/0	0	20	20

You can add any of the Top 10 reports to the Top 10 dashboard.

Unlike the Home and Device dashboards, the Top 10 dashboard is designed with only the General dashboard view. You can customize the general view in the same way you can other dashboard views by removing the default dashboard reports and/or adding other Top 10 and Threshold dashboard reports.

- Add the reports you want to see here by clicking **Add Content**. For more information, see Adding dashboard reports to a dashboard view.

- Change options for individual reports by clicking **Menu** > **Configure** for each report.
- Add additional views by clicking the plus sign (+). Remove views by dragging them to the trash. For more information, see Working with dashboard views.

The Top 10 dashboard also displays threshold reports. These reports let you set a threshold to filter out items that do not match a specified criteria. For example, the Interface Utilization Threshold report could have been used (in the example above) instead of the Interface Top 10 report, to filter out the interfaces that are not above 50% utilization. Using this approach, only interfaces with significant usage would be shown.

Thresholds

Report percentages are displayed in colors that represent the utilization thresholds:

- **Red**. Above 90%
- **Yellow**. Above 80%
- **Green**. 80% or less

Logs

In This Section

Working with logs

In This Chapter

Learning about Logs

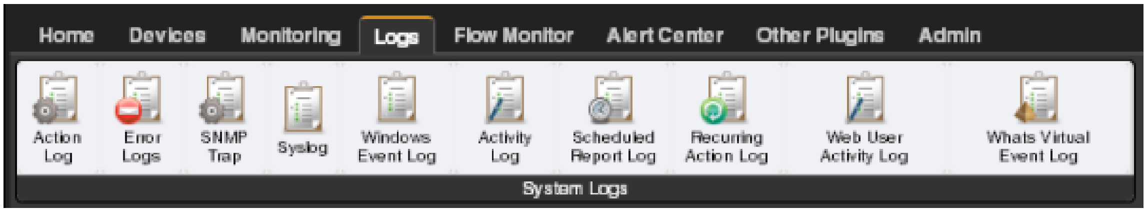
The WhatsUp Gold Logs tab provides device information to help you monitor and troubleshoot device performance and historical data that WhatsUp Gold and WhatsUp Gold plug-in products collect. The logs provide a view of: activity that has occurred on devices and device groups, actions and monitors applied, and summary reports so you have a view of network performance. This information provides insight into network issues and trends so you can tune and troubleshoot WhatsUp Gold server and network performance.

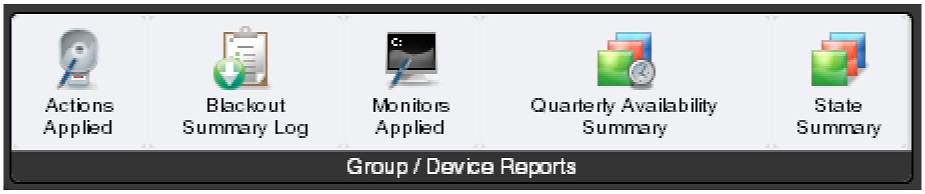
Most of the data in the logs can be exported to a formatted text file, Microsoft Excel, or a PDF. You can also email reports as a PDF, or send on scheduled intervals.

The Logs tab includes the following groups:

§ **System Logs**. Display system-wide information and information about the WhatsUp Gold server. System log reports usually do not focus on a specific device nor a specific device group. For example, the Action Log displays all actions for all network devices.

- **Group/Device Reports**. Group reports display information relating to a specific device group. For example, the Quarterly Availability and the State Summary reports are group reports. Device reports display information relating to a specific device. For example, the Monitors Applied report for a single device is a device report.





Selecting a device to view logs

Many of the logs in the Logs tab are general logs that do not require a specific device selection to view the log. However, some of the logs require that you select a device to view the log. Following are common methods to select a device.

To select a device from the Device tab:

1 Select a device from the **Devices** tab by double-clicking a device in the Details View or Map View. The Device Status appears.

2 Click the **Logs** tab, then select the log you want to view for that device. The log data for the device currently in context displays.

To select a device from the Logs tab:

1 Click the **Logs** tab, then click the log you want to view for the selected device.

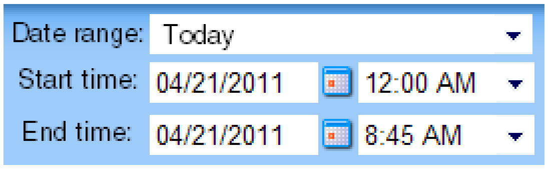
2 Click **View All Entries/Select a Device**. The Select a Device dialog box appears.

3 Select the device for which you want to view a log.

4 Click **OK**. The log data for the selected device displays.

Changing the report or log date range

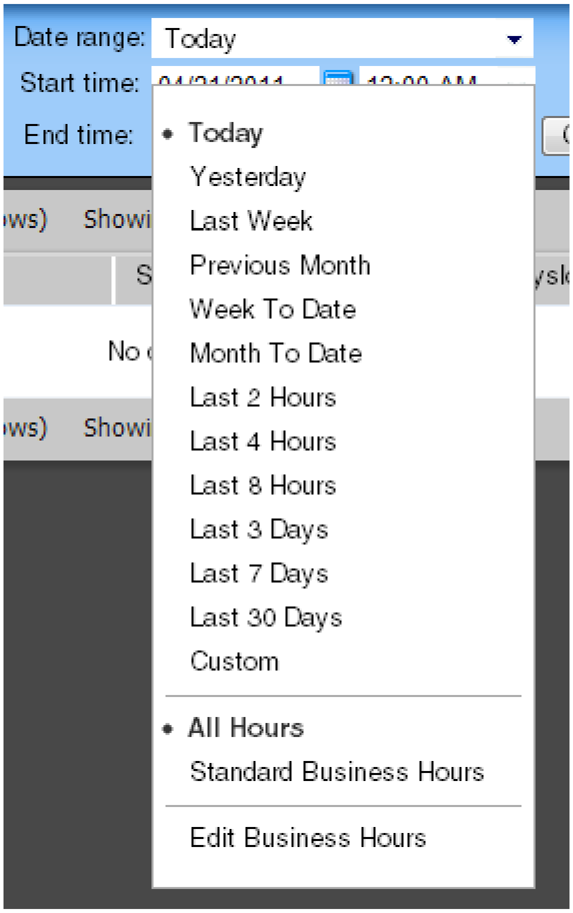
Use the *date/time picker* (on page 358) at the top of a report or log to select a date range and time frame.



Date range: Today
Start time: 04/21/2011 12:00 AM
End time: 04/21/2011 8:45 AM

In the **Date range** list, many group reports also allow you to specify and customize the business hour report times for reports to display. Selecting this option allows you to view the network activity only for specified business hours.

Note: The Business Hours setting is available for group reports only.



Date range: Today

Changing the date range

Use the time and date menus in the control bar to select the time period you want to view the data for. You can select a pre-configured time period from the **Date Range** list, or select **Custom** and enter the start and end time manually. If no data exists for that time period, the following message displays: **No data available for the selected date range**.

To change the date range for a report or log:

- Click the calendar icon next to the date box to select the specific date from the calendar.
- Click the left and right arrows on the calendar to browse through the months.
- In the Date range list, click **Today** to navigate back to the current date. When you click a date, the calendar closes and the box is populated with the selected date.

Note: The date and time format on this report or log matches the format specified in the WhatsUp Gold console (**Configure > Program Options > Regional**).

You can also use the report *zoom tool* (on page 358) to select a date and time for monitor reports.

To control the date/time picker display:

- Hide the control bar by clicking the **Hide** link in the control bar. The selected date/time range displays instead and allows more rows of the report or log to display.
- To redisplay the date/time picker, click anywhere in the control bar summary.

Using paging options

At both the bottom and the top of a report or log table are paging controls that allow you to move through large amounts of data.

Use the **Page** list to select the specific page to view. Next, use the **Showing ___ rows per page** list to specify the number of rows to display in the report. You can choose to display 25, 50, 100, 250, or 500 rows. The default maximum is 50 rows.

The paging buttons allow you to move from page to page, or go to the first or last page:

Click:	To view:
⇤	§ The first page of values
⇦	§ The previous page of values
⇨	§ The next page of values
⇥	§ The last page of values

Navigating between logs

Change the log you are viewing by selecting a different log from the **Logs** tab.

Printing reports and logs

To print a report or log:

1. Open the report you want to print.
2. Right-click anywhere inside the report window, then select **Print**.
   - or -
   Click **File > Print** from the browser menu options.

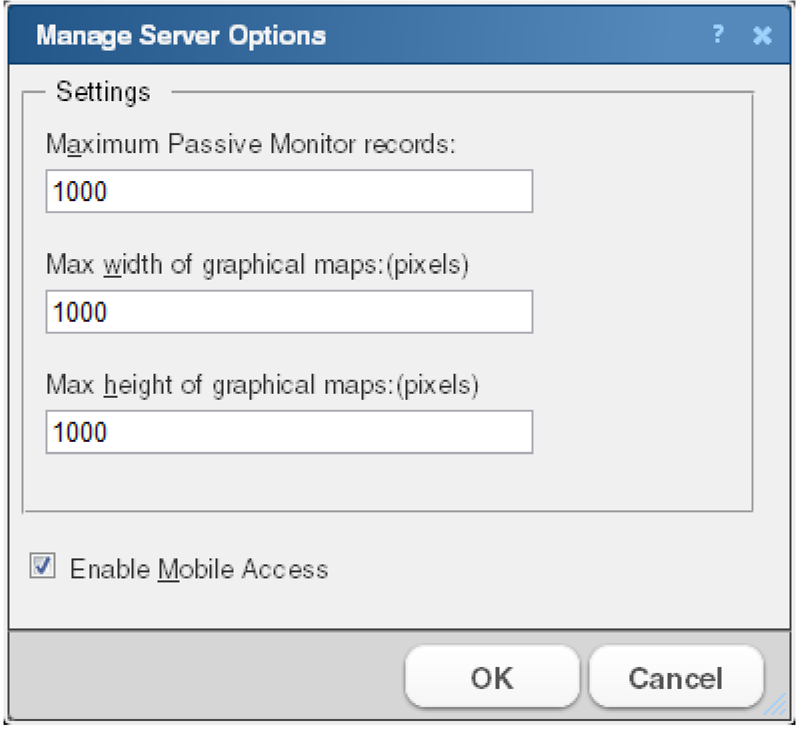
Using the WhatsUp Gold toolbar buttons

Click:	To:
Email	§ Email a report or log as a PDF attachment. § Schedule the report or log to be emailed at regular intervals.
Add Content	§ Add additional dashboard reports to the current dashboard view using the Add Content panel.
Edit View	§ Edit settings for the currently displayed dashboard view.
Properties	§ View and configure dynamic group properties. Note: This button only appears when you are viewing a device group other than the default *All Devices* dynamic group.
Status	§ Display the Device Status of the device currently in context. This icon does not appear when a group is in the current context.
Export	§ Export a report or log: § To a text file § To an Excel file § To a PDF file
Help	§ View help for the current page.

Note: Different sets of icons appear on different types of pages.

Managing server options

1 From the WhatsUp Gold web interface, go to **Admin > Server Options** in the System Administration group. The Manage Server Options dialog appears.



Manage Server Options

Settings

Maximum Passive Monitor records: 1000

Max width of graphical maps:(pixels) 1000

Max height of graphical maps:(pixels) 1000

☑ Enable Mobile Access

2 Enter or select the appropriate information:

- **Maximum Passive Monitor records**. Enter the maximum number of device and system level passive monitor records to collect for full reports. The default value is 1000 max records for WhatsUp Gold v14.2 and later.

Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance.

- **Max width of graphical maps**. Enter the maximum width of maps viewed through the web browser. The size is in pixels and the default is 1000.
- **Max height of graphical maps.** Enter the maximum height of maps viewed through the web browser. The size is in pixels and the default is 1000.
- **Enable Mobile Access**. Select this option to enable WhatsUp Gold Mobile access, which allows you to connect to WhatsUp Gold from a mobile device.

3 Click **OK** to save changes.

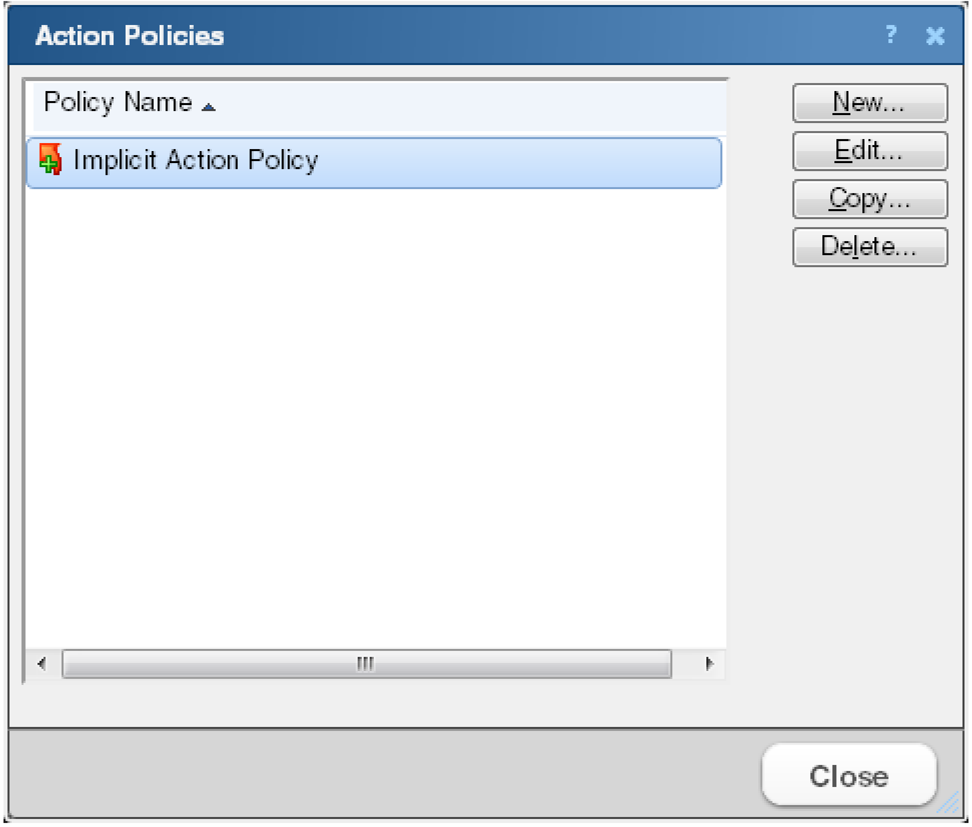
Managing Action Policies

The Action Policy dialog shows the action policies that you can assign to any device or monitor. Use this dialog to create a new action policy, modify or copy an existing policy, or delete a policy.

For more information, see *Using Action Policies* (on page 348).

To create an action policy:

1 From the WhatsUp Gold web interface, go to **Admin > Action Policies**. The Action Policies dialog appears.



2 Click **New** and enter a name for the new policy in the **Policy name** box. Give the policy a descriptive name that helps you remember its function.

3 Click **Add**. The Action Builder wizard appears.

4 Follow the directions in the wizard.

5 Click **Finish** at the end of the wizard to add the action to the policy.

6 Add as many actions as you need to complete the policy. You can move actions up and down in the list by clicking **Up** and **Down** above the action list.

> **Note**: If you select **Only execute first action**, WhatsUp Gold executes the actions in the list for each state, starting at the top, and stops as soon as an action successfully fires.

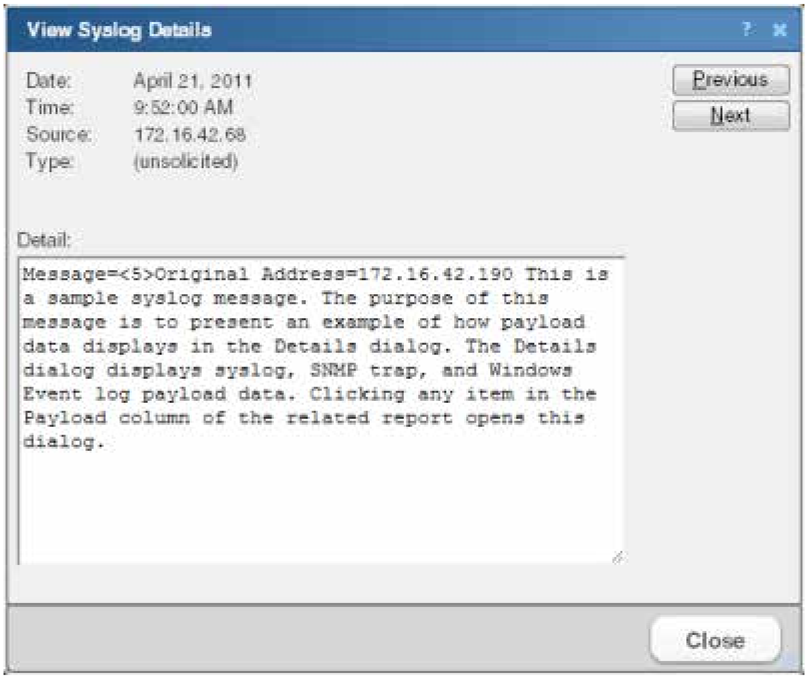
7 After you have added all of the actions you want to use for the policy, click **OK** to create the policy and add it to the active list.

> **Note**: During Device Discovery, you can assign an existing action policy (if one has been created previously), create a simple action policy through a wizard, or access the Action Policy Editor to create an action policy yourself.

Viewing payload details

Click any link in the Payload column of a log to access payload details.

Use this dialog to view the full payload of the entries in the SNMP Trap Log, Syslog, or WinEvent Log.



Date: April 21, 2011
Time: 9:52:00 AM
Source: 172.16.42.68
Type: (unsolicited)

Detail:

```
Message=<5>Original Address=172.16.42.190 This is
a sample syslog message. The purpose of this
message is to present an example of how payload
data displays in the Details dialog. The Details
dialog displays syslog, SNMP trap, and Windows
Event log payload data. Clicking any item in the
Payload column of the related report opens this
dialog.
```

The following information is displayed for the currently viewed payload:

- **Date**. The date the payload reached WhatsUp Gold.
- **Time**. The time the event occurred or the message was received.
- **Source**. The device or monitor that sent the message.
- **Type**. The type of payload.
- **Detail**. The complete details of the message payload.

Use the **Previous** and **Next** buttons to browse through the log payloads in the same column. Click **Close** to exit the dialog and return to viewing the log.

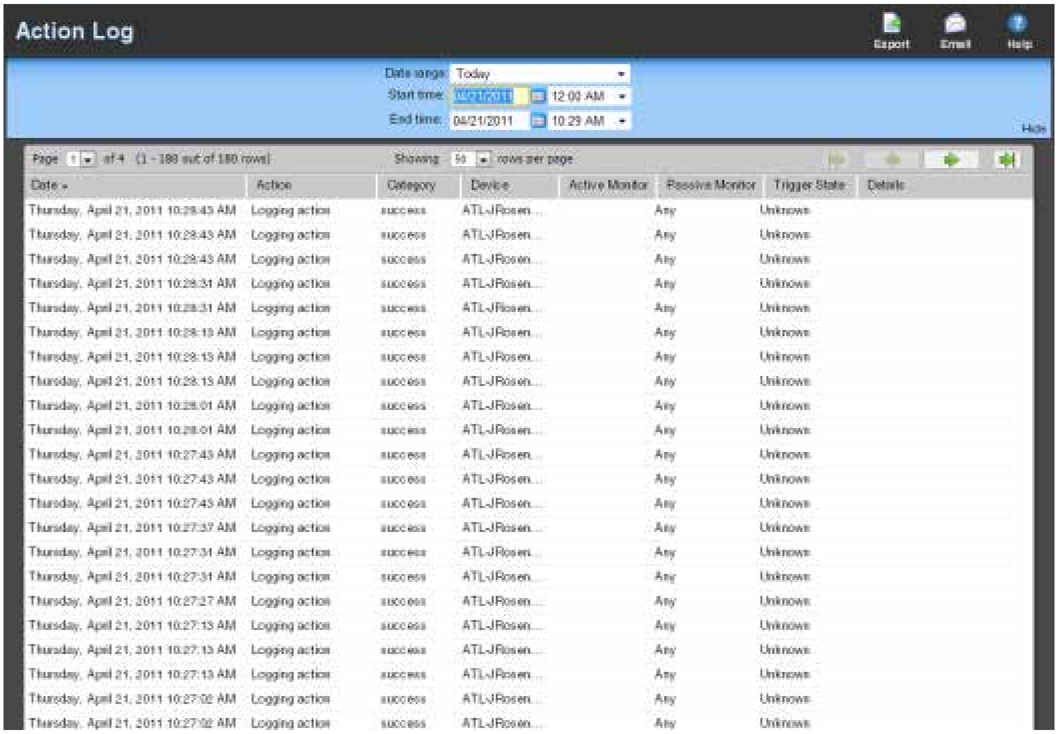
Using WhatsUp Gold System Logs

In This Chapter

The *system logs* display passively collected information on the WhatsUp Gold server or on selected devices. Logs contain information and display the data in the order in which it was received. You can sort log information by clicking the headings of the different log columns.

About the Action Log

The Action Log shows all actions that WhatsUp Gold has attempted to fire, based on the configuration of the action.



Date range: Today
Start time: 04/21/2011 12:00 AM
End time: 04/21/2011 10:29 AM

Page 1 of 4 (1 - 180 out of 180 rows) Showing: 50 rows per page

Date	Action	Category	Device	Active Monitor	Passive Monitor	Trigger State	Details
Thursday, April 21, 2011 10:28:43 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:43 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:43 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:31 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:31 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:13 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:13 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:13 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:01 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:28:01 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:43 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:43 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:43 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:37 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:31 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:31 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:27 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:13 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:13 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:13 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:02 AM	Logging action	success	ATL-JRosen...		Any	Unknown	
Thursday, April 21, 2011 10:27:02 AM	Logging action	success	ATL-JRosen...		Any	Unknown	

Log body

The following information is displayed in the log:

- **Date**. The date the action fired.
- **Action**. The specific action type that was fired. This corresponds to the name of the action in the Actions Library.
- **Category**. Shows the category that the action fits in here in the log. Either success, failure, cancel, retry, or blacked out.
- **Device**. The device that the action is assigned to.
- **Active Monitor**. The Active Monitor to which the action is assigned.
- **Passive Monitor**. The Passive Monitor to which the action is assigned.
- **Trigger State**. The state that caused the action to fire. The trigger state is determined when the Action is configured on the device.
- **Details**. Text that shows the reason for the category that is used in the log.

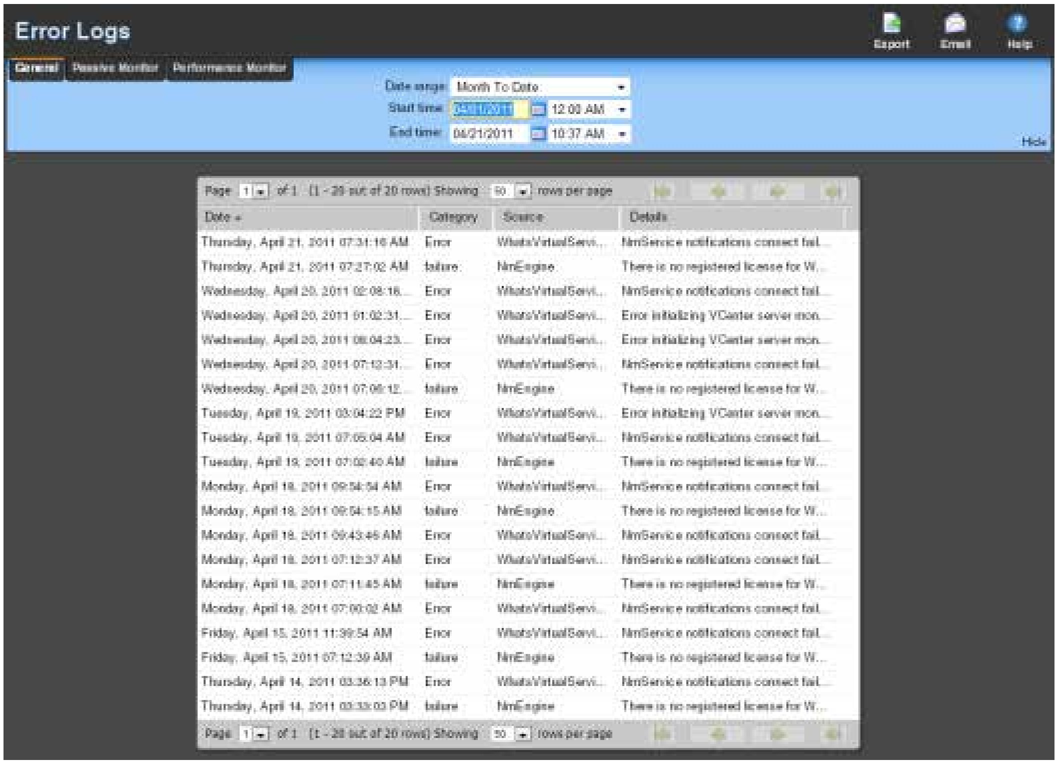
Note: A *skipped due to priority* message displays in the Action Log when an action is NOT executed because the **Only execute first action (for each state)** option is enabled in the Action Policy. For more information, see *Add/Edit Action Policy* (on page 425).

Error Logs

In This Chapter

About the General Error Log

The General Error Log shows a list of error messages generated by WhatsUp Gold for the selected time period.



Date range: Month To Date

Start time: 04/01/2011 12:00 AM

End time: 04/21/2011 10:37 AM

Page 1 of 1 (1 - 20 out of 20 rows) Showing 50 rows per page

Date	Category	Source	Details
Thursday, April 21, 2011 07:31:16 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Thursday, April 21, 2011 07:27:02 AM	failure	NmEngine	There is no registered license for W...
Wednesday, April 20, 2011 02:08:16...	Error	WhatsVirtualServi...	NmService notifications connect fail...
Wednesday, April 20, 2011 01:02:31...	Error	WhatsVirtualServi...	Error initializing VCenter server mon...
Wednesday, April 20, 2011 08:04:23...	Error	WhatsVirtualServi...	Error initializing VCenter server mon...
Wednesday, April 20, 2011 07:12:31...	Error	WhatsVirtualServi...	NmService notifications connect fail...
Wednesday, April 20, 2011 07:08:12...	failure	NmEngine	There is no registered license for W...
Tuesday, April 19, 2011 03:04:22 PM	Error	WhatsVirtualServi...	Error initializing VCenter server mon...
Tuesday, April 19, 2011 07:05:04 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Tuesday, April 19, 2011 07:02:40 AM	failure	NmEngine	There is no registered license for W...
Monday, April 18, 2011 09:54:54 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Monday, April 18, 2011 09:54:15 AM	failure	NmEngine	There is no registered license for W...
Monday, April 18, 2011 09:43:46 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Monday, April 18, 2011 07:12:37 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Monday, April 18, 2011 07:11:45 AM	failure	NmEngine	There is no registered license for W...
Monday, April 18, 2011 07:00:02 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Friday, April 15, 2011 11:39:54 AM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Friday, April 15, 2011 07:12:39 AM	failure	NmEngine	There is no registered license for W...
Thursday, April 14, 2011 03:36:13 PM	Error	WhatsVirtualServi...	NmService notifications connect fail...
Thursday, April 14, 2011 03:33:03 PM	failure	NmEngine	There is no registered license for W...

Page 1 of 1 (1 - 20 out of 20 rows) Showing 50 rows per page

Log body

The following information is displayed in the log:

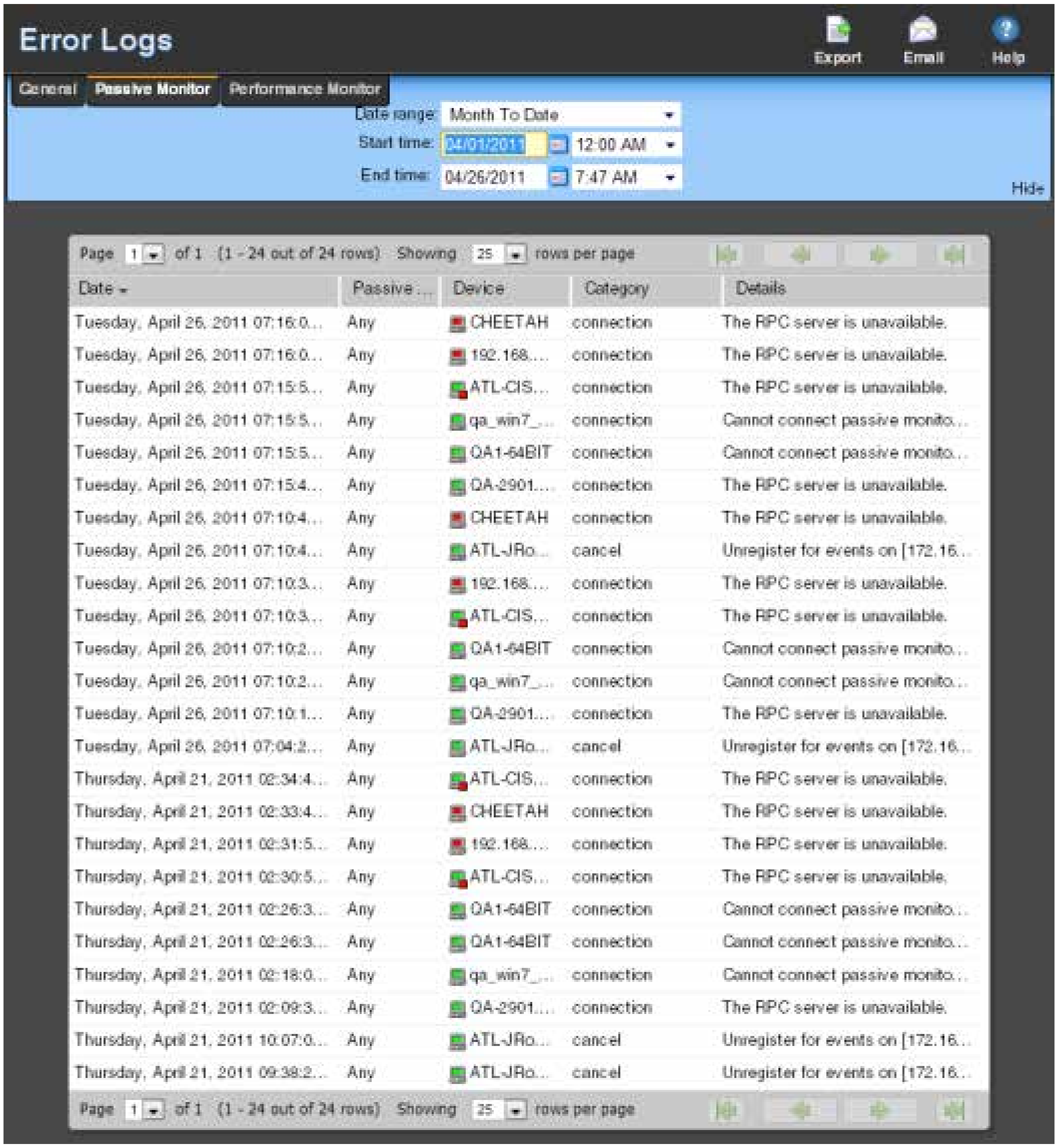
- **Date**. The date the error occurred.
- **Category**. The category of error.
- **Source**. Where the error originated.
- **Details**. The details of the error.

The following is a list of the types of errors that are logged:

- All errors due to SQL statement failure
- Recurring Report load error
- Engine startup errors (Device load error, Group load error)
- Statistics update error
- State update error
- Roll-up activity and failure
- Device or Monitor deletion error
- Exception thrown (check service, process internal event)
- Passive Monitor startup errors

About the Passive Monitor Error Log

The Passive Monitor Error Log shows all passive monitor errors that occurred during the selected time period.



Date range: Month To Date

Start time: 04/01/2011 12:00 AM

End time: 04/26/2011 7:47 AM

Page 1 of 1 (1 - 24 out of 24 rows) Showing 25 rows per page

Date	Passive ...	Device	Category	Details
Tuesday, April 26, 2011 07:16:0...	Any	CHEETAH	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:16:0...	Any	192.168....	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:15:5...	Any	ATL-CIS...	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:15:5...	Any	qa_win7_...	connection	Cannot connect passive monito...
Tuesday, April 26, 2011 07:15:5...	Any	QA1-64BIT	connection	Cannot connect passive monito...
Tuesday, April 26, 2011 07:15:4...	Any	QA-2901....	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:10:4...	Any	CHEETAH	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:10:4...	Any	ATL-JRo...	cancel	Unregister for events on [172.16...
Tuesday, April 26, 2011 07:10:3...	Any	192.168....	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:10:3...	Any	ATL-CIS...	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:10:2...	Any	QA1-64BIT	connection	Cannot connect passive monito...
Tuesday, April 26, 2011 07:10:2...	Any	qa_win7_...	connection	Cannot connect passive monito...
Tuesday, April 26, 2011 07:10:1...	Any	QA-2901....	connection	The RPC server is unavailable.
Tuesday, April 26, 2011 07:04:2...	Any	ATL-JRo...	cancel	Unregister for events on [172.16...
Thursday, April 21, 2011 02:34:4...	Any	ATL-CIS...	connection	The RPC server is unavailable.
Thursday, April 21, 2011 02:33:4...	Any	CHEETAH	connection	The RPC server is unavailable.
Thursday, April 21, 2011 02:31:5...	Any	192.168....	connection	The RPC server is unavailable.
Thursday, April 21, 2011 02:30:5...	Any	ATL-CIS...	connection	The RPC server is unavailable.
Thursday, April 21, 2011 02:26:3...	Any	QA1-64BIT	connection	Cannot connect passive monito...
Thursday, April 21, 2011 02:26:3...	Any	QA1-64BIT	connection	Cannot connect passive monito...
Thursday, April 21, 2011 02:18:0...	Any	qa_win7_...	connection	Cannot connect passive monito...
Thursday, April 21, 2011 02:09:3...	Any	QA-2901....	connection	The RPC server is unavailable.
Thursday, April 21, 2011 10:07:0...	Any	ATL-JRo...	cancel	Unregister for events on [172.16...
Thursday, April 21, 2011 09:38:2...	Any	ATL-JRo...	cancel	Unregister for events on [172.16...

Page 1 of 1 (1 - 24 out of 24 rows) Showing 25 rows per page

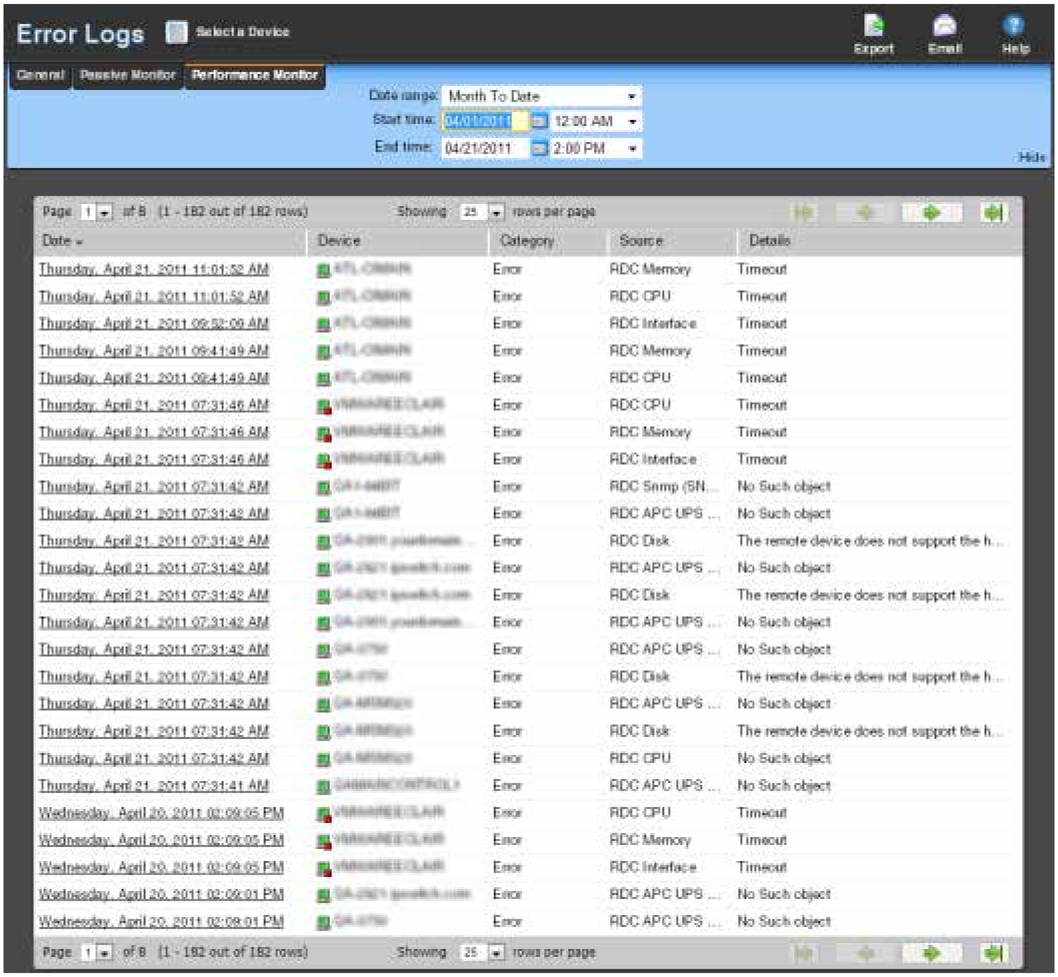
Log Body

The following information is displayed in the log:

- **Date**. The date of the error.
- **Passive Monitor**. The name of the passive monitor that received the error.
- **Device**. The host name of the device that the Passive Monitor is assigned to.
- **Category**. The category code of the error: Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error).
- **Details**. Text that describes the error.

About the Performance Monitor Error Log

The Performance Monitor Error Log shows all performance monitor errors that occur during the selected time period.



Date range: Month To Date
Start time: 04/01/2011 12:00 AM
End time: 04/21/2011 2:00 PM

Page 1 of 8 (1 - 182 out of 182 rows) Showing 25 rows per page

Date	Device	Category	Source	Details
Thursday, April 21, 2011 11:01:52 AM	[redacted]	Error	RDC Memory	Timeout
Thursday, April 21, 2011 11:01:52 AM	[redacted]	Error	RDC CPU	Timeout
Thursday, April 21, 2011 09:52:09 AM	[redacted]	Error	RDC Interface	Timeout
Thursday, April 21, 2011 09:41:49 AM	[redacted]	Error	RDC Memory	Timeout
Thursday, April 21, 2011 09:41:49 AM	[redacted]	Error	RDC CPU	Timeout
Thursday, April 21, 2011 07:31:46 AM	[redacted]	Error	RDC CPU	Timeout
Thursday, April 21, 2011 07:31:46 AM	[redacted]	Error	RDC Memory	Timeout
Thursday, April 21, 2011 07:31:46 AM	[redacted]	Error	RDC Interface	Timeout
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC Snmp (SN...	No Such object
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC APC UPS ...	No Such object
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC Disk	The remote device does not support the h...
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC APC UPS ...	No Such object
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC Disk	The remote device does not support the h...
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC APC UPS ...	No Such object
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC APC UPS ...	No Such object
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC Disk	The remote device does not support the h...
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC APC UPS ...	No Such object
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC Disk	The remote device does not support the h...
Thursday, April 21, 2011 07:31:42 AM	[redacted]	Error	RDC CPU	No Such object
Thursday, April 21, 2011 07:31:41 AM	[redacted]	Error	RDC APC UPS ...	No Such object
Wednesday, April 20, 2011 02:09:05 PM	[redacted]	Error	RDC CPU	Timeout
Wednesday, April 20, 2011 02:09:05 PM	[redacted]	Error	RDC Memory	Timeout
Wednesday, April 20, 2011 02:09:05 PM	[redacted]	Error	RDC Interface	Timeout
Wednesday, April 20, 2011 02:09:01 PM	[redacted]	Error	RDC APC UPS ...	No Such object
Wednesday, April 20, 2011 02:09:01 PM	[redacted]	Error	RDC APC UPS ...	No Such object

Page 1 of 8 (1 - 182 out of 182 rows) Showing 25 rows per page

Log body

The following information is displayed in the log:

- **Date**. The date of the error.
- **Device**. The host name of the device that the Performance Monitor is assigned to.
- **Category**. The category of the error.
- **Source**. Where the error came from (such as Ping, CPU, Memory,Disk, Interface, and Custom Performance Monitors).
- **Details**. Description of the error that was received.

About the Logger Error Log

The Logger Error Log displays a list of error messages generated by the remote poller for the selected time period.

To access the Logger Error Log in the WhatsUp Gold web interface, go to **Logs > Error Logs > Logger**.

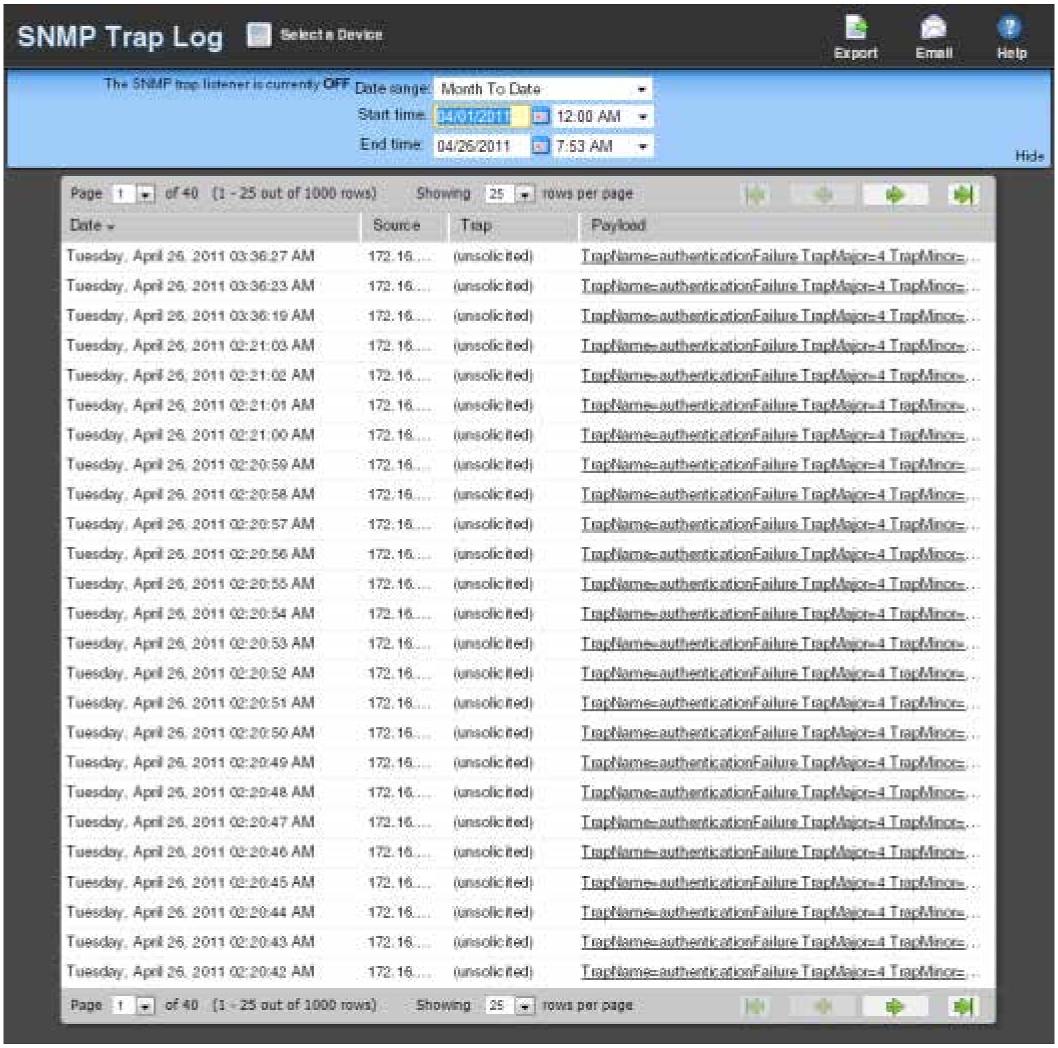
Log body

The following information is displayed in the log:

- **Date**. When the event occurred.
- **Assembly**. The process name that owns the log message. This is an `.exe` file.
- **Sub Assembly**. This is the generator of the log message. This can be an `.exe` or `.dll` file.
- **Severity**. The severity of the message. Values are:
- Error - Used for all errors and exceptions that occur.
- Information - Used to indicate that a process is starting or stopping.
- **Message**. The data that is used to indicate what has occurred.

About the SNMP Trap Log

The SNMP Trap Log provides a history of SNMP traps that have occurred for all devices in the selected group during a time period. If the SNMP Trap Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.



The SNMP trap listener is currently OFF

Date range: Month To Date

Start time: 04/01/2011 12:00 AM

End time: 04/26/2011 7:53 AM

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

Date	Source	Trap	Payload
Tuesday, April 26, 2011 03:36:27 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 03:36:23 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 03:36:19 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:21:03 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:21:02 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:21:01 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:21:00 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:59 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:58 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:57 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:56 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:55 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:54 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:53 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:52 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:51 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:50 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:49 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:48 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:47 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:46 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:45 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:44 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:43 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...
Tuesday, April 26, 2011 02:20:42 AM	172.16....	(unsolicited)	TrapName=authenticationFailure TrapMajor=4 TrapMinor=...

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

- To add an SNMP monitor for a specific device, select the device from the Devices list and select **Properties > Passive Monitors > SNMP Trap**.
- To accept SNMP messages from any device, access the console and select **Program Options > Passive Monitor Listeners > SNMP Trap**. Click **Configure** and select **Accept unsolicited SNMP traps**.

Note: In order for entries to be added to this log, the SNMP Trap Listener must be enabled. For more information, see Enabling the SNMP Trap Listener. Additionally, if the trap receiving port is not on the list of firewall exceptions, traps may not be receivable and as a result will not be added to the SNMP Trap Log. Please ensure that the trap receiving port is on the firewall exceptions list.

Tip: If you experience page load delays for device or system passive monitor logs (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records displaying for the selected time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report and log display performance. For more information, see *Managing server options* (on page 425).

This log includes the time the message was received as well as its source, the trap that triggered it, and its payload.

Log body

The following information is displayed in the log:

- **Date**. The date the trap occurred.
- **Source**. The device or program that originated the trap.
- **Trap**. The type of trap received.
- **Payload**. The vital data (such as trap name, the IP address from which the trap came, date of the trap, etc.) that passed within a packet or other transmission unit.

Tip: Move your mouse over the payload entry to view more of the payload information.

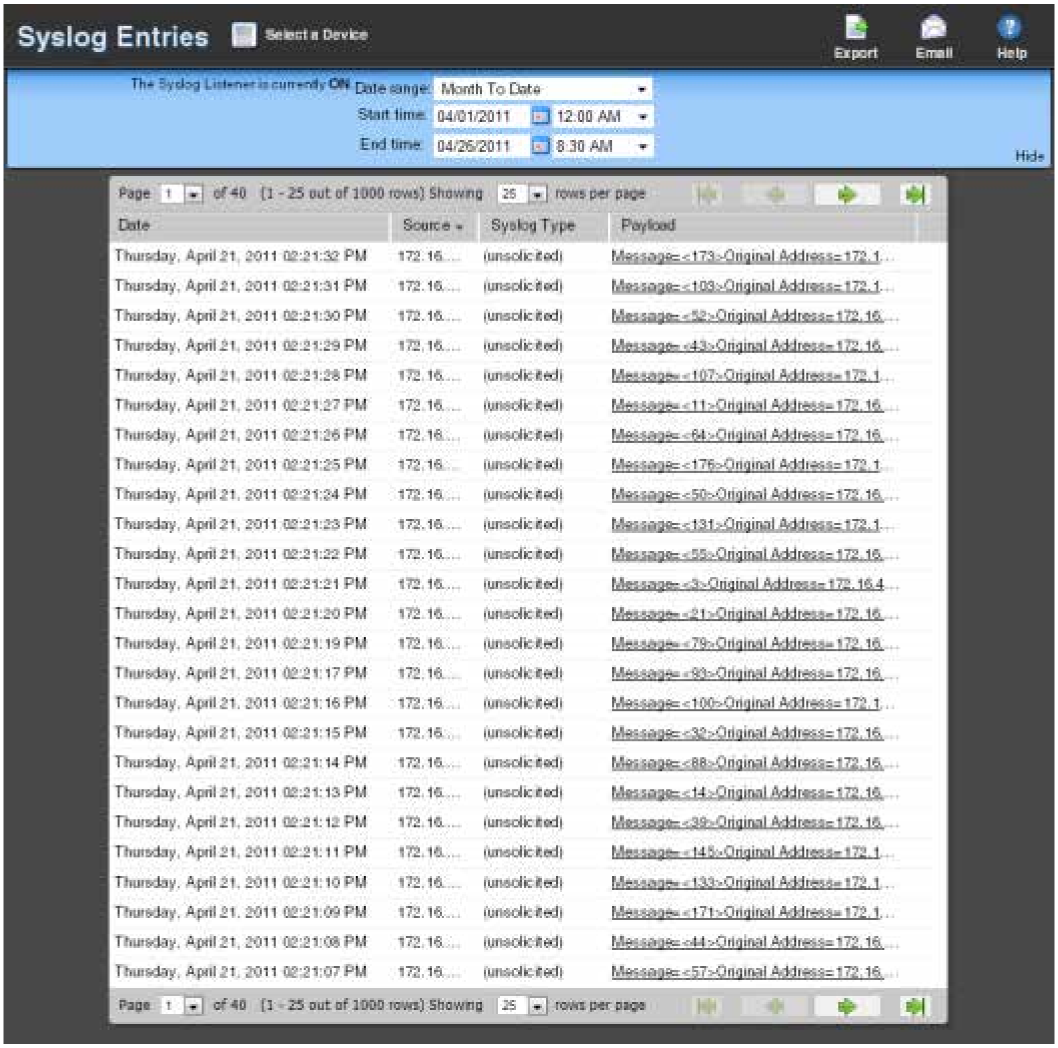
Note: The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to *view the payload details* (on page 427).

Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the log. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

About the Syslog Events Log

This log shows Syslog events recorded for selected devices on the network during the time period displayed at the top of the log. WhatsUp Gold can accept Syslog messages from specific devices or from all devices, depending on the selected options.

A Syslog event is used to examine Syslog messages forwarded from other devices for a specific record and/or specific text within a record. Usually Syslog messages are forwarded from the "Syslog" on a system that runs UNIX, but they can also come from non-UNIX devices as well. They might contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.



The Syslog Listener is currently ON

Date range: Month To Date

Start time: 04/01/2011 12:00 AM

End time: 04/26/2011 8:30 AM

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

Date	Source	Syslog Type	Payload
Thursday, April 21, 2011 02:21:32 PM	172.16....	(unsolicited)	Message=<173>Original Address=172.1...
Thursday, April 21, 2011 02:21:31 PM	172.16....	(unsolicited)	Message=<103>Original Address=172.1...
Thursday, April 21, 2011 02:21:30 PM	172.16....	(unsolicited)	Message=<52>Original Address=172.16....
Thursday, April 21, 2011 02:21:29 PM	172.16....	(unsolicited)	Message=<43>Original Address=172.16....
Thursday, April 21, 2011 02:21:28 PM	172.16....	(unsolicited)	Message=<107>Original Address=172.1...
Thursday, April 21, 2011 02:21:27 PM	172.16....	(unsolicited)	Message=<11>Original Address=172.16....
Thursday, April 21, 2011 02:21:26 PM	172.16....	(unsolicited)	Message=<64>Original Address=172.16....
Thursday, April 21, 2011 02:21:25 PM	172.16....	(unsolicited)	Message=<176>Original Address=172.1...
Thursday, April 21, 2011 02:21:24 PM	172.16....	(unsolicited)	Message=<50>Original Address=172.16....
Thursday, April 21, 2011 02:21:23 PM	172.16....	(unsolicited)	Message=<131>Original Address=172.1...
Thursday, April 21, 2011 02:21:22 PM	172.16....	(unsolicited)	Message=<55>Original Address=172.16....
Thursday, April 21, 2011 02:21:21 PM	172.16....	(unsolicited)	Message=<3>Original Address=172.16.4...
Thursday, April 21, 2011 02:21:20 PM	172.16....	(unsolicited)	Message=<21>Original Address=172.16....
Thursday, April 21, 2011 02:21:19 PM	172.16....	(unsolicited)	Message=<79>Original Address=172.16....
Thursday, April 21, 2011 02:21:17 PM	172.16....	(unsolicited)	Message=<93>Original Address=172.16....
Thursday, April 21, 2011 02:21:16 PM	172.16....	(unsolicited)	Message=<100>Original Address=172.1...
Thursday, April 21, 2011 02:21:15 PM	172.16....	(unsolicited)	Message=<32>Original Address=172.16....
Thursday, April 21, 2011 02:21:14 PM	172.16....	(unsolicited)	Message=<88>Original Address=172.16....
Thursday, April 21, 2011 02:21:13 PM	172.16....	(unsolicited)	Message=<14>Original Address=172.16....
Thursday, April 21, 2011 02:21:12 PM	172.16....	(unsolicited)	Message=<39>Original Address=172.16....
Thursday, April 21, 2011 02:21:11 PM	172.16....	(unsolicited)	Message=<145>Original Address=172.1...
Thursday, April 21, 2011 02:21:10 PM	172.16....	(unsolicited)	Message=<133>Original Address=172.1...
Thursday, April 21, 2011 02:21:09 PM	172.16....	(unsolicited)	Message=<171>Original Address=172.1...
Thursday, April 21, 2011 02:21:08 PM	172.16....	(unsolicited)	Message=<44>Original Address=172.16....
Thursday, April 21, 2011 02:21:07 PM	172.16....	(unsolicited)	Message=<57>Original Address=172.16....

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

If the Syslog Listener is configured to listen for messages, any messages received are recorded in WhatsUp Gold Syslog.

- To add a Syslog monitor for a specific device, select the device from the Devices list and select **Properties > Passive Monitors > Syslog**.
- To accept Syslog messages from any device, access the console and select **Program Options > Passive Monitor Listeners > Syslog**. Click **Configure** and select **Accept unsolicited passive monitors**.

Note: In order for this log to receive syslog messages, the Syslog Listener must be enabled. For more information, see Enabling the Syslog Listener. Additionally, if the receiving port is not on the list of firewall exceptions, messages may not be receivable and as a result will not be added to Syslog. Please ensure that the syslog receiving port is on the firewall's list of exceptions.

Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance. For more information, see *Managing server options* (on page 425).

This report includes the time the message was received, the syslog type, and its payload.

Report body

The following information is displayed in the log:

- **Date**. The date the message was received.
- **Source**. The device where the message originated.
- **Syslog Type**. The type of syslog message received.
- **Payload**. The information contained in the syslog message.

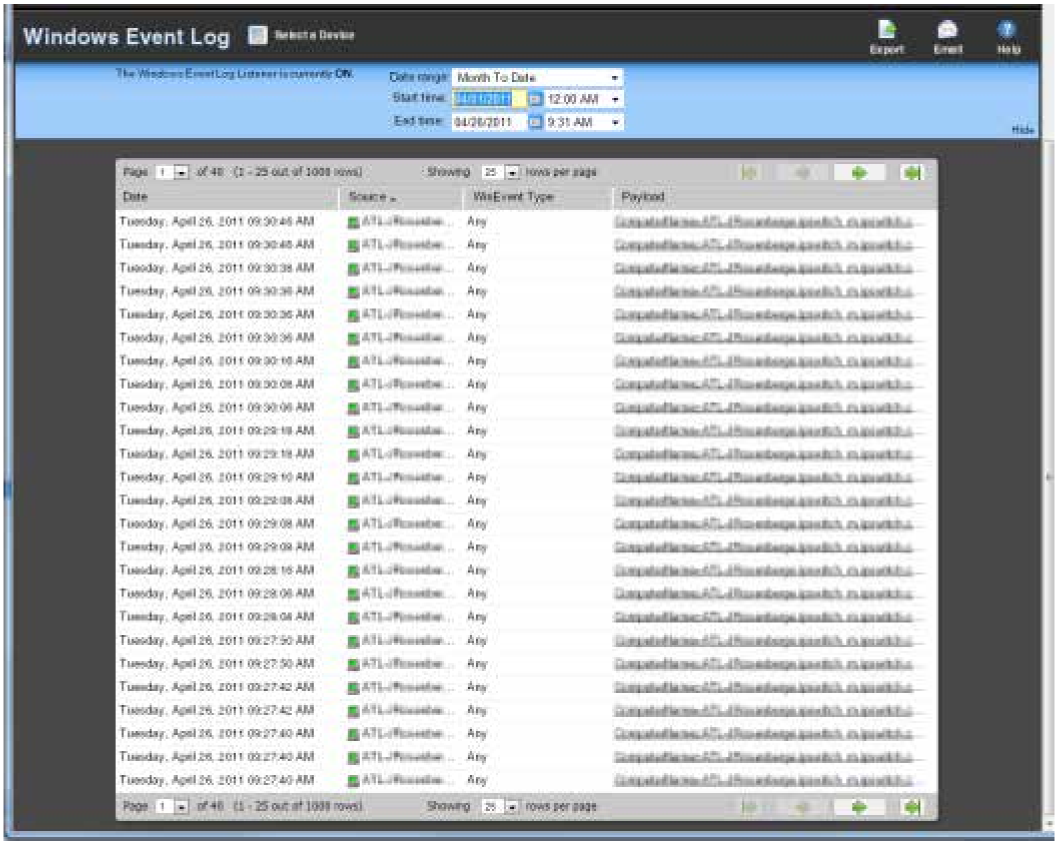
Tip: Move your mouse over the entry to see more of the payload.

Note: The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to *view the payload details* (on page 427).

Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

About the Windows Event Log

This report shows Windows events logged for the selected device during the time period displayed at the bottom of the report.



The Windows EventLog Listener is currently ON.

Date range: Month To Date
Start time: 04/01/2011 12:00 AM
End time: 04/26/2011 9:31 AM

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

Date	Source	WinEvent Type	Payload
Tuesday, April 26, 2011 09:30:46 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:46 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:38 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:36 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:36 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:36 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:16 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:08 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:30:06 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:29:18 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:29:18 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:29:10 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:29:08 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:29:08 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:29:08 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:28:16 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:28:06 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:28:04 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:50 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:50 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:42 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:42 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:40 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:40 AM	ATL-[illegible]	Any	[illegible]
Tuesday, April 26, 2011 09:27:40 AM	ATL-[illegible]	Any	[illegible]

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

§ To add a Windows Event Log monitor for a specific device, select the device from the Devices list and select **Properties > Passive Monitors > Windows Event Log**.

Note: In order for entries to be added to this report, the Windows Event Log listener must be enabled and a Windows Event passive monitor must be added to the device. For more information on the Windows Event Log listener, see Enabling the Windows Event Log Listener.

Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance.

Note: WhatsUp Gold v14.1 and prior used a default value of 10,000 max records; WhatsUp Gold v14.2 and later use a default value of 1,000 max records. For more information, see *Managing server options* (on page 425).

A Windows log event is a Windows Event Viewer entry monitored by WhatsUp Gold. This could be monitoring when a service is started or stopped, if there was a logon failure, or any other entry in the Windows Event Viewer.

Log report body

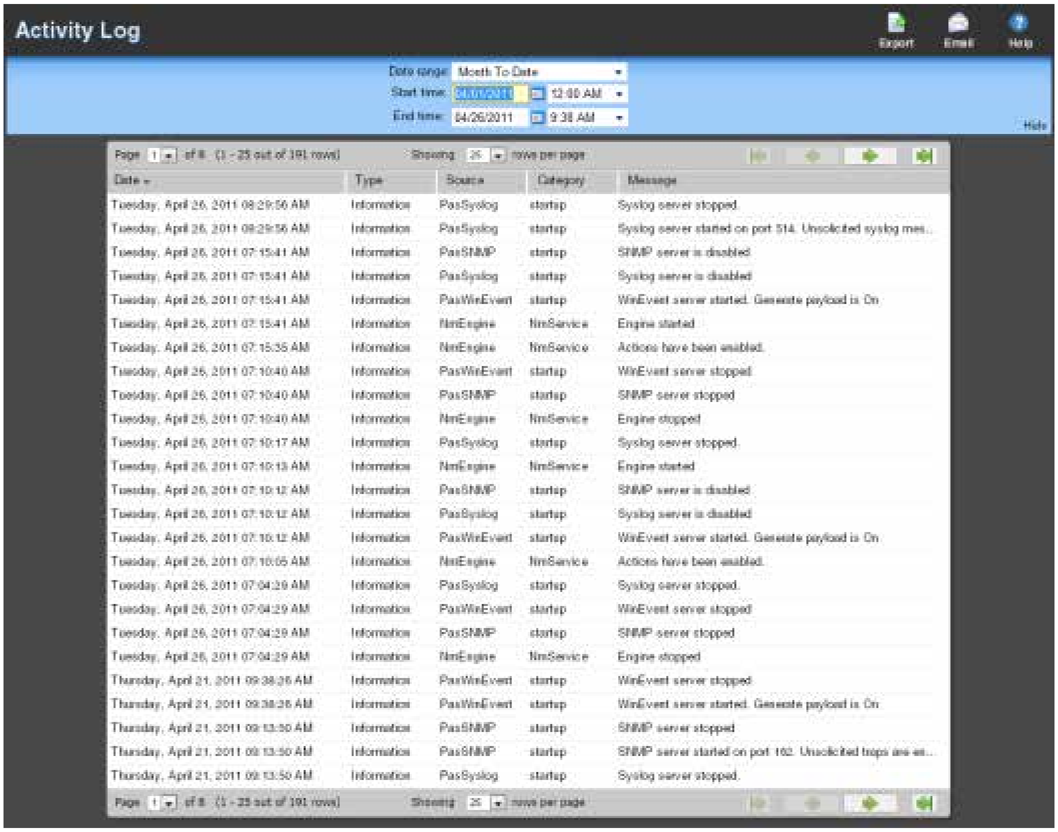
The following information is displayed in the log:

- **Date**. The time event was received by WhatsUp Gold.
- **WinEvent Type**. The type of message received.
- **Payload**. The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed within a packet or other transmission unit. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to *view the payload details* (on page 427).

Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

About the Activity Log

This report is a history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the time period selected at the top of the report. All messages found in this Log are also written to the Windows Event log.



Date range: Month To Date
Start time: 04/01/2011 12:00 AM
End time: 04/26/2011 9:38 AM

Page 1 of 8 (1 - 25 out of 191 rows) Showing 25 rows per page

Date	Type	Source	Category	Message
Tuesday, April 26, 2011 08:29:56 AM	Information	PasSyslog	startup	Syslog server stopped.
Tuesday, April 26, 2011 08:29:56 AM	Information	PasSyslog	startup	Syslog server started on port 514. Unsolicited syslog mes...
Tuesday, April 26, 2011 07:15:41 AM	Information	PasSNMP	startup	SNMP server is disabled
Tuesday, April 26, 2011 07:15:41 AM	Information	PasSyslog	startup	Syslog server is disabled
Tuesday, April 26, 2011 07:15:41 AM	Information	PasWinEvent	startup	WinEvent server started. Generate payload is On
Tuesday, April 26, 2011 07:15:41 AM	Information	NmEngine	NmService	Engine started
Tuesday, April 26, 2011 07:15:35 AM	Information	NmEngine	NmService	Actions have been enabled.
Tuesday, April 26, 2011 07:10:40 AM	Information	PasWinEvent	startup	WinEvent server stopped
Tuesday, April 26, 2011 07:10:40 AM	Information	PasSNMP	startup	SNMP server stopped
Tuesday, April 26, 2011 07:10:40 AM	Information	NmEngine	NmService	Engine stopped
Tuesday, April 26, 2011 07:10:17 AM	Information	PasSyslog	startup	Syslog server stopped.
Tuesday, April 26, 2011 07:10:13 AM	Information	NmEngine	NmService	Engine started
Tuesday, April 26, 2011 07:10:12 AM	Information	PasSNMP	startup	SNMP server is disabled
Tuesday, April 26, 2011 07:10:12 AM	Information	PasSyslog	startup	Syslog server is disabled
Tuesday, April 26, 2011 07:10:12 AM	Information	PasWinEvent	startup	WinEvent server started. Generate payload is On
Tuesday, April 26, 2011 07:10:05 AM	Information	NmEngine	NmService	Actions have been enabled.
Tuesday, April 26, 2011 07:04:29 AM	Information	PasSyslog	startup	Syslog server stopped.
Tuesday, April 26, 2011 07:04:29 AM	Information	PasWinEvent	startup	WinEvent server stopped
Tuesday, April 26, 2011 07:04:29 AM	Information	PasSNMP	startup	SNMP server stopped
Tuesday, April 26, 2011 07:04:29 AM	Information	NmEngine	NmService	Engine stopped
Thursday, April 21, 2011 09:38:26 AM	Information	PasWinEvent	startup	WinEvent server stopped
Thursday, April 21, 2011 09:38:26 AM	Information	PasWinEvent	startup	WinEvent server started. Generate payload is On
Thursday, April 21, 2011 09:13:50 AM	Information	PasSNMP	startup	SNMP server stopped
Thursday, April 21, 2011 09:13:50 AM	Information	PasSNMP	startup	SNMP server started on port 162. Unsolicited traps are en...
Thursday, April 21, 2011 09:13:50 AM	Information	PasSyslog	startup	Syslog server stopped.

Page 1 of 8 (1 - 25 out of 191 rows) Showing 25 rows per page

Each entry shows the type of activity logged as well as the date, source, category and actual message of the activity.

- Click the link above the **Type** column to group the entries by message severity (Information, Warning, or Error).

Log Body

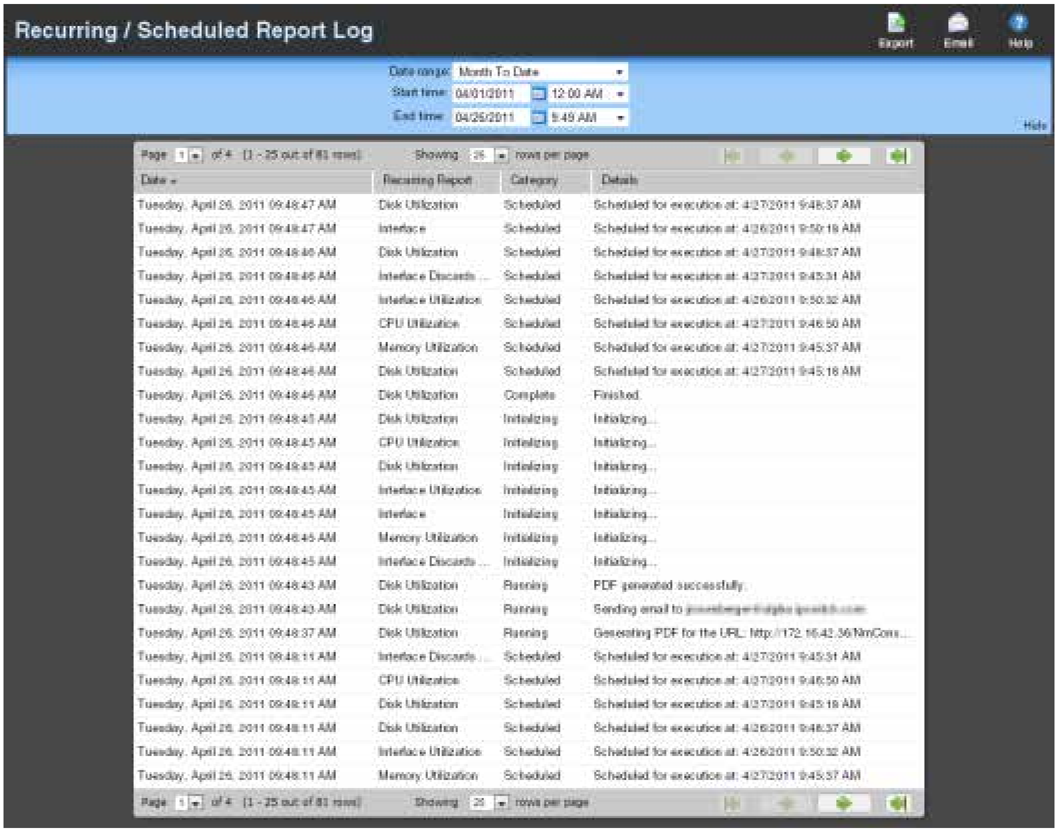
The following information is displayed in the log:

- **Date**. The date the activity took place.
- **Type**. The type of activity, for example *Information*.
- **Source**. Where the activity originated, for example, *NmEngine*.
- **Category**. The category of the activity, for example, *startup*.
- **Message**. The activity message, for example, *Engine started*.

Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

About the Scheduled Report Log

This log shows a log of all recurring and scheduled reports that have occurred during the selected time period.



Date range: Month To Date
Start time: 04/01/2011 12:00 AM
End time: 04/26/2011 5:49 AM

Page 1 of 4 (1 - 25 out of 81 rows) Showing 25 rows per page

Date	Recurring Report	Category	Details
Tuesday, April 26, 2011 09:48:47 AM	Disk Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:48:37 AM
Tuesday, April 26, 2011 09:48:47 AM	Interface	Scheduled	Scheduled for execution at: 4/26/2011 9:50:18 AM
Tuesday, April 26, 2011 09:48:46 AM	Disk Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:48:37 AM
Tuesday, April 26, 2011 09:48:46 AM	Interface Discards ...	Scheduled	Scheduled for execution at: 4/27/2011 9:45:31 AM
Tuesday, April 26, 2011 09:48:46 AM	Interface Utilization	Scheduled	Scheduled for execution at: 4/26/2011 9:50:32 AM
Tuesday, April 26, 2011 09:48:46 AM	CPU Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:46:50 AM
Tuesday, April 26, 2011 09:48:46 AM	Memory Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:45:37 AM
Tuesday, April 26, 2011 09:48:46 AM	Disk Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:45:18 AM
Tuesday, April 26, 2011 09:48:46 AM	Disk Utilization	Complete	Finished.
Tuesday, April 26, 2011 09:48:45 AM	Disk Utilization	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:45 AM	CPU Utilization	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:45 AM	Disk Utilization	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:45 AM	Interface Utilization	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:45 AM	Interface	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:45 AM	Memory Utilization	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:45 AM	Interface Discards ...	Initializing	Initializing...
Tuesday, April 26, 2011 09:48:43 AM	Disk Utilization	Running	PDF generated successfully.
Tuesday, April 26, 2011 09:48:43 AM	Disk Utilization	Running	Sending email to [redacted]
Tuesday, April 26, 2011 09:48:37 AM	Disk Utilization	Running	Generating PDF for the URL: http://172.16.42.36/NmCons...
Tuesday, April 26, 2011 09:48:11 AM	Interface Discards ...	Scheduled	Scheduled for execution at: 4/27/2011 9:45:31 AM
Tuesday, April 26, 2011 09:48:11 AM	CPU Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:46:50 AM
Tuesday, April 26, 2011 09:48:11 AM	Disk Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:45:18 AM
Tuesday, April 26, 2011 09:48:11 AM	Disk Utilization	Scheduled	Scheduled for execution at: 4/26/2011 9:48:37 AM
Tuesday, April 26, 2011 09:48:11 AM	Interface Utilization	Scheduled	Scheduled for execution at: 4/26/2011 9:50:32 AM
Tuesday, April 26, 2011 09:48:11 AM	Memory Utilization	Scheduled	Scheduled for execution at: 4/27/2011 9:45:37 AM

Page 1 of 4 (1 - 25 out of 81 rows) Showing 25 rows per page

Log body

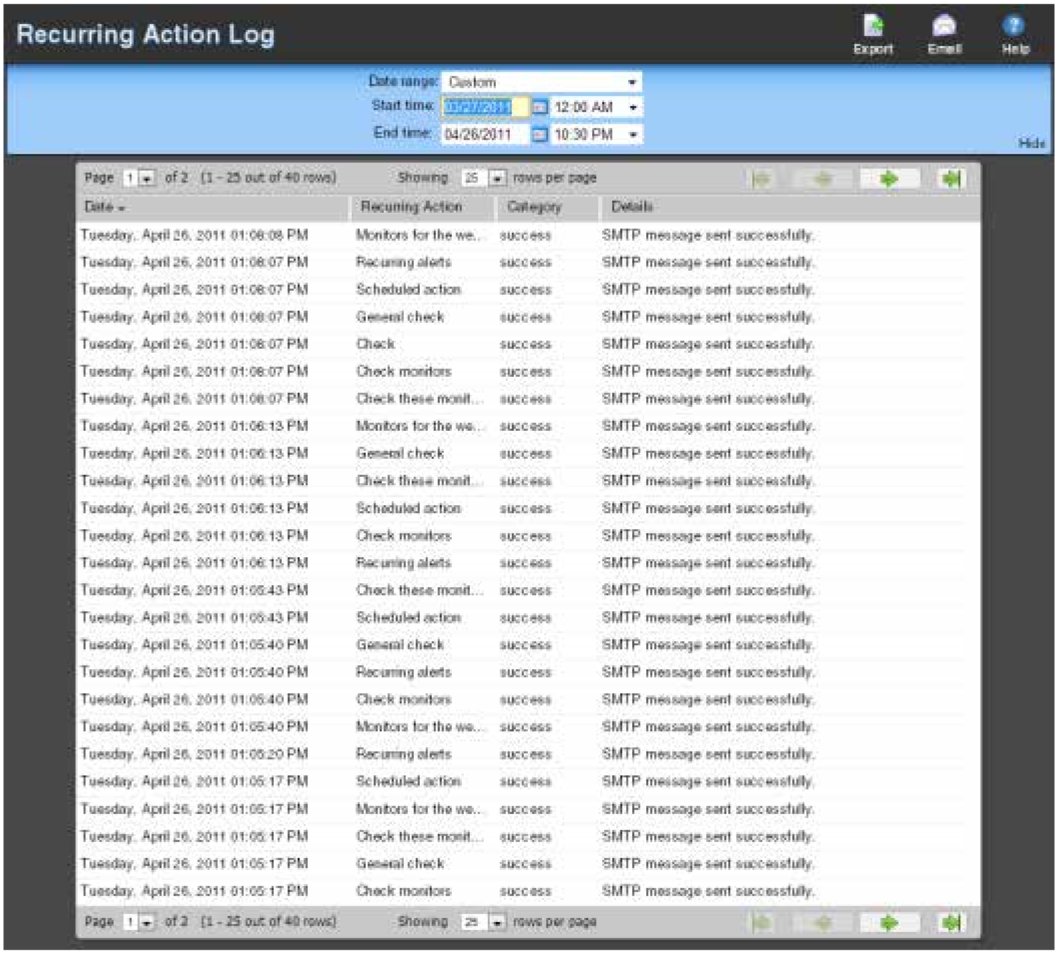
The following information is displayed in the log:

- **Date**. The date that the report was run.
- **Recurring Report**. The name of the recurring report as is appears on the Recurring Report dialog.
- **Category**. The result of the report attempt: *Success*, *Failure*, *Disabled*.
- **Details**. Describes the results of the report.

> **Note**: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

About the Recurring Action Log

This log shows a log of recurring actions that were scheduled to fire.



Date range: Custom
Start time: 03/27/2011 12:00 AM
End time: 04/26/2011 10:30 PM

Page 1 of 2 (1 - 25 out of 40 rows) Showing 25 rows per page

Date	Recurring Action	Category	Details
Tuesday, April 26, 2011 01:08:08 PM	Monitors for the we...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:08:07 PM	Recurring alerts	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:08:07 PM	Scheduled action	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:08:07 PM	General check	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:08:07 PM	Check	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:08:07 PM	Check monitors	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:08:07 PM	Check these monit...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:06:13 PM	Monitors for the we...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:06:13 PM	General check	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:06:13 PM	Check these monit...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:06:13 PM	Scheduled action	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:06:13 PM	Check monitors	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:06:13 PM	Recurring alerts	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:43 PM	Check these monit...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:43 PM	Scheduled action	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:40 PM	General check	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:40 PM	Recurring alerts	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:40 PM	Check monitors	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:40 PM	Monitors for the we...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:20 PM	Recurring alerts	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:17 PM	Scheduled action	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:17 PM	Monitors for the we...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:17 PM	Check these monit...	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:17 PM	General check	success	SMTP message sent successfully.
Tuesday, April 26, 2011 01:05:17 PM	Check monitors	success	SMTP message sent successfully.

Page 1 of 2 (1 - 25 out of 40 rows) Showing 25 rows per page

Log body

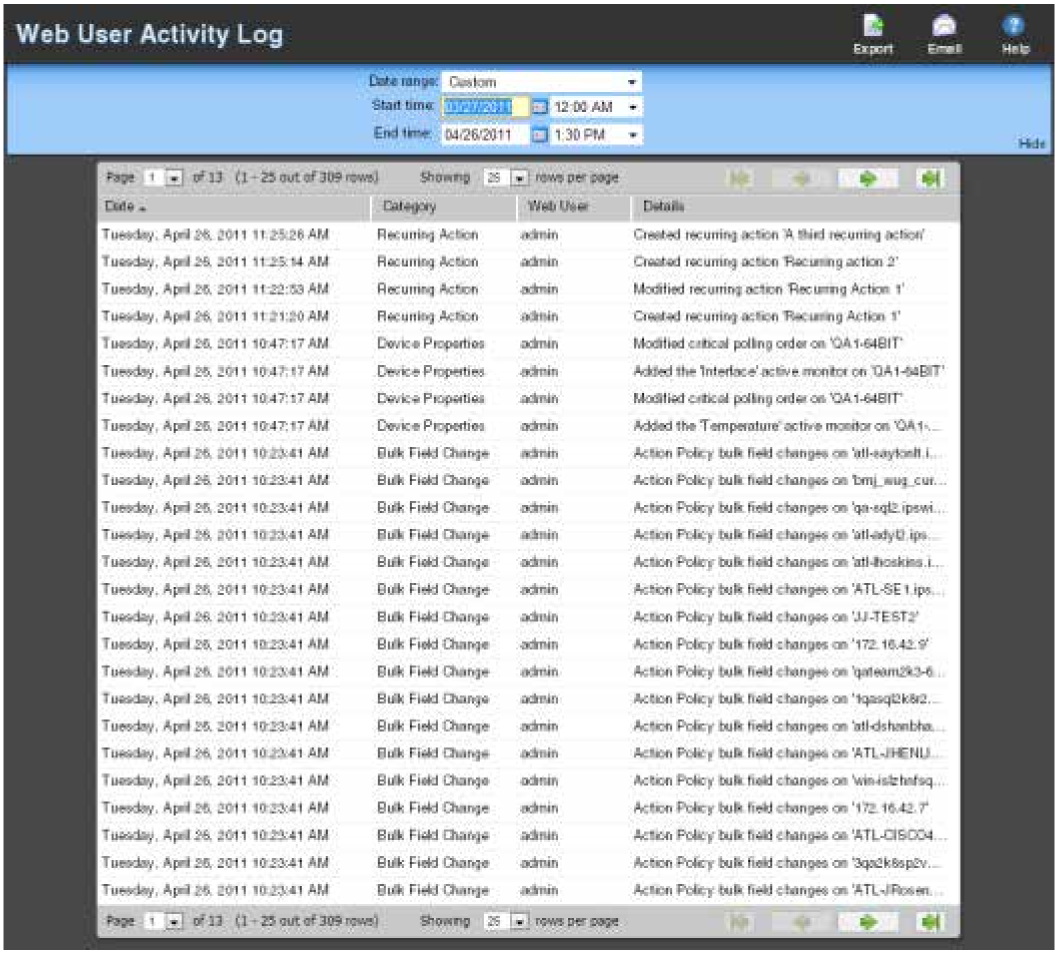
The following information is displayed in the log:

- **Date**. The date and time the attempt to fire the action occurred.
- **Recurring Action**. The name of the recurring action that was scheduled to fire.
- **Category**. The result of the attempt to fire the action (*success*, *failure*, *information*, or *cancel*).
- **Details**. This column displays information about the specific action that was scheduled to fire. If the category is information, details show that the scheduled action occurred during a blackout period. If the category is cancel, details show that the action was stopped while it was in the process of being fired, either manually by the user, or by the shutdown of the Ipswitch WhatsUp Engine service.

Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

About the Web User Activity Log

This log records when a user logs on or off the web interface, and the actions taken while logged on.



Date range: Custom

Start time: 03/27/2011 12:00 AM

End time: 04/26/2011 1:30 PM

Page 1 of 13 (1 - 25 out of 309 rows) Showing 25 rows per page

Date	Category	Web User	Details
Tuesday, April 26, 2011 11:25:26 AM	Recurring Action	admin	Created recurring action 'A third recurring action'
Tuesday, April 26, 2011 11:25:14 AM	Recurring Action	admin	Created recurring action 'Recurring action 2'
Tuesday, April 26, 2011 11:22:53 AM	Recurring Action	admin	Modified recurring action 'Recurring Action 1'
Tuesday, April 26, 2011 11:21:20 AM	Recurring Action	admin	Created recurring action 'Recurring Action 1'
Tuesday, April 26, 2011 10:47:17 AM	Device Properties	admin	Modified critical polling order on 'QA1-64BIT'
Tuesday, April 26, 2011 10:47:17 AM	Device Properties	admin	Added the 'Interface' active monitor on 'QA1-64BIT'
Tuesday, April 26, 2011 10:47:17 AM	Device Properties	admin	Modified critical polling order on 'QA1-64BIT'
Tuesday, April 26, 2011 10:47:17 AM	Device Properties	admin	Added the 'Temperature' active monitor on 'QA1-...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'atl-saytonll.i...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'bmj_wug_cur...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'qa-sql2.ipswi...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'atl-adyl2.ips...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'atl-lhoskins.i...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'ATL-SE1.ips...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'JJ-TEST2'
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on '172.16.42.9'
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'qateam2k3-6...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on '1qasql2k8r2...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'atl-dshanbha...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'ATL-JHENU...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'win-islzhnfsq...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on '172.16.42.7'
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'ATL-CISCO4...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on '3qa2k8sp2v...
Tuesday, April 26, 2011 10:23:41 AM	Bulk Field Change	admin	Action Policy bulk field changes on 'ATL-JRosen...

Page 1 of 13 (1 - 25 out of 309 rows) Showing 25 rows per page

Log body

The following information is displayed in the log:

- **Date**. The date the activity took place.
- **Category**. The category of activity, for example, *login*.
- **Web user**. The web user account.
- **Details**. The details of the activity, for example, *Logged in*.

Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 359) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 360) dialog.

Using WhatsUp Gold Group / Device Logs

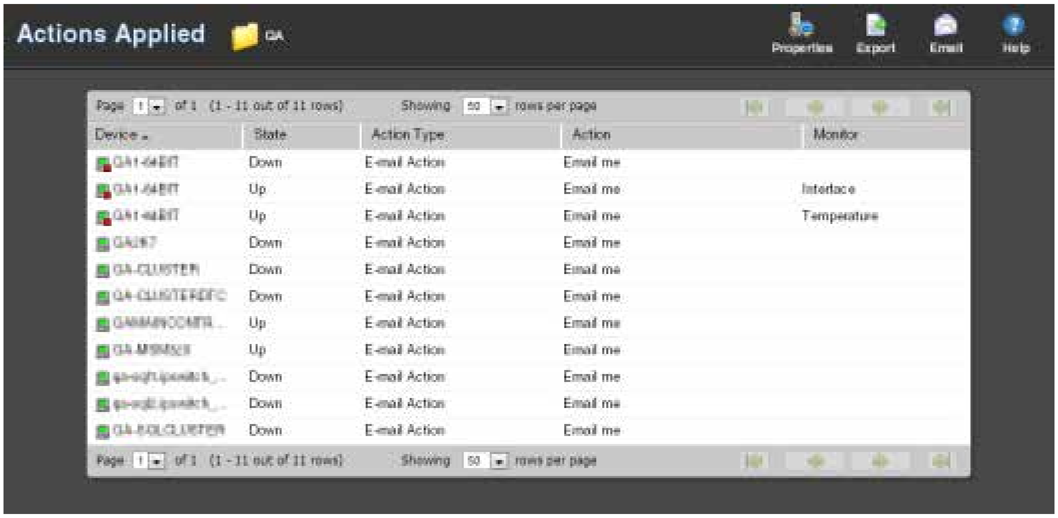
In This Chapter

The Group / Device logs provide information on the devices in your network.

Groups are user-defined logical collections of devices. Groups let you put devices of interest together, and group logs provide information on these logical groups. *Device logs* provide information on individual devices.

About the Actions Applied Log

This log shows actions that are applied to devices and monitors in the group currently in context (displayed in the log title bar). Each entry shows an action and the device, monitor and state that triggered it. To view a different group, click the group currently in context. Select a different group from the dialog.



Page 1 of 1 (1 - 11 out of 11 rows) Showing 50 rows per page

Device	State	Action Type	Action	Monitor
QA1-64BIT	Down	E-mail Action	Email me	
QA1-64BIT	Up	E-mail Action	Email me	Interface
QA1-64BIT	Up	E-mail Action	Email me	Temperature
QA2K7	Down	E-mail Action	Email me	
QA-CLUSTER	Down	E-mail Action	Email me	
QA-CLUSTERDFC	Down	E-mail Action	Email me	
QAMAINCOMTR...	Up	E-mail Action	Email me	
QA-MSMQ	Up	E-mail Action	Email me	
qa-sql1.ipswitch_...	Down	E-mail Action	Email me	
qa-sql2.ipswitch_...	Down	E-mail Action	Email me	
QA-SQLCLUSTER	Down	E-mail Action	Email me	

Page 1 of 1 (1 - 11 out of 11 rows) Showing 50 rows per page

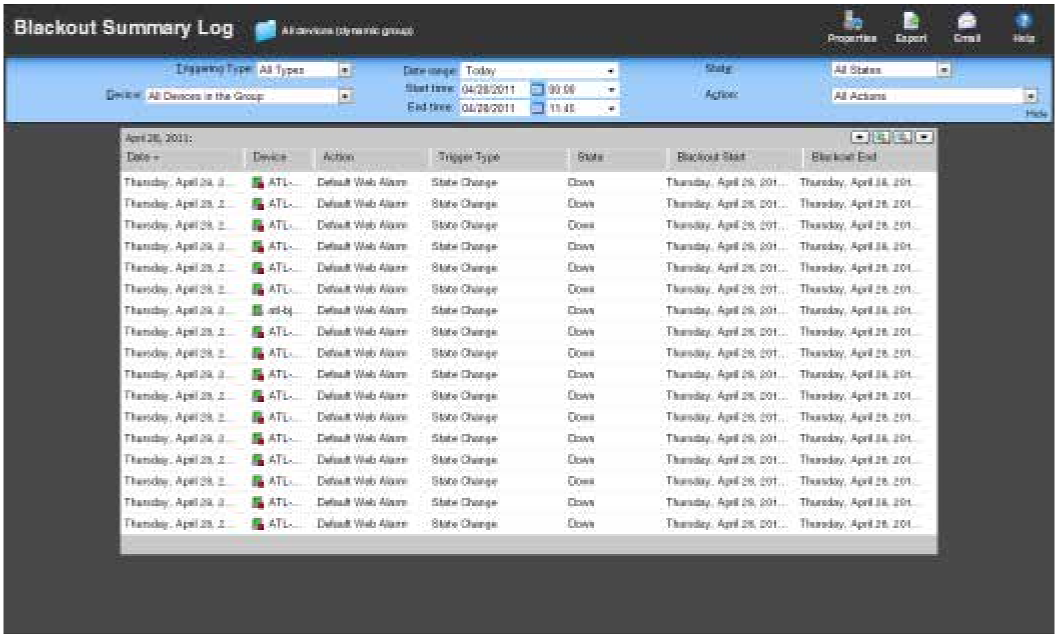
Log body

- **Device**. The IP address or name of the network device.
- **State**. The state of the action at the time of the last poll, relative to the time selected in the date/time picker.
- **Action Type**. The type of action applied to the device.

- **Action**. The action applied to the device.
- **Monitor**. The type of monitor.

About the Blackout Summary Log

This log displays a detailed list of actions that were not fired as a result of a scheduled blackout period. The information in the report can be filtered by date, device, action, triggering type, state, and blackout start and end time.



Triggering Type: All Types
Device: All Devices in the Group
Date range: Today
Start time: 04/28/2011 00:00
End time: 04/28/2011 11:45
State: All States
Action: All Actions

April 28, 2011:

Date	Device	Action	Trigger Type	State	Blackout Start	Blackout End
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	atl-bj...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...
Thursday, April 28, 2...	ATL-...	Default Web Alarm	State Change	Down	Thursday, April 28, 201...	Thursday, April 28, 201...

Log Body

Below the date/time picker is a table detailing the action and its coinciding blackout period.

- **Date**. The date on which the action would have fired were it not in a blackout period.
- **Device**. The device for which the action would have fired were it not in a blackout period.
- **Action**. The specific action that was triggered.

Tip: Click an **Action** to view the Action Log.

- **Trigger Type**. The type of trigger that initiated the action; either State Change, Passive Monitor, or All Types.
- **State**. The state of the device at the time of the action.

Tip: Click a **State** to view the State Change Timeline report.

Note: The State column displays N/A for Passive Monitor entries. No Passive Monitor entries appear in the State column unless you have configured the log to display All States.

- **Blackout Start**. The date and time the blackout period began.
- **Blackout End**. The date and time the blackout period ended.

Filtering the log

You can refine the log in several ways:

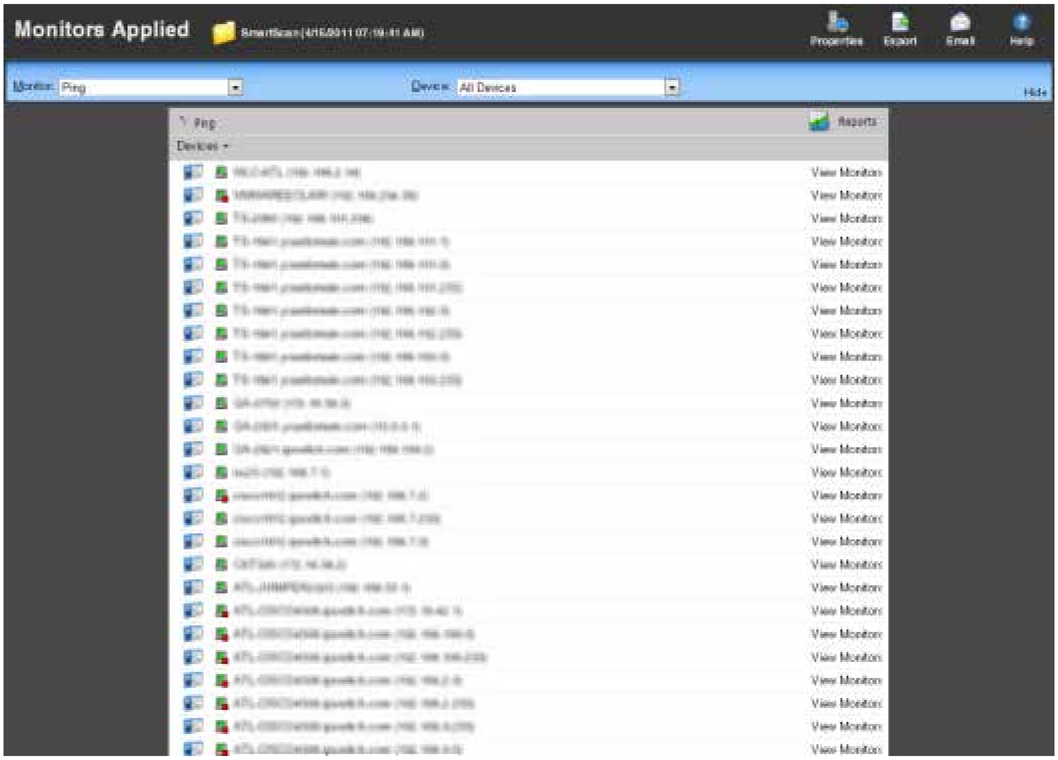
- **Select a Triggering Type**. Use the **Triggering Type** list at the top left of the page to select the triggering type for which to view log data. You can select either All Types, State Change, or Passive Monitor.
- **Select a device**. Use the **Device** list to select the specific device(s) for which to view log data. You can select a specific device, or view data for all devices in the group.

> **Tip**: To change device groups, use the **Device Group** link at the top of the page to the right of the web interface tabs. The name of the device group for which you are currently viewing log data is displayed as the title for this link.

- **Select a different date range**. Use the **Date range** list at the top of the log to change the time frame for which log data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range.
- **Select a device state**. Use the **State** list to select the state(s) for which to view log data. You can select All States, or a specific device state.
- **Select an action**. Use the **Action** list to select the action(s) for which to view log data. You can select a specific action, or view data for all actions.

About the Monitors Applied Log

This log displays a list of all monitors applied to devices in the selected device group. The information displayed in the log depends on the device(s) and monitor you select.



Monitor. Use this list to select the specific monitor for which you would like to view data. You can select from the following types of monitors:

- Active
- Performance
- Passive

Note: The list of monitors is populated with monitors currently configured for the device(s) you have selected.

Device. Use this list to select the specific group device for which to view data.

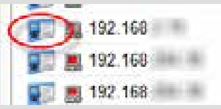
Note: The list of devices is populated with the devices that reside in the group for which you have selected to view log data. To change the the device group, click the Device Group icon located to the right of the web interface tabs.

Log Body

A table displays below the Monitor and Device lists containing data specific to your log selections. For example, if you have selected to view all devices in the group for which a Ping monitor has been configured and assigned, you will see a list of devices on the left-hand side of the log, and a series of View Monitors links on the right-hand side of the log.

Tip: Click the **View Monitor** link for a device for which you would like to view all of the monitors that have been configured and assigned to that specific device.

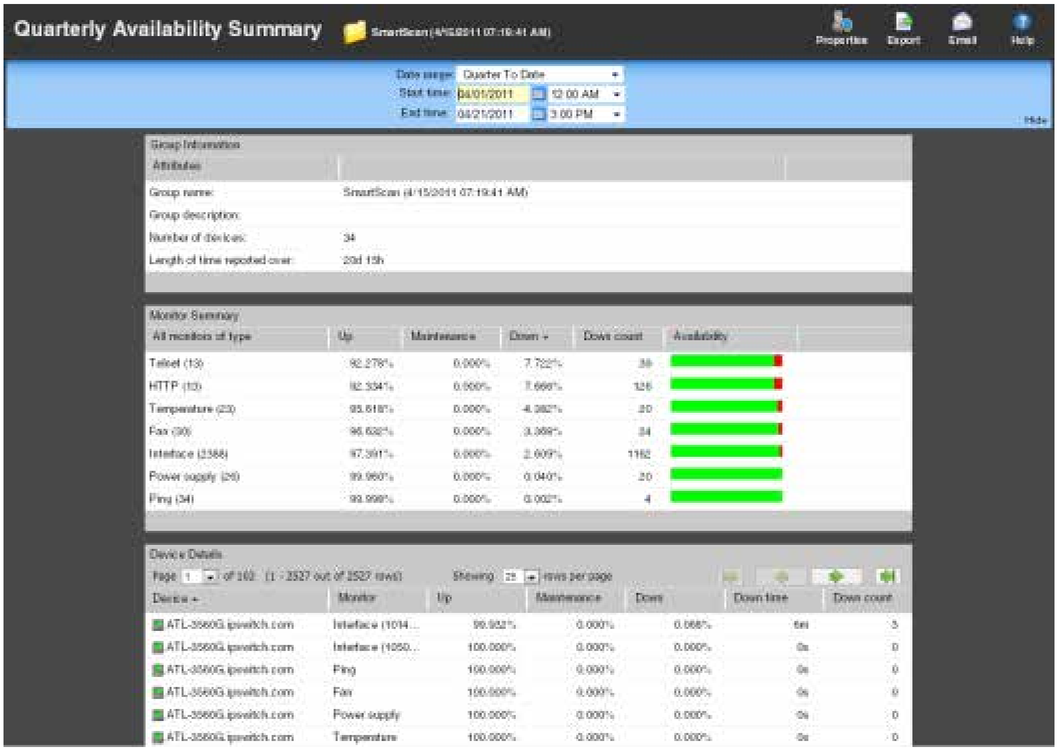
Tip: Click the **Device Properties** icon to the left of each device to view the properties for a specific device.



192.168
192.168
192.168

About the Quarterly Availability Summary

This Service Level Agreement report shows the state of all Active Monitors within a device group for the selected time period. The Quarterly Availability Summary is a combination of the WhatsUp Gold Active Monitor Outage and Active Monitor Availability monitors, located under the Monitors tab.



Quarterly Availability Summary SmartScan (4/15/2011 07:19:41 AM)

Date range: Quarter To Date
Start time: 04/01/2011 12:00 AM
End time: 04/21/2011 3:00 PM

Group Information

Attributes	
Group name:	SmartScan (4/15/2011 07:19:41 AM)
Group description:	
Number of devices:	34
Length of time reported over:	20d 15h

Monitor Summary

All monitors of type	Up	Maintenance	Down	Down count	Availability
Telnet (13)	92.278%	0.000%	7.722%	38	🟩🟥
HTTP (13)	92.334%	0.000%	7.666%	126	🟩🟥
Temperature (23)	95.618%	0.000%	4.382%	20	🟩🟥
Fan (30)	96.632%	0.000%	3.368%	24	🟩🟥
Interface (2388)	97.391%	0.000%	2.609%	1162	🟩🟥
Power supply (26)	99.960%	0.000%	0.040%	20	🟩
Ping (34)	99.998%	0.000%	0.002%	4	🟩

Device Details

Page 1 of 102 (1 - 2527 out of 2527 rows) Showing 25 rows per page

Device	Monitor	Up	Maintenance	Down	Down time	Down count
ATL-3560G.ipswitch.com	Interface (1014...	99.932%	0.000%	0.068%	6m	3
ATL-3560G.ipswitch.com	Interface (1050...	100.000%	0.000%	0.000%	0s	0
ATL-3560G.ipswitch.com	Ping	100.000%	0.000%	0.000%	0s	0
ATL-3560G.ipswitch.com	Fan	100.000%	0.000%	0.000%	0s	0
ATL-3560G.ipswitch.com	Power supply	100.000%	0.000%	0.000%	0s	0
ATL-3560G.ipswitch.com	Temperature	100.000%	0.000%	0.000%	0s	0

Report body

Group Information

§ **Group name**. The device group for which the report displays activity data. You can change the group by clicking the group context at the top of the log to the right of the log title.

- **Group description**. A short description for the device group.
- **Number of devices**. The number of monitored devices in the selected group.
- **Length of time reported over**. The amount of time the information displayed represents.

Monitor Summary

- **All monitors of type**. The type of Active Monitor. The number in parenthesis next to the monitor name depicts the total number of that type of monitor in the device group.
- **Up**. The percentage of time the Active Monitor was up during the selected time period for all devices.
- **Maintenance**. The percentage of time the Active Monitor was in maintenance during the selected time period for all devices.
- **Down**. The percentage of time the Active Monitor was down during the selected time period for all devices.
- **Down count**. The number of times the Active Monitor was in the down state during the selected time period for all devices.
- **Availability**. The overall availability for the Active Monitor during the selected time period, by color. The colors in this section match the Device States colors (configured in **Program Options** > **Device States**).

Note: When hovering over any percentage data listed, a popup appears displaying the total number of seconds the monitor has been in the listed state.

Device Details

- **Device**. The group device's display name (or IP address if a display name isn't specified in its Device Properties) and device state icon.
- **Monitor**. The Active Monitor configured for this device.
- **Up**. The percentage of time the Active Monitor on this device was up during the selected time period.
- **Maintenance**. The percentage of time the Active Monitor on this device was in maintenance during the selected time period.
- **Down**. The percentage of time the Active Monitor on this device was down during the selected time period.
- **Down time**. Specifies how long the Active Monitor on this device was in the down state during the selected time period.
- **Down count**. Specifies the number of times the Active Monitor on these devices went down during the selected time period.

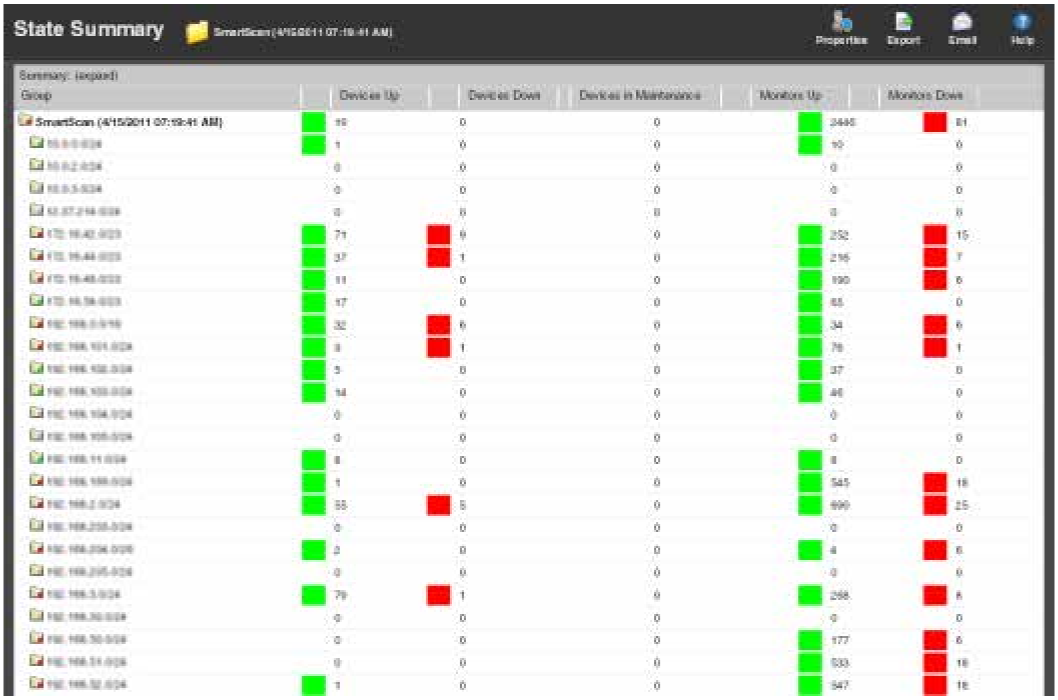
Note: When hovering over any percentage data listed, a popup appears displaying the total number of seconds the monitor has been in the listed state.

Rounded percentages

When calculating percentages of uptime for a monitor, WhatsUp Gold rounds values to the nearest thousandth of one percent (three decimal places). If this rounded value is greater than 99.999 percent, the uptime is displayed as 100% with an asterisk notation to indicate the displayed value is slightly larger than the actual value. The precise downtime value is always visible in the **Down time** column for the monitor.

About the State Summary

This log is a summary of device states in the current selected group.



Summary: (expand)

Group	Devices Up	Devices Down	Devices in Maintenance	Monitors Up	Monitors Down
SmartScan (4/15/2011 07:19:41 AM)	🟩 15	0	0	🟩 3445	🟥 81
10.0.0.0/24	🟩 1	0	0	🟩 10	0
10.0.2.0/24	0	0	0	0	0
10.0.3.0/24	0	0	0	0	0
62.37.214.0/24	0	0	0	0	0
172.16.42.0/23	🟩 71	🟥 9	0	🟩 252	🟥 15
172.16.44.0/23	🟩 37	🟥 1	0	🟩 216	🟥 7
172.16.46.0/23	🟩 11	0	0	🟩 190	🟥 6
172.16.56.0/23	🟩 17	0	0	🟩 65	0
192.168.0.0/16	🟩 32	🟥 6	0	🟩 34	🟥 6
192.168.101.0/24	🟩 8	🟥 1	0	🟩 76	🟥 1
192.168.102.0/24	🟩 5	0	0	🟩 37	0
192.168.103.0/24	🟩 14	0	0	🟩 46	0
192.168.104.0/24	0	0	0	0	0
192.168.105.0/24	0	0	0	0	0
192.168.11.0/24	🟩 8	0	0	🟩 8	0
192.168.199.0/24	🟩 1	0	0	🟩 545	🟥 18
192.168.2.0/24	🟩 55	🟥 5	0	🟩 690	🟥 25
192.168.255.0/24	0	0	0	0	0
192.168.206.0/26	🟩 2	0	0	🟩 4	🟥 6
192.168.205.0/24	0	0	0	0	0
192.168.3.0/24	🟩 79	🟥 1	0	🟩 268	🟥 6
192.168.30.0/24	0	0	0	0	0
192.168.50.0/24	0	0	0	🟩 177	🟥 6
192.168.51.0/24	0	0	0	🟩 533	🟥 18
192.168.52.0/24	🟩 1	0	0	🟩 547	🟥 18

Log body

The top section of the log displays the following information:

- Devices Up
- Devices Down
- Devices in Maintenance
- Monitors Up
- Monitors Down

To use the log:

- Click a number in the Summary area to view a list of devices that match the selected device state.
- Click **expand** or **collapse** in the Group Summary to show or hide the subgroups within the current groups shown.
  The bottom section shows a list of the items that correspond to the number at the top of the log.
- Click the device name to open the *Device Properties* (on page 117) dialog for that device.

Admin

In This Section

Using WhatsUp Gold Admin features

In This Chapter

Using Admin features

From the Admin tab, you can access the following features:

- **Admin Panel**. The Admin Panel allows you to start, stop, and restart WhatsUp Gold services. This feature provides a list of all your WhatsUp Gold processes, along with a real-time states, as well as information about the type and size of databases used by WhatsUp Gold.
- **Monitors**. The Monitor Library (active, passive, and performance) allows you to configure new or existing monitors. The Monitor Library includes separate libraries for active monitors, passive monitors, and performance monitors.
- **Actions**. The Action Library displays all actions currently configured for use in WhatsUp Gold. WhatsUp Gold includes five pre-configured actions. These actions display in the Action Library. As you create new actions, they are also added to the Action Library.
- **Action Policies**. The Action Policy Library displays a list of action policies.
- **Credentials**. The Credentials Library stores login, community string, and database connection information in a central area for Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), Telnet, SSH, ActiveX Data Objects (ADO), and VMware connections used in WhatsUp Gold.
- **Recurring Actions**. Recurring actions provide the ability to fire actions based on a regular schedule, independent of the status of devices. Among other things, this can be used to send regular heartbeat messages to a pager or cellular phone, letting users know the system is up and running.
- **Scheduled Reports**. The Report Scheduler feature allows you to manage all scheduled reports that the WhatsUp Event Analyst Service is responsible for producing on a regular basis.
- **Server Options**. From the Server Options feature, you can manage WhatsUp Gold server settings (example; height and width of maps and the maximum number of passive monitor records).
- **SNMP MIB**. The SNMP MIB Manager provides a list of all of the MIB files installed in the WhatsUp Gold MIB directory. Using this feature, you can import new MIB files to the MIB Manager. SNMP MIB Manager validates imported MIB files and flags errors if there is a problem with a file.
- **LDAP Credentials**. The LDAP credentials feature allows you to configure LDAP or Active Directory (AD) credentials and to configure WhatsUp Gold to connect with an Active Directory server to import group information from a Microsoft Domain Controller into WhatsUp Gold.

- **Translation**. The WhatsUp Gold translation features allows you to change the language in which WhatsUp Gold appears. You can export the entire user interface for translation, or, you can translate one page each time.
- **Users**. User accounts allow you to log into the web interface of WhatsUp Gold and control access to data and functionality either through direct assignment of user rights or by membership in a user group. You can also access group information.
- **Polling**. The Polling Configuration Library allows you to manage all pollers configured for use with WhatsUp Gold.
- **Tasks**. The Task Library allows you to schedule engine tasks through the WhatsUp Gold web interface.
- **Email**. The Email Settings feature allows you to manage default global email settings.
- **Preferences**. The Preferences feature allows you to change various Web user options. Changes made here only change settings for the current user web account.
- **Dashboard Views**. WhatsUp Gold comes with a several pre-configured dashboard views. You can create your own dashboard views to use in addition to the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting.

Home

In This Chapter

Using Admin Console

Access the Admin Panel by clicking **Admin > Admin Panel**. Use the Admin Panel to start, stop, and restart WhatsUp Gold services. The Admin Panel provides a list of all your WhatsUp Gold processes, along with a real-time state. The Admin Panel also provides information about the type and size of WhatsUp Gold databases.

Opening NM Console from the Web interface

The ability to open the WhatsUp Gold Console from within the Web interface is only available using Microsoft Internet Explorer; this functionality is not available using Mozilla Firefox, Google Chrome, or other Internet browsers.

To open NM Console from the WhatsUp Gold Web interface, click the **Admin** tab, then click **Open NM Console**.

This functionality uses Remote Desktop. Ensure that the machine on which you have WhatsUp Gold installed has Remote Desktop enabled.

For more information about Remote Desktop, visit *Microsoft's Web site* (http://www.whatsupgold.com/MicrosoftRDP), where you can watch videos and learn more about using Remote Desktop.

Libraries

In This Chapter

Using the Monitor Library

Use the Monitor Library to configure new or existing monitors. The Monitor Library includes separate libraries for active monitors, passive monitors, and performance monitors. From the monitor library, select the appropriate tab to view the other libraries. The monitor library allows you to create new monitors, edit existing monitors, or delete existing monitors. After creating monitors, assign them to devices.

For more information, see:

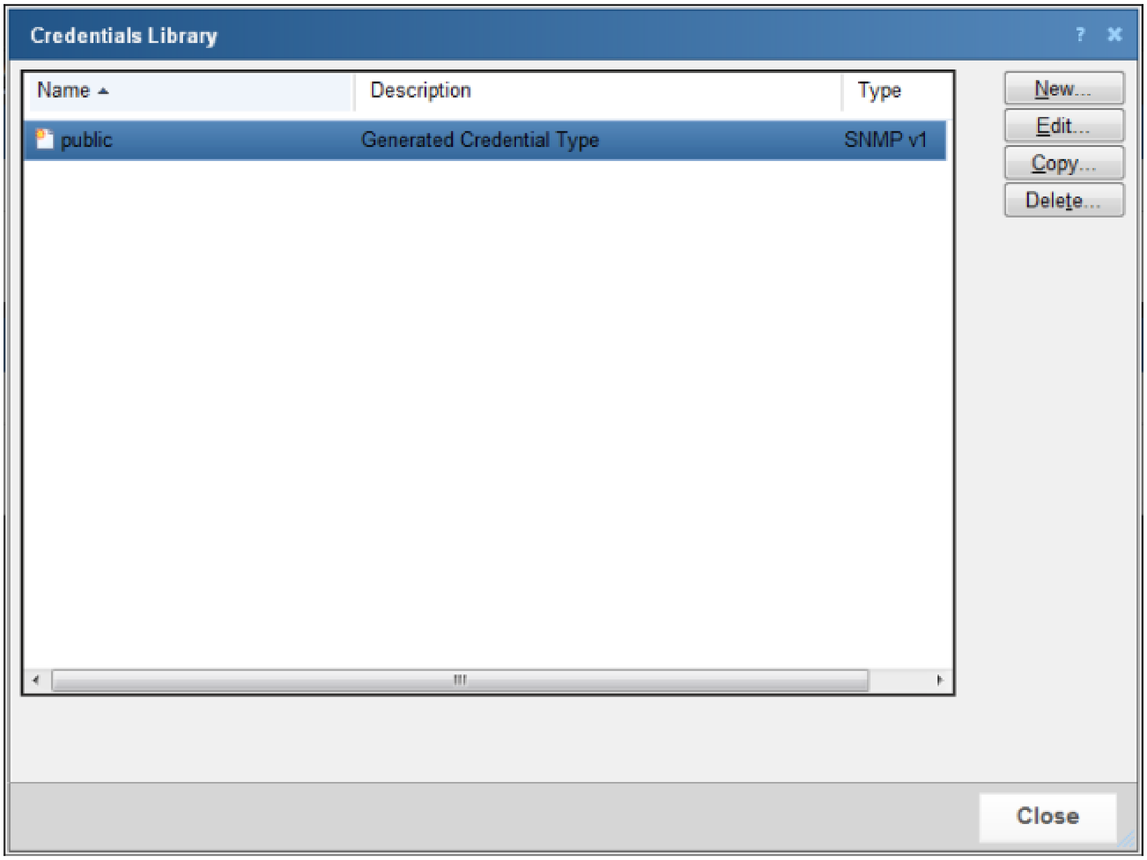
§ *Using Active Monitors* (on page 153)

§ *Using Passive Monitors* (on page 247)

§ *Using Performance Monitors* (on page 260)

Using the Credentials Library

The credentials library stores login, community string, and database connection information in a central area for Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), Telnet, SSH, ActiveX Data Objects (ADO), and VMware connections used in WhatsUp Gold. Use the credentials library to manage the credentials required to connect to devices and read from devices you monitor and databases you query.



Name ▲	Description	Type
public	Generated Credential Type	SNMP v1

- Click **New** to create a new credential to add to the library.
- Select an existing credential from the list and click **Edit** to make changes to that credential.
- Select an existing credential from the list and click **Copy** to make an exact copy of the selected credential.
- Select an existing credential from the list and click **Delete** to remove the credential from the library.

Selecting a credential type

Select the type of credential that you want to create; after selecting the credential type, click **OK** to configure the selected credential type.

- *SNMP v1* (on page 459)
- *SNMP v2* (on page 459)
- *SNMP v3* (on page 460)

- *Windows* (on page 460)
- *ADO* (on page 461)
- *Telnet* (on page 462)
- *SSH* (on page 462)
- *VMware* (on page 463)

Adding and editing a new SNMP v1 credential

The Credentials Library stores community string information for SNMP devices in your WhatsUp Gold database to be used whenever a read or write community string is needed to monitor a device. SNMP v1 uses a plain text read and write community string.

To add or edit a new SNMP v1 credential:

1. From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.
2. Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.
3. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
   - **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
   - **SNMP read community**. Enter the read community string you want to use for this credential. See SNMP Security for more information on community strings.
   - **SNMP write community**. Enter the write community string you want to use for this credential, if needed. See SNMP Security for more information on community strings.
4. Click **OK** to save changes.

Adding and editing a new SNMP v2 credential

The Credentials Library stores community string information for SNMP devices in your WhatsUp Gold database to be used whenever a read or write community string is needed to monitor a device. SNMP v2 uses a plain text read and write community string (also known as SNMP V2c).

To add or edit a new SNMP v2 credential:

1. From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.
2. Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.
3. Enter or select the appropriate information:
   - **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
   - **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
   - **SNMP read community**. Enter the read community string you want to use for this credential. See SNMP Security for more information on community strings.

- **SNMP write community**. Enter the write community string you want to use for this credential. See SNMP Security for more information on community strings.

4 Click **OK** to save changes.

Adding and editing a new SNMP v3 credential

The Credentials Library stores community string information for SNMP devices in your WhatsUp Gold database to be used whenever a read or write community string is needed to monitor a device. For more information, see *Using Credentials* (on page 68).

To add or edit a new SNMP v3 credential:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.

2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
- **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
- **Username**. Enter the username that is configured for the SNMP agent. This username is included in every SNMP packet in the authentication header. An SNMP device, upon reception of a packet, uses this username to look for configured authentication and encryption parameters and applies them to the received message.
- **Context**. Enter the context needed to identify specific SNMP instances on your network. This box is optional.
- **Authentication**. If required, select the authentication protocol for this SNMP credential.
  - **Protocol**. Select the algorithm method for authenticating SNMP v3 packets. MD5 creates a 128 bit digital signature and SHA-1 creates a 160 bit digital signature.
  - **Password**. Enter the authentication password.
  - **Confirm password**. Re-enter the authentication password a second time for confirmation.
- **Encryption.** If supported, and an authentication protocol was selected for the SNMP v3 device, select the encryption protocol for the SNMP credential.
  - **Protocol**. Select the algorithm method for encrypting SNMP v3 packets. DES56 uses a 56 bit encryption scheme and AES-128 uses a 128 bit encryption scheme.
  - **Password**. Enter the encryption password.
  - **Confirm password**. Re-enter the authentication password a second time for confirmation.

4 Click **OK** to save changes.

Adding and editing a new Windows credential

The Credentials Library stores Windows account information for monitors and devices in your WhatsUp Gold database. For more information, see *Using credentials* (on page 68).

To add or edit a new Windows credential:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.

2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
- **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
- **Domain\UserID**. Enter the domain and user login to use with this credential. To monitor a service on your devices, configure the Windows credential with the correct domain, user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, the expected user name format is *domain\user*. If the device is on a workgroup, there are two possible user names: *workgroup name\user* or *machine name\user*. In any case, the Domain\UserID must contain the backslash (\) character.
- **Password**. Enter the password for the login used above. To monitor NT services on a XP machine with an account that has an empty password, the XP Local Security Settings might have to be modified. To do this:
  - Go to **Administrative tools > Local Security Settings**.
  - Select **Security Settings > Local Policies > Security Options**.
  - Right-click on the setting **Account: Limit local account use of blank passwords to console logon only**, choose **Properties**, then select **Disable.**
- **Confirm password**. Re-enter the authentication password for confirmation.

4 Click **OK** to save changes.

Adding and editing a new ADO credential

The Credentials Library stores ADO database connection string information in your WhatsUp Gold database. For more information, see *Using Credentials* (on page 68).

To add or edit a new ADO credential:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.

2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
- **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
- **Username**. Enter a username. This username is used to authenticate to the device.
- **Password**. Enter a password. This password is used with the above username to authenticate to the device

- **Confirm password**. Re-enter the authentication password for confirmation.

4 Click **OK** to save changes.

Adding and editing a new Telnet credential

The Credentials Library allows you to create a new Telnet credential type for use with WhatsUp Gold and WhatsConfigured plug-in. For more information, see *Using Credentials* (on page 68).

To add or edit a new Telnet credential:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.

2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.

3 Enter the appropriate information:

- **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
- **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
- **Password**. Enter a password. This password is used with the above username to authenticate to the device.
- **Confirm password**. Re-enter the authentication password for confirmation.
- **Enable/privilege password**. Enter the password that enables the router to go to privileged EXEC mode, enabling you to configure the router. If the username and password provided above provide the privilege needed to run the required commands, the enable/privilege password is not needed.
- **Confirm enable/privilege password**. Re-enter the authentication privilege password for confirmation.
- **Port**. Enter the Telnet port associated with the router. The default Telnet port is 23.
- **Timeout**. Enter a timeout (in seconds) for the length of time the connection should be attempted. The default timeout is 10 seconds.

4 Click **OK** to save changes.

Adding and Editing a New SSH Credential

The Credentials Library stores SSH authentication data for devices in your WhatsUp Gold database to be used whenever authentication is needed to connect to and gather data from a device. For more information, see *Using credentials* (on page 68).

To add or edit a new SSH credential:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.

2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.

3 Enter the appropriate information:

- **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.

- **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
- **Username**. Enter a username. This username is used to authenticate to the device.
- **Password**. Enter a password. This password is used with the above username to authenticate to the device.
- **Confirm password**. Re-enter the authentication password for confirmation.
- **Enable/privilege password**. Enter the password that enables the router to go to privileged EXEC mode, enabling you to configure the router. If the username and password provided above provide the privilege needed to run the required commands, the enable/privilege password is not needed.
- **Confirm enable/privilege password**. Re-enter the authentication privilege password for confirmation.
- **Port**. Enter the SSH port associated with the router. The default SSH port is 22.
- **Timeout**. Enter a timeout (in seconds) for the length of time the connection should be attempted. The default timeout is 10 seconds.

4 Click **OK** to save changes.

Adding and editing a new VMware credential

The Credentials Library stores VMware authentication data for VMware hosts and vCenter servers in your WhatsUp Gold database to be used whenever authentication is needed to connect to and gather data from the vCenter server or VMware host. For more information, see *Using Credentials* (on page 68).

To add or edit a new VMware credential:

1 From the WhatsUp Gold web interface, go to **Admin > Credentials**. The Credentials Library appears.

2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, then click **Edit**.

3 Enter the appropriate information:

- **Name**. Enter a unique name for the credential. This name displays in the Credentials Library.
- **Description**. (Optional) Enter additional information about the credential. This information displays next to the credential in the Credentials Library.
- **Username**. Enter a username. This username is used to authenticate to the device.
- **Password**. Enter a password. This password is used with the above username to authenticate to the device.
- **Confirm password**. Re-enter the authentication password for confirmation.

4 Click **OK** to save changes.

Scheduling

In This Chapter

Adding and editing a Recurring Action

Recurring Actions provide users with the ability to fire actions based on a regular schedule, independent of the status of devices. Among other things, this can be used to send regular heartbeat messages to a pager or cellular phone, letting users know the system is up and running.

After an action is configured through the *Action Library* (on page 305), use this dialog to configure the schedule for the action. The recurring action list shows the name of the action and the recurring schedule configured for the action.

Note: Recurring actions can be configured to adhere to a blackout schedule.

To add or edit a recurring action:

1 From the WhatsUp Gold web interface, go to **Admin > Recurring Actions**. The Recurring Actions Library appears.

2 Click **New** to create a new recurring action *or* from the list of recurring actions, select the action you want to change, then click **Edit**.

3 Enter a name into the **Recurring action name** box.

4 Select a type of action from the **Select an Action** list.

Note: Web Alarm actions cannot be used as recurring actions.

Note: Click browse (**...**) to open the Action Library and *create a new action* (on page 305).

5 Click **Next**. The Add Recurring Action - Schedule dialog appears.

6 Complete the following boxes:

§ **Enable Schedule**. Select this option to activate the recurring action schedule; clear the option to disable the recurring report schedule.

§ **Blackout Schedule**. Select to access the Weekly Blackout Schedule dialog.

§ **Monthly**. Select the time, day, and month or months you want the action to fire. The action only fires during the month selected from this list. Quarterly actions can be created by selecting the last day of each quarter. If a day is entered that does not exist in a selected month (September 31, February 30, etc.) then the action is fired on the last day of that month.

- **Weekly**. Select the day and time each week you want the action to fire.

> **Note**: To fire an action more frequently than daily, select **Every _ minutes** and enter the number of minutes WhatsUp Gold should wait before firing the recurring action.

7 Click **Finish** to save your changes.

Scheduling a Recurring Action

Complete the following boxes, and then click **Finish**.

- **Enable Schedule**. Select this option to activate the recurring action schedule; clear the option to disable the recurring report schedule.
- **Blackout Schedule**. Click this button to access the Weekly Blackout Schedule dialog.
- **Monthly**. Select the time, day, and month or months you want the action to fire. The action only fires during the month selected from this list. Quarterly actions can be created by selecting the last day of each quarter.

If a day is entered that does not exist in a selected month (September 31, February 30, etc.) then the action is fired on the last day of that month.

- **Weekly**. Select the day and time each week you want the action to fire.

To fire an action more frequently than daily, select **Every _ minutes** and enter a number of minutes for WhatsUp Gold to wait before firing the recurring action.

> **Note**: To schedule multiple time periods, you must create another recurring action.

Scheduling maintenance

Select the day and time you want the device to be placed in maintenance mode, and when you want WhatsUp Gold to restart polling. You can select multiple days for a single time period. To schedule multiple time periods, you must create another maintenance entry.

Click **OK** to add the schedule to the device.

> **Note**: When in maintenance mode, device active monitors will not be polled, actions will not be triggered, and logging activity is disabled. To resume polling, actions, and logging, take the device out of maintenance mode.

Managing scheduled reports

The Scheduled Reports functionality allows you to manage all scheduled reports that the WhatsUp Event Analyst Service is responsible for producing on a regular basis. You can schedule a new report, edit an existing report's settings, delete a report from the scheduling database, or perform a test run of a scheduled report.

To manage scheduled reports:

1 From the WhatsUp Gold web interface, go to **Admin > Scheduled Reports**. The Scheduled Reports dialog appears.

2 Click one of the following options to manage scheduled reports:

§ **Edit**. Select a report you want to modify, then click **Edit**. The scheduled report opens in the Scheduled Report dialog where you can change the report settings.

§ **Disable**. Select a report you want to stop sending at scheduled intervals, then click Disable. To return a report to a scheduled interval, select the report, then click **Enable**.

§ **Delete**. Select a report you want to remove, then click **Delete**.

§ **Send Email**. Select a report, then click **Send Email**. The scheduled email report is sent to the intended recipients immediately.

System Administration

In This Chapter

Managing WhatsUp Gold server options

To manage the WhatsUp Gold server:

1. From the WhatsUp Gold web interface, go to **Admin > Server Options**. The Manage Server Options dialog appears.
2. Enter or select the appropriate information:
   - **Maximum Passive Monitor Records**. Enter the maximum number of passive monitor records. Default is 1000.
   - **Max width of graphical maps**. Enter the maximum width of maps viewed through the web browser. The size is in pixels and the default is 1000.
   - **Max height of graphical maps**. Enter the maximum height of maps viewed through the web browser. The size is in pixels and the default is 1000.
   - **Enable Mobile Access**. Select this option to enable WhatsUp Gold mobile access, which allows you to connect to WhatsUp Gold from a mobile device.
3. Click **OK** to save changes.

Using the SNMP MIB Manager

The SNMP MIB Manager provides a list of all of the MIB files installed in the WhatsUp Gold MIB directory. Using this tool, you can import new MIB files to the MIB Manager. SNMP MIB Manager validates imported MIB files and flags errors if there is a problem with a file. For more information, see *Using the SNMP MIB Manager to troubleshoot MIB files* (on page 468).

To access the SNMP MIB Manager from the WhatsUp Gold web interface, go to **Admin > SNMP MIB**.

Use the SNMP MIB Manager to configure new or existing MIBs:

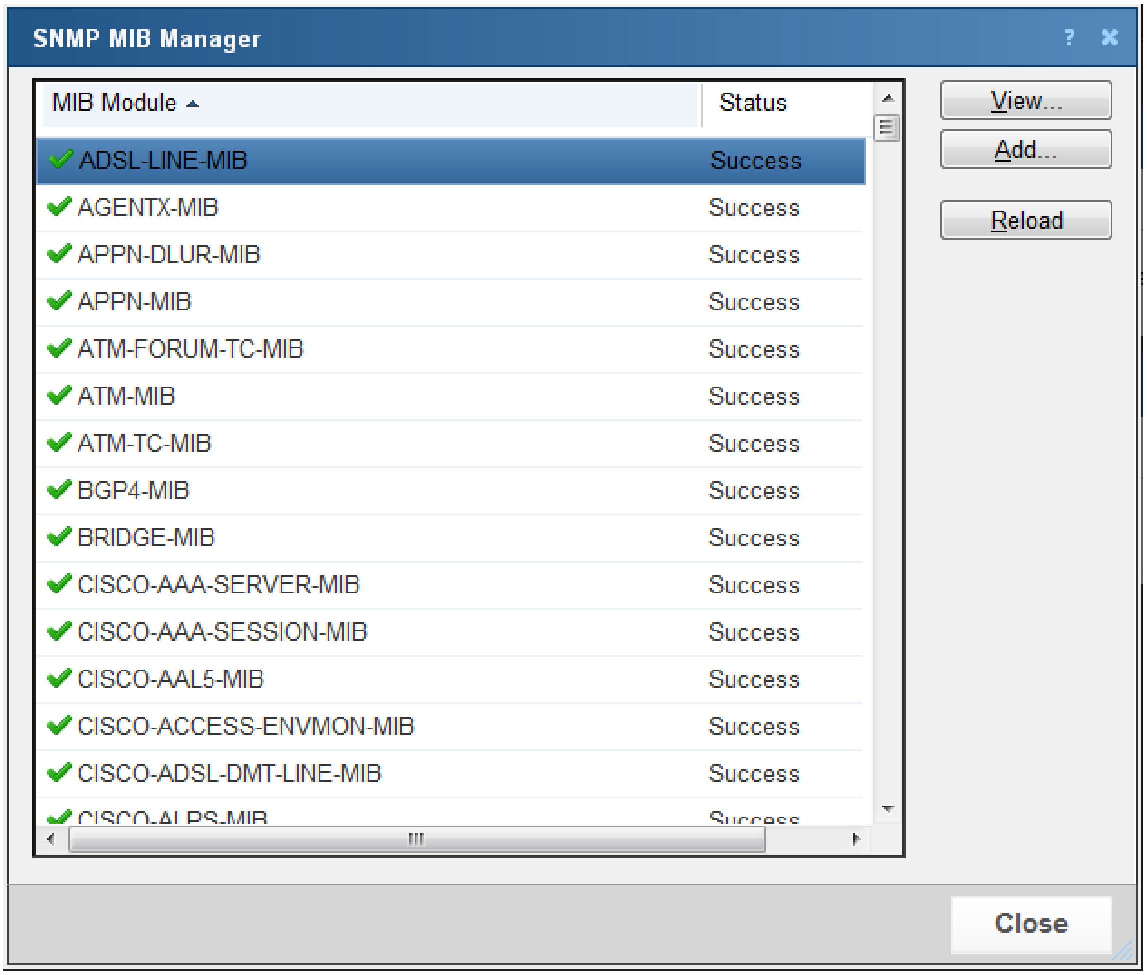
- Select an MIB file in the list, then click **View** to open the MIB and view the code.
- Click **Add** to import a new MIB file.

- After you import a new MIB file or are troubleshooting code in a MIB file, click **Reload** to refresh the MIB Module list and the Status list.

Note: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

Using the SNMP MIB Manager to troubleshoot MIB files

The SNMP MIB Manager validates all MIB files that are imported into or already exists in WhatsUp Gold. If an error is identified in a MIB file, the Status column displays the number of errors and warnings in the file. If the MIB file syntax is correct and all MIB file dependencies are fulfilled, then a check mark is displayed next to the MIB file name and a Success message displays in the Status column.



MIB Module ▲	Status
✓ ADSL-LINE-MIB	Success
✓ AGENTX-MIB	Success
✓ APPN-DLUR-MIB	Success
✓ APPN-MIB	Success
✓ ATM-FORUM-TC-MIB	Success
✓ ATM-MIB	Success
✓ ATM-TC-MIB	Success
✓ BGP4-MIB	Success
✓ BRIDGE-MIB	Success
✓ CISCO-AAA-SERVER-MIB	Success
✓ CISCO-AAA-SESSION-MIB	Success
✓ CISCO-AAL5-MIB	Success
✓ CISCO-ACCESS-ENVMON-MIB	Success
✓ CISCO-ADSL-DMT-LINE-MIB	Success
✓ CISCO-ALPS-MIB	Success

Identifying MIB file problems and errors

If an error exists in a MIB file, you can use the MIB manager to identify where code problems exist, then open the MIB file in a text editor (for example, Notepad) and correct the code. There are a variety of issues that may exist in the code; for example, there may be a simple syntax error in the MIB file or there could be a MIB file that has a dependency on another MIB file. Use the error messages when you view a MIB file to find and correct the problem.

There are two types of errors that may display in the SNMP MIB Manager list:

- ⚠ (Warning). This indicates a minor issue with the MIB file (for example, a small syntax problem). A MIB file that contains a warning may continue to work, but it is best to identify and correct the issue in the MIB file.
- 🛑 (Error). This indicates there is a problem in the MIB file that prevents it from working. A MIB file that contains an error must have the error corrected in order for the MIB file to function.

Tip: The most common MIB errors are caused by a MIB dependency on another MIB file that is not included in the MIB library. Often, when this issue is corrected, many of the MIB issues are resolved.

Example: If a MIB is missing, the MIB Manager indicates the issue in an error as shown in this example excerpt from a MIB status report:

```
22      ipMRouteGroup, ipMRouteSource,
23      ipMRouteSourceMask, ipMRouteNextHopGroup,
24      ipMRouteNextHopSource, ipMRouteNextHopSourceMask,
25      ipMRouteNextHopIfIndex,
26      ipMRouteNextHopAddress          FROM IPMROUTE-STD-MIB
Error: Cannot find module (IANA-RTPROTO-MIB): At line 26 in
C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/IPMROUTE-STD-MIB.my
```

The important information in this report is:

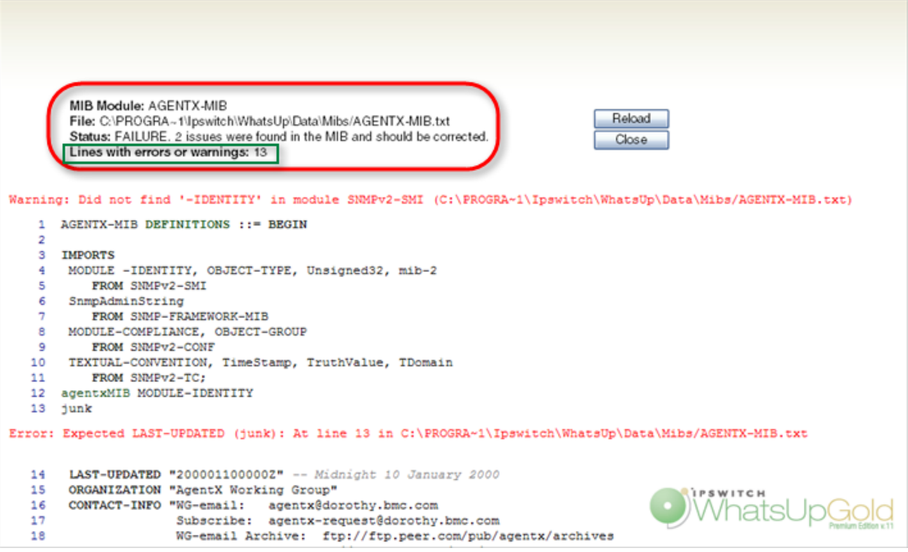
`Cannot find module (IANA-RTPROTO-MIB).`

This information indicates that the IANA-RTPROTO-MIB is missing from the MIB library in `C:\Program Files\Ipswitch\WhatsUp\Data\Mibs`

If you determine that a MIB file is missing, you can manually copy the file to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory or use the *SNMP MIB Manager* (on page 467) to add (import) a new MIB file.

To identify and correct MIB file code:

1 Select the MIB file that has an error message in the Status column, then click **View**. The viewer opens with summary information at the top of the page that identifies the number of errors or warnings. In the **Lines with errors or warnings** summary information, you can click the line number to jump directly to a line of code with the error.



MIB Module: AGENTX-MIB
File: C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/AGENTX-MIB.txt
Status: FAILURE. 2 issues were found in the MIB and should be corrected.
Lines with errors or warnings: 13

```
Warning: Did not find '-IDENTITY' in module SNMPv2-SMI (C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/AGENTX-MIB.txt)

   1  AGENTX-MIB DEFINITIONS ::= BEGIN
   2
   3  IMPORTS
   4   MODULE -IDENTITY, OBJECT-TYPE, Unsigned32, mib-2
   5      FROM SNMPv2-SMI
   6   SnmpAdminString
   7      FROM SNMP-FRAMEWORK-MIB
   8   MODULE-COMPLIANCE, OBJECT-GROUP
   9      FROM SNMPv2-CONF
  10   TEXTUAL-CONVENTION, TimeStamp, TruthValue, TDomain
  11      FROM SNMPv2-TC;
  12  agentxMIB MODULE-IDENTITY
  13  junk
Error: Expected LAST-UPDATED (junk): At line 13 in C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/AGENTX-MIB.txt

  14   LAST-UPDATED "200001100000Z" -- Midnight 10 January 2000
  15   ORGANIZATION "AgentX Working Group"
  16   CONTACT-INFO "WG-email:   agentx@dorothy.bmc.com
  17                 Subscribe:  agentx-request@dorothy.bmc.com
  18                 WG-email Archive:  ftp://ftp.peer.com/pub/agentx/archives
```

2 Now that the Viewer has helped you identify the problems in the code, open a text editor and correct the code. The MIB files are located in `..\Program Files\Ipswitch\WhatsUp\Data\Mibs`.

3 After you have made code changes, save the MIB file, then click **Reload** in the SNMP MIB Manager dialog.

4 Look for the MIB file, that you made changes to, in the list to determine of all the errors have been corrected. If all the errors have been corrected, click **Close.** If the SNMP MIB Manager dialog (validator) displays errors, continue repeating steps 1 through 3 until you have corrected all of the code issues.

Setting LDAP credentials

Use the LDAP Credentials dialog to configure LDAP or Active Directory (AD) credentials and to configure WhatsUp Gold to connect with an Active Directory server to import group information from a Microsoft Domain Controller into WhatsUp Gold.

To configure WhatsUp Gold to use Windows Active Directory for authentication:

1 From the WhatsUp Gold web interface, go to **Admin > LDAP Credentials**. The LDAP Credentials dialog appears.

2 Enter or select the appropriate information:

§ **Domain Controller or LDAP Server**. Enter the Domain Controller IP address or hostname for the Domain Controller or LDAP server. If you are authenticating to an Active Directory domain, the LDAP server for your domain is a DC (domain controller).

§ **Server port**. Enter the port the Active Directory server uses to listen for connections (Default: 389).

§ **Secure**. Select this option if you want Active Directory domain or LDAP queries to be encrypted using SSH (Default port:636).

3. In the Server Type area, select **Active Directory** to enable Active Directory domain credentials. The **Logon Domain** box is activated.
4. Enter the Active Directory **Logon Domain** from which you want to access and import AD groups.
5. (Optional) Click **Test** to open the Test dialog. The Test dialog allows you to verify that your credentials are configured correctly. For more information, see *Test LDAP credentials* (on page 472).
6. Click **Browse** to open the Browse Active Directory dialog. The Browse Active Directory dialog allows you to select the AD groups you would like to map to map to existing WhatsUp Gold user groups. For more information, see *Browse Active Directory* (on page 472).
7. In the Active Directory group list, select the WhatsUp Gold group you want to map to each AD group.

Note: Before you can map AD groups to WhatsUp Gold groups, you must create the WhatsUp Gold groups using the *Add User Group* (on page 482) dialog. When you have added the WhatsUp Gold user groups you can then select the AD groups you want to map to WhatsUp Gold groups using the *Browse Active Directory* (on page 472) dialog.

Note: When a member of an AD group logs into WhatsUp Gold using their Windows Domain credentials, they will be added as a member of the WhatsUp Gold group mapped to that AD group.

8. Click **OK** to save changes. WhatsUp Gold saves the Active Directory credentials and the LDAP Credentials dialog closes.

To configure WhatsUp Gold to use an LDAP server for authentication:

1. From the WhatsUp Gold web interface, go to **Admin > LDAP Credentials**. The LDAP Credentials dialog appears.
2. Enter or select the appropriate information:

§ **Domain Controller or LDAP Server**. Enter the Domain Controller IP address or hostname for the Domain Controller or LDAP server. If you are authenticating to an Active Directory domain, the LDAP server for your domain is a DC (domain controller).

§ **Server port**. Enter the port the Active Directory server uses to listen for connections (Default: 389).

§ **Secure**. Select this option if you want Active Directory domain or LDAP queries to be encrypted using SSH (Default port:636).

3. In the In the Server Type area, select **Standard LDAP** to enable Active Directory domain credentials. The Authorize DN box is activated.
4. Enter the path to the container which holds the users you want to access the WhatsUp Gold web interface in **Authorize DN**.

Note: The following is an example of how a specific LDAP server might CN=%s, OU=Users, o=yourdomain.net where %s is replaced by the username and password of the user.

Note: If you are not sure about the LDAP attributes to use or the path to specify, contact your LDAP administrator or LDAP vendor.

5 (Optional) Click **Test** to open the Test dialog. The Test dialog allows you to verify that your credentials are configured correctly.

6 Click **OK** to save changes. WhatsUp Gold saves the LDAP credentials and the LDAP Credentials dialog closes.

Note: After you have entered the LDAP credentials you can create user accounts for those users that you want to allow access by authenticating using the username and passwords that are available on the LDAP server with which you have configured WhatsUp Gold to communicate.

Test LDAP credentials

Use the Test LDAP Credentials dialog to test the LDAP or Active Directory credentials you have entered in the LDAP Credentials dialog.

To test LDAP or Active Directory credentials:

1 From the WhatsUp Gold web interface, go to **Admin > LDAP Credentials**. The LDAP Credentials dialog appears.

2 Enter the LDAP Credentials you want to test using the LDAP Credentials dialog.

3 Click **Test**. The Test LDAP Credentials dialog appears.

4 Enter the appropriate information:

§ **User name**. Enter a valid user name that has access to the LDAP or Active Directory server.

§ **Password**. Enter the password associated with the user name.

5 Click **Test**. WhatsUp Gold attempts to connect using the credentials and returns a test success or failure message in the **LDAP authentication** box.

6 Click **Close**. The Test LDAP Credentials dialog closes.

7 Click **OK** to save changes.

Browse Active Directory

Use the Browse Active Directory dialog to select the Active Directory (AD) groups from which you want to allow users to log in to WhatsUp Gold.

To select groups from the Browse Active Directory dialog:

1 From the WhatsUp Gold web interface, go to **Admin > LDAP Credentials**. The LDAP Credentials dialog appears.

Note: Ensure the correct Active Directory server is configured (Domain Controller, port and server type). For more information see *Setting LDAP Credentials* (on page 470).

2 Click **Browse**. The Browse Active Directory dialog appears.

3 Enter a valid user name that has access to the LDAP or Active Directory server in the **User Name** box.

4 Enter the password associated with the user name in the **Password** box.

5 Press **Tab**. The list of the most used AD groups appears.

Tip: You can see all of the groups available on the AD server by selecting Show all groups.

6 Select the AD groups you want to map to WhatsUp Gold groups.

Tip: Click **Check all** to select all of the displayed AD groups. Click **Clear all** to clear all of the selected AD groups.

7 Click **OK** to save changes. The Browse Active Directory dialog closes and the selected AD groups appear on the LDAP Credentials dialog in the AD group list.

8 Click **OK** to save changes.

Translation Groups

The language in which WhatsUp Gold is displayed is dependant on the user's web browser settings by default. However, languages can be configured in the WhatsUp Gold web interface (**Admin > Translation**). The language can be changed by selecting another language from the **Language** list. To choose a language not included in the list, click browse (**...**) to go to the Language Library.

You can use the Translation Groups dialog to translate content in one of two ways. You can either export the entire user interface for translation, or you can translate one page each time.

Note: To use the import/export translation features, you must have the Translations rights option turned on.

§ To edit the translation for a dialog, select the page from the Translation Group list, then click **Edit**.

§ To view only dialogs used in WhatsUp Gold Mobile Access, select **Show mobile only**.

For more information about translation, see the *WhatsUp Gold Translation Guide* (http://www.ipswitch.com/Wug16Trans).

About the Language Library

The Language Library shows the languages that you can use to translate a dialog on the WhatsUp Gold web interface. From here you can add a new language, modify an existing language, or delete a language from the library.

§ Click **New** to create a new language.

§ Click **Edit** to make changes to an existing language.

§ Click **Delete** to delete a language from the library.

- Click **Import** to import a language into the library.
- Click **Export** to export a language from the library.

New Language

Adding a language to the language library creates a framework for the language pack, and must be done before you can add the translated user interface text.

- **Locale ID (LCID)**. The 32-bit Locale ID (LCID) decimal value determined by Microsoft Windows. For example, the LCID for US English is 1033 and the LCID for Russian is 1049.
- **Language**. The title of the language. This title is listed in the Language Library.
- **Language code**. The abbreviated code for the language. For example, the Language code for English is "en" and the language code for Russian is "ru".

The following language data can be used to add a new language to WhatsUp Gold:

Language	LCID	Language Code
Chinese (Traditional)	1028	tw
Chinese (Simplified)	2052	cn
French	1036	fr
German	1031	de
Italian	1040	it
Japanese	1041	jp
Portuguese	1046	br
Spanish	3082	es
Russian	1049	ru

Additional information about translating WhatsUp Gold using the LCIDs, languages, and codes referenced here, see the *WhatsUp Gold Translation Guide* (http://www.ipswitch.com/Wug16Trans).

Managing users and groups

In This Chapter

Managing Users

Use this dialog to manage user accounts and user groups.

User Accounts

User accounts allow users to log in to the web interface of WhatsUp Gold and control access to data and functionality either through direct assignment of user rights or by membership in a user group.

User accounts can authenticate using:

- **Internal authentication**. The user account is created using the Add User dialog, and will authenticate using an Internal password.
- **LDAP authentication**. The user account is created using the Add User dialog, however its authentication type is set to LDAP. The user will log in using the credentials they use to authenticate with their LDAP server. The credentials for their LDAP server must be configured in WhatsUp Gold using the LDAP credentials dialog. For more information see *LDAP credentials* (on page 470).
- **Active Directory authentication**. The user account is created when a user that belongs to an AD group that has been mapped to a WhatsUp Gold group initially authenticates with WhatsUp Gold. The user will log in to WhatsUp Gold using their Windows domain credentials which must be configured using the LDAP credentials dialog. For more information see *LDAP credentials* (on page 470).

User accounts gain user rights when:

- Directly assigned those rights using the Add/Edit user accounts dialog. User rights directly assigned to the user account supersede any rights prohibited by membership in a WhatsUp Gold user group.
- The user is a member of a WhatsUp Gold user group. The user will gain those rights assigned to the WhatsUp Gold user group.
- The user is a member of a AD group that has been mapped to a WhatsUp Gold user group. The user will gain those rights assigned to the WhatsUp Gold user group.

There are two default user accounts:

1 **Admin**. The **admin** account is given all user rights, including **Manage Users**, which grants the the right to create and edit user accounts. The Administrator is also given all group access rights, so that when enabled, this account will be able to view and edit devices in all device groups.

2 **Guest**. The Guest account allows users to see the application without giving them the ability to modify any settings. By default, all user rights and all group access rights are disabled for this account. This limits the account to only seeing a limited number of information in the application. The **admin** account (or anyone else with **Manage User** rights) can modify the Guest account rights using the Manage Users dialog.

The **admin** account can be used to create additional user accounts as needed.

Note: We recommend limiting the number of users to whom you grant the **Manage Users** right. If multiple user accounts are given permission to create and delete user accounts, confusion could surface as a result. Open communication between all user accounts with the **Manage Users** right is crucial to a smooth network management operation.

To manage users:

§ To add a new user account, click **New.** The Add User dialog appears.

§ To update the displayed user rights of a user account that has the Manage Users right following upgrade to WhatsUp Gold v15.0 or later, select a user account from the account list, then click **Edit**. The Edit User dialog appears. Without making any changes to the user rights, click **OK**. The user rights available to the user prior to the upgrade will be updated. Log out of WhatsUp Gold and log back in. The user account will correctly display the user rights assigned to the user account and the Admin Panel in the Admin tab (**Admin > Admin Panel**) and other areas of the user interface previously hidden will display.

Important: When upgrading from WhatsUp Gold v14.x or earlier to WhatsUp Gold v15.0 or later, if the Manage Users rights was assigned to an account prior to the upgrade, the displayed user rights may reflect rights that have not been assigned to the user account, causing portions of the web interface to be hidden such as the Admin Panel in the Admin tab. To update the user account to reflect that the rights are assigned to the account, it is necessary to open the edit dialog for the user account, and without making any changes, click **OK**. This will update the user rights assigned to the account, and after logging out and back into the WhatsUp Gold web interface, the user rights assigned to the user will be correctly displayed.

§ To change an existing user account, select a user account from the user account list, then click **Edit**. The Edit User dialog appears.

§ To remove a user account, select the user account from the user account list, then click **Delete**. A confirmation message will appear. Click **Yes**. The user account will be removed from the user account list.

User Groups

User groups efficiently manage assignment of permissions and rights to user accounts. You can map WhatsUp Gold user groups to Active Directory groups so that users can authenticate and be assigned to WhatsUp Gold groups using their Windows domain credentials.

domain-guests. The domain-guests group is created if you attempt to map AD groups before any WhatsUp Gold user groups have been created, this group is not given any user rights. Any user account with Manage Users can add user group rights to this group.

To manage groups:

- To add a new user group, click **New.** The Add User Group dialog appears.
- To change an existing user group, select a user group from the user group list, then click **Edit**. The Edit User dialog appears.
- To remove a user group, select the user group from the user group list, then click **Delete**. A confirmation message will appear. Click **Yes**. The user account will be removed from the user account list.

To enforce access rights set up in the Device Group Properties dialog:

Click **Enable Group Access Rights** to enforce access rights set up in the Device Group Properties dialog.

About user rights

User rights govern what actions users in WhatsUp Gold can perform. Any user who has been granted the Manager Users right or belongs to a group that has this right can manage user rights.

⚠ **Caution**: When creating an account for a novice user, do not grant all user rights. An inexperienced user with too many user rights may make inappropriate selections that accidentally interrupt network monitoring. In the case of a new user, we recommend that you restrict the account to only those rights that they will need to gain familiarity with the application. Grant additional rights as the user gains confidence and application knowledge.

The table below lists and describes each of the user rights.

Account Administration	
Change your Password	Enables users to change their own password from the Preferences dialog (**Admin > Preferences**).
Manage Dashboard Views	Enables users to add, delete and copy dashboard views. Allows users to modify the properties of a specific dashboard view.
Mobile Access	Enables users to access the mobile web interface.
System Administration	
Manage Users	This right is intended for system administrators as it grants access to all features and functionality in the WhatsUp Gold web interface. Enabling this right enables all user rights. Note: When upgrading to future releases of WhatsUp, user accounts with this right enabled are automatically given access to any new

	right(s) included in the new version of WhatsUp.
Configure LDAP Credentials	Enables user to configure LDAP credentials for connecting to an LDAP server for user authentication in the web interface.
Configure Dashboards	Enables users to add dashboard views, as well as configure, move and delete dashboard reports within dashboard views.
Translations	Enables users to view the translation system as well as import and export languages.
Manage SNMP MIBs	Enables users to download and delete SNMP MIBs through the SNMP MIB Manager.
System Administration	Enables users to edit system configuration items, including the maximum number of passive monitor records, maximum dimensions of maps, and enabling and disabling mobile access.
Configure Credentials	Enables users to configure SNMP and Windows credentials.
Configure WhatsConfigured Tasks	Enables users to configure WhatsConfigured tasks and task scripts on devices in the groups to which the user has access.
Configure Alert Center	Enables users to create, edit and delete WhatsUp Gold Alert Center thresholds and policies.
Configure Flow Monitor	Enables users to create, edit and delete WhatsUp Gold Flow Monitor sources, collection intervals and data intervals for reports.
Email Settings	Enables users to configure WhatsUp Gold email settings from the Email Settings dialog (**Admin > Email Settings**).
Access Virtualization Actions Menu	Enables users to perform VM actions (stop, pause, restart, etc) on any virtual host within WhatsUp Gold.
Access Wireless	Enables users to monitor wireless infrastructure devices within WhatsUp Gold Wireless.
Configure Wireless	Enables users to manage wireless infrastructure devices within WhatsUp Gold Wireless.
Access Layer-2	Enables users to view all layer 2 data, including reports and tools.
Manage Layer-2	Enables users to use all layer 2 Group/Map manipulation features including Map Properties and right-click map operations. Note: Selecting this user right automatically selects the Access Layer-2 and Manage Device Groups user rights.
Monitoring	
Configure Active Monitors	Enables users to create, edit, and remove active monitors on devices in the groups to which the user has access.
Configure Actions	Enables users to create, edit, and remove actions on devices in the groups to which the user has access.
Configure Passive Monitors	Enables users to create, edit, and remove passive monitors on devices in the groups to which the user has access.

Manage Recurring Actions	Enables users to create, edit, and remove recurring actions on devices in the groups to which the user has access.
Configure Performance Monitors	Enables users to create, edit, and remove performance monitors on devices in the groups to which the user has access.
Configure Action Policies	Enables users to create, edit, and remove action policies on devices in the groups to which the user has access.
Access Group and Device Reports	Enables users to view group and device reports for the groups which the user has access.
Access SSG Reports	Enables users to view Split Second Graphs in dashboard and full reports.
Manage Scheduled Reports	Enables users to view other user's Scheduled Reports in the WhatsUp Gold web interface (**Admin > Scheduled Reports**).
Create Scheduled Reports	Enables users to configure Scheduled Reports in the WhatsUp Gold web interface (**Admin > Scheduled Reports**).
E-Mail Reports	Enables users to email an exported report to a specific email address.
Administer Alert Center Threshold Items	Enables users to resolve or acknowledge Alert Center Threshold alerts.
Devices	
Manage Devices	Enables users to add new devices and edit existing devices in the groups in which the user has access. Note: A user must have this right to view and hear Web Alarms.
Manage Device Groups	Enables users to create, edit, or remove device groups on the network.
Access Discovery Console	Enables users to access the Discovery Console. Granting users access to this dialog also enables users to discover network devices, define device roles that help identify specific device features, and add them to the WhatsUp Gold database.
Reports	
Access System Reports	Enables users to view system reports.
Manage Business Hours	Enables users to configure Business Hours filters for group reports.
Access Alert Center Reports	Enables users to view WhatsUp Gold Alert Center reports.
Access Flow Monitor Reports	Enables users to view WhatsUp Gold Flow Monitor reports.

About Remote User Rights

Remote (WhatsUp Gold Central and Remote Site Editions) - (optional)	
Access Remote Reports	Enables users to view reports on WhatsUp Gold remote sites.
Configure Remote Sites	Enables users to create, edit, and delete remote sites for use with WhatsUp Gold Central and Remote Site Editions.

When using WhatsUp Gold Distributed or MSP editions, make sure that **Access Remote Reports** is selected on the Central Site for each user that you want to provide access to the Remote Site reports. Also, make sure that you select **Configure Remote Sites** if you want a user to be able to access and change options in the Configure Remote Sites dialog. This dialog provides a list of all of the Remote Sites that have connected to the Central Site. You can view and edit two important settings in this dialog:

§ **Accept remote site connection**. Allows authorized users to enable or disable accepting connections from Remote Sites. This option is checked by default. The primary reason to clear the option is if you need to disable the Central Site from accepting any connections from this Remote Site. For example, this option could be helpful if one of the Remote Sites connected to the Central Site has an unusual amount of activity and is using too much bandwidth between sites. This option lets you temporarily disable a single Central Site from accepting remote site connections until you determine what the problem is.

§ **Local device**. Allows authorized users to select a local device to associate with the Remote Site. Click the browse (**...**) button to select a device. This device is often the computer that is running the WhatsUp software on a Remote Site. Associating a local device allows you to view the device status from the Remote Site, keeping you informed about the connection status with the Remote Site. It also provides easy access to the Network Tools for the local device you selected.

Adding and editing user accounts

Use the Add User or Edit User dialog to create a new user account or edit an existing user account.

When creating or editing a user account you can:

§ Determine the authentication type for the user account.

§ Set the language in which WhatsUp Gold is displayed for the user account.

§ Set and confirm the password when using internal authentication.

§ Select the home device group.

§ Set user rights.

You must have the **Manage Users** right to add or edit a user account.

Note: You do not need to add users that will be authenticating through an Active Directory server. When a user logs in to WhatsUp Gold using their Windows domain credentials for the first time, a user account will be created for that user. They will be added to the group which was mapped to which the AD group that the user account is a member.

Important: When new Active Directory users are automatically provisioned using LDAP, the Home Device Group setting for the Web Group mapped to the user's Active Directory group at the time of provisioning is set as the initial Home Device Group for the new user. The Home Device Group for the user is now maintained independently from the Home Device Group settings of any Web Groups to which the user is assigned.

To create or edit a user account:

1 From the WhatsUp Gold web interface, go to **Admin > Users**. The Manage Users dialog appears.

2 Click **New**. The Add User dialog appears.

3 Enter or select the appropriate information:

§ **User name**. Enter a unique name for the user account.

§ **Authentication type**. Select **Internal** for internal authentication using a password entered on this dialog. Select **LDAP** for remote authentication using an LDAP server (other than an Active Directory server) configured on the LDAP credentials dialog.

Note: When you select **LDAP**, the Internal password and Confirm password boxes are deactivated.

Note: When a user is being edited that has authenticated through an Active Directory server, the Authentication type for that user will appear as **Active Directory**.

§ **Internal password**. If your Authentication type is **Internal**, enter the password to be used with the user account.

§ **Confirm password**. If your Authentication type is **Internal**, re-enter the password to be used with the user account.

§ **Home device group**. Enter the device group that will be used to provide information for monitoring and dashboard reports.

§ **Member of**. Select the user groups to which you want the user account to be a member. Groups must be added prior to adding a user to a group. For more information on adding user groups, see *Adding and Editing user groups* (on page 482).

Note: When you add a user account to a group it will inherit all of the rights assigned to that group.

Tip: Select **Show rights inherited from group membership + user rights** to show the user rights the user will inherit from membership in the groups selected in the **Member of** box. The first column of check boxes in the User Rights list indicate the user rights acquired through group membership.

4 Select the **User rights** that you want to grant to the user account. For more information, see About User Rights.

Tip: You can click **Check all** to select all of the available user rights.

Note: If you grant the **Manage Users** right, the user account will acquire all user rights.

5 Click **OK** to save changes. The user account is added to the user account list on the Manage Users dialog.

Adding and editing user groups

Use the Add User Group or Edit User Group dialog to create or edit a user group. When creating or editing a user group, you can:

- Name the group.
- Choose the default language which will be displayed in the web interface for members of the group.
- Select group rights.

Note: You must have the Manage User rights to add or edit a user group.

To add or edit a user group:

1 From the WhatsUp Gold web interface, go to **Admin > Manage Users**. The Manage Users dialog appears.

2 In the User Group area, click **New** *or* select a group, then click **Edit**. The Add User Group *or* Edit User Group dialog appears.

3 Enter or select the appropriate information:

- **User group**. Enter a unique name for the user group. This name will appear on the user group list when the group is created.
- **Home device group**. Click browse (**...**) to select a device group.

Note: If the WhatsUp Gold user group has been mapped to an Active Directory group, the AD group is displayed in the AD groups list. Any user that authenticates from one of the AD groups mapped to the WhatsUp Gold user group appear as a user in the **Members** box.

Note: All users that are members of the group are displayed in the **Members** box.

Important: When new Active Directory users are automatically provisioned using LDAP, the Home Device Group setting for the Web Group mapped to the user's Active Directory group at the time of provisioning is set as the initial Home Device Group for the new user. The Home Device Group for the user is now maintained independently from the Home Device Group settings of any Web Groups to which the user is assigned.

1 In the **User group rights** box, select the rights you want to assign to the members of this group. The user group rights you select will be inherited by all user accounts that are assigned to this group.

2 Click **OK** to save changes. The Add User Group dialog closes and the user group appears on the user group list.

About device group access rights

Device group access rights enable WhatsUp Gold users to see or make changes to specific groups and devices. These rights can be enabled or disabled by the administrator and are disabled by default.

Device group access rights are useful when users need to view and edit only those groups that are pertinent to them, as would be the case with a large network with multiple network administrators. Device group access rights allow an administrator to grant each user rights to only the devices on the network for which that user is responsible.

Note: Elements in group folders are displayed based on the user right options selected for the parent folder.

Types of device group access rights

There are four types of device group access rights:

1 **Group Read**. This right allows users to view groups and devices in the selected group. This right allows users to see the group's map and device list. Group-level reports are not affected by group access rights but are affected by user rights.

2 **Group Write**. This right allows users to edit group properties and add, edit, and delete devices and other groups within the selected group.

3 **Device Read**. This right allows users to view the device properties of all devices within the selected group. Device-level reports are not affected by group access rights but can be affected by user rights.

4 **Device Write**. This right allows users to edit the device properties of any device within the selected group. Device Write also allows users delete the device from the group if they also have Group Write access.

Note: To add a device to a group, a user must have Group Write rights to that group.

Tip: When enabled, group access rights are applied throughout WhatsUp Gold. Device pickers, group pickers, and group views all respect what a user account is granted permission to view and edit. Reports are not affected by group access rights but are affected by user rights.

The following is a list of operations and the group access rights that must be assigned for the user to perform that task:

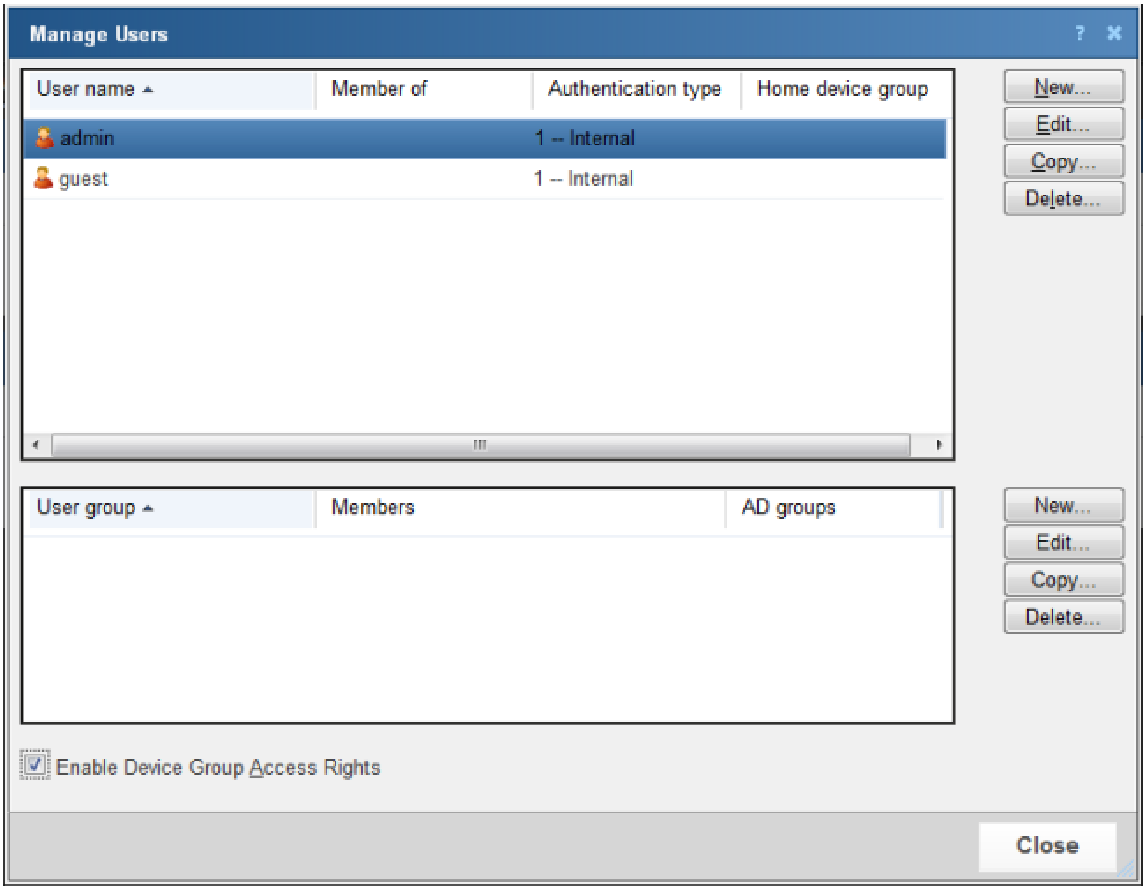
- List and Map in the Group Views menu require **Group Read** access.
- Create Group and Group Properties in the Group Operations menu require **Group Read** and **Group Write** access.
- Copy Group requires **Group Read** in the source group, and **Group Read** and **Group Write** in the destination group. (Permissions to groups and sub-groups are copied, not inherited from the new parent.)

- Move Group requires **Group Read** and **Group Write** in both the source and the destination groups. (Permissions of the group and sub-groups remain the same.)
- Delete Group requires **Group Read**, **Group Write**, **Device Read**, and **Device Write** recursively. (Device Read Write may not be required if the group is empty.)
- Create Device requires **Group Read**, **Group Write**, **Device Read**, and **Device Write**. If the device already exists in other group(s), you must also have **Group Read**, **Group Write**, **Device Read**, and **Device Write** in one or more of those groups.
- Copy Device requires **Group Read** in the source group and **Group Read** and **Group Write** in the destination group. The level of device permissions must be the same in both groups. Downgrade from **Device Read** and **Device Write** to **Device Read** is also permitted.
- Move Device requires **Group Read** and **Group Write** in both the source and the destination groups. The level of device permissions must be the same in both groups. Downgrade from **Device Read** and **Device Write** to **Device Read** is also permitted.
- Viewing Device Properties requires **Device Read**.
- Modifying Device Properties, Bulk Field Change, and Acknowledgement require **Device Read** and **Device Write**.

Enabling device group access rights

Device group access rights may be enabled and disabled from the Manage Users dialog.

Note: WhatsUp groups can only be managed from the WhatsUp Gold web interface.



User name ▲	Member of	Authentication type	Home device group
admin		1 -- Internal	
guest		1 -- Internal	

User group ▲	Members	AD groups

☑ Enable Device Group Access Rights

To enable device group access rights:

1. From the WhatsUp Gold web interface, go to **Admin > Manage Users**. The Manage Users dialog appears.
2. Select **Enable Device Group Access Rights** at the bottom of the dialog. The setting is immediately saved.

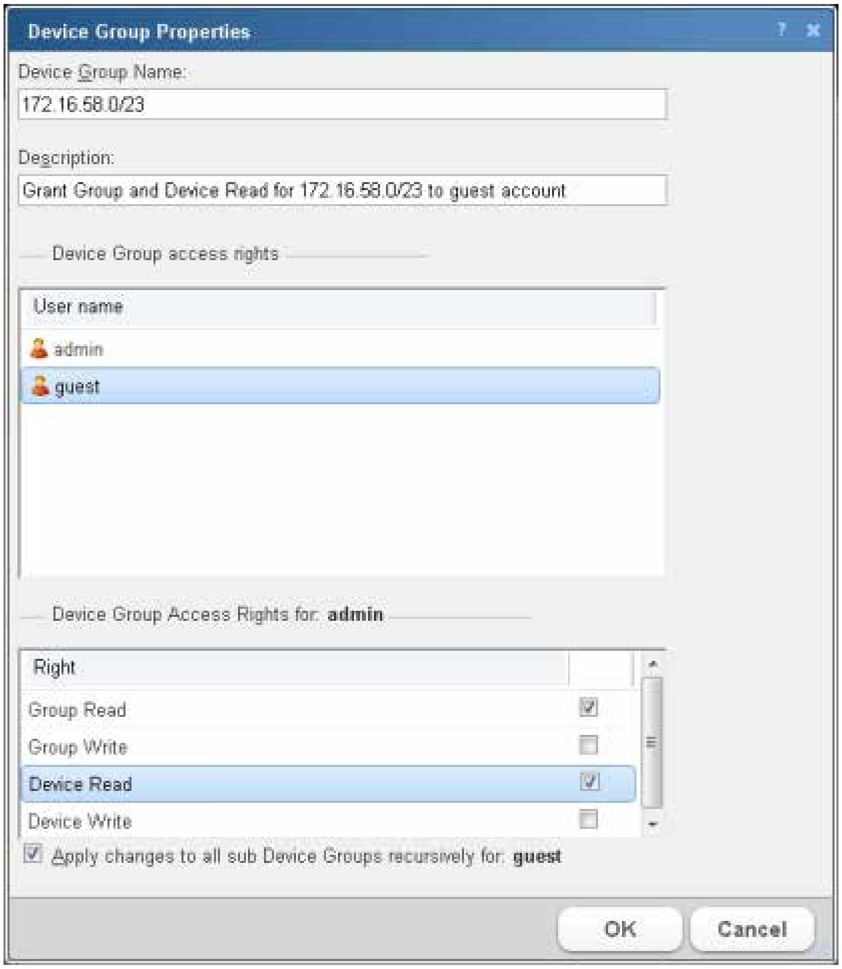
Note: Simply enabling group access rights does not ensure that the rights are set up the way that you want. You also need to assign group access rights to each group on your network.

Assigning group access rights

From the web interface, select a device group and go to Properties for that group. There are several ways to do this:

- Select a device group from the Devices tab in either Map View or Device View, and right-click. From the right-click menu, select **Properties**.
- Select a device group from the Devices tab in either Map View or Device View. From the Devices Menu bar, go to **Edit > Properties**.

From the Device Group Properties dialog, you can add and edit the access rights for the selected group.



Device Group Properties

Device Group Name: 172.16.58.0/23

Description: Grant Group and Device Read for 172.16.58.0/23 to guest account

Device Group access rights

User name
admin
guest

Device Group Access Rights for: **admin**

Right	
Group Read	☑
Group Write	□
Device Read	☑
Device Write	□

☑ Apply changes to all sub Device Groups recursively for: **guest**

Important: You must enable device group access rights for a user account before a user can add or edit access rights for a device group. To do this, the WhatsUp Gold Administrator must enable group access rights in the Manage Users dialog (on the WhatsUp Gold web interface, go to **Admin > Manage Users**).

Note: Device group access rights cannot be assigned directly to Dynamic Groups. Instead, devices are governed by the group access rights assigned to the other group or groups where the device is located. For more information, please see *About device group access rights* (on page 483).

Propagating group access rights to subgroups

Group access rights are passed from parent group to subgroup: when a new a group is created, all of the group access rights that exist in the parent group are copied to the new group. If the rights on a parent group are modified after subgroups have been created, you can propagate the changes to the subgroup by selecting **Apply changes to all sub Device Groups recursively** on the Device Group Properties dialog.

Determining the highest right

Devices can belong to more than one device group, and each group can specify a different set of group access rights. When a device exists in multiple groups, the group access rights from all of the groups are added together to determine the rights granted to a user when accessing the device. This means that if a device is granted a right (Device Read, for example) in one group, it has that right from every group to which the device belongs.

The table below demonstrates the effective rights granted to a user accessing a device that exists in three groups that each have different group access rights.

	Device Read right	Device Write right
Rights granted in Group A	X	
Rights granted in Group B		X
Rights granted in Group C		
Effective rights when accessing device from any group	X	X

In this example, the device is granted Device Read by its membership in Group A and Device Write by its membership in Group B. The result is that the user can access the device with full rights from any device group to which the device belongs, even Group C where no explicit rights are set.

Understanding device group access rights and user access rights

When device group access rights are enabled, WhatsUp Gold determines effective rights by first negotiating user rights, then group access rights. This means that, while device group access rights govern access to device groups, a user must first have user access rights to a device or group before group access rights are considered. If a user does not have the Manage Devices user access right, for example, then Device Write group access rights are not honored.

Tip: By disabling the Manage Groups and Manage Devices user access rights, you can prevent a user from modifying any groups or devices in WhatsUp Gold.

About group access rights and users' home groups

Users are given Group Read rights for their Home group by default. If Group Read rights are removed from a user's home group, the user cannot access the Device List until the Group Read right is restored or the user's Home group is changed to a group for which the user has Group Read rights.

Note: Changing a user's Home group does not change the user's Group Access rights for original Home group. Be careful to prevent unintentionally granting access to a device group to which you do not want a user to have access.

For example, an administrator creates a new user account and leaves the Home group as the default My Network. The new user account automatically receives Group Read rights to My Network. At a later date, the administrator changes the user account to use a subgroup as the user's Home group. Unless the administrator deliberately removes the Group Read right from My Network, the user continues to have Group Read rights to My Network, potentially granting the user more visibility into WhatsUp Gold than the administrator intended. Changing the user's Home group is not enough to restrict what he or she can see in WhatsUp Gold.

About group access rights and dynamic device groups

Group access rights cannot be assigned to dynamic device groups. However, every device within a dynamic device group belongs to at least one other group. Therefore, when a user accesses a device accessed through a dynamic device group, the rights he or she is granted to the device are equal to the sum of the rights granted in each of the groups to which the device belongs.

For more information, see *Determining the highest right* (on page 487).

Using the Polling Configuration Library

The Polling Configuration Library displays all pollers configured for use with WhatsUp Gold. To access the Polling Configuration Library from the web interface, go to **Admin > Polling**. For additional information about WhatsUp Gold polling, see *WhatsUp Gold Polling Engine Overview* (on page 36).

✓ **Important**: Verify that at least one poller is configured for load balancing at all times to ensure that all devices are being polled.

✓ **Important**: To ensure that at least one poller has access to your polled devices at any given time, verify that your WhatsUp Gold PC and PC that your poller is installed on have the same user access privileges. If a poller is not participating in load balancing, but is setup to poll a particular subnet, those devices in that subnet must be updated to allow SNMP requests from the associated poller.

Note: Local devices can *only* be polled by the local poller.

The Polling Configuration Library provides you with the following information:

§ **Name**. The name of the poller. The state of the poller also displays as a circle next to the poller name. The poller states are:

§ *Green* - started, registered, idle

§ *Yellow* - starting, registering, stopping, restarting

§ *Red* - error, not found, unknown

§ **Description**. Additional information about the poller.

§ **Enabled**. Whether or not the poller is currently enabled.

Use the Polling Configuration Library to configure new or existing pollers.

To add a poller installed on your network to the Poller Configuration Library:

1 Click **New**.
2 Enter a **Name** and **Description** for the poller.
3 To enable the poller, select **Is Enabled**.
4 To use this poller for load balancing, select **Use for load balance**.
5 Click **OK**.

To edit an existing poller in the Polling Configuration Library:

1 Select the poller you want to edit.
2 Click **Edit**.
3 Modify poller configuration as desired. You can:
   § Change the name and or description of the poller.
   § Enable/disable the poller.
   § Enable/disable load balancing for the poller.
   § Assign/remove specific devices or subnets to/from the poller.
4 Click **OK**.

To remove a poller from the Polling Configuration Library:

1 Select the poller you want to delete.
2 Click **Delete**.
3 When prompted by WhatsUp Gold, "Are you sure you want to delete this configuration?", click **Yes**.
4 Click **OK**.

Configuring a poller

Use this dialog to configure a WhatsUp Gold poller. For additional information about WhatsUp Gold polling, see *WhatsUp Gold Polling Engine Overview* (on page 36).

Enter the appropriate information:

§ **Name**. Enter a name for the poller. This name is used to identify the poller in the Polling Configuration Library.

§ **Description**. Enter additional information about the poller. This description is used to identify the poller in the Polling Configuration Library.

§ **Use for load balance**. Select this option to allow the poller to assist with the load on the WhatsUp Gold system.

§ **Is Enabled**. Select this option to enable the poller.

✓ **Important**: Verify that at least one poller is configured for load balancing at all times to ensure that all devices are being polled.

Important: If you are restricting SNMP access to certain IP addresses in your network and your pollers are participating in load balancing, you must add all of the IP addresses for the pollers to the list of accepted IP addresses. This is necessary to ensure that at least one poller has access to your SNMP polled devices at any given time. If a poller is not participating in load balancing, but is setup to poll a particular subnet, those devices in that subnet must be updated to allow SNMP requests from the associated poller.

Note: After a remote poller is installed, you can modify the poller User name and Password in the Windows Credential Manager, accessible via the Windows Control Panel. Ensure you log in to the remote polling machine using the same user credentials used during the poller installation. You can also run the remote poller install program (repair install) on the target poller system to change the user name and password.

Devices Tab

Use the Devices tab to select the device(s) you want to apply to the poller.

To apply a device to a poller:

1 Click **Add**. The Select a Device dialog appears.

2 Select a single device, multiple devices, or device group from the list, then click **OK**. The device(s) appear on the Devices tab.

Note: When adding multiple devices or a group of devices, you must add less than 500 devices at a time.

3 Click **OK** to save changes.

Note: To remove a device from a poller, select a device from the list, then click **Remove**.

Subnets Tab

To apply a subnet to a poller:

1 Click **Add**. The Add Subnet dialog appears.

2 Enter the subnet address into the **Address** box in the *x.x.x.x/xx* format, then click **OK**. The subnets appear on the Subnets tab.

Note: Prefix lengths and masks are equivalent. A prefix length indicates how many bits of the subnet IP address consist of the subnet prefix, or the number of bits of the masks that are set to 1. For example, the subnet 192.168.3.0 255.255.255.0 has a prefix of 192.168.3. Its mask, 255.255.255.0, consists of 24bits set to 1 and 8 bits set to 0. Its prefix length is 24, which is often times written as 192.168.3.0/24.

Note: The subnet you enter must include devices that have been discovered through the WhatsUp Gold *Discovery Console*.

3 (Optional) Click **Test** to verify the connection with the devices in the IP address range.

4 Click **OK** to save changes.

Note: To remove a subnet from a poller, select a subnet from the list, then click **Remove**.

Adding a subnet

Use this dialog to add a group of devices (subnet) to a poller. This is helpful if you have multiple locations that you want to monitor with WhatsUp Gold. For example, instead of polling devices at an off-site location through VPN and using a large amount of network bandwidth, you can *install a poller at the off-site location* and set it up to only poll devices at that location. By doing so, only the results of the polls are sent by the poller through VPN to WhatsUp Gold.

To add a subnet to a poller:

1 Enter the subnet address into the **Address** box in the *x.x.x.x/xx* format, then click **OK**. The subnets appear on the Subnets tab.

Note: Prefix lengths and masks are equivalent. A prefix length indicates how many bits of the subnet IP address consist of the subnet prefix, or the number of bits of the masks that are set to 1. For example, the subnet 192.168.3.0 255.255.255.0 has a prefix of 192.168.3. Its mask, 255.255.255.0, consists of 24 bits set to 1 and 8 bits set to 0. Its prefix length is 24, which is often times written as 192.168.3.0/24.

Note: The subnet you enter must include devices that have been discovered through the WhatsUp Gold *Discovery Console*.

2 (Optional) Click **Test** to verify the connection with the devices in the IP address range.

3 Click **OK** to save changes.

Using the Task Library

In This Chapter

Using the Task Library

The Task Library allows you to schedule engine tasks through the WhatsUp Gold web interface. There are many pre-configured tasks available in the Task Library. The following tasks are available by default:

- Statistical Cache Updater
- Group Updater
- Alert Center DB Maintenance
- Defrag Performance Tables
- Purge Log Tables

To access the Task Library, go to **Admin > Tasks**. The Task Library dialog appears.

Use the WhatsUp Gold Task Library to configure new or existing web tasks:

- Click **New** to create a new task.
- Select an existing task, then click **Edit** to modify its configuration.
- Select an existing task, then click **Copy** to create a new task based on the selected task.
- Select an existing task, then click **Delete** to remove it from the list.

Note: Some tasks cannot be copied or deleted and therefore, the Copy and Delete buttons will be disabled when these tasks are selected.

Logging and web tasks

By default, all registry key tables are set to 8760 hours (or 1 year). If you want to change this setting, go to the following location on your computer: `HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Network Monitor\WhatsUp Engine\Database Settings\Log Expiration Settings`

The following table displays which tables are associated with each registry key:

Registry Key Name	Associated Report Name
Action Activity Log Expiration Time Limit	*Action Log* (on page 429)
General Error Log Expiration Time Limit	*General Error Log* (on page 430)
Passive Monitor Error Log Expiration Time Limit	*Passive Monitor Error Log* (on page 432)
Performance Monitor Log Expiration Time Limit	*Performance Monitor Error Log* (on page 433)
Recurring Report Log Expiration Time Limit	*Recurring/Scheduled Report Log* (on page 441)
Remote Server Log Expiration Time Limit	Remote Site Log
System Activity Log Expiration Time Limit	*Activity Log* (on page 440)
Web Alarm Log Expiration Time Limit	N/A
Web User Activity Log Expiration Time Limit	*Web User Activity Log* (on page 444)
WhatsConfigured Config Expiration Time Limit	Configured Task Log
WhatsVirtual Events Expiration Time Limit	Virtual Event Log
Logger Expiration Time Limit	*Logger Error Log* (on page 433)
Wireless Logger (WrlsLog) Expiration Time Limit	Wireless Log

Create/Edit a WhatsUp Gold task

To create a new task:

1 From the WhatsUp Gold web interface, go to **Admin > Task**s. The Task Library dialog appears.

2 Click **New**. The Select Web Task Type dialog appears.

3 Select a type of task from the list, then click **OK**. The New WhatsUp Gold Task dialog appears.

4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the task. This name displays in the *Task Library* (on page 492).

§ **Description**. (Optional) Enter additional information about the task. This description displays next to the monitor in the *Task Library* (on page 492).

§ **Enable this schedule**. Select this option to begin configuring the task's schedule. For more information, see *Configuring tasks* (on page 494).

- **Run this task.** Use this section to configure a schedule on which you would like the task performed. You can configure the task to run daily, weekly, monthly, yearly, or on a custom schedule.

5 Click **OK** to save changes.

To edit an existing task:

1 From the WhatsUp Gold web interface, go to **Admin > Task**s. The Task Library dialog appears.

2 Choose a task from the list, then click **Edit**. The Edit WhatsUp Gold Task dialog appears.

3 Enter or select the appropriate information:

- **Name**. Enter a unique name for the task. This name displays in the *Task Library* (on page 492).
- **Description**. (Optional) Enter additional information about the task. This description displays next to the monitor in the *Task Library* (on page 492).
- **Enable this schedule**. Select this option to begin configuring the task's schedule. For more information, see *Configuring tasks* (on page 494).
- **Run this task.** Use this section to configure a schedule on which you would like the task performed. You can configure the task to run daily, weekly, monthly, yearly, or on a custom schedule.

4 Click **OK** to save changes.

Configuring task schedules

To configure a daily task schedule:

1 From the WhatsUp Gold web interface, go to **Admin > Tasks**. The Task Library dialog appears.

2 Select **New**. The Select Web Task Type dialog appears.

3 Select a task type from the list and click **OK**. The New WhatsUp Gold Task dialog appears.

4 Enter the appropriate information:

- **Name**. Enter a name for the task. This name displays in the Task Library.
- **Description**. (Optional) Enter additional information for the task. This description displays next to the monitor in the Task Library.

5 Select **Enable this schedule**.

6 Select **Daily** from the Interval list.

7 Specify the **Start Time**.

8 Specify how often the task should be performed. For example, if you want the task to run every other day, specify that the task should repeat every 2 days. You can select to have the task **every ___ day (s)**, or **every week day(s)** at the specified time.

9 Click **OK** to save changes.

To configure a weekly task schedule:

1 From the WhatsUp Gold web interface, go to **Admin > Tasks**. The Task Library dialog appears.

2 Select **New**. The Select Web Task Type dialog appears.

3 Select a task type from the list and click **OK**. The New WhatsUp Gold Task dialog appears.

4 Enter the appropriate information:

- § **Name**. Enter a name for the task. This name displays in the Task Library.
- § **Description**. (Optional) Enter additional information for the task. This description displays next to the monitor in the Task Library.

5 Select **Enable this schedule**.

6 Select **Weekly** from the Interval list.

7 Specify the **Start Time**.

8 Specify how often the task should be performed. For example, if you want the task to run to run every other week during the work week, specify that the task run every 2 weeks and select Monday through Friday.

9 Click **OK** to save changes.

To configure a monthly task schedule:

1 From the WhatsUp Gold web interface, go to **Admin > Tasks**. The Task Library dialog appears.

2 Select **New**. The Select Web Task Type dialog appears.

3 Select a task type from the list and click **OK**. The New WhatsUp Gold Task dialog appears.

4 Enter the appropriate information:

- § **Name**. Enter a name for the task. This name displays in the Task Library.
- § **Description**. (Optional) Enter additional information for the task. This description displays next to the monitor in the Task Library.

5 Select **Enable this schedule**.

6 Select **Monthly** from the Interval list.

7 Specify the **Start Time**.

8 Specify the day of the month the task should run. You can select a numerical date, such as the 15th, or a generic date, such as the third Wednesday.

9 Specify how often the task should be performed. For example, if you want the task to run every other month, specify that the task repeat every 2 months.

10 Click **OK** to save changes.

To configure a yearly task schedule:

1 From the WhatsUp Gold web interface, go to **Admin > Tasks**. The Task Library dialog appears.

2 Select **New**. The Select Web Task Type dialog appears.

3 Select a task type from the list and click **OK**. The New WhatsUp Gold Task dialog appears.

4 Enter the appropriate information:

- § **Name**. Enter a name for the task. This name displays in the Task Library.
- § **Description**. (Optional) Enter additional information for the task. This description displays next to the monitor in the Task Library.

5 Select **Enable this schedule**.

6 Select **Yearly** from the Interval list.

7 Specify the **Start Time**.

8 Specify the day and month the task should run. You can select a month with a numerical date, such as the June 1st, or a generic date with a month, such as the first Friday of June.

9 Click **OK** to save changes.

To configure a custom task schedule:

1 From the WhatsUp Gold web interface, go to **Admin > Tasks**. The Task Library dialog appears.

2 Select **New**. The Select Web Task Type dialog appears.

3 Select a task type from the list and click **OK**. The New WhatsUp Gold Task dialog appears.

4 Enter the appropriate information:

- § **Name**. Enter a name for the task. This name displays in the Task Library.
- § **Description**. (Optional) Enter additional information for the task. This description displays next to the monitor in the Task Library.

5 Select **Enable this schedule**.

6 Select **Custom** from the Interval list.

7 Specify the **Start Time**.

8 Specify how often the task should be performed. You can select seconds, minutes, hours, or days. For example, you can specify that the task run every two hours starting at 2:57:59 AM.

9 Click **OK** to save changes.

To disable an existing task:

1 From the web interface, go to **Admin > Tasks**. The Task Library dialog appears.

2 Select the desired task, then click **Edit**. The New/Edit WhatsUp Gold Web Task dialog appears.

3 Select **Enable this Schedule** to disable the current task.

4 Click **OK** to save changes.

Options

In This Chapter

Configuring Email settings

Use this dialog to configure the default global settings for Email actions.

To configure Email settings:

5 From the WhatsUp Gold web interface, go to **Admin > Email**. The Configure Email Settings dialog opens.

6 Enter or select the appropriate information:

§ **Destination email address**. Enter the address that the Email action message should be sent.

§ **From email address**. Enter the address to be listed as "From" in the email sent by the Email action.

§ **SMTP server**. Enter the address of the server on which SMTP is running (email server).

§ **Port**. Enter the number of the port on which the SMTP service is listening. The standard SMTP port is 25.

§ **Timeout (sec)**. Enter the amount of time (in seconds) that WhatsUp Gold should wait for a response from the SMTP server for each command WhatsUp Gold issues. If the time limit is exceeded, the email fails. The default timeout is 30 seconds.

§ **Use SMTP authentication**. Select this option if your SMTP server requires user authentication.

§ **Username**. Enter the username to be used with SMTP authentication.

§ **Password**. Entre the password of the username to be used with SMTP authentication.

§ **Use an encrypted connection (SSL/TLS)**. If your SMTP server supports encrypting data over a TLS connection (formerly known as SSL), select this option to encrypt SMTP traffic.

7 Click **OK** to save changes.

Changing preferences

Use this dialog to change various web user preferences. Changes made in this dialog only change settings for the *current* user web account. To access the Preferences dialog, go to **Admin > Preferences.**

General

§ **Change your password**. Select this option to change your account password.

§ **Show Getting Started Pane**. Select this option to display the Getting Started pane. The Getting Started pane includes links to resources to help you resolve issues and learn more about WhatsUp Gold.

Note: If you have an evaluator license, this box displays as **Show Evaluator Pane.** This option is not selectable with an evaluator license.

Refresh intervals

§ **Dashboard report**. Enter a time (in seconds) for how often dashboard reports should refresh.

§ **Full report**. Enter a time (in seconds) for how often *monitor reports* (on page 370) should refresh.

§ **Devices list**. Enter a time (in seconds) for how often the content Devices tab should refresh.

Reports

§ **Default records per page for long reports**. Enter a number to control the maximum number of rows reports and logs display. If a report contains a number of rows greater than the maximum number specified, you can use either the page controls to view the data. The default max records setting is 50.

§ **Collapse legends on split second graph dashboard reports**. Select this option to hide the legends on split second graph dashboard reports until the mouse pointer moves over a graph. When multiple split second graph dashboard reports display in a dashboard view, selecting this option can help reduce the percentage of the screen area used by reports. This option affects split second graph dashboard reports only; legends are always displayed in popups.

Web Alarms

§ **Enable web alarms**. Select this option to enable *Web alarms* (on page 114).

Note: Web alarms are enabled by default.

§ **Check every**. If you enable Web alarms, enter a time (in seconds) for how often WhatsUp Gold should check for Web alarms.

Instant Info (popups)

§ **Show popups on device list**. Select this option to enable popups on the device list. If this option is cleared, popups are not displayed when you hover device or group names in the device list.

§ **Show popups on dashboard reports**. Select this option to enable popups on dashboard reports. If this option is cleared, popups are not displayed on dashboard reports.

§ **Show popups on full reports**. Select this option to enable popups on monitor reports. If this option is cleared, popups are not displayed on monitor reports.

Note: By default, popups are enabled on both dashboard and reports.

Note: Popups are not available in WhatsUp Gold Standard Edition.

Managing dashboard views

WhatsUp Gold comes with a several pre-configured dashboard views. You can create your own dashboard views to use in addition to the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting.

To create a new dashboard view:

8 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

9 Click **New**. The New Dashboard View dialog appears.

10 Enter or select the appropriate information:

§ **View name**. Enter a unique name for the dashboard view.

§ **View Type**. Select the type of view on which to base the new view.

§ **Start with**. Select how you would like the dashboard view to begin. You may choose on of the pre-configured views or choose **An empty view** to create your own customized dashboard view.

§ **Number of columns**. If creating a customized view, enter the number of columns to include in the view.

§ **Column 1 width**. If creating a customized view, enter the width of the first column in the view (in pixels).

§ **Column 2 width**. If creating a customized view, enter the width of the second column in the view (in pixels).

11 Click **OK** to save changes.

To edit an existing dashboard view:

12 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

13 Select a view from the list, then click **Edit**. The Edit Dashboard View dialog appears.

14 Enter the appropriate information:

§ **View name**. Enter a unique name for the dashboard view.

§ **Number of columns**. If creating a customized view, enter the number of columns to include in the view.

§ **Column 1 width**. If creating a customized view, enter the width of the first column in the view (in pixels).

§ **Column 2 width**. If creating a customized view, enter the width of the second column in the view (in pixels).

15 Click **OK** to save changes.

To copy an existing dashboard view:

16 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

17 Select a view from the list, then click **Copy**. The Edit Dashboard View dialog appears.

18 Enter the appropriate information:

§ **View name**. Enter a unique name for the dashboard view.

§ **Number of columns**. If creating a customized view, enter the number of columns to include in the view.

§ **Column 1 width**. If creating a customized view, enter the width of the first column in the view (in pixels).

§ **Column 2 width**. If creating a customized view, enter the width of the second column in the view (in pixels).

19 Click **OK** to save changes.

To copy a dashboard view to another WhatsUp Gold user:

20 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

21 Click **Copy to**. The Edit Dashboard View dialog appears.

22 Enter the appropriate information:

§ **View name**. Enter a unique name for the dashboard view.

§ **Copy to user**. Select the user account from where you want to copy the dashboard view.

23 Click **OK** to save changes.

To delete a dashboard view:

24 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

25 Select a view from the list, then click **Delete**. A confirmation dialog appears.

26 Click **Yes** to confirm the deletion.

Using SNMP

In This Chapter

SNMP overview

The Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a device (a host, gateway, server, etc.).

A monitoring or management application on the remote user's system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device can provide information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the Management Information Base (MIB). The MIB defines the SNMP objects that can be managed and the format for each object.

The SNMP protocol together with the MIB provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. For a detailed description of SNMP, see Request for Comments (RFC) 1157. For a description of the MIB, see RFC 1213. The MIB information used by WhatsUp Gold is contained in MIB files in the MIB directory (`..\Program Files\Ipswitch\WhatsUp\Data\Mibs`).

Enabling SNMP on Windows devices

Before you can collect performance data on a Windows computer using SNMP, you must first install and enable the Microsoft SNMP Agent on the device itself. For more information, see *Using SNMP* (on page 501).

To install SNMP Monitoring:

1. From the Windows Control Panel, click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. From the Components list, select **Management and Monitoring Tools**.
4. Click **Details** to view the list of Subcomponents.
5. Make sure Simple Network Management Protocol is selected.
6. Click **OK**.
7. Click **Next** to install the components.
8. After the install wizard is complete, click **Finish** to close the window.

To enable SNMP Monitoring:

1. In the Control Panel, click **Administrative Tools**.
2. Double-click **Services**. the Services console appears.
3. In the Services (Local) list, double-click **SNMP Service** to view the Properties.
4. On the **Agent** tab, enter the **Contact** name for the person responsible for the upkeep and administration of the computer, then enter the **Location** of the computer. These items are returned during some SNMP queries.
5. On the **Security** tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like WhatsUp to read information about the computer. This community string will be later used to create credentials for connecting to this device.
6. On the **General** tab, click **Start** to start the service (if necessary).
7. Click **OK** to close the dialog.

You can test the device by connecting to it through SNMP View.

Monitoring an SNMP Service

You can add an SNMP active monitor to check that the SNMP service is running on a device. For more information, see *Assigning active monitors* (on page 240).

To assign an SNMP Active Monitor to a device:

1. Under the **Devices** tab, on the **Device View** or **Map View** tab, right-click a device, then click **Properties**. The Device Properties dialog appears.
2. Click **Active Monitors**. The Device Properties Active Monitor dialog appears.
3. Click **Add**. The Select Active Monitor Type dialog appears.
4. Select the **SNMP** Active Monitor, then click **Next**. The Set Polling Properties dialog appears.

5 Click to select **Enable polling for this Active Monitor**, select the **Network interface to use for poll** from the list, then click **Next**.

6 (Optional) Set up an Action for the monitor state changes.

7 Click **Finish** to add the monitor to the device.

Note: An SNMP-manageable device is identified on the map by a star in the upper-right corner of the device.

About the SNMP Agent or Manager

SNMP agent software must be installed and enabled on any devices for which you want to receive SNMP information. Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 all provide an SNMP agent in their default installations. Network systems manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

For more information, see *About the SNMP operations* (on page 507) and *Enabling SNMP on Windows devices* (on page 502).

About the SNMP Management Information Base

The SNMP Management Information Base (MIB) contains the essential objects that make up the management information for a device. The Internet TCP/IP MIB, commonly referred to as MIB-II, defines the network objects to be managed for a TCP/IP network and provides a standard format for each object.

The MIB is structured as a hierarchical object tree divided into logically related groups of objects. For example, MIB-II contains the following groups of objects:

- **System**. Contains general information about the device, for example: sysDescr (description), sysContact (person responsible), and sysName (device name).
- **Interfaces**. Contains information about network interfaces, such as Ethernet adapters, or point-to-point links; for example: ifDescr (name), ifOperStatus (status), ifPhysAddress (physical address), ifInOctets, and ifOutOctets (number of octets received and sent by the interface).
- **IP**. Contains information about IP packet processing, such as routing table information: ipRouteDest (the destination), and ipRouteNextHop (the next hop of the route entry).
- Other groups provide information about the operation of a specific protocol, for example, TCP, UDP, ICMP, SNMP, and EGP.
- The **enterprise** group contains vendor-provided objects that are extensions to the MIB.

Each object of the MIB is identified by a numeric object identifier (OID) and each OID can be referred to by its text label. For example, the system group contains an object named sysDescr, which provides a description of the device. The sysDescr object has the following object identifier:

```
iso.org.dod.Internet.mgmt.mib.system.sysDescr
1.3.6.1.2.1.1.1
```

This object identifier is `1.3.6.1.2.1.1.1` to which is appended an instance sub-identifier of 0. That is, `1.3.6.1.2.1.1.1.0` identifies the one and only instance of sysDescr.

All of the MIB-II objects (for TCP/IP networks) are under the "mib" sub tree (so all these objects will have an identifier that starts with `1.3.6.1.2.1`).

For a detailed description of the MIB, see RFC 1213.

About SNMP Object Names and Identifiers

Each SNMP object has a name and numeric identifier. For example, in the *system* group, the network object named *SysDescr* with object identifier `1.3.6.1.2.1.1.1` contains a description of the device.

An object can have one or more instances, depending on the configuration of the monitored device. For example, a device can have two network adapters, in which case there will be two instances of the *ifPhysAddress* object, which has object identifier `1.3.6.1.2.1.2.2.1.6`. In this case, you need to specify an instance number at the end of the object identifier (such as `1.3.6.1.2.1.2.2.1.6.1`). If you do not specify an instance, it defaults to zero.

Using the SNMP MIB Manager

The SNMP MIB Manager provides a list of all of the MIB files installed in the WhatsUp Gold MIB directory. Using this tool, you can import new MIB files to the MIB Manager. SNMP MIB Manager validates imported MIB files and flags errors if there is a problem with a file.

To use the SNMP MIB Manager:

1 Go to the SNMP MIB Manager.

- From the web interface, go to **Admin > SNMP MIB Manager**. The SNMP MIB Manager appears.

2 Use the following options in the SNMP MIB Manager:

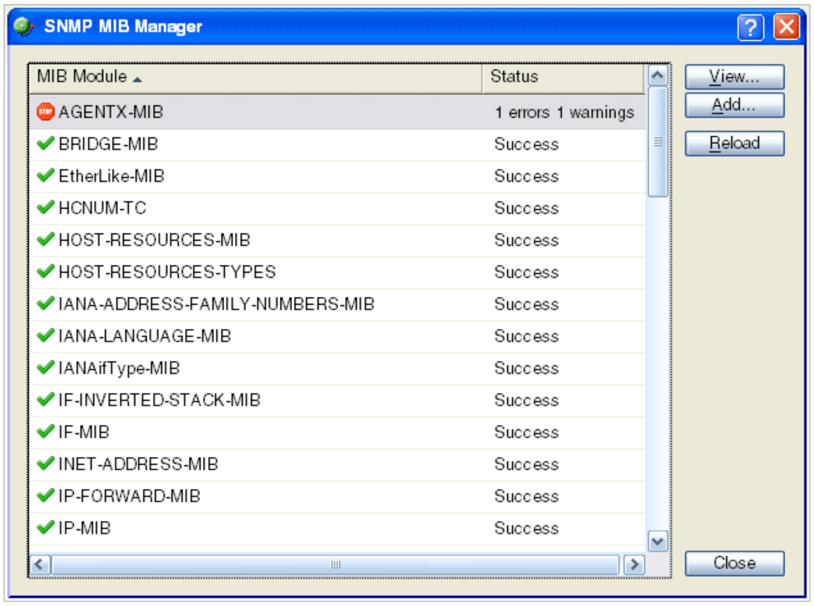
- **View**. Select a MIB file in the list, then click **View** to open the MIB and view the code.
- **Add**. Click **Add** to import a MIB file to the MIB Manager. Follow the dialogs to complete the process.

> **Note**: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

- **Reload**. When you import a new MIB file or are troubleshooting code in a MIB file, click Reload to refresh the MIB Module list and the Status list.

Using the SNMP MIB Manager to troubleshoot MIB files

The SNMP MIB Manager validates all MIB files that are imported into or already exists in WhatsUp Gold. If an error is identified in a MIB file, the Status column displays the number of errors and warnings in the file. If the MIB file syntax is correct and all MIB file dependencies are fulfilled, then a check mark is displayed next to the MIB file name and a Success message displays in the Status column.



MIB Module ▲	Status
🛑 AGENTX-MIB	1 errors 1 warnings
✓ BRIDGE-MIB	Success
✓ EtherLike-MIB	Success
✓ HCNUM-TC	Success
✓ HOST-RESOURCES-MIB	Success
✓ HOST-RESOURCES-TYPES	Success
✓ IANA-ADDRESS-FAMILY-NUMBERS-MIB	Success
✓ IANA-LANGUAGE-MIB	Success
✓ IANAifType-MIB	Success
✓ IF-INVERTED-STACK-MIB	Success
✓ IF-MIB	Success
✓ INET-ADDRESS-MIB	Success
✓ IP-FORWARD-MIB	Success
✓ IP-MIB	Success

Identifying MIB file problems and errors

If an error exists in a MIB file, you can use the MIB manager to identify where code problems exist, then open the MIB file in a text editor (for example, Notepad) and correct the code. There are a variety of issues that may exist in the code; for example, there may be a simple syntax error in the MIB file or there could be a MIB file that has a dependency on another MIB file. Use the error messages when you view a MIB file to find and correct the problem.

There are two types of errors that may display in the SNMP MIB Manager list:

- ⚠ (Warning). This indicates a minor issue with the MIB file (for example, a small syntax problem). A MIB file that contains a warning may continue to work, but it is best to identify and correct the issue in the MIB file.
- 🛑 (Error). This indicates there is a problem in the MIB file that prevents it from working. A MIB file that contains an error must have the error corrected in order for the MIB file to function.

Tip: The most common MIB errors are caused by a MIB dependency on another MIB file that is not included in the MIB library. Often, when this issue is corrected, many of the MIB issues are resolved.

Example: If a MIB is missing, the MIB Manager indicates the issue in an error as shown in this example excerpt from a MIB status report:

```
22      ipMRouteGroup, ipMRouteSource,
23      ipMRouteSourceMask, ipMRouteNextHopGroup,
24      ipMRouteNextHopSource, ipMRouteNextHopSourceMask,
25      ipMRouteNextHopIfIndex,
26      ipMRouteNextHopAddress             FROM IPMROUTE-STD-MIB
Error: Cannot find module (IANA-RTPROTO-MIB): At line 26 in
C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/IPMROUTE-STD-MIB.my
```

The important information in this report is:

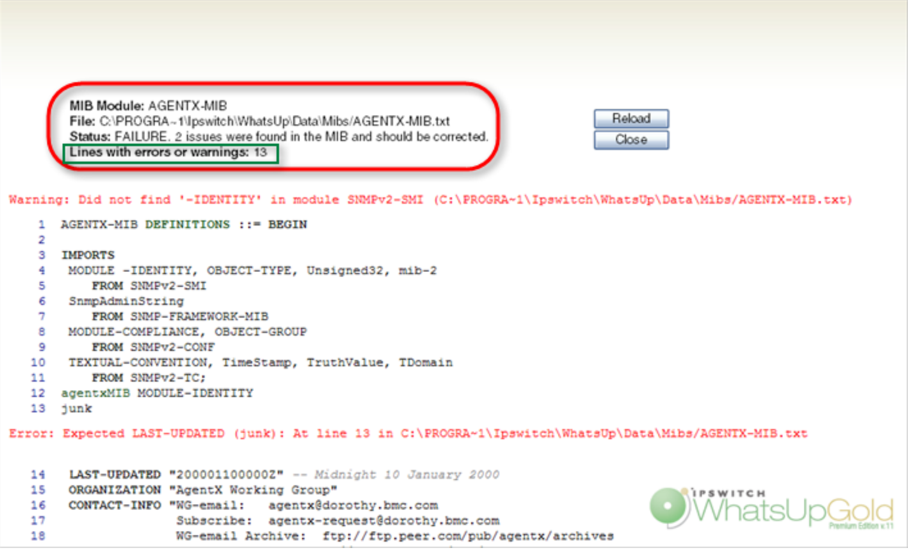
`Cannot find module (IANA-RTPROTO-MIB).`

This information indicates that the IANA-RTPROTO-MIB is missing from the MIB library in `C:\Program Files\Ipswitch\WhatsUp\Data\Mibs`

If you determine that a MIB file is missing, you can manually copy the file to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory or use the SNMP MIB Manager dialog to add (import) a new MIB file.

To identify and correct MIB file code:

1 Select the MIB file that has an error message in the Status column, then click **View**. The viewer opens with summary information at the top of the page that identifies the number of errors or warnings. In the **Lines with errors or warnings** summary information, you can click the line number to jump directly to a line of code with the error.



MIB Module: AGENTX-MIB
File: C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/AGENTX-MIB.txt
Status: FAILURE. 2 issues were found in the MIB and should be corrected.
Lines with errors or warnings: 13

```
Warning: Did not find '-IDENTITY' in module SNMPv2-SMI (C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/AGENTX-MIB.txt)

  1  AGENTX-MIB DEFINITIONS ::= BEGIN
  2
  3  IMPORTS
  4   MODULE -IDENTITY, OBJECT-TYPE, Unsigned32, mib-2
  5      FROM SNMPv2-SMI
  6   SnmpAdminString
  7      FROM SNMP-FRAMEWORK-MIB
  8   MODULE-COMPLIANCE, OBJECT-GROUP
  9      FROM SNMPv2-CONF
 10   TEXTUAL-CONVENTION, TimeStamp, TruthValue, TDomain
 11      FROM SNMPv2-TC;
 12  agentxMIB MODULE-IDENTITY
 13  junk
Error: Expected LAST-UPDATED (junk): At line 13 in C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/AGENTX-MIB.txt


 14   LAST-UPDATED "200001100000Z" -- Midnight 10 January 2000
 15   ORGANIZATION "AgentX Working Group"
 16   CONTACT-INFO "WG-email:   agentx@dorothy.bmc.com
 17                 Subscribe:  agentx-request@dorothy.bmc.com
 18                 WG-email Archive:  ftp://ftp.peer.com/pub/agentx/archives
```

2 Now that the Viewer has helped you identify the problems in the code, open a text editor and correct the code. The MIB files are located in `..\Program Files\Ipswitch\WhatsUp\Data\Mibs`.

3 After you have made code changes, save the MIB file, then click **Reload** in the SNMP MIB Manager dialog.

4 Look for the MIB file, that you made changes to, in the list to determine of all the errors have been corrected. If all the errors have been corrected, click **Close.** If the SNMP MIB

Manager dialog (validator) displays errors, continue repeating steps 1 through 3 until you have corrected all of the code issues.

About the SNMP operations

An SNMP application can read values for the SNMP objects (for monitoring of devices) and some applications can also change the variables (to provide remote management of devices). Basic SNMP operations include:

§ **Get**. Gets a specified SNMP object for a device.

§ **Get next**. Gets the next object in a table or list.

§ **Set**. Sets the value of an SNMP object on a device.

§ **Trap**. Sends a message about an event (that occurs on the device) to the management application.

The SNMP agent software on a device listens on port 161 for requests from an SNMP application. The SNMP agent and application communicate using User Datagram Protocol (UDP). Trap messages, which are unsolicited messages from a device, are sent to port 162.

Note: If an SNMP application makes a request for information about a device but an SNMP agent is not enabled on the device, the UDP packets are discarded.

Using a custom name for SNMP device interfaces

This feature lets you rename SNMP device interfaces to help you manage network interfaces more efficiently and intuitively. Without this feature you must reference device interface names, on a router for example, by their default names. Often, the device interface names are not intuitive and it is difficult to determine the specific interface you are selecting when setting up an interface utilization monitor for performance monitors and active monitors. This feature also helps you easily select the interface you want to view in interface utilization logs and other applicable dashboard reports and split second graphs.

Configuring a custom name (ifAlias) for an SNMP device interface

In order to configure a custom name (IfAlias) for a device's SNMP interface, you need to access the device configuration console and rename each interface according to your naming convention preference.

After the interface(s) are renamed, you can add them as performance monitors and active monitors. You can also select the custom interface in various dashboard reports and split second graphs. If the device interface(s) already have performance monitors and/or active monitors set up, the new interface name displays in WhatsUp Gold accordingly.

Use the following example instructions for how to change a Cisco router interface name. If you have other devices, refer to the device documentation for instructions on how to change interface names.

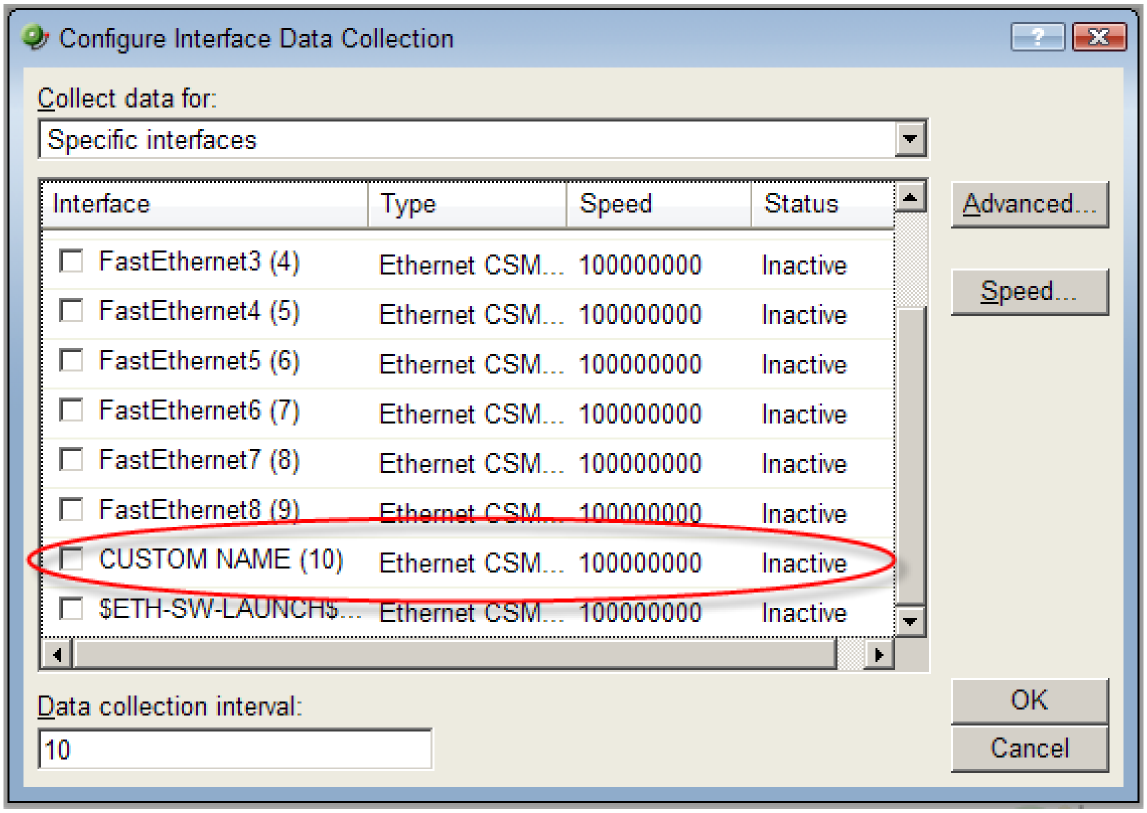
To configure a device custom name for an SNMP interface on a Cisco router:

§ Open the Cisco Command Line Interface (CLI) and enter the following commands:

```
Cisco1812# configure
Cisco1812(config)# interface FastEthernet 9
Cisco1812(config-if)# description CUSTOM NAME
Cisco1812(config-if)# ^Z
Cisco1812#
```

To add a Performance Monitor for a newly renamed device interface:

1. On the **Devices** tab, in **Device View** or **Map View**, right-click a device, then click **Properties**. The Device Properties dialog appears.
2. Click **Performance Monitors**. The Performance Monitors dialog appears.
3. In the **Enable global performance monitors** section, click to select the **Interface Utilization** option, then click **Configure**. The Configure Interface Data Collection dialog appears.
4. In the **Collect data for** list, select **Specific Interfaces**. In this example, CUSTOM NAME is the interface name created for the Cisco router. Click to select **CUSTOM NAME**, then click **OK**.



Collect data for: Specific interfaces

Interface	Type	Speed	Status
☐ FastEthernet3 (4)	Ethernet CSM...	100000000	Inactive
☐ FastEthernet4 (5)	Ethernet CSM...	100000000	Inactive
☐ FastEthernet5 (6)	Ethernet CSM...	100000000	Inactive
☐ FastEthernet6 (7)	Ethernet CSM...	100000000	Inactive
☐ FastEthernet7 (8)	Ethernet CSM...	100000000	Inactive
☐ FastEthernet8 (9)	Ethernet CSM...	100000000	Inactive
☐ CUSTOM NAME (10)	Ethernet CSM...	100000000	Inactive
☐ $ETH-SW-LAUNCH$...	Ethernet CSM...	100000000	Inactive

Data collection interval: 10

5. Click **OK**, then click **Close** to close the Device Properties dialog.

To add an Active Monitor for a newly renamed device interface:

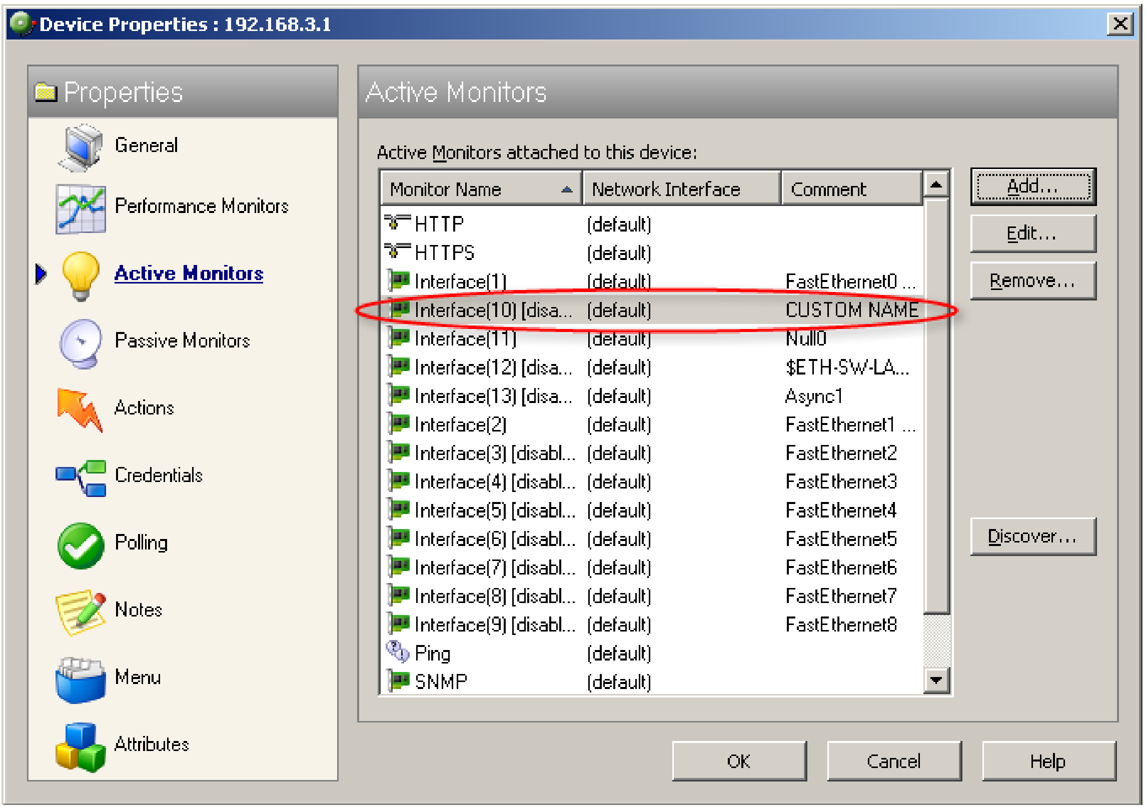
1 On the **Device View** (Console) or **Details View** (Web) or **Map View** tab, right-click a device, then click **Properties**. The Device Properties dialog appears.

2 Click **Active Monitors**. The Active Monitors dialog appears.

> **Important**: If a device has active monitors set up prior to renaming the device's interface(s), then after renaming the device's interface(s), remove the old interface(s) from the Active Monitor dialog, then click **Discover** to refresh the device interface list. Use the console application for the discover process.
> If a device has performance monitors set up prior to renaming the device's interface(s), the device interface names are automatically updated.

3 (Optional) If a device has active monitors set up for a device prior to renaming the device's interface(s), select the interface(s) that you renamed from the list of interfaces, then click **Remove**.

4 (Optional) Click **Discover**. The interface list refreshes and populates with the new interface names in the Comment list.



Monitor Name	Network Interface	Comment
HTTP	(default)	
HTTPS	(default)	
Interface(1)	(default)	FastEthernet0 ...
Interface(10) [disa...	(default)	CUSTOM NAME
Interface(11)	(default)	Null0
Interface(12) [disa...	(default)	$ETH-SW-LA...
Interface(13) [disa...	(default)	Async1
Interface(2)	(default)	FastEthernet1 ...
Interface(3) [disabl...	(default)	FastEthernet2
Interface(4) [disabl...	(default)	FastEthernet3
Interface(5) [disabl...	(default)	FastEthernet4
Interface(6) [disabl...	(default)	FastEthernet5
Interface(7) [disabl...	(default)	FastEthernet6
Interface(8) [disabl...	(default)	FastEthernet7
Interface(9) [disabl...	(default)	FastEthernet8
Ping	(default)	
SNMP	(default)	

5 Click **OK**, then click **Close** to close the Device Properties dialog.

To select a newly renamed device interface for the Interface Utilization report:

1 From the web interface, go to **Monitoring > Interface**. The Interface log appears.

2 Click the device name/IP address (shown above) to select the device you want to view. The Select a Device dialog appears.

3 Expand the network tree list to view the SNMPScan devices, then select the device for which you want to view the Interface Utilization log. The Interface Utilization log appears.

4 In the **Select Interface** list, select the newly named device interface. In this example, the interface is named `CUSTOM NAME`. View the interface utilization log.

About SNMP security

In WhatsUp Gold, credentials are used like passwords to limit access to a device's SNMP data. The credentials system supports SNMP v1, v2, and v3.

Credentials are configured and stored in Credentials Library (**Configure > Credentials Library**) and used in several places throughout the application. They can be assigned to devices in **Device Properties > Credentials** or through the Credentials Bulk Box Change option.

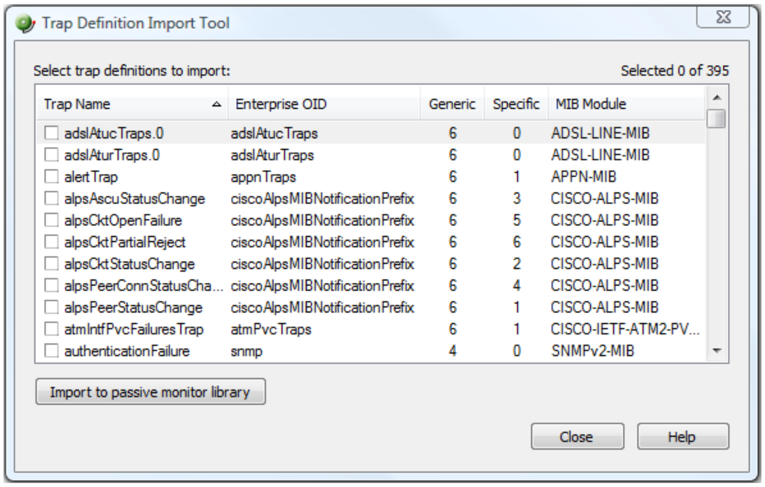
Devices need SNMP credentials assigned to them before SNMP-based Active Monitors will work.

Using the Trap Definition Import Tool

The Trap Definition Import tool is used to import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your WhatsUp Gold MIB folder (`\Program Files\Ipswitch\WhatsUp\Data\Mibs`).

To import SNMP trap definitions into the Passive Monitor Library:

1 In the WhatsUp Gold console, click **Tools > Import Trap Definitions**. The Trap Definition Import Tool dialog appears.



Select trap definitions to import:

Selected 0 of 395

Trap Name	Enterprise OID	Generic	Specific	MIB Module
□ adslAtucTraps.0	adslAtucTraps	6	0	ADSL-LINE-MIB
□ adslAturTraps.0	adslAturTraps	6	0	ADSL-LINE-MIB
□ alertTrap	appnTraps	6	1	APPN-MIB
□ alpsAscuStatusChange	ciscoAlpsMIBNotificationPrefix	6	3	CISCO-ALPS-MIB
□ alpsCktOpenFailure	ciscoAlpsMIBNotificationPrefix	6	5	CISCO-ALPS-MIB
□ alpsCktPartialReject	ciscoAlpsMIBNotificationPrefix	6	6	CISCO-ALPS-MIB
□ alpsCktStatusChange	ciscoAlpsMIBNotificationPrefix	6	2	CISCO-ALPS-MIB
□ alpsPeerConnStatusCha...	ciscoAlpsMIBNotificationPrefix	6	4	CISCO-ALPS-MIB
□ alpsPeerStatusChange	ciscoAlpsMIBNotificationPrefix	6	1	CISCO-ALPS-MIB
□ atmIntfPvcFailuresTrap	atmPvcTraps	6	1	CISCO-IETF-ATM2-PV...
□ authenticationFailure	snmp	4	0	SNMPv2-MIB

2 Select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog appears and provides a message about the import results.

Note: Traps that already exist in the database are not imported.

Tip: Use the dialog's scroll bar to scan available traps.

Extending WhatsUp Gold with custom scripting

In This Chapter

Extending WhatsUp Gold with scripting

This section explains how to use the native development tools included in WhatsUp Gold to extend the product beyond its stock capabilities with Active Script Active Monitors, Performance Monitors, and Actions.

WhatsUp Gold includes three types of Active Scripts, which allow you to write custom JScript and VBScript code to do tasks that WhatsUp Gold cannot natively perform.

- **Active Script Active Monitors** perform specific customized checks on a device. They report their status as a success or failure, and the monitor's status effects the device's status in the same way that stock active monitors do. For more information, see *Scripting Active Monitors* (on page 513).
- **Active Script Performance Monitors** track specific values over time and can be used to generate logs and graphs of historical data. For more information, see *Scripting Performance Monitors* (on page 529).
- **Active Script Actions** can be configured to trigger when an active monitor's state changes. They can be programmed to perform a variety of tasks, from running automated remediation scripts to posting data to external, third party services via API. For more information, see *Scripting Actions* (on page 539).

About Active Script languages

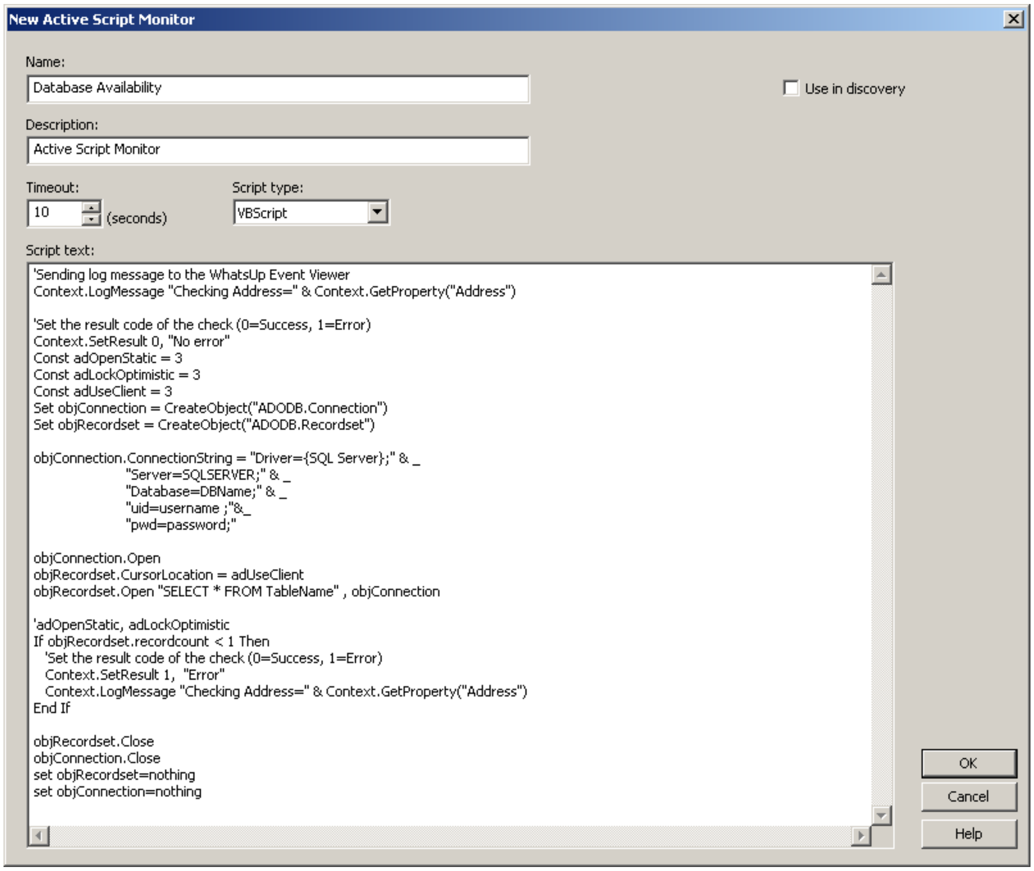
Active scripts can be written in JScript or VBScript. For more information on either of these languages, consult the MSDN Language Reference for that language.

- *MSDN JScript User's Guide* (http://www.whatsupgold.com/msdnjscript)
- *MSDN VBScript User's Guide* (http://www.whatsupgold.com/msdnvbscript)

Note: Not all aspects of JScript and VBScript can be used in Active Scripts. In general, any function or method that involves the user interface level, such as VBScript's `MsgBoxes` or JScript's `alert()`, are not allowed.

Scripting Active Monitors

Active Script Active Monitors perform specific customized checks on a device. They report their status as a success or failure, and the monitor's status effects the device's status in the same way that stock active monitors do.



Name: Database Availability

Description: Active Script Monitor

Timeout: 10 (seconds)

Script type: VBScript

Script text:

```
'Sending log message to the WhatsUp Event Viewer
Context.LogMessage "Checking Address=" & Context.GetProperty("Address")

'Set the result code of the check (0=Success, 1=Error)
Context.SetResult 0, "No error"
Const adOpenStatic = 3
Const adLockOptimistic = 3
Const adUseClient = 3
Set objConnection = CreateObject("ADODB.Connection")
Set objRecordset = CreateObject("ADODB.Recordset")

objConnection.ConnectionString = "Driver={SQL Server};" & _
                "Server=SQLSERVER;" & _
                "Database=DBName;" & _
                "uid=username ;"&_
                "pwd=password;"

objConnection.Open
objRecordset.CursorLocation = adUseClient
objRecordset.Open "SELECT * FROM TableName" , objConnection

'adOpenStatic, adLockOptimistic
If objRecordset.recordcount < 1 Then
  'Set the result code of the check (0=Success, 1=Error)
  Context.SetResult 1,  "Error"
  Context.LogMessage "Checking Address=" & Context.GetProperty("Address")
End If

objRecordset.Close
objConnection.Close
set objRecordset=nothing
set objConnection=nothing
```

Keep In Mind

- You need to include error handling in your monitor script. You must use `Context.SetResult` to report the status of the script to WhatsUp Gold.
- Errors from this active monitor appear in EventViewer.exe.

Using the context object with active monitors

The context object provides an interface for your script to interact with WhatsUp Gold.

All methods and properties are retrieved using the `Context` namespace.

Methods	Method description
`LogMessage(sText);`	This method allows for a message to be written to the WhatsUp Gold debug log. **Example**

JScript

```
Context.LogMessage( "Checking Monitor name using
Context.GetProperty()");
```

VBScript

```
Context.LogMessage "Checking Address using
Context.GetProperty()"
```

`PutProperty(sPropertyName);`

This method allows you to store a value in the INMSerialize object. This value is retained across polls.

Example

JScript

```
var nCount = parselnt(nNum) +1;
Context.PutProperty("MyNumeric",nCount);
```

`SetResult(nCode, sText);`

This method allows for a result code and result message to be set. This is how you can tell the WhatsUp Gold system if the monitor succeeded or not.

Every script should call SetResult. If SetResult is not called, the script is always assumed to have succeeded.

Example

JScript

```
Context.SetResult(0, "Script completed successfully.");
//Success
Context.SetResult(1, "An error occurred."); //Failure
```

VBScript

```
Context.SetResult 1, "An error occurred."
```

`GetProperty(sPropertyName);` This method offers access to any of the device properties listed below. These names are case sensitive.

Property	Description
"ActiveMonitorTypeName"	The active monitor display name
"Address"	The IP address of the device
"DeviceID"	The device ID
"Mode"	1 = doing discovery 2 = polling 3 = test
"ActiveMonitorTypeID"	The active monitor's type ID
"CredSnmpV1:ReadCommunity"	SNMP V1 Read community
"CredSnmpV1:WriteCommunity"	SNMP V1 Write community
"CredSnmpV2:ReadCommunity"	SNMP V2 Read community
"CredSnmpV2:WriteCommunity"	SNMP V2 Write community
"CredSnmpV3:Username"	SNMP V3 Username
"CredSnmpV3:Context"	SNMP V3 Context
"CredSnmpV3:AuthPassword"	SNMP V3 Authentication password
"CredSnmpV3:AuthProtocol"	SNMP V3 Authentication protocol
"CredSnmpV3:EncryptPassword"	SNMP V3 Encrypt password
"CredSnmpV3:EncryptProtocol"	SNMP V3 Encrypt protocol
"CredWindows:DomainAndUserid"	Windows Domain and User ID
"CredWindows:Password"	Windows NT Password

Example

JScript

```
var sAddress = Context.GetProperty("Address");
var sReadCommunity =
Context.GetProperty("CredSnmpV1:ReadCommunity");
var nDeviceID = Context.GetProperty("DeviceID");
```

Properties

Property	Description
`GetDB;`	This property returns an open connection to the WhatsUp Gold database.

Example active script active monitors

These scripts demonstrate a few potential uses of Active Script Active Monitors. To view other Active Script Active Monitors created by other WhatsUp Gold users, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

§ *Monitoring printer ink level and utilization* (on page 516)

§ *Alert when temperature exceeds or drops out of range* (on page 517)

§ *Determine invalid user account activity* (on page 518)

§ *Monitor bandwidth utilization on an interface* (on page 523)

§ *Monitor an SNMP agent running on a non standard port* (on page 525)

§ *Monitor for unknown MAC addresses* (on page 526)

Monitoring printer ink level and utilization

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This active monitor polls an object of the printer mib to gather the ink level information and then computes the ink percent utilization of a printer.

The active monitor will fire an alert if the utilization exceeds a value set on the first line of the script.

Note: This script was tested on an HP MIB.

Run the SNMP MIB Walker net tool to check the OIDs of the two polled objects and eventually adjust their instance (1.1 in this example):

1.3.6.1.2.1.43.11.1.1.8.1.1 and 1.3.6.1.2.1.43.11.1.1.9.1.1.

Note: This script is included as a code example only. The Printer Active Monitor should be used to monitor printers.

```
var nMarkerPercentUtilization = 70; // This monitor will fail if the printer ink
utilization is above this value %.
```

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed) {
    Context.SetResult(1, oComResult.GetErrorMsg);
}
else {
    // poll the two counters
    Context.LogMessage("Polling marker maximum level");
    var oResponse = oSnmpRqst.Get("1.3.6.1.2.1.43.11.1.1.8.1.1");
    if (oResponse.Failed) {
        Context.SetResult(1, oResponse.GetErrorMsg);
    }
    var prtMarkerSuppliesMaxCapacity = oResponse.GetValue;
    Context.LogMessage("Success. Value=" + prtMarkerSuppliesMaxCapacity);

    Context.LogMessage("Polling marker current level");
    oResponse = oSnmpRqst.Get("1.3.6.1.2.1.43.11.1.1.9.1.1");
    if (oResponse.Failed) {
        Context.SetResult(1, oResponse.GetErrorMsg);
    }
    var prtMarkerSuppliesLevel = oResponse.GetValue;
    Context.LogMessage("Success. Value=" + prtMarkerSuppliesLevel);

    var nPercentUtilization = 100 * prtMarkerSuppliesLevel /
prtMarkerSuppliesMaxCapacity;

    if (nPercentUtilization > nMarkerPercentUtilization) {
        Context.SetResult(1, "Failure. Current Utilization (" + (nPercentUtilization +
"%) is above the configured threshold (" + nMarkerPercentUtilization) + "%)");
    }
    else {
        Context.SetResult(0, "Success. Current Utilization (" + (nPercentUtilization +
"%) is below the configured threshold (" + nMarkerPercentUtilization) + "%)");
    }
}
```

Alert when temperature exceeds or drops out of range

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This active monitor polls an SNMP-enabled temperature sensor. If the temperature exceeds or drops below the configured acceptable range, an alert is fired.

```
// This jscript script polls the temperature from an snmp-enabled sensor from "uptime
devices" (www.uptimedevices.com),
// and makes sure the temperature is within an acceptable range configured right below.
// The OID of the temperature object for that device is
1.3.6.1.4.1.3854.1.2.2.1.16.1.14.1
var nMinAllowedTemp = 65;
var nMaxAllowedTemp = 75;
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed) {
    Context.SetResult(1, oComResult.GetErrorMsg);
}
else {
    // poll the two counters
    Context.LogMessage("Polling the temperature");
    var oResponse = oSnmpRqst.Get("1.3.6.1.4.1.3854.1.2.2.1.16.1.14.1");
    if (oResponse.Failed) {
        Context.SetResult(1, oResponse.GetErrorMsg);
    }
    else {
        var nTemperature = oResponse.GetValue / 10.0;
        // comment out the following line to convert the temperature to Celcius degrees
        //nTemperature = (nTemperature - 32) * 5 / 9;
        Context.LogMessage("Success. Value=" + nTemperature + " degrees");

        if (nTemperature < nMinAllowedTemp || nTemperature > nMaxAllowedTemp) {
            Context.SetResult(1, "Polled temperature " + nTemperature + " is outside of
the defined range " + nMinAllowedTemp + " - " + nMaxAllowedTemp);
        }
        else {
            Context.SetResult(0, "Success");
        }
    }
}
```

Determine invalid user account activity

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This active monitor will change a device's state to Down if an invalid, or unexpected user account logs on. The monitor will stay up if the valid, expected account is logged on, or if no one is logged on.

```
sComputer = Context.GetProperty("Address")
nDeviceID = Context.GetProperty("DeviceID")

'Assuming ICMP is not blocked and there's a ping monitor on the
device, we want to
'perform the actual check only if the Ping monitor is up.
ConnectServer method of
'the SWbemLocator has a long time out so it would be good to avoid
unnecessary tries.
'Please note: there's no particular polling order of active
monitors on a device.
'During each polling cycle, it's possible that this monitor could
be polled before
'Ping is polled. If the network connection just goes down but Ping
is not polled yet,
'and therefore still has an up state, this active monitor will
still do an actual
'check and experience a real down. But for the subsequent polls, it
won't be doing a
'real check (ConnectServer won't be called) as Ping monitor has a
down state, and this
'monitor will be assumed down.
If IsPingUp(nDeviceID) = false Then
      Context.SetResult 1,"Actual check was not performed due to
ping being down. Automatically set to down."
Else
      sAdminName =
Context.GetProperty("CredWindows:DomainAndUserid")
      sAdminPasswd = Context.GetProperty("CredWindows:Password")
      sLoginUser = GetCurrentLoginUser(sComputer, sAdminName,
sAdminPasswd)
      sExpectedUser = "administrator"

      If Not IsNull(sLoginUser) Then
            If instr(1,sLoginUser, sExpectedUser,1) > 0  Then
```

```
                  Context.SetResult 0,"Current login user is " &
sLoginUser
            ElseIf sLoginUser = " " Then
                  Context.SetResult 0,"No one is currently logged
in."
            Else
                  Context.SetResult 1,"an unexpected user " &
sLoginUser & " has logged in " & sComputer
            End If
      End If
End If

'Check if Ping monitor on the device specified by nDeviceID is up.
'If nDeviceID is not available as it's in the case during
discovery, then assume
'ping is up.
'If ping monitor is not on the device, then assume it's up so the
real check will be
'performed.
Function IsPingUp(nDeviceID)
      If nDeviceID > -1 Then
            'get the Ping monitor up state.
            sSqlGetUpState = "SELECT sStateName from
PivotActiveMonitorTypeToDevice as P join " & _
            "ActiveMonitorType as A on
P.nActiveMonitorTypeID=A.nActiveMonitorTypeID " & _
            "join MonitorState as M on P.nMonitorStateID =
M.nMonitorStateID " & _
            "where nDeviceID=" & nDeviceID & " and
A.sMonitorTypeName='Ping' and " & _
            " P.bRemoved=0"

            Set oDBconn = Context.GetDB
            Set oStateRS = CreateObject("ADODB.Recordset")
            oStateRS.Open sSqlGetUpState,oDBconn,3
            'if recordset is empty then
            If oStateRS.RecordCount = 1 Then
                  If instr(1,oStateRS("sStateName"),"up",1) > 0 Then
                        IsPingUp = true
                  Else
                        IsPingUP = false
                  End If
            Else
                  'if there's no ping on the device, then just
assume up, so regular check will happen.
                  IsPingUp= true
            End If

            oStateRS.Close
            oDBconn.Close
            Set oStateRS = Nothing
            Set oDBconn = Nothing

      Else
            'assume up, since there's no device yet. It's for
scanning during discovery.
            IsPingUP = true
      End If
End Function

'Try to get the current login user name.
Function GetCurrentLoginUser(sComputer, sAdminName, sAdminPasswd)
      GetCurrentLoginUser=Null
      Set oSWbemLocator = CreateObject("WbemScripting.SWbemLocator")
      On Error Resume Next
      Set oSWbemServices = oSWbemLocator.ConnectServer _
      (sComputer, "root\cimv2",sAdminName,sAdminPasswd)

      If Err.Number <> 0 Then
```

```
            Context.LogMessage("The 1st try to connect to " &
sComputer & " failed. Err:" & Err.Description)
            Err.Clear
            'If the specified user name and password for WMI
connection failed, then
            'try to connect without user name and password. Can't
specify user name
            'and password when connecting to local machine.
            On Error Resume Next
            Set oSWbemServices =
oSWbemLocator.ConnectServer(sComputer, "root\cimv2")

            If Err.Number <> 0 Then
                  Err.Clear
                  On Error Resume Next
                  Context.SetResult 1,"Failed to access " &
sComputer & " " & _
                  "using username:" & sAdminName & " password."  & "
Err:  " &  Err.Description
                  Exit Function
            End If

      End If

      Set colSWbemObjectSet =
oSWbemServices.InstancesOf("Win32_ComputerSystem")

      For Each oSWbemObject In colSWbemObjectSet
            On Error Resume Next
            'Context.SetResult 0,"User Name: " &
oSWbemObject.UserName & " at " & sComputer
            sCurrentLoginUser = oSWbemObject.UserName
            Err.Clear
      Next
```

```
        If Cstr(sCurrentLoginUser) ="" Then
              GetCurrentLoginUser = " "
        Else
              GetCurrentLoginUser = sCurrentLoginUser
        End If

        Set oSWbemServices = Nothing
        Set oSWbemLocator = Nothing

End Function
```

Monitor bandwidth utilization on an interface

> **Note**: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This active monitor is used to monitor the total bandwidth utilization (both in and out octets) of an interface by polling values of the interface MIB.

```
// Settings for this monitor:
// the interface index ifIndex:
var nInterfaceIndex = 65540;

// this monitor will fail if the interface utilization goes above this current ratio:
// current bandwidth / maxBandwidth > nMaxInterfaceUtilizationRatio
var nMaxInterfaceUtilizationRatio = 0.7; // Set to 70%

// Create an SNMP object, that will poll the device.
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");

// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");

// This function polls the device returns the ifSpeed of the inteface indexed by
nIfIndex.
// ifSpeed is in bits per second.
function getIfSpeed(nIfIndex) {
    var oResult = oSnmpRqst.Initialize(nDeviceID);
    if (oResult.Failed) {
        return null;
    }
    return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.5." + nIfIndex)); // ifSpeed
}
// Function to get SNMP ifInOctets for the interface indexed by nIfIndex (in bytes).
// Returns the value polled upon success, null in case of failure.
function getInOctets(nIfIndex) {
    var oResult = oSnmpRqst.Initialize(nDeviceID);
    if (oResult.Failed) {
        return null;
    }
    return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.10." + nIfIndex)); // inOctets
}

// Function to get SNMP ifOutOctets for the interface indexed by nIfIndex (in bytes).
// Returns the value polled upon success, null in case of failure.
function getOutOctets(nIfIndex) {
    var oResult = oSnmpRqst.Initialize(nDeviceID);
    if (oResult.Failed) {
        return null;
    }
    return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.16." + nIfIndex)); //  outOctets
}

// Helper function to get a specific SNMP object (OID in sOid).
// Returns the value polled upon success, null in case of failure.
function SnmpGet(sOid) {
    var oResult = oSnmpRqst.Get(sOid);
    if (oResult.Failed) {
        return null;
    }
    else {
        return oResult.GetPayload;
    }
}

// Get the current date. It will be used as a reference date for the SNMP polls.
var oDate = new Date();
var nPollDate = parseInt(oDate.getTime()); // get the date in millisec in an integer.
// Do the actual polling:
var nInOctets = getInOctets(nInterfaceIndex);
var nOutOctets = getOutOctets(nInterfaceIndex);
var nIfSpeed = getIfSpeed(nInterfaceIndex);
if (nInOctets == null || nOutOctets == null || nIfSpeed == null) {
    Context.SetResult(1, "Failure to poll this device.");
}
else {
    var nTotalOctets = nInOctets + nOutOctets;
    // Retrieve the octets value and date of the last poll saved in a context variable:
    var nInOutOctetsMonitorPreviousPolledValue =
Context.GetProperty("nInOutOctetsMonitorPreviousPolledValue");
    var nInOutOctetsMonitorPreviousPollDate =
Context.GetProperty("nInOutOctetsMonitorPreviousPollDate");
    if (nInOutOctetsMonitorPreviousPolledValue == null ||
nInOutOctetsMonitorPreviousPollDate == null) {
        // the context variable has never been set, this is the first time we are
polling.
        Context.LogMessage("This monitor requires two polls.");
        Context.SetResult(0, "success");
    }
    else {
        // compute the bandwidth that was used between this poll and the previous poll
        var nIntervalSec = (nPollDate - nInOutOctetsMonitorPreviousPollDate) / 1000; //
time since  last poll in seconds
        var nCurrentBps = (nTotalOctets - nInOutOctetsMonitorPreviousPolledValue) * 8 /
nIntervalSec;
        Context.LogMessage("total octets for interface " + nInterfaceIndex + " = " +
nTotalOctets);
        Context.LogMessage("previous value = " + nInOutOctetsMonitorPreviousPolledValue);
        Context.LogMessage("difference: " + (nTotalOctets -
nInOutOctetsMonitorPreviousPolledValue) + " bytes");
        Context.LogMessage("Interface Speed: " + nIfSpeed + "bps");
        Context.LogMessage("time elapsed since last poll: " + nIntervalSec + "s");
        Context.LogMessage("Current Bandwidth utilization: " + nCurrentBps + "bps");
        if (nCurrentBps / nIfSpeed > nMaxInterfaceUtilizationRatio) {
            Context.SetResult(1, "Failure: bandwidth used on this interface " +
nCurrentBps + "bps / total available: " + nIfSpeed + "bps is above the specified ratio: "
+ nMaxInterfaceUtilizationRatio);
        }
        else {
            Context.SetResult(0, "Success");
        }
    }
    // Save this poll information in the context variables:
    Context.PutProperty("nInOutOctetsMonitorPreviousPolledValue", nTotalOctets);
    Context.PutProperty("nInOutOctetsMonitorPreviousPollDate", nPollDate);
}
```

Monitor an SNMP agent running on a non standard port

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This active monitor watches an SNMP agent running on a non-standard port (the standard SNMP port is 161).

```
var nSNMPPort = 1234; // change this value to the port your agent is running on
var oSnmpRqst =  new ActiveXObject("CoreAsp.SnmpRqst");
// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");

// Initialize the SNMP request object
var oResult = oSnmpRqst.Initialize(nDeviceID);

if(oResult.Failed)
{
Context.SetResult(1, oResult.GetPayload);
}
else
{
        // Set the request destination port.
        var oResult = oSnmpRqst.SetPort(nSNMPPort);

        // Get sysDescr.
        var oResult = oSnmpRqst.Get("1.3.6.1.2.1.1.1.0");
        if (oResult.Failed)
        {
            Context.SetResult(1, "Failed to poll device using port " + nSNMPPort + ".
Error=" + oResult.GetPayload);
        }
        else
        {
            Context.SetResult(0, "SUCCESS. Detected an SNMP agent running on port " +
nSNMPPort );
        }
}
```

Monitor for unknown MAC addresses

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This active monitor watches MAC addresses present on a network by polling an SNMP-managed switch and the bridge MIB. In the example script, you define a list of MAC addresses you will allow to connect to the network. This monitor will fail if it finds devices that do not match the addresses specified in the list.

```
// Modify the list below. It defines a list of allowed mac addresses with mapping to
```

```
switch interface
// on the network.
// This script will poll a managed switch using SNMP and the bridge MIB to detect MAC
addresses present
// on your network that should not be and to detect misplaced machines (connected to the
wrong port).
//
// The MAC addresses should be typed lowercase with no padding using ':' between each
bytes
// for instance "0:1:32:4c:ef:9" and not "00:01:32:4C:EF:09"
//
var arrAllowedMacToPortMapping =  new ActiveXObject("Scripting.Dictionary");
arrAllowedMacToPortMapping.add("0:3:ff:3b:df:1f", 17);
arrAllowedMacToPortMapping.add("0:3:ff:72:5c:bf", 77);
arrAllowedMacToPortMapping.add("0:3:ff:e2:e5:76", 73);
arrAllowedMacToPortMapping.add("0:11:24:8e:e0:a5", 63);
arrAllowedMacToPortMapping.add("0:1c:23:ae:b0:4c", 48);
arrAllowedMacToPortMapping.add("0:1d:60:96:e5:58", 73);
arrAllowedMacToPortMapping.add("0:e0:db:8:aa:a3", 73);

var ERR_NOERROR = 0;
var ERR_NOTALLOWED = 1;
var ERR_MISPLACED = 2;
function CheckMacAddress(sMacAddress, nPort)
{
        sMacAddress = sMacAddress.toLowerCase();

        if (!arrAllowedMacToPortMapping.Exists(sMacAddress))
        {
                return ERR_NOTALLOWED;
        }

        var nAllowedPort = arrAllowedMacToPortMapping.Item(sMacAddress);
        if (nAllowedPort != nPort)
        {
                return ERR_MISPLACED;
        }
        return ERR_NOERROR;
}

var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");

var oComResult = oSnmpRqst.Initialize(Context.GetProperty("DeviceID"));

if (oComResult.Failed)
{
        Context.SetResult(1, oComResult.GetErrorMsg);
}
```

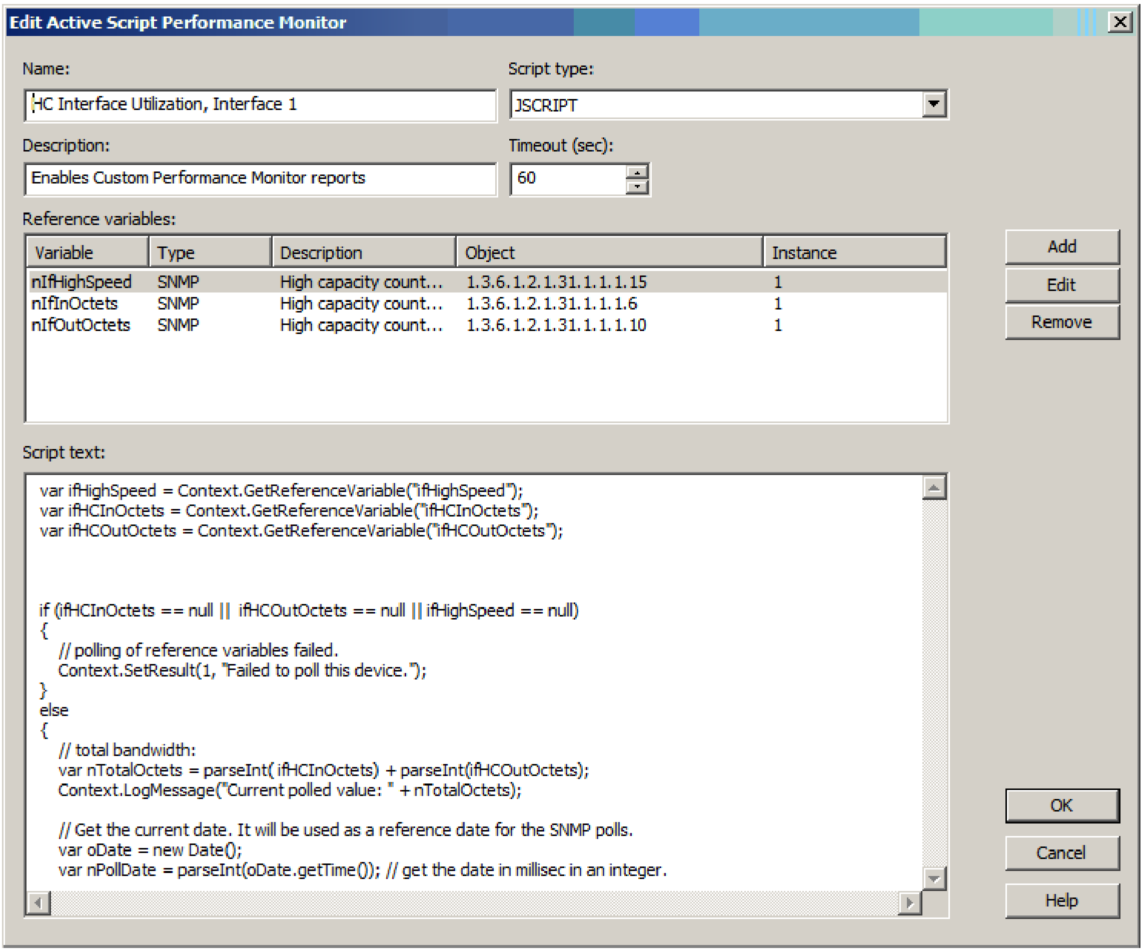
```
else
{
        var DOT1DTOFDBPORT_OID = "1.3.6.1.2.1.17.4.3.1.2";
        var DOT1DTOFDBADDRESS_OID = "1.3.6.1.2.1.17.4.3.1.1";
        var sOid = DOT1DTOFDBPORT_OID
        var bStatus = true;
        var arrMisplacedAddresses = new Array();
        var arrNotAllowedAddresses = new Array();
        var i=0;
        while (i++<1000)
        {
                oComResult = oSnmpRqst.GetNext(sOid);
                if (oComResult.Failed)
                {
                        break;
                }
                sOid = oComResult.GetOID;
                if (sOid.indexOf(DOT1DTOFDBPORT_OID) == -1)
                {
                        // we are done walking
                        break;
                }
                var nPort = oComResult.GetPayload;

                // the last 6 elements of the OID are the MAC address in OId format
                var sInstance = sOid.substr(DOT1DTOFDBPORT_OID.length+1, sOid.length);

                // get it in hex format...
                oComResult = oSnmpRqst.Get(DOT1DTOFDBADDRESS_OID + "." + sInstance);
                if (oComResult.Failed)
                {
                        continue;
                }
                var sMAC = oComResult.GetValue;

                var nError = CheckMacAddress(sMAC, nPort);

                switch (nError)
                {
                case ERR_NOTALLOWED:
                        arrNotAllowedAddresses.push(sMAC + "(" + nPort + ")");
                        break;
                case ERR_MISPLACED:
                        arrMisplacedAddresses.push(sMAC + "(" + nPort + ")");
                        break;
                case ERR_NOERROR:
                default:
                        // no problem
```

```
               }
       }

       //Write the status
       Context.LogMessage("Found " + i + " MAC addresses on your network.");
       if (arrMisplacedAddresses.length > 0)
       {
               Context.LogMessage("Warning: Found " + arrMisplacedAddresses.length + "
misplaced addresses: " + arrMisplacedAddresses.toString());
       }
       if (arrNotAllowedAddresses.length > 0)
       {
               Context.SetResult(1, "ERROR: Found " + arrNotAllowedAddresses.length + "
unknown MAC addresses on your network: " + arrNotAllowedAddresses.toString());
       }
       else
       {
               Context.SetResult(0, "SUCCESS. No anomaly detected on the network");
       }
}
```

Scripting Performance Monitors

Active Script Performance Monitors let you write VBScript and JScript to easily poll one or more SNMP or WMI values, perform math or other operations on those values, and graph a single output value. You should only use the Active Script Performance Monitor when you need to perform calculations on the polled values. Keep in mind that although you can poll multiple values using the feature, only one value will be stored to the database: the outcome of your scripted calculation.

Reference Variables



Name: HC Interface Utilization, Interface 1

Script type: JSCRIPT

Description: Enables Custom Performance Monitor reports

Timeout (sec): 60

Reference variables:

Variable	Type	Description	Object	Instance
nIfHighSpeed	SNMP	High capacity count...	1.3.6.1.2.1.31.1.1.1.15	1
nIfInOctets	SNMP	High capacity count...	1.3.6.1.2.1.31.1.1.1.6	1
nIfOutOctets	SNMP	High capacity count...	1.3.6.1.2.1.31.1.1.1.10	1

Script text:

```
var ifHighSpeed = Context.GetReferenceVariable("ifHighSpeed");
var ifHCInOctets = Context.GetReferenceVariable("ifHCInOctets");
var ifHCOutOctets = Context.GetReferenceVariable("ifHCOutOctets");



if (ifHCInOctets == null ||  ifHCOutOctets == null || ifHighSpeed == null)
{
   // polling of reference variables failed.
   Context.SetResult(1, "Failed to poll this device.");
}
else
{
   // total bandwidth:
   var nTotalOctets = parseInt( ifHCInOctets) + parseInt(ifHCOutOctets);
   Context.LogMessage("Current polled value: " + nTotalOctets);

   // Get the current date. It will be used as a reference date for the SNMP polls.
   var oDate = new Date();
   var nPollDate = parseInt(oDate.getTime()); // get the date in millisec in an integer.
```

Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They take care of the underlying SNMP or WMI mechanisms that you would normally have to use to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable` (variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses a device's credentials to connect to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script.

✓ **Important**: The use of reference variables in the Active Script Performance Monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed.

Keep In Mind

§ You need to include error handling in your monitor script. Your script either needs a value to graph by using `Context.SetValue`, or you must use `Context.SetResult` to tell WhatsUp Gold that the script failed.

- `Context.GetReferenceVariable` will return 'null' if the poll fails for any reason.
- If you do not have a call to `SetValue` or `SetResult`, the script does not report any errors and no data is graphed.
- If `SetValue` is used, it is not necessary to use `SetResult`, as `SetValue` implicitly sets `SetResult` to 0, or "good."
- Results from this performance monitor are displayed on *Custom Performance Monitors* (on page 389) full and dashboard reports.
- Errors from this performance monitor are displayed in the *Performance Monitor Error log* (on page 433) as well as EventViewer.exe.

Using the context object with performance monitors

The context object provides an interface for your script to interact with WhatsUp Gold.

All methods and properties are retrieved using the `Context` namespace.

Note: You may have to remove the copyright information from the cut and paste if it appears when you copy from this help file.

Methods — **Method description**

`LogMessage(sText);`

This method allows for a message to be written to the WhatsUp Gold debug log.

Example

JScript

```
Context.LogMessage( "Checking Monitor name using
Context.GetProperty()");
```

VBScript

```
Context.LogMessage "Checking Address
using Context.GetProperty()"
```

`PutProperty(sPropertyName);`

This method allows you to store a value in the INMSerialize object. This value is retained across polls.

Example

JScript

```
var nCount = parselnt(nNum) +1;
Context.PutProperty("MyNumeric",nCount);
```

`SetResult(nCode, sText);`

This method allows for a result code and result message to be set. This is how you can tell the WhatsUp Gold system if the monitor succeeds or fails.

Every script should call SetResult. If SetResult is not called, the script is always assumed to have succeeded.

Example

JScript

```
Context.SetResult(0, "Script completed
successfully."); //Success
Context.SetResult(1, "An error occurred.");
//Failure
```

VBScript

```
Context.SetResult 1, "An error

occurred."
```

`GetReferenceVariable(sRefVarName);`

This method allows the code to grab a reference variable to be used in the monitor.

Example

JScript

```
Context.GetReferenceVariable("A")
```

A reference variable "A" would have had to have been created.

`SetValue(nValue);`

This method allows you to graph a value.

Example

JScript

```
Context.SetValue(245)
```

`GetProperty(sPropertyName);`

This method offers access to any of the device properties listed below. These names are case sensitive.

Property	Description
"ActiveMonitorTypeName"	The active monitor display name
"Address"	The IP address of the device
"DeviceID"	The device ID
"Mode"	1 = doing discovery 2 = polling 3 = test
"ActiveMonitorTypeID"	The active monitor's type ID
"CredSnmpV1:ReadCommunity"	SNMP V1 Read community
"CredSnmpV1:WriteCommunity"	SNMP V1 Write community
"CredSnmpV2:ReadCommunity"	SNMP V2 Read community
"CredSnmpV2:WriteCommunity"	SNMP V2 Write community
"CredSnmpV3:Username"	SNMP V3 Username
"CredSnmpV3:Context"	SNMP V3 Context
"CredSnmpV3:AuthPassword"	SNMP V3 Authentication password
"CredSnmpV3:AuthProtocol"	SNMP V3 Authentication protocol
"CredSnmpV3:EncryptPassword"	SNMP V3 Encrypt password
"CredSnmpV3:EncryptProtocol"	SNMP V3 Encrypt protocol
"CredWindows:DomainAndUserid"	Windows NT Domain and User ID
"CredWindows:Password"	Windows NT Password

Example

JScript

```
var sAddress = Context.GetProperty("Address");
var sReadCommunity =
Context.GetProperty("CredSnmpV1:ReadCommunity");
var nDeviceID = Context.GetProperty("DeviceID");
```

Example active script performance monitors

These scripts demonstrate a few potential uses of Active Script Performance Monitors. To view other Active Script Performance Monitors created by other WhatsUp Gold users, visit *the WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

- *Graphing printer ink level percent utilization* (on page 534)
- *Poll a reference variable and perform a calculation* (on page 535)
- *Graph a temperature monitor* (on page 536)
- *Poll the storage table using SNMP GetNext* (on page 537)
- *Poll multiple reference variables* (on page 538)

Graphing printer ink level utilization

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This performance monitor uses two reference variables to poll and compute the ink level percent utilization of a printer for later graphing.

Note: This was tested on an HP MIB.

Run the SNMP MIB Walker net tool to check the OIDs of the two reference variables and eventually adjust their instance (1.1 in this example):

1.3.6.1.2.1.43.11.1.1.8.1.1 and 1.3.6.1.2.1.43.11.1.1.9.1.1.

```
// prtMarkerSuppliesLevel is an snmp reference variable defined
with an OID or 1.3.6.1.2.1.43.11.1.9 and an instance of 1.1
// prtMarkerSuppliesMaxCapacity is an snmp reference variable
defined with an OID or 1.3.6.1.2.1.43.11.1.8 and an instance of 1.1

Context.LogMessage("Print the current marker level");
var prtMarkerSuppliesLevel =
Context.GetReferenceVariable("prtMarkerSuppliesLevel");
Context.LogMessage("Print the maximum marker level");
var prtMarkerSuppliesMaxCapacity =
Context.GetReferenceVariable("prtMarkerSuppliesMaxCapacity");
```

```
if (prtMarkerSuppliesMaxCapacity == null || prtMarkerSuppliesLevel
== null) {
    Context.SetResult(0, "Failed to poll printer ink levels.");
}
else {
    Context.LogMessage("marker lever successfully retrieved");
    var nPercentMarkerUtilization = 100 * prtMarkerSuppliesLevel /
prtMarkerSuppliesMaxCapacity;
    Context.LogMessage("Percent utilization=" +
nPercentMarkerUtilization + "%");
    Context.SetValue(nPercentMarkerUtilization);
```

Poll a reference variable and perform a calculation

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This performance monitor polls a reference variable, and then performs an arithmetic calculation with the returned value.

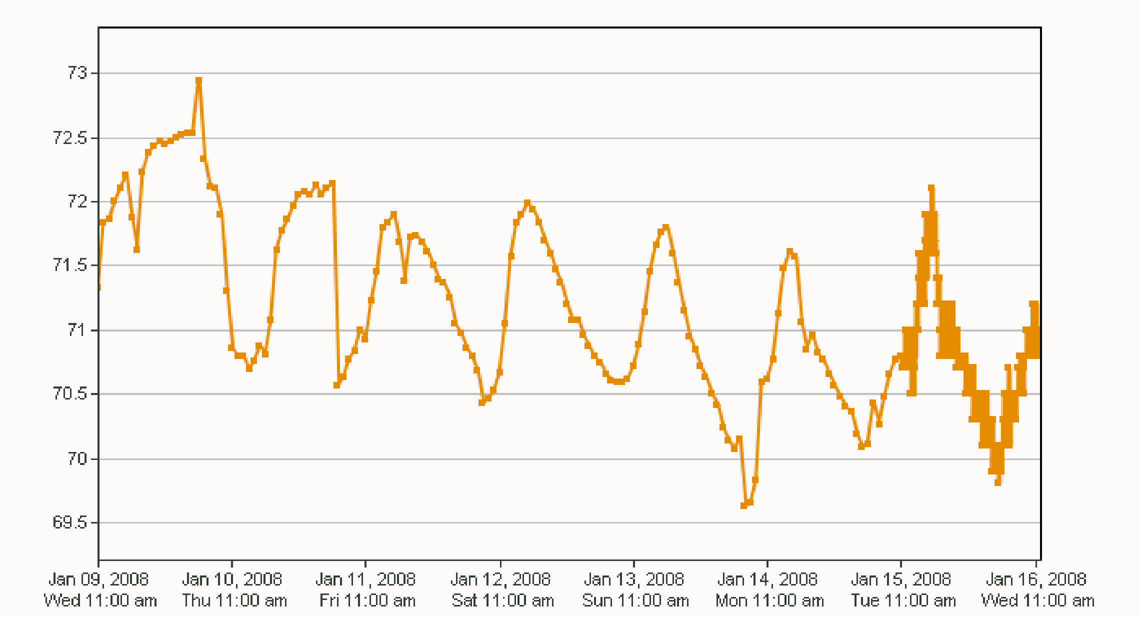
```
// This script is a JScript that demonstrates how to use a reference variable in a
script.
// The reference variable "RVsysUpTime" is an SNMP reference variable defined
// with an OID of 1.3.6.1.2.1.1.3 and instance of 0.

// Poll reference variable RVsysUpTime
var RVsysUpTime = Context.GetReferenceVariable("RVsysUpTime");

if (RVsysUpTime == null) {
    // Pass a non zero error code upon failure with an error message.
    // The error message will be logged in the Performance Monitor Error Log
    // and in the eventviewer.
    Context.SetResult(1, "Failed to poll the reference variable.");
}
else {
    // Success, use the polled value to convert sysUpTime in hours.
    // sysUpTime is an SNMP timestamp which is in hundredths of seconds:
    var sysUpTimeHours = RVsysUpTime / 3600 / 100;
    // Save the final value to graph:
    Context.SetValue(sysUpTimeHours);
}
```

Graph a temperature monitor

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This performance monitor polls an SNMP-enabled temperature sensor using the CurTemp reference variable.

A typical graph for this script:



```
// This script is a JScript script that polls the temperature of an snmp-enabled sensor
from "uptime devices" (www.uptimedevices.com).
// It uses an SNMP reference variable named CurTemp defined with an OID of
1.3.6.1.4.1.3854.1.2.2.1.16.1.14
// and an instance of 1.
//
// That device indicates the temperature in degrees Fahrenheit.

var oCurTemp = Context.GetReferenceVariable("CurTemp");
if (oCurTemp == null) {
    Context.SetResult(1, "Unable to poll Temperature Sensor");
}
else {
    // convert temperature from tenth of degrees to degrees
    var nFinalTemp = oCurTemp / 10.0;
    // comment out the line below to convert the temperature in Celsius degrees:
    //nFinalTemp = (nFinalTemp - 32) * 5 / 9;
    Context.SetValue(nFinalTemp);
}
```

Use SNMP GetNext.

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This performance monitor walks the hrStorageType MIB to find hard disks in the storage table. After a hard disk is found, it obtains indexes of it and polls new objects (the storage size and units).

```
// This scripts walks hrStorageType to find hard disks in the storage table.
// A hard disk as a hrStorageType of "1.3.6.1.2.1.25.2.1.4" (hrStorageFixedDisk).
// Then it gets the indexes of the hard disk in that table and for each index, it polls
two new
// objects in that table, the storage size and the units of that entry.
// It adds everything up and converts it in Gigabytes.
var hrStorageType = "1.3.6.1.2.1.25.2.3.1.2";

// Create and initialize the snmp object
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oResult = oSnmpRqst.Initialize(nDeviceID);

var arrIndexes = new Array(); // array containing the indexes of the disks we found
// walk the column in the table:
var oSnmpResponse = oSnmpRqst.GetNext(hrStorageType);
if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload);
var sOid = String(oSnmpResponse.GetOid);
var sPayload = String(oSnmpResponse.GetPayload);

while (!oSnmpResponse.Failed && sOid < (hrStorageType + ".99999999999"))
{
    if (sPayload == "1.3.6.1.2.1.25.2.1.4") {
        // This storage entry is a disk, add the index to the table.
        // the index is the last element of the OID:
        var arrOid = sOid.split(".");
        arrIndexes.push(arrOid[arrOid.length - 1]);
    }

    oSnmpResponse = oSnmpRqst.GetNext(sOid);
    if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload);
    sOid = String(oSnmpResponse.GetOid);
    sPayload = String(oSnmpResponse.GetPayload);
}
Context.LogMessage("Found disk indexes: " + arrIndexes.toString());
if (arrIndexes.length == 0) Context.SetResult(1, "No disk found");

// now that we have the indexes of the disks. Poll their utilization and units
var nTotalDiskSize = 0;
for (var i = 0; i < arrIndexes.length; i++) {

    oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.25.2.3.1.5." + arrIndexes[i])
    if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload);
    nSize = oSnmpResponse.GetPayload;
    oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.25.2.3.1.4." + arrIndexes[i])
    if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload);
    nUnits = oSnmpResponse.GetPayload;

    nTotalDiskSize += (nSize * nUnits);
}
// return the total size in gigabytes.
Context.SetValue(nTotalDiskSize / 1024 / 1024 / 1024); // output in Gigabytes
```

Poll multiple reference variables

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

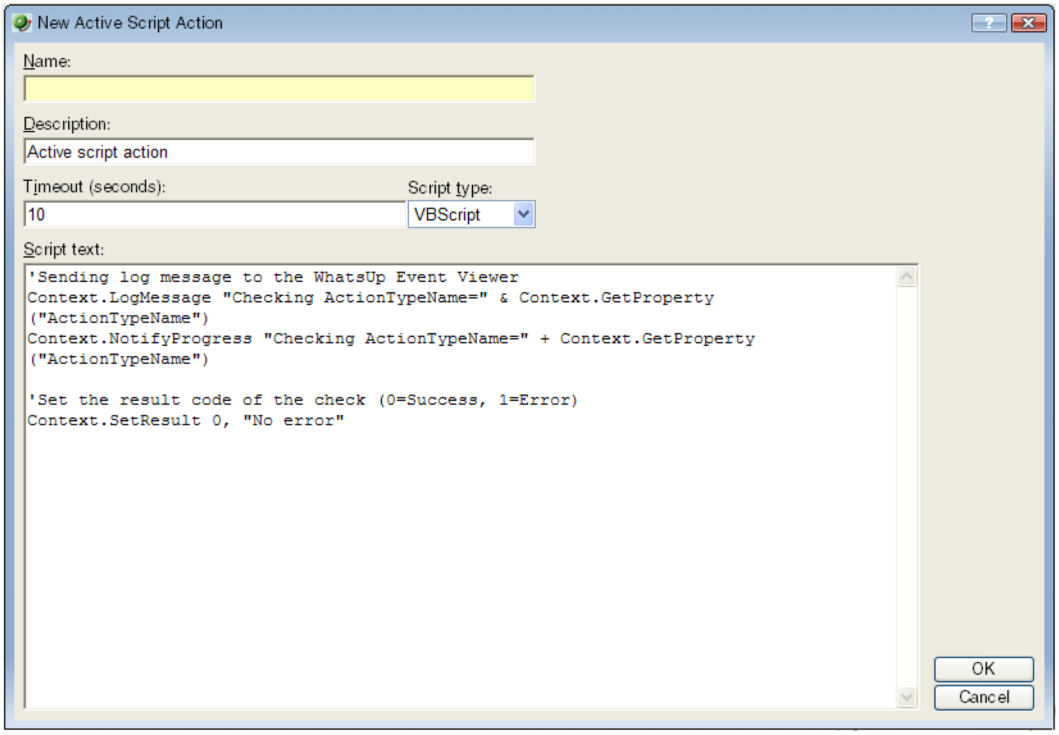
This performance monitor graphs the percentage of retransmitted TCP segments over time using two reference variables: RVtcpOytSegs and RVtcpRetransSegs.

```
// This script is a JScript that will allow you to graph the percentage of restransmitted
TCP
//' segments over time on a device.
// For this script, we use two SNMP reference variables:
//' The first Reference variable RVtcpOutSegs is defined with OID 1.3.6.1.2.1.6.11 and
instance 0. It polls the
//' SNMP object tcpOutSegs.0, the total number of tcp segments sent out on the network.
var RVtcpOutSegs = parseInt(Context.GetReferenceVariable("RVtcpOutSegs"));

// The second reference variable RVtcpRetransSegs is defined with OID 1.3.6.1.2.1.6.12
and instance 0. It polls
// the SNMP object tcpRetransSegs.0, the total number of TCP segments that were
retransmitted on the system.
var RVtcpRetransSegs = parseInt(Context.GetReferenceVariable("RVtcpRetransSegs"));
```

```
if (isNaN(RVtcpRetransSegs) || isNaN(RVtcpOutSegs)) {
    Context.SetResult(1, "Failed to poll the reference variables.");
}
else {
    // Compute the percentage:
    var TCPRetransmittedPercent = 100 * RVtcpRetransSegs / RVtcpOutSegs;
    // Set the performance monitor value to graph
    Context.SetValue(TCPRetransmittedPercent);
}
```

Scripting Actions

Active Script Actions can be configured to trigger when an active monitor's state changes. They can be programmed to perform a variety of tasks, from running automated remediation scripts to posting data to external, third party services via API.



Name:

Description: Active script action

Timeout (seconds): 10

Script type: VBScript

Script text:

```
'Sending log message to the WhatsUp Event Viewer
Context.LogMessage "Checking ActionTypeName=" & Context.GetProperty
("ActionTypeName")
Context.NotifyProgress "Checking ActionTypeName=" + Context.GetProperty
("ActionTypeName")

'Set the result code of the check (0=Success, 1=Error)
Context.SetResult 0, "No error"
```

Keep In Mind

- You need to include error handling in your monitor script. Your script must use `Context.SetResult` to report the status of the action to WhatsUp Gold.
- Your script should check periodically to see if it has been canceled by the user. To do this, use the `IsCancelled()` method described in Using the Context object with Actions.

Using the context object with actions

The context object provides an interface for your script to interact with WhatsUp Gold.

All methods and properties are retrieved using the `Context` namespace.

> **Note**: You may need to remove the copyright information from the cut and paste if it appears when you copy from this help file.

Method	Method description

`LogMessage(sText);`	This methods allows for a message to be written to the WhatsUp Gold debug log. Messages are displayed in the Event Viewer.
	Example
	JScript
	`Context.LogMessage( "Checking action name using Context.GetProperty()");`
	VBScript
	`Context.LogMessage "Checking Address using Context.GetProperty()"`

`SetResult(LONG nCode, sText);`	This method allows for a result code and result message to be set. This is how you can tell the WhatsUp Gold system if the action succeeded or failed.
	Example
	JScript
	`Context.SetResult(0, "Script completed successfully."); //Success`
	`Context.SetResult(1, "An error occurred."); //Failure`
	VBScript
	`Context.SetResult 1, "An error occurred."`

`NotifyProgress(sText);`	This method allows for a message to be written to the actions progress dialog. Messages are displayed in the Test dialog and Running Actions dialog. **Example** JScript `Context.NotifyProgress( "Checking action name using Context.GetProperty()");` VBScript

```
Context.NotifyProgress "Checking Address
using Context.GetProperty()"
```

`IsCancelled();`	This method tests whether the action has been canceled by the user. If the return is true, then the script should terminate. A cancel can be issued by the user in the action progress dialog and by the WhatsUp Gold engine when shutting down.
`GetProperty(sPropertyName);`	This property offers access to many device specific aspects. You obtain access to these items using the names listed. Theses names are case sensitive.

`"ActionName"`	The action display name
`"Address"`	The IP Address of the device
`"Name"`	Network name of the device
`"DisplayName"`	Display name of the device
`"DeviceID"`	The device ID
`"ActionTypeID"`	The action type ID
`"TriggerCondition"`	The reason the action was fired. **Trigger values:** 1 Monitor changed from DOWN to UP 2 Monitor changed from UP to DOWN 4 A Passive Monitor was received... 8 The "Test" Button was hit 16 This is a recurring action... 32 Device is UP 64 Device is DOWN

Example

JScript

```
var sAddress = Context.GetProperty("Address");
var nDeviceID = Context.GetProperty("DeviceID");
```

Example active script actions

These scripts demonstrate a few potential uses of Active Script Actions. To view other Active Script Actions created by other WhatsUp Gold users, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

§ *Post device status to Twitter* (on page 542)

§ *Acknowledge all devices* (on page 543)

Post device status to Twitter

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This action posts the status of the device to which it's applied to the microblogging service Twitter. This is useful for creating an externally viewable and off-site list of device status.

```
Dim xml
Set xml = createObject("Microsoft.XMLHTTP")

'Update to include your account's username and password.
sUser = "username"
sPass = "password"

sStatus = "WhatsUp Gold says, '%Device.DisplayName %Device.State at
%System.Time on %System.Date'"

xml.Open "POST", "http://" & sUser & ":" & sPass &
"@twitter.com/statuses/update.xml?status=" & sStatus, False
xml.setRequestHeader "Content-Type", "content=text/html;
charset=iso-8859-1"
xml.Send

Context.SetResult 0, xml.responseText
Set xml = Nothing
```

Acknowledge all devices

Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (http://www.whatsupgold.com/wugspace).

This action resets the acknowledge flag on all devices. When a device is unacknowledged, the label on its icon renders as white text on black. If you don't use the acknowledge feature, this action can be used to make sure that icons always show as acknowledged.

```
// This JScript action sets the acknowledge flag to true for all devices.
// Written by Tim Schreyack of Dynamics Research Corporation

// Get the database info
var oDb = Context.GetDB;

if (null == oDb) {
   Context.SetResult( 1, "Problem creating the DB object");
}
else {
  var sSql = "UPDATE ActiveMonitorStateChangeLog SET bAcknowledged = 1 WHERE
bAcknowledged = 0";
  var oRs = oDb.Execute(sSql);
  var sSql = "UPDATE Device SET nUnAcknowledgedActiveMonitors = 0 WHERE
nUnAcknowledgedActiveMonitors = 1";
  var oRs = oDb.Execute(sSql);
  var sSql = "UPDATE Device SET nUnAcknowledgedPassiveMonitors = 0 WHERE
nUnAcknowledgedPassiveMonitors = 1";
  var oRs = oDb.Execute(sSql);
}
```

APPENDIX A

Using the SNMP API

The WhatsUp Gold SNMP COM API has been enhanced to improve the performance of your scripted monitors and actions. With the addition of `GetMultiple`, you have the ability to get multiple OIDs within a single SNMP request. `GetNext` issues the SNMP GetNext command to retrieve the value of the object that follows a specified object. Finally, the addition of the `SetFunction` allows you to send SNMP set commands to your SNMP manageable devices.

The SNMP API includes the following objects:

- `CoreAsp.SnmpRqst`. The main SNMP object used to send SNMP requests (Get, GetNext, Set) to a remote device.
- `CoreAsp.ComResult`. An object returned by certain methods of the SnmpRqst object to indicate success or failure.
- `CoreAsp.ComResponse`. A response object returned by certain methods of the SnmpRqst object that contain the status (either error or success) of an SNMP request and the value of the polled object(s).

> **Note**: There are several things to keep in mind when attempting to use the SNMP API. If you are experiencing errors, please see *Troubleshooting the SNMP API* (on page 551).

CoreAsp.SnmpRqst

This object is used to send SNMP requests to a remote device.

`Initialize` or `Initialize2` must be called prior to any other members.

CoreAsp.SnmpRqst uses a three step process:

1. Calls `Initialize` or `Initialize2` to initialize the object against a particular device.
2. Sets optional parameters such as timeout value, port, etc.
3. Performs any number of `Get`, `GetNext`, `GetMultiple` or `Set` operations against a device. Those operations return an `ComSnmpResponse` object that contains the status of the operation and the value either directly (use `Failed/GetValue/GetOid`) or as a list of SNMP variable binding returned as XML data (use `GetPayload`).

Method	Description	Returns
Initialize(`nDeviceID`)	Initializes the `SnmpRqst` object for the device with the device ID specified in `nDeviceID`. If a device is not configured with a valid SNMP credential, the operation will fail. § `nDeviceID`. A positive integer	ComResult object

Method	Description	Returns
	corresponding to the device ID of a device configured in WhatsUp Gold. **Tip**: In Active Script Monitor and Script Performance Monitors, the device ID of the device to which the monitor is assigned can be obtained from the Context object: `Context.GetProperty("DeviceID")`	

Initialize2(
`sDeviceAddress,`
`nCredentialID`
)
	Initializes the `SnmpRqst` object by creating a connection to a device using the IP address of a device and a credential stored in WhatsUp Gold. This method can be used to initialize `SnmpRqst` for a device that is not configured in WhatsUp Gold as long as the credentials for the device are configured in the credential library.
	§ `sDeviceAddress`. The address or hostname of the device to be queried.
	§ `nCredentialID`. A positive integer corresponding to the credential ID of a credential configured in WhatsUp Gold.
		ComResult object

SetTimeoutMs(`nTimeoutInMilliSec`)	Sets the timeout value in milliseconds. If not specified, the timeout defaults to 2000 milliseconds. `nTimeoutInMilliSec`. A positive integer representing the number of milliseconds after which unresolved requests should be terminated. **Note**: This method returns a value if the method fails and requires an object variable to capture this value. For example: `varComResult = SnmpRqst.SetTimeoutMs(5000)`; where `varComResult` is a ComResult object.	ComResult object
SetNumRetries(`nNumberRetries`)	Sets the number of times to retry a request that has timed out. If not specified, failed requests are retried one time. § `nNumberRetries`. A positive integer representing the number of times to retry timed out requests. **Tip**: To send only one SNMP packet per request, set `nNumberRetries` to `0` (zero).	ComResult object
SetPort(`nPort`	Sets the TCP/IP port to be used by `SnmpRqst`. If not specified, port 161 is used.	ComResult object

Method	Description	Returns
)	§ `nPort`. A positive integer between 1 and 65535 corresponding to the port to be used.	
Get(`sOid`)	Issues an SNMP Get command to retrieve the value of the specified object. § `sOid`. A string containing a valid OID.	ComSnmpResponse object
GetNext(`sOid`)	Issues an SNMP GetNext command to retrieve the value of the object that follows the specified object in lexicographic order. § `sOid`. A string containing a valid OID.	ComSnmpResponse object
GetMultiple(`sListOfOids`)	Issues an SNMP Get command for each of the objects specified. `GetMultiple` sends all commands in a single SNMP protocol data unit, so it is more efficient than issuing multiple `Get` commands independently. § `sListOfOids`. A comma-separated list of valid OIDs.	ComSnmpResponse object
Set(`sOid`, `sType`, `sValue`)	Issues an SNMP Set command to set an OID value on a device. § `sOid`. A string containing a valid OID for the object for which you want to set the value. § `sType`. A single character corresponding to the type of value to set. `i` = integer `u` = unsigned integer `s` = string `x` = hexadecimal string `d` = decimal string `n` = NULL object `o` = object ID `t` = timeticks `a` = IPv4 address `b` = bits § `sValue`. A string containing the value to set.	ComSnmpResponse object

Note: The Set function will not work unless the MIB object and the community string for the device have the Read Write access right.

CoreAsp.ComResult

This object is returned by members of the `SnmpRqst` object or other objects to indicate the status of an operation.

Member	Description
Failed	Returns `true` if this object contains a failure and `false` if the object contains a success.
GetErrorMsg	If **Failed** is `true`, this member returns the associated error message.

Note: All the members of the `ComResult` object are methods. They have no arguments and should be called without parenthesis.

CoreAsp.ComSnmpResponse

This object contains a response from an SNMP request. It is returned by `SnmpRqst` member functions: `Get`, `GetNext`, `GetMultiple` and `Set`.

Member	Description
GetOid	Returns the OID of the polled object. This member cannot be used with operations that poll multiple objects, such as `SnmpRqst.GetMultiple`. **Note**: This member is only useful when used with `SnmpRqst.GetNext`. It can be used with `SnmpRqst.Get` and `SnmpRqst.Set`, but it returns the same OID that you specified when calling those functions.
GetValue	Returns the value of the polled object. This member can only be used with functions that poll a single object (`SnmpRqst.Get`, `SnmpRqst.GetNext` and `SnmpRqst.Set`)
Failed	If the request succeeded, returns `false`. If the request failed, returns `true`. **Note**: When polling multiple objects, `Failed` returns `true` if even one error exists in the results returned by `GetPayload`.
GetErrorMsg	If Failed returns true, this member returns the associated error message.

GetPayload	Returns XML data describing SNMP variable bindings (each containing OID, Type and Value).
	This XML data consists of a single `VarBindList` node which contains one or many `SnmpVarBind` nodes.
	`<VarBindList>`
	`   <SnmpVarBind bHasError="false" sError="" sOid="1.3.6.1.2.1.1.1.0" sValue="HELLO" />`
	`   <SnmpVarBind bHasError="false" sError="" sOid="1.3.6.1.2.1.1.1.1" sValue="WORLD" />`
	`</VarBindList>`
	You can use the Microsoft XML DOM object to access this information. For more information, see the **Read multiple objects in one request** example.

Note: All the members of the ComSnmpResponse object are methods. They have no arguments and should be called without using parenthesis.

Example scripts using the SNMP API

These example scripts demonstrate the SNMP API in use. All of these examples are written in JScript.

Initialize an SNMP object with error check from a device ID

The SnmpRqst.Initialize method returns a ComResult object that tells if the initialization succeeded or failed.

This script uses the Failed method to detect an error and logs an error message using GetErrorMsg if the initialization failed:

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}
```

Alternatively, initialization using a device address and an SNMP credential ID:

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var sAddress = "192.168.3.1";
var nCredentialID = 1;
var oComResult = oSnmpRqst.Initialize2(sAddress, nCredentialID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}
```

Send a standard Get and log the polled value

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}
var oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.2.1.0");
if (oSnmpResponse.Failed)
{
        Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
        Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ", got " +
oSnmpResponse.GetValue);
}
```

Send a Get using non-standard port and timeout

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}
oComResult = oSnmpRqst.SetPort(1234);
oComResult = oSnmpRqst.SetTimeoutMs(5000); // 5 second timeout
var oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.2.1.0");
if (oSnmpResponse.Failed)
{
        Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
        Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ", got " +
oSnmpResponse.GetValue);
}
```

Walk the MIB using GetNext

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}
var sOid = "1.3.6.1.2";
//get the next 10 objects
for (i=0; i<10; i++)
{
        var oSnmpResponse = oSnmpRqst.GetNext(sOid);
        if (oSnmpResponse.Failed)
        {
                Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
                break;
        }
        else
        {
                sOid = oSnmpResponse.GetOid;
                Context.LogMessage(sOid + "=" + oSnmpResponse.GetValue);
        }
}
```

Read multiple objects in one request

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}

// Get three objects in one packet:
var oSnmpResponse =
oSnmpRqst.GetMultiple("1.3.6.1.2.1.1.1.0,1.3.6.1.2.1.1.2.0,1.3.6.1.2.1.1.3.0");

if (oSnmpResponse.Failed)
{
        Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
        var sXML = oSnmpResponse.GetPayload;

        var objXMLDocument = new ActiveXObject("Microsoft.XMLDOM");
        objXMLDocument.async = false;
        objXMLDocument.loadXML(sXML);

        var oVarBinds = objXMLDocument.getElementsByTagName("SnmpVarBind");

        // For each variable binding, log OID=VALUE
        for (var i=0; i<oVarBinds.length; i++)
        {
                Context.LogMessage(oVarBinds(i).getAttribute("sOid") + "=" +
oVarBinds(i).getAttribute("sValue"));
        }
}
```

Reboot a Cisco device using Set

Note: As of WhatsUp Gold v14, SNMP values can be set using the built-in SNMP Set Action. For more information, see Using an SNMP Set Action.

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
        Context.LogMessage(oComResult.GetErrorMsg);
}
var oSnmpResponse = oSnmpRqst.Set("1.3.6.1.4.1.9.2.9.9.0", 'i', 2); /* reload */
if (oSnmpResponse.Failed)
{
        Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
        Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ", got " +
oSnmpResponse.GetValue);
}
```

Troubleshooting the SNMP API

There are several things to keep in mind as you attempt to use the SNMP API.

Different results for different versions

Although the SNMP API works on all SNMP capable devices, the results returned depend on the SNMP version. For example, SNMPv1 and v2 return different results for the `GetMultiple` function. If one of the OIDs used in the fuction is incorrect, SNMPv1 returns only an error, while SNMPv2 returns results for the correct OIDs and an error for the incorrect OID.

The inability to work on certain versions of Windows with IPv6

The SNMP API does not work on the following versions of Windows when using IPv6:

- Windows 2003
- Windows XP
- Windows Vista

Maximum packet size on routers and switches

Routers and switches have a default packet size limitation of 1500 bytes. The `GetMultiple` will return an error if the parameter size exceeds the limit.

APPENDIX B

Using the Dashboard Screen Manager

In This Chapter

Ipswitch Dashboard Screen Manager overview

The Dashboard Screen Manager is a stand-alone application designed to display a series of Web pages, or a "playlist," on one or multiple monitors.

The Dashboard was created as a complement to the Ipswitch network monitoring application, WhatsUp Gold, and as an aid to keeping your network visible. The Dashboard application is included in the WhatsUp Gold and WhatsUp Gold Central and Remote Site installations.

The Dashboard can run on a display console and cycle through various pages from the WhatsUp Gold web interface. Network administrators then have important and pertinent network information on display at all times, cycling and changing on its own without the need of constant configuration. It also provides the capability to view multiple networks that you are monitoring simultaneously.

Though the Dashboard Screen Manager was created to work along-side WhatsUp Gold, it can display virtually any Web page. For example, an Internet business providing service to a small town in the desert glances at one screen on the Dashboard and sees that the connectivity to the town is down. By displaying the weather for this town on another screen at the same time, the network administrator is able to see that the extreme temperatures of the day have likely caused problems for the cable transmitters.

Note: If you want to display a password protected page for another Web application, you must supply a valid username and password for the page. For more information, see the Dashboard application Help.

For more information about the Dashboard playlists, see *Configuring a Dashboard Playlist* (on page 556).

For more information about configuring a multi-monitor network display, see *Setting up a WhatsUp Multi-Monitor Network Display*, located on the *WhatsUp Gold Support Site* (http://www.whatsupgold.com/support/index.aspx).

How does the Dashboard Screen Manager work?

In order for the Dashboard to work, it needs:

1. A monitor, or several monitors
2. A playlist for each monitor

The Dashboard displays a single playlist on every monitor you configure for use with the Dashboard. You can configure as many monitors as you would like for use with the Dashboard.

What is a Dashboard playlist?

On the Dashboard Screen Manager, a playlist is a list of Web pages the Dashboard displays on a single monitor. A playlist can consist of one single, or multiple Web pages. When a playlist is configured with a single Web page, this single page is refreshed on a user-specified refresh interval. When a playlist is configured with multiple Web pages, the playlist cycles through the pages also on a user-specified interval.

Installing the Dashboard Screen Manager

On the device you wish to install the Ipswitch Dashboard Screen Manager:

1. Log on to an Administrator account.
2. Start the installation program:

   If you downloaded the Dashboard from the Ipswitch Web site, run the downloaded installation application.
3. Read the Welcome screen. Click **Next** to continue.
4. Read the license agreement. Select the appropriate option, then click **Next**.
5. Select the install directory for the Dashboard. The default is:

   `C:\Program Files\Ipswitch\Dashboard`

   To browse and select an install directory different than that of the default location, click **Change**.

   Click **Next** to continue.
6. Click **Install** to install the Ipswitch Dashboard.

Note: To terminate the installation once it has began, click **Cancel**.

7. Make your selection, then click **Finish**.

Disable script debugging in Internet Explorer

After you have installed the Dashboard Screen Manager, it is important that you make sure script debugging is disabled. Otherwise, a debugging program will pop-up and could crash the Dashboard. By default, script debugging is disabled, but if you are unsure or know that you have it enabled, you can check this setting in Internet Explorer.

To disable script debugging in Internet Explorer:

1. Open Internet Explorer and go to **Tools > Internet Options**. The Internet Options dialog appears.
2. Click the **Advanced** tab.
3. Scroll down and check the **Disable Script Debugging (Internet Explorer)** and the **Disable Script Debugging (Other)** options.
4. Click **OK** to save changes.

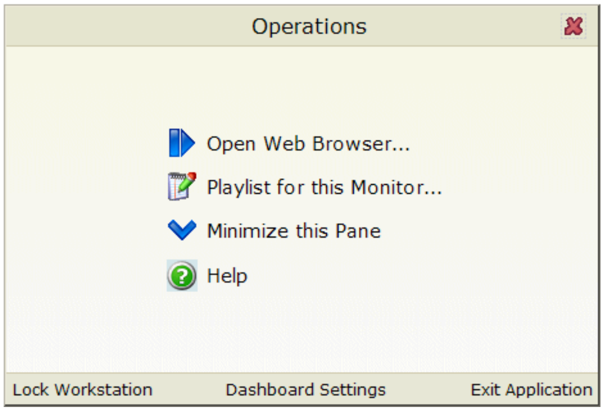
Opening the Dashboard Screen Manager

After successfully installing the Dashboard, you can access the application from your Windows Start Menu by clicking **Ipswitch Dashboard > Dashboard**.

Note: This changes if after the initial setup of the Dashboard, you choose to run the Dashboard at Startup (on the Dashboard Settings dialog). If you choose to do so, the Dashboard Screen Manager will automatically take you to the blank screen discussed below.

When the dashboard first opens, a blank screen is displayed. The blank page's title bar reads, "Ipswitch Dashboard [Configure the 'Playlist' for the Dashboard by clicking a mouse button] - aboutblank."

If you have multiple displays, you will see a Dashboard application instance for each display in the taskbar. For example, if you have three display devices, DISPLAY1, DISPLAY2, or DISPLAY3 shows in the taskbar. Select the display you want to configure first, then click a button on your mouse to open the Dashboard Operations dialog. From here, you can *configure Dashboard playlists* (on page 556).



Configuring a Dashboard Screen Manager playlist

Keep in mind that you need to set up a playlist for each physical monitor on which you want to display Web pages through the Dashboard Screen Manager.

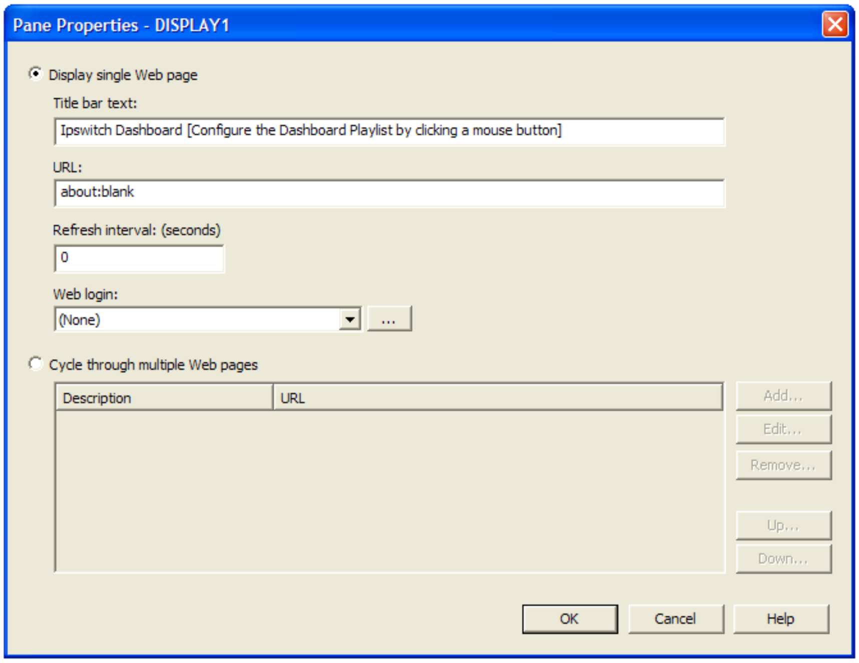
To configure a single Web page playlist:

If you have chosen not to run the Dashboard Screen Manager upon Startup, click **Start > Programs > Ipswitch Dashboard > Dashboard**. The Dashboard Operations dialog appears.

- or -

If you have chosen to run the Dashboard Screen Manager upon Startup, on the display you want to configure a playlist for, click on the screen and the Dashboard Operations dialog appears.

1 On the Dashboard Operations dialog, select **Playlist for this Monitor**. The Pane Properties dialog appears.



Pane Properties - DISPLAY1

● Display single Web page

Title bar text: Ipswitch Dashboard [Configure the Dashboard Playlist by clicking a mouse button]

URL: about:blank

Refresh interval: (seconds) 0

Web login: (None)

○ Cycle through multiple Web pages

Description	URL

2 Select **Display single Web page**.

3 Enter the appropriate information in the following boxes:

§ **Title bar text**. Enter the title bar name for the Dashboard display.

§ **URL**. Enter or paste the URL for the Web page you want to display in the following format:

`http://www.websitename.com/webpagename`

§ **Refresh interval (in seconds)**. Enter an amount of time (in seconds) for how often you would like the Web page to refresh.

§ **WhatsUp Gold Web login**. Either select a user from the list, or click the browse (**...**) button to choose a user from the WhatsUp Gold Web Login Library. This user account is used for the Dashboard application to log-in to a password protected site. Without a proper user account, the application is not able to display a password-protected Web page. If you are using a non-WhatsUp Gold Web page, set the Web login to **None**.

Note: Other applications requiring a username and password to display Web pages can be used in the Dashboard Screen Manager. You can specify these other application username and passwords in the **URL** box, appended to the Web page URL.

4 Click **OK** to save changes.

✓ **Important**: The Web Login list is empty until you populate the Web Login Library with users. You can do this via the Web Login Library dialog.

To configure a multiple Web page playlist:

If you have chosen not to run the Dashboard Screen Manager upon Startup, click **Start > Programs > Ipswitch Dashboard > Dashboard**. The Dashboard Operations dialog appears.

- or -

If you have chosen to run the Dashboard Screen Manager upon Startup, on the display you want to configure a playlist for, click on the screen and the Dashboard Operations dialog appears.

1 On the Dashboard Operations dialog, select **Playlist for this Monitor**. The Pane Properties dialog appears.

2 On the display for which you want to configure a playlist, select **Playlist for this Monitor**. The Pane Properties dialog appears.

3 Select **Cycle through multiple Web pages**.

4 Click the **Add** button to add Web pages to the list. The Add URL to Playlist dialog appears.

5 Enter the appropriate information in the following boxes:

§ **Title bar text**. Enter the title bar name for the Dashboard display.

§ **URL**. Enter or paste the URL for the Web page you want to display in the following format:

```
http://www.websitename.com/webpagename
```

§ **Refresh interval (in seconds)**. Enter an amount of time (in seconds) for how long you would like the Web page to be on the screen.

§ **WhatsUp Gold Web login**. Either select a user from the list, or click the browse (**...**) button to choose a user from the WhatsUp Gold Web Login Library. This user account is used for the Dashboard application to log-in to a WhatsUp Gold Web page. Without a proper user account, the application is not able to display a password-protected Web page. If you are using a non-WhatsUp Gold Web page, set the Web login to **None**.

Note: Other applications requiring a username and password to display Web pages can be used in the Dashboard Screen Manager. You can specify these other application username and passwords in the **URL** box, appended to the Web page URL.

6 Click **OK** to add the new Web page to the playlist.

7 Edit and Remove Web pages by selecting a Web page from the list and then clicking the **Edit** or **Remove** button.

8 Click **OK** to save changes.

APPENDIX C

Troubleshooting and Maintenance

In This Chapter

Troubleshooting your network

WhatsUp Gold is a tool used to monitor your network. It is up to you to fix the items that WhatsUp Gold brings to light.

The following are questions you should think about while troubleshooting problems detected through WhatsUp Gold.

§ Is the entire subnet affected, or a single device?

§ Is the entire device affected, or a service monitor on the device?

§ What type of device is down?

Actions to take

After you have determined the scope of the network problems, one of the following may help you fix the problem.

- If it is the entire subnet that appears to be down, you should check your hub, router, or switch.
- Begin with checking the physical connections of the device to the network and to the power supply. Check the network cables and power cables.
- Check wireless network cards and signal strength.
- Check the Device Health log to see whether a single monitor or the entire device is down. If the device is down, all of the monitors will appear to be down.
- Using the Ping monitor, verify that the connection between the device and the network is up.
- If a monitor appears to be down, try restarting the service that the monitor is watching. To restart a service, you must access the device directly; this cannot be done through WhatsUp Gold.

Maintaining the Database

You can use the WhatsUp database utilities to back up and restore the database and to perform database maintenance and troubleshooting. If you have a WhatsUp Gold Flow Monitor license, you can also back up and restore the Flow Monitor databases via the WhatsUp database utilities.

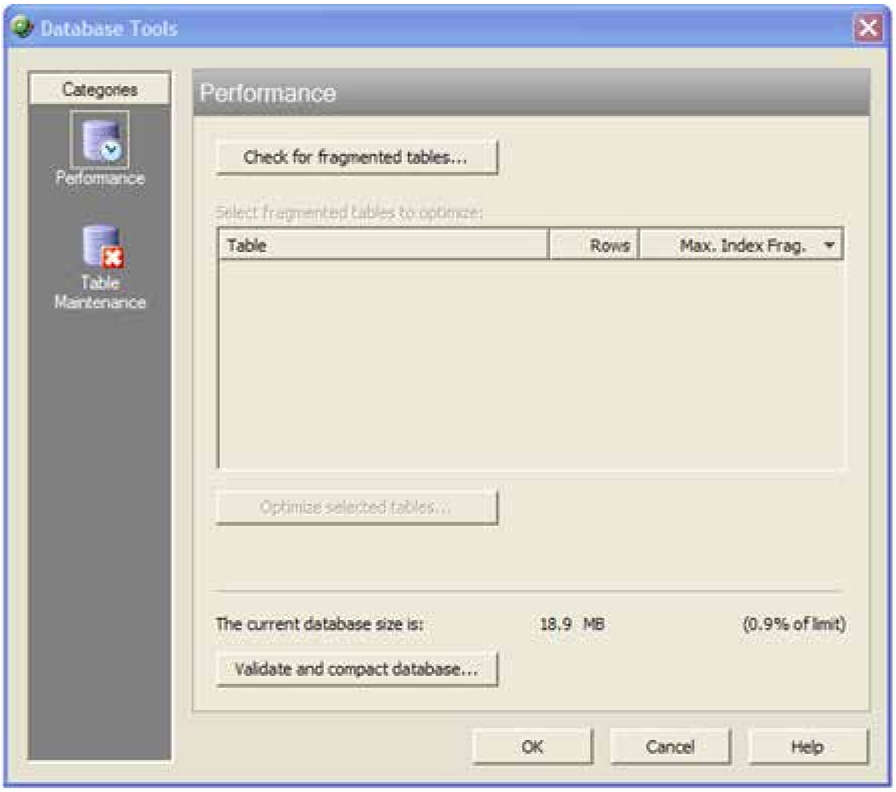
To access the database utilities, open the WhatsUp Gold console, then click **Tools > Database Utilities** from the main menu.

About the database tools

The database tools let you manage index fragmentation and purge expired data.

To access the tools:

1 From the main menu in the WhatsUp Gold console, click **Tools > Database Utilities > Tools**. The Database Tools dialog appears.


Database Tools
Categories
Performance
Table Maintenance
Performance
Check for fragmented tables...
Select fragmented tables to optimize:
Table
Rows
Max. Index Frag.
Optimize selected tables...
Validate and compact database...
OK
Cancel
Help

The current database size is: 18.9 MB (0.9% of limit)

2 Select one of the tools:

- Performance
- Table Maintenance

Database Performance Tool

The Database Performance Tool is used to monitor the size of your database, and to manage the index fragmentation percentage of the individual tables. Fragmented indexes can cause database operations to slow down considerably, in much the same way that disk fragmentation causes your computer to run slower.

Click **Check for fragmented tables** to begin. This may take a considerable amount of time (up to a few minutes), depending on how many records are in your database.

- **Select fragmented tables to optimize**. This list shows all database tables with greater than 10% index fragmentation, along with the total number of data rows in that table.
- **Optimize selected tables**. Select the tables in the list above to defragment those database tables. WhatsUp Gold automatically stops and restarts the WhatsUp Service. The status of the operation appears on the dialog, next to this button.

§ **The current database size is**. This section of the dialog shows the total amount of space used by the database. If you are using SQL Server 2005 Express as the WhatsUp Gold database, this section also displays the percentage of the 4 GB file size limit currently in use.

§ **Validate and compact database**. Click this button to execute commands that validate the database, index, and database links, and to compact the database. WhatsUp Gold automatically stops the Ipswitch Service Control Manager (ISCM) and restarts it once the operation is complete.

The validation phase executes the SQL Server commands `DBCC CHECKCONSTRAINT`, `DBCC CHECKCATALOG`, and `DBCC CHECKDB`. These commands check the integrity of all constraints in the database, check for consistency in and between system tables in the database, and check the allocation and structural integrity of all the objects in the database.

The compacting phase executes the SQL Server command `DBCC SHRINKDATABASE`, which shrinks the size of the data files in the database. Note that no compression is used; the database is simply compacted by removing empty space.

For more information on validating or compacting the database, see *Getting Started with SQL Server* (http://www.whatsupgold.com/MSSQLServer200xExp) on the Microsoft website.

Database Tools Table Maintenance

This feature lets you purge expired data from data tables in your database. Be very careful when using this dialog, as data that is purged through this process is lost and cannot be restored.

§ **Select tables to purge**. The data tables are grouped by the purpose they serve (active monitors, report data collection, and other). Select the tables you want to purge from the three lists.

§ **Total Rows**. The total number of data rows in this table that currently holds data. This includes live and expired rows.

§ **Expired Rows**. The total number of expired data rows in this table. Expired data is data that has been rolled up, and has not yet been purged by the application or has not been reused. These are rows that are marked for deletion, or have been kept longer than needed, according to your data roll-up settings. See Program Options - Report Data for more information on setting your data roll-up settings.

Click **Purge Expired Rows** to remove those records from the database.

Group Policy Object 503 Service Unavailable Error

A Group Policy Object (GPO) applied on your domain which has removed or altered the user rights of the `WhatsUpGold_User` account on the WhatsUp Gold server can cause a generic 503 Service Unavailable Error to be displayed following WhatsUp Gold installation. The account is created during WhatsUp Gold installation and is used for the identity of the WhatsUp Gold application pool in IIS as well as the account with rights to the WhatsUp virtual directory. This user should be added to the Local Administrators group and should not be removed.

To correct the error, verify/restore applicable settings using the following procedures:

1 Ensure the `WhatsUpGold_User` account exists on the WhatsUp Gold server:

   a) From the WhatsUp Gold server desktop, click **Start > Control Panel > Administrative Tools > Computer Management**.

   b) Expand Local Users and Groups in the Computer Management navigation tree.

   c) Click **Users**. If the `WhatsUpGold_User` account is not displayed, a GPO conflict exists and needs to be resolved at the Domain Controller.

2 Ensure the `WhatsUp_Gold User` is a member of the Local Administrators group on the WhatsUp Gold server:

   a) From the WhatsUp Gold server desktop, click **Start > Control Panel > Administrative Tools > Computer Management**.

   b) Expand Local Users and Groups in the Computer Management navigation tree.

   c) Click **Groups**.

   d) Double-click **Administrators**. If the `WhatsUpGold_User` account is not displayed, a GPO conflict exists and needs to be resolved at the Domain Controller.

3 Ensure the Local Administrators group has the Logon as a batch job Local Security option enabled:

   a) From the WhatsUp Gold server desktop, click **Start > Control Panel > Administrative Tools > Local Security Policy**.

   b) Expand Local Policies in the Security Settings navigation tree.

   c) Click **User Rights Assignment**.

   d) Double-click **Logon as batch job**. If the Administrators group is not displayed, a GPO conflict exists and needs to be resolved at the Domain Controller.

✓ **Important**: If changes are made using these procedures, in IIS the Application pool Nmconsole is stopped. IIS needs to be restarted prior to continuing. Additionally, Event Viewer displays the following:

Application pool ASP.NET v4.0 has been disabled. Windows Process Activation Service (WAS) encountered a failure when it started a worker process to serve the application pool.

Application pool ASP.NET v4.0 has been disabled. Windows Process Activation Service (WAS) did not create a worker process to serve the application pool because the application pool identity is invalid.

Recovering from a "Version Mismatch" error

When starting the WhatsUp Gold or Flow Monitor application, you may get a "Version Mismatch" error if the program version does not match the database version. The WhatsUp Gold and Flow Monitor applications can only use a database that is compatible with the version of the software currently installed.

If the install encounters an error during upgrade, and you abort the database upgrade portion of the install, or you choose the Ignore option and allow the upgrade process to continue the install, the database may not not be upgraded properly. To attempt to resolve this issue, reboot your machine and run the same install again. During the install, select the Repair option.

✓ **Important**: If running the repair does not correct the database issue, review your log file to help identify the issue (located in the `..\Program Files\Ipswitch\WhatsUp\RemoteDBConfig.txt`, search the *Ipswitch Knowledge Base* (http://www.whatsupgold.com/wugtechsupport) for technical support resources, or contact *Ipswitch Technical Support* (http://www.whatsupgold.com/wugtechsupport) for troubleshooting help.

You may also get a "Version Mismatch" error if you restore a WhatsUp Gold or Flow Monitor database from an earlier version of the application. To attempt to resolve this issue, reboot your machine and run the same install again. During the install, select the Repair option.

✓ **Important**: The WhatsUp Gold polling engine will not run, nor can the WhatsUp Gold, Alert Center, or Flow Monitor applications be used until this database version mismatch error is corrected.

Task Tray Application fails on Windows Vista

After installing WhatsUp Gold on Microsoft Vista, the WhatsUp Gold Task Tray Application does not connect to the database if you log in to Windows using any account other than the account used to install the application. To correct this issue, execute this script from the command line in the `C:\Program Files\Ipswitch\WhatsUp\DB Scripts\` folder:

```
sqlcmd -E -S (local)\WHATSUP -d WHATSUP -i
grant_all_users_read_access.sql
```

✓ **Important**: If you run the above script, all database users (admin and others) are granted read access to the WhatsUp Gold database.

Co-located SQL Server and WhatsUp Gold server clocks must be synchronized

If a WhatsUp Gold and SQL Server is not located on the same physical machine (server) and the system clocks are not synchronized to the same time zone, inaccurate data may occur in reports. To correct this issue, set the system clock for the same time zone and ensure that the clocks are synchronized to the same time.

Connecting to a remote desktop

WhatsUp Gold provides a quick link to the Remote Desktop/Terminal Services client that allows you to connect to your devices remotely. If the client is installed on your WhatsUp Gold computer, and the Remote Desktop/Terminal Services is installed and activated on the device you want to connect to, you are prompted for the user name and password for that device.

This application allows you to troubleshoot problems with your devices and monitors identified by WhatsUp Gold.

To connect to a remote desktop:

1. Right-click the device you want to connect to.
2. From the right-click menu, click **Remote Desktop**. If the connection is successful, the log in dialog appears. If the connection fails, an error message appears.

Note: For more information about the Remote Desktop feature, see the online help for the Remote Desktop client itself.

WhatsUp Gold engine message

This message means that WhatsUp Gold is not operating properly, because the WhatsUp Gold Engine service has stopped.

To stop and restart the WhatsUp Gold engine from the console:

1. From the console, click **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
2. Select **WhatsUp Polling Engine**, click **Stop**, then click **Start**.

Troubleshooting SNMP and WMI connections

If you experience connection problems when connecting to a device via the Web Task Manager, Web Performance Monitor, or any other WhatsUp Gold feature that uses WMI or SNMP, please consult the lists below to troubleshoot the problem.

Troubleshooting a WMI connection

Important: You must have administrative credentials to establish WMI connections. For more information, see *Using Credentials* (on page 68). Also, see Microsoft article *875605* (http://support.microsoft.com/default.aspx?scid=kb;en-us;875605).

§ Establishing a WMI connection can be very slow.

This slow connection time can worsen when attempting to connect with devices running Microsoft Vista.

We recommend that you open RPC port 135 on both the WhatsUp device's firewall and the firewall for device to which you are attempting to connect. Also be sure to open this port on any firewall between the connecting devices. Refer to the operating system Help for more information.

§ Connected devices that are running different versions of Microsoft software (i.e. - Microsoft XP and Vista) may experience delayed or slow communication.

§ WMI over VPN connections can take up to 120 seconds (possibly longer) to establish an initial connection. After the initial connection is made, subsequent connections take 8 to 10 seconds.

§ Again, we recommend that you open RPC port 135 on each device's firewall, and any firewall between the connecting devices.

§ A WMI memory leak exists in Windows 2003 and XP. Microsoft has developed hotfix *911262* (http://support.microsoft.com/kb/911262/en-us) that minimizes the leak in XP, and completely fixes the leak in Windows 2003.

For more information regarding WMI and connection problems, see Microsoft articles *389290* (http://msdn2.microsoft.com/en-us/library/aa389290.aspx), *389286* (http://msdn2.microsoft.com/en-us/library/aa389286.aspx), and the section entitled "I can't connect to a remote computer" in the Microsoft Script Center article, *WMI Isn't Working!* (http://www.microsoft.com/technet/scriptcenter/topics/help/wmi.mspx#E2C).

Troubleshooting an SNMP connection

✓ **Important**: The SNMP Trap Listener must be enabled to collect data for the SNMP Trap Log. To enable the WhatsUp Gold SNMP Trap Listener, the Microsoft SNMP Trap Listener must be disabled. Also, be sure to open SNMP port 162 for incoming SNMP traps.

§ If you receive invalid values when attempting to monitor the IfOperStatus OID from a device running Vista, download Microsoft's hotfix *935876* (http://support.microsoft.com/kb/935876) to solve the problem.

§ If you experience connection problems with a specific device, ensure that the device has SNMP enabled. Also ensure that SNMP port 161 is open on the device you are attempting to monitor.

§ If you get what looks like a "stair-step" in your CPU and Process Utilization graphs, this is caused by Microsoft's 60-second polling interval. Increasing WhatsUp Gold's polling interval could help compensate for the lengthy Microsoft polling interval.

§ Similarly, if you experience delays and/or unexpected, weird spikes in your graphs, try increasing the polling interval.

False negative returned from WMI monitors

Have your NT Service or WMI Active Monitors been reporting errors when in fact your services or counters are up? You may need to increase the default length of the RPCPingTimeout registry value so that you are given a longer chance to connect. For example, if you wish to set the timeout to 10 seconds, set RCPingTimeout to 10000 (decimal).

To edit the RPCPingTimout registry value:

1. Go to **Start > Run > Regedit.exe**
2. From the Registry Editor go to: `HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Network Monitor\WhatsUp Engine\Settings`
3. Within the Settings folder, select **RPCPingTimeout** and right-click. From the right-click menu, select **Modify**.
4. In the Edit DWORD Value dialog, enter in a new value for the timeout and click **OK**.

✓ **Important**: The default timeout is 5 seconds, expressed as 5000 (decimal), or 0x00001388 (hexadecimal). We strongly recommend that you do not exceed a timeout of 30 seconds.

After making any changes to the registry, you need to restart the Polling Engine.

To restart the Polling Engine from the web:

1. Click the **Admin** tab, then click **Admin Panel**.
2. Select **Polling Engine** and click **Restart**.

To restart the Polling Engine from the WhatsUp Gold server console:

1. Click **Start > All Programs > Ipswitch WhatsUp Gold > Utilities**.
2. Click **Service Manager**.
3. Select **Polling Engine** and click **Restart**.

Re-enabling the Telnet protocol handler

The Telnet protocol handler is disabled by default in Microsoft Internet Explorer 7. In order to use the Telnet tool in WhatsUp Gold, you need to re-enable the Telnet protocol.

To re-enable the Telnet protocol:

1. Click **Start > Run**. The Run dialog opens.
2. In the Open box, enter: `Regedit`, then click **OK**. The Registry Editor opens.

3 Go to the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl`

4 Under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl`, create a new key named `FEATURE_DISABLE_TELNET_PROTOCOL`.

5 Add a `DWORD` value named `iexplore.exe` and set the value to `0` (decimal).

6 Close the Registry Editor and restart Microsoft Internet Explorer. The Telnet protocol is enabled.

Passive Monitor payload limitation

Passive monitors have a payload limitation of 3 KB for WMI, SNMP, and Syslog Passive Monitors.

Receiving entries in the SNMP Trap Log

In order for entries to be added to the SNMP Trap Log, the SNMP Trap Listener must be enabled. For more information, see Enabling the SNMP Trap Listener.

Additionally, if the trap receiving port is not on the firewall's list of exceptions, traps may not be receivable, and as a result, will not be added to the SNMP Trap Log. Please ensure that the trap receiving port is on the firewall's list of exceptions.

Recommended SMS modems and troubleshooting tips

Ipswitch has tested the following SMS modems for use with the SMS Direct Action (not the SMS Action):

- *ConiuGo GPRS GSM Quadband Modem / USB-Busp (850, 900, 1800 & 1900 MHz)* http://www.coniugo.com/pdf/e_gprs_gsm_quadband_modem_rs232_usb.pdf
- *Falcom Samba 75 (GSM/GPRS/EDGE)* (http://www.falcomusa.com)

Note: Falcom Samba 75 modem is not supported on Windows Server operating systems.

- Encore Electronics modem v.92/56K model: VD56UL (USB Support)
- *Motorola® RAZR V3* (http://www.motorola.com) (Recommended)

This cell phone was connected to the WhatsUp device acting as a GSM modem.

- *MultiModem® GPRS external wireless modem* (http://www.multitech.com/PRODUCTS/Families/MultiModemGPRS/), models: MTCBA-G-F2, MTCBA-G-U-F4, MTCBA-G-F4 - RS-232 version
- *Siemens TC65 Terminal* (http://www.usa.siemens.com)

Unlike the other modems that have their own drivers to install, this modem did not have specific drivers to install. The Windows Standard 56000 bps modem driver was used with the maximum port speed set to 115200.

- *Vodaphone USB modem for SMS Direct (* (http://www.vodafone.com/index.VF.html)tested on Huawei, Model E220, HSDPA USB modem)
- *Zoom 56k serial modem* (http://www.zoomtel.com/graphics/datasheets/dial_up/30481101.pdf)

To consider

- GSM networks operate in the 850/900/1800/1900 Mhz bands.
- GSM modems are typically either dual or quad band.

Note: You must acquire a dual modem that operates at the correct frequency, or purchase a quad band modem.

- European markets typically use 900/1800 Mhz capable devices.
- The U.S. and Canada use 850/1900 Mhz capable devices.

Troubleshooting SMS Modems

If an SMS modem is not working as expected, verify that the communications port (COM port) to which the modem is attached is configured to use settings supported by the modem.

1. In the Windows Control Panel, double-click **Device Manager**. The Device Manager appears.
2. Expand **Ports**.
3. Double-click the communications port used by the SMS modem. The Communications Port Properties dialog appears.
4. Select the **Port Settings** tab.
5. Using the documentation provided by the modem manufacturer, verify that the port settings listed are supported by the modem. If the listed settings are not supported, make any necessary changes.

Note: If you are using the MultiModem® GPRS external wireless modem, model MTCBA-G-F2, set **Flow Control** to **Hardware**.

6. Click **OK** to save changes.

Using line feeds and carriage returns to correct SMS modem issues

Some SMS Direct enabled phones do not work correctly with SMS Direct Actions because new line characters are not always handled properly. This issue may be corrected by adding the following new registry key entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Network Monitor\Whatsup plug-
ins\Actions\ActSmsDirect\NewLine
```

In the **Value data** box, enter a combination of a carriage return (`\r`) and/or line feed (`\n`) command. For example enter one of the following:

- `newline \r\n` (recommended)
- `newline \r`
- `newline \n`

Uninstalling Ipswitch WhatsUp Gold

To uninstall Ipswitch WhatsUp Gold:

1. Click **Start > Control Panel > Programs and Features > Uninstall a Program**.
2. Select **Ipswitch WhatsUp Gold**.
3. Select **Uninstall**.

You can also run the Ipswitch WhatsUp Gold installation program, then select **Remove WhatsUp Gold**.

Select one of the following dialog options:

- **Keep my configuration data but uninstall WhatsUp Gold**. This uninstalls the WhatsUp Gold program but keeps all your WhatsUp configuration data as well as the monitoring data you have collected. SQL Server 2005 Express will not be uninstalled.
- **Remove my configuation data and uninstall WhatsUp Gold**. This uninstalls the WhatsUp program and removes all of your WhatsUp configuration and monitoring data.
- **Also remove the WHATSUP instance of SQL Server Express Edition**. This also removes the "WhatsUp" SQL Server Express Edition instance that was created during the installation. Select this option to remove **ALL** WhatsUp components from the system.

Note: When this option is selected, WhatsUp Gold leaves SOME data behind, such as the `\HTML` directory and the `\Data` directory for situations where there may be user-modified or user-created files in those directories.

Troubleshooting the WhatsUp Health Threshold

If you are encountering errors in the Alert Center Log after configuring and running the WhatsUp Health Threshold's service checks, there are several steps you can take to troubleshoot the occurrence of these errors.

First, from a CMD window, run the following commands:

Windows XP and later

wmiadap/clearadap

wmiadap/resyncperf

Windows 2000

winmgmt/clearadap

winmgmt/resyncperf

Note: These commands may take some time to execute.

If after running these commands the errors persists, run the Microsoft WMI Diagnosis Utility, found on Microsoft's web site: http://www.microsoft.com/downloads/details.aspx?familyid=d7ba3cd6-18d1-4d05-b11e-4c64192ae97d&displaylang=en

Terminal Services

Additionally, you may encounter problems with your service-level threshold checks if you are using Microsoft Terminal Services (Remote Desktop Services) to run the WhatsUp Gold web server. If more than one person is logged in to Terminal Services at a time, the following WhatsUp Health Threshold service checks/performance counters may fail:

§ WhatsUp polling service SQL query check

§ WhatsUp web service HTTP response check

§ WhatsUp web service SQL query check

You may experience a high volume of errors logged to the Alert Center Log from these service checks until the number of Terminal Service users drops to one or none.

Copyright notice

This document was published on Monday, September 28, 2012 at 10:56.