



IPSWITCH

WhatsUp Gold v16.3

User Guide

Overview

WhatsUp Gold Overview.....	1
Welcome to Ipswitch WhatsUp Gold	1
WhatsUp Gold Editions.....	3
New in Ipswitch WhatsUp Gold	5
Using the WhatsUp Gold community site	5
Using the WhatsUp Customer Portal for product account information.....	5
Finding more information and updates	5
Security guidelines overview.....	6
Security best practices.....	6
Best practices for administrators.....	7
Best practices for web users.....	7
Limiting access to the WhatsUp Gold Administration Console.....	8
Limiting Access to the WhatsUp Gold Tools and Utilities	8
Issuing User Rights and Device Access Rights conservatively.....	9
Monitoring WhatsUp Gold health and disk usage to prevent data loss.....	9
Monitoring WhatsUp Gold health.....	9
Monitoring WhatsUp Gold server disk usage.....	9
Backing up the WhatsUp Gold database.....	10
Set the WhatsUp Gold server platform to use FIPS cryptography.....	10
Using FIPS 140-2 cryptography	11
Setting WhatsUp Gold server to use FIPS cryptography.....	12
Using WhatsUp Gold password management	13
Getting Familiar with WhatsUp Gold	14
Using the WhatsUp Gold Web Interface.....	15
Using the WhatsUp Gold Console	21
Using the Discovery Console	24
Using WhatsUp Gold Mobile Access	25

About Polling

WhatsUp Gold Polling Engine Overview.....	35
Poller Installation and Removal.....	37
WhatsUp Gold Poller installation and configuration.....	37
WhatsUp Gold Poller Removal	38
Configuring WhatsUp Gold to use additional pollers	39
Poller Health Dashboard.....	39
Polling Performance Tuning	39
Using Polling with WhatsUp Gold Failover and Distributed editions.....	40

Poller usage in WhatsUp Gold.....	41
-----------------------------------	----

Dashboard

Understanding and using dashboards.....	43
Learning about dashboards	43
About the Home Dashboard.....	44
About the Device Status dashboard	45
About the Top 10 dashboard.....	46
Overview of dashboard report categories.....	47
Adding dashboard reports to a dashboard view.....	48
Searching for dashboard reports.....	50
Working with dashboard views.....	50
Changing dashboard content	51
Using the dashboard report menu	52
Configuring a dashboard report	52
Moving dashboard reports within a dashboard view	53
Navigating dashboard views	53
Using Favorites.....	55
Understanding favorites	55
Adding favorites	55
Editing favorites.....	56
Viewing Dashboard reports.....	58
Alert Center reports.....	59
APM Dashboard Reports.....	61
CPU Utilization reports	63
Custom Performance Monitor reports.....	68
Disk Utilization reports	73
General reports.....	80
Interface Errors and Discards reports.....	96
Interface Utilization reports.....	104
Inventory reports.....	113
Memory Utilization reports.....	117
Performance-Historic reports.....	123
Performance-Last Poll reports.....	141
Ping Availability and Response Time reports.....	152
Problem Areas reports.....	161
Problem Areas Specific Device.....	172
Remote/Central reports.....	178
Split Second Graph reports.....	206

Threshold reports.....	221
Top 10 reports.....	229

Devices

Discovery Console.....	240
Discovering network devices.....	240
Using Device Roles.....	255
Managing device roles.....	262
Using Devices.....	264
Viewing devices in WhatsUp Gold.....	264
Understanding device and monitor states.....	265
Understanding state changes.....	266
About device icons.....	266
Using Credentials.....	267
Searching for devices.....	267
Understanding group access and user rights for Find Device.....	268
Searching for devices with interface traffic.....	269
Using Maps.....	271
Using Map View.....	271
About Map View device limitations.....	274
Using Map Options commands.....	274
Creating Layer 2 Groups.....	275
Managing devices.....	281
Learning about devices.....	281
Using Device Properties.....	304
Working with Device Properties.....	305
Using Device Properties - Summary.....	306
Using Device Properties - General.....	307
Device Properties - Performance Monitors.....	307
Using Device Properties - Active Monitors.....	308
Using Device Properties - Passive Monitors.....	309
Using Device Properties - Actions.....	309
Using Device Properties - Credentials.....	310
Using Device Properties - Polling.....	310
Using Device Properties - Virtualization.....	311
Using Device Properties - Notes.....	313
Using Device Properties - Custom Links.....	313
Using Device Properties - Attributes.....	313
Using the DeviceIdentifier attribute.....	314

Using Device Property - Menu	314
Using WhatsConfigured Device Properties - Tasks.....	315
Using Device Properties - Wireless.....	316
Using Network Tools.....	316
Using the Ping tool.....	317
Using the Traceroute tool.....	318
Using the Lookup tool.....	318
Using the SNMP MIB Walker.....	319
Using the SNMP MIB Explorer.....	323
Using the MAC Address tool.....	324
Using the Web Performance Monitor.....	326
Using the Web Task Manager.....	328
Using Layer 2 Trace.....	337
Using IP/MAC Address Finder.....	338
Monitoring Devices.....	340
Using Active Monitors.....	341
Using Passive Monitors.....	436
Using Performance Monitors.....	451
Enabling global performance monitors.....	475
Creating custom performance monitors.....	480
Scenario:.....	496
Using the Active Script Performance Monitor	496

Alerting and actions

Getting started with WhatsUp Gold alerting.....	498
Step 1: Identify important devices	499
Step 2: Ensure monitors are configured for important devices.....	499
Step 3: Configure alerts for important devices.....	499
Step 4: Configure action policies	514
Working with Alert Center reports.....	520
Using Alert Center reports	520
Filtering the Items report.....	520
Using the Item History report.....	521
Updating Alert Center items.....	521
A note about notifications	523
Understanding resolving items - examples.....	523
Filtering the Log report	524
Configuring Alert Center records to expire.....	525
Using the Alerts Home reports.....	526

Using the Performance CPU threshold report.....	528
Using the Performance Custom threshold report.....	528
Using the Performance Disk threshold report.....	529
Using the Performance Interface threshold report.....	529
Using the Interface Errors and Discards threshold report.....	530
Using the Performance Memory threshold report.....	530
Using the Performance Ping Availability threshold report.....	530
Using the Ping Response Time threshold report.....	531
Using the SNMP Trap threshold report.....	531
Using the Syslog threshold report.....	532
Using the Windows Event Log threshold report	532
Using the Flow Monitor Conversation Partners threshold report.....	532
Using the Flow Monitor Custom threshold report	533
Using the Flow Monitor Failed Connections threshold report	533
Flow Monitor Interface Traffic threshold report	534
Using the Flow Monitor Top Sender/Receiver threshold report.....	534
Using the Blackout Summary threshold report.....	534
Using the WhatsUp Health threshold report.....	535
Failover threshold report.....	535
Using the WhatsConfigured Threshold report	535
WhatsVirtual events threshold report	536
Using the All Wireless Thresholds report	536
Using the Wireless Access Point RSSI report.....	536
Using the Wireless Banned Client MAC Addresses report	537
Using the Wireless CPU report.....	537
Using the Wireless Client Bandwidth report.....	537
Using the Wireless Device Over Subscription report.....	537
Using the Wireless Excessive Rogue Alert report	538
Using the Wireless Memory report.....	538
Using the Wireless Rogue Access Point MAC Address Alert report	538
Using the Wireless Rogue Hidden SSID Alert report.....	538
Using the Wireless Rogue Specific SSID Alert report.....	538
Using the Wireless Rogue Unknown SSID Alert report.....	539
Configuring notifications.....	540
Alert Center Percent Variables	540
Using Alert Center Notification Policy options.....	542
Configuring a notification policy	542
Configuring an Alert Center email notification.....	544
Configuring an Alert Center SMS Direct notification.....	546

Configuring an Alert Center SMS Action notification.....	548
Configuring email notification message settings	550
Stopping a running notification policy	551
Using the E-mail Action.....	552
Using the SMS Direct Action.....	552
Using the SMS Action.....	552
Configuring thresholds.....	553
Configuring Alert Center thresholds.....	553
Selecting threshold devices	554
Configuring performance thresholds.....	558
Configuring passive thresholds.....	573
Configuring Flow Monitor thresholds.....	580
Configuring system thresholds.....	593
Configuring wireless thresholds.....	601
Using Actions	611
Actions overview	611
Managing Action Strategies.....	611
About the Action Library	612
Selecting an action type.....	613
Configuring an action	613
About Percent Variables.....	649
Testing an action	652
Assigning an action	652
Removing an action	654
Creating a Blackout Period.....	655
Action Policies.....	656

Reports

Working with monitor reports	663
Viewing device reports.....	663
Viewing group reports.....	665
Using Business Hours settings in monitor reports.....	667
Viewing real-time data in monitor reports.....	668
About report refresh intervals.....	668
Changing the date range.....	669
Using the Zoom tool.....	670
Using paging options.....	670
Changing preferences.....	671
Using the WhatsUp Gold toolbar buttons.....	672

Configuring monitor report charts.....	672
Resizing and sorting report columns.....	673
Disabling Instant Info popups.....	674
Understanding graph types.....	675
Using Favorites.....	677
Understanding favorites.....	677
Adding favorites	677
Editing favorites.....	679
Using WhatsUp Gold monitor reports.....	680
List of reports and logs	680
Learning about monitor reports	682
Device Properties - Performance Monitors	685
Using the Performance Monitor Library	686
Scheduling reports	688
Exporting reports and logs.....	689
Emailing reports and logs.....	690
Printing reports and logs.....	691
Viewing scheduled reports.....	691
Performance monitor reports.....	692
Learning about performance monitor reports.....	692
CPU Utilization.....	692
About the Disk Utilization report.....	694
About the Memory Utilization report	696
About the Custom performance monitor report	698
Network monitor reports.....	700
Learning about network monitors.....	700
About the Interface Utilization report.....	700
About the Interface Traffic report.....	702
About the Ping Availability report.....	704
About the Ping Response Time report.....	706
About the Interface Discards report.....	709
About the Interface Errors report.....	710
Using Device monitor reports.....	712
Learning about Device monitors	712
About the Active Monitor Availability report.....	713
About the Active Monitor Outages report	714
About the Device Uptime report	714
About the Device Health report	715
About the State Change Acknowledgment report	716

About the State Change Timeline report.....	716
About the Top 10 dashboard.....	718

Logs

Working with logs.....	721
Learning about Logs.....	721
Selecting a device to view logs.....	722
Changing the report or log date range.....	722
Changing the date range.....	722
Using paging options.....	723
Navigating between logs.....	723
Printing reports and logs.....	723
Using the WhatsUp Gold toolbar buttons.....	723
Managing server options.....	724
Managing Action Policies.....	725
Viewing payload details.....	726
Using WhatsUp Gold System Logs.....	727
About the Action Log.....	727
Error Logs.....	729
About the SNMP Trap Log.....	731
About the Syslog Events Log.....	732
About the Windows Event Log.....	733
About the Activity Log.....	734
About the Scheduled Report Log.....	734
About the Recurring Action Log.....	735
About the Web User Activity Log.....	735
Using WhatsUp Gold Group / Device Logs.....	736
About the Actions Applied Log.....	736
About the Blackout Summary Log.....	736
About the Monitors Applied Log.....	737
About the Quarterly Availability Summary.....	738
About the State Summary.....	740

Inventory

Viewing Inventory Reports.....	742
About the Device Info report.....	742
About the Asset Inventory report.....	752
About the Device Connectivity report.....	754
About the Installed Software report.....	755

About the Switch Port Utilization report.....	756
About the VLAN View.....	758
About the Subnet View	759
About the Computer System report	760
About the BIOS report.....	761
Windows Software Update Report.....	762
About the Windows Services report.....	764
About the Warranty Information report.....	765

Alert Center

Working with Alert Center reports.....	768
Using Alert Center reports	768
Filtering the Items report.....	768
Using the Item History report.....	769
Updating Alert Center items.....	769
A note about notifications	771
Understanding resolving items - examples.....	771
Filtering the Log report	772
Configuring Alert Center records to expire.....	773
Using the Alerts Home reports.....	774
Using the Performance CPU threshold report.....	774
Using the Performance Custom threshold report.....	774
Using the Performance Disk threshold report.....	775
Using the Performance Interface threshold report	775
Using the Interface Errors and Discards threshold report.....	776
Using the Performance Memory threshold report	776
Using the Performance Ping Availability threshold report.....	776
Using the Ping Response Time threshold report.....	777
Using the SNMP Trap threshold report.....	777
Using the Syslog threshold report.....	778
Using the Windows Event Log threshold report	778
Using the Flow Monitor Conversation Partners threshold report.....	778
Using the Flow Monitor Custom threshold report	779
Using the Flow Monitor Failed Connections threshold report	779
Flow Monitor Interface Traffic threshold report	780
Using the Flow Monitor Top Sender/Receiver threshold report.....	780
Using the Blackout Summary threshold report.....	780
Using the WhatsUp Health threshold report.....	781
Failover threshold report.....	781

Using the WhatsConfigured Threshold report	781
WhatsVirtual events threshold report	782
Using the All Wireless Thresholds report	782
Using the Wireless Access Point RSSI report	782
Using the Wireless Banned Client MAC Addresses report	783
Using the Wireless CPU report	783
Using the Wireless Client Bandwidth report	783
Using the Wireless Device Over Subscription report	783
Using the Wireless Excessive Rogue Alert report	784
Using the Wireless Memory report	784
Using the Wireless Rogue Access Point MAC Address Alert report	784
Using the Wireless Rogue Hidden SSID Alert report	784
Using the Wireless Rogue Specific SSID Alert report	784
Using the Wireless Rogue Unknown SSID Alert report	785
Configuring notifications	786
Using Alert Center and actions	786
Alert Center Percent Variables	786
Using Alert Center Notification Policy options	788
Configuring a notification policy	788
Configuring an Alert Center email notification	790
Configuring an Alert Center SMS Direct notification	792
Configuring an Alert Center SMS Action notification	794
Configuring email notification message settings	796
Stopping a running notification policy	797
Using the E-mail Action	798
Using the SMS Direct Action	798
Using the SMS Action	798
Configuring thresholds	799
Configuring Alert Center thresholds	799
Selecting threshold devices	800
Configuring performance thresholds	804
Configuring passive thresholds	819
Configuring Flow Monitor thresholds	826
Configuring system thresholds	839
Configuring wireless thresholds	847

Admin

Using WhatsUp Gold Admin features	858
Using Admin features	858

Home.....	860
Using Admin Console.....	860
Opening NM Console from the Web interface.....	860
Scheduling.....	861
Adding and editing a recurring action.....	861
Managing scheduled reports.....	863
System Administration	865
Managing WhatsUp Gold server options.....	865
Using the SNMP MIB Manager	865
Setting LDAP or Cisco ACS credentials.....	868
Translation Groups	871
Managing users and groups.....	874
Using the Polling Configuration Library	888
Using the Task Library	892
Options.....	897
Configuring Email settings.....	897
Changing preferences.....	897
Managing dashboard views.....	899
Using the Program Options.....	901

Using SNMP

SNMP overview	911
Enabling SNMP on Windows devices.....	912
Monitoring an SNMP Service	912
About the SNMP Agent or Manager.....	913
About the SNMP Management Information Base.....	913
About SNMP Object Names and Identifiers.....	914
Using the SNMP MIB Manager	914
Using the SNMP MIB Manager to troubleshoot MIB files	915
About the SNMP operations	917
Using a custom name for SNMP device interfaces.....	917
Configuring a custom name (ifAlias) for an SNMP device interface.....	917
About SNMP security.....	918
Using the Trap Definition Import Tool	919

Extending WhatsUp Gold with custom scripting

Extending WhatsUp Gold with scripting.....	920
Scripting Active Monitors.....	921
Using the context object with active monitors.....	921

Example active script active monitors.....	924
Scripting Performance Monitors.....	937
Using the context object with performance monitors.....	939
Example active script performance monitors.....	942
Scripting Actions	947
Using the context object with actions.....	947
Example active script actions.....	950

Using the SNMP API

CoreAsp.SnmpRqst.....	952
CoreAsp.ComResult.....	955
CoreAsp.ComSnmpResponse.....	955
Example scripts using the SNMP API.....	956
Troubleshooting the SNMP API.....	959

Using the Dashboard Screen Manager

Ipswitch Dashboard Screen Manager overview	960
How does the Dashboard Screen Manager work?.....	961
What is a Dashboard playlist?.....	961
Installing the Dashboard Screen Manager.....	961
Opening the Dashboard Screen Manager.....	962
Configuring a Dashboard Screen Manager playlist.....	962

Troubleshooting and Maintenance

Troubleshooting your network.....	966
Maintaining the Database.....	967
About the database tools.....	967
Group Policy Object 503 Service Unavailable Error.....	969
Recovering from a "Version Mismatch" error	970
Task Tray Application fails on Windows Vista	971
Co-located SQL Server and WhatsUp Gold server clocks must be synchronized.....	971
Connecting to a remote desktop.....	972
WhatsUp Gold engine message	972
Troubleshooting SNMP and WMI connections	972
False negative returned from WMI monitors.....	973
Re-enabling the Telnet protocol handler.....	974
Passive Monitor payload limitation	975
Receiving entries in the SNMP Trap Log.....	975

Recommended SMS modems and troubleshooting tips.....	975
Troubleshooting IIS configuration	977
Uninstalling Ipswitch WhatsUp Gold	978
Troubleshooting the WhatsUp Health Threshold.....	979

Frequently Asked Questions

Monitors and actions FAQ.....	980
Alert Center FAQ.....	981
Dashboard FAQ.....	982
Wireless FAQ.....	982
User accounts and permissions FAQ.....	983
Flow Monitor FAQ.....	984
Admin FAQ.....	985
WhatsConfigured FAQ.....	987
APM FAQ	988

Copyright notice

WhatsUp Gold Overview

In This Chapter

Welcome to Ipswitch WhatsUp Gold.....	1
WhatsUp Gold Editions.....	3
New in Ipswitch WhatsUp Gold.....	5
Using the WhatsUp Gold community site.....	5
Using the WhatsUp Customer Portal for product account information	5
Finding more information and updates.....	5

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

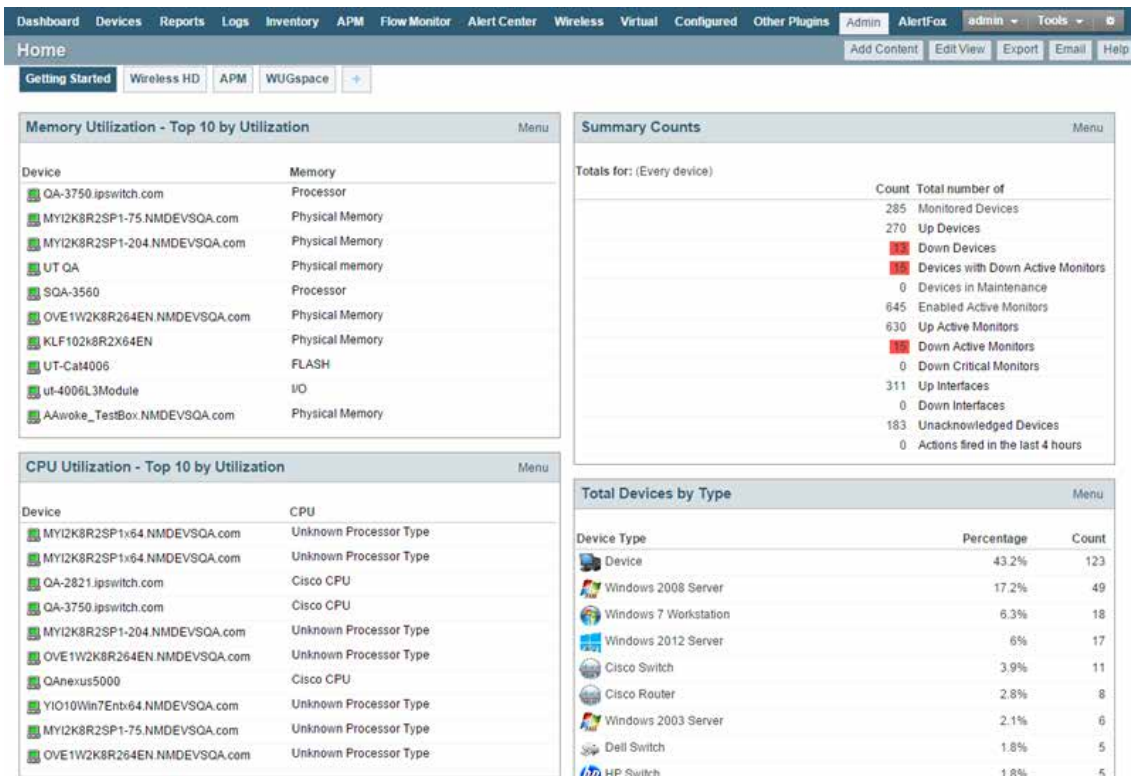
WhatsUp Gold actively polls devices to determine their status. You can use active monitors to poll services on a device and passively listen for messages sent across the network. Performance monitors track device performance by checking and reporting on device resources, such as disk, CPU, and interfaces.

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.



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 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 APM. This plug-in monitors applications across multiple devices, servers, and systems, providing performance statistics and overall application health, while alerting on performance degradation and potential problems before they result in service outages. APM helps IT organizations measure and guarantee Service Level Agreements (SLAs) and assists in pinpointing application performance bottlenecks and points of failure. For more information, see the *WhatsUp Gold web site* (<http://www.whatsupgold.com/APM>).

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. This plug-in for WhatsUp Gold leverages Cisco NetFlow, NetFlow v9 (Lite), sFlow, J-Flow, IPFIX, 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 site* (<http://www.whatsupgold.com/LogManagement>).

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/WUG163releasenotes>) 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 15) for highlight information about the web user interface.

Using the WhatsUp Gold community site

WUGspace is a 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 19).

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/WUG162releasenotes>).
- § **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/wug163gsg>).
- § **WhatsUp Community.** WUGspace is a 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>).

Security guidelines overview

WhatsUp Gold provides a number of important security features that you may configure and manage to maintain a secure deployment that defends against unauthorized access to the server as well as to devices providing data to the server.

Ipswitch recommends security best practices for WhatsUp Gold server deployment, configuration and management, including securing communication between the WhatsUp Gold server and external entities such as users and network devices that interact with or provide data to the server.

WhatsUp Gold stores sensitive user information and system credentials in encrypted format using AES 256-bit encryption. This important feature is enforced by default and no additional procedure is needed to enable or use it.

Security best practices

Ipswitch recommends the following best practices to establish a secure WhatsUp Gold system deployment and to maintain secure operation.

Best practices for administrators

- § Identify trusted administrators to install, configure, manage, and maintain the WhatsUp Gold system. These users may have access to complete server functionality and to sensitive information and they may even bypass auditing functions.
- § Install all WhatsUp Gold components in a locked room or equipment cabinet to limit physical server access to trusted administrators.
- § Install WhatsUp Gold software components on dedicated servers. Do not use these servers for any other purpose.
- § WhatsUp Gold secure operation depends on a trustworthy DNS server in the operational environment. A variety of steps are required to secure a DNS server. Contact your server vendor for relevant procedures.
- § If using an external LDAP or Active Directory server for authentication, configure the connection to use SSL. For more information, see *Setting LDAP credentials* (on page 868).
- § Use strong Windows passwords to prevent unauthorized access to the Windows operating system on server platforms where WhatsUp Gold components are installed.
- § Require all WhatsUp Gold users to use strong web UI passwords by following the password complexity rules defined in *WhatsUp Gold password management* (on page 13).
- § Require users to change password regularly.
- § Avoid using the WhatsUp Gold Administration Console Windows application (WhatsUp Gold Console) for routine operations because the Administration Console does not log any user actions or enforce device group access rights. Limit its use to initial configuration procedures of enabling WhatsUp Gold FIPS mode and enabling failover, and for occasional procedures like WhatsUp Gold backup and restore operations. For instructions see *Limiting access to the WhatsUp Gold Administration Console* (on page 8).
- § Restrict access to WhatsUp Gold Tools and Utilities because they are not regulated by device group access rights. Users can interact with any device that is accessible on the network. For instructions, see *Limiting Access to the WhatsUp Gold Tools and Utilities* (on page 8).
- § When establishing a connection with a network device, use the most secure method of communication supported by a particular device. For more information about using secure protocols, see *Using FIPS 140-2 cryptography* (on page 11).
- § Set WhatsUp Gold to FIPS mode and set WhatsUp Gold platforms (WhatsUp Gold servers, and any additional pollers) to use FIPS cryptography. These modes enforce the use of validated FIPS approved cryptographic algorithms which are more resistant to attacks than non-FIPS approved algorithms. For more information, see *Using FIPS 140-2 cryptography* (on page 11).
- § Inspect WhatsUp Gold logs regularly looking for signs of suspicious actions or the use of weak algorithms where stronger ones are available. In particular inspect the *Web User Activity Log* (on page 735) as that is the audit log for the WhatsUp Gold server.

Best practices for web users

- § Use strong web UI passwords by following the password complexity rules defined in *WhatsUp Gold password management* (on page 13).

- § Change your password at least once every three months.
- § When establishing a connection with a network device, use the most secure method of communication supported by a particular device. For more information about using secure protocols, see *Using FIPS 140-2 cryptography* (on page 11).

Limiting access to the WhatsUp Gold Administration Console

The Administration Console Windows application (WhatsUp Gold Console) does not log user actions and it does not enforce device group access rights. Users accessing the Administration Console can perform operations including setting web user passwords, ping, and traceroute operations on any device regardless of its device group associations.

Ipswitch recommends limiting use of the Administration Console to only trusted administrators such as the default Admin account, or to initial WhatsUp Gold configuration procedures like setting FIPS mode and ongoing (but occasional) procedures like WhatsUp Gold backup and restore operations.

To block access for most users:

- § Limit the **Access WhatsUp Gold Console** user right to only the default Admin account.
- § If WhatsUp Gold is not operating with FIPS Mode enabled, the **Access WhatsUp Gold Console** user right is not available. In this case, rely on the Windows administrator password to block users from accessing the Administration Console.

Limiting Access to the WhatsUp Gold Tools and Utilities

WhatsUp Gold Tools and Utilities are not regulated by device group access rights. Any user accessing these tools can perform ping, traceroute, DNS lookup, MIB walker, Layer 2 Trace, and other operations on any device that is accessible on the network.

Ipswitch recommends limiting use of the Tools and Utilities to only trusted administrators such as the default Admin account.

To block user access:

- § Do not give the **Access Tools and Utilities** user right to users.

Issuing User Rights and Device Access Rights conservatively

When you first start using WhatsUp Gold, device group access rights are not enabled. This approach makes it easy for users to discover and monitor network devices.

When you start adding users to the WhatsUp Gold system Ipswitch recommends enabling device group access rights and assigning users to home device groups. This limits users to specific sets of devices and also restricts the operations a user can perform on a device.

When you create new user accounts, no user rights are assigned to users by default. When assigning user rights, either directly or by using user groups, make sure that you assign only those rights required by users to perform their jobs.

A good general rule is to give users the minimum access needed to perform their job. For more information, see *Managing user accounts and user groups* (on page 874) for relevant procedures and additional information.

Monitoring WhatsUp Gold health and disk usage to prevent data loss

WhatsUp Gold stores sensitive data collected from devices as well as its own log data maintained in log files. You can avoid losing any of this critical data by configuring WhatsUp Gold to monitor itself by performing regular backups of the WhatsUp Gold database.

Monitoring WhatsUp Gold health

The WhatsUp Gold Alert Center includes a health monitoring function that alerts when any of the specified thresholds reaches or exceeds a set threshold. One important setting is to trigger an alert whenever the database size exceeds 80% of its capacity (the default threshold value is 80%). This gives you a chance to back up and purge the database of older device data so you do not exhaust database capacity and drop new incoming device data.

For more information, see *Configuring a WhatsUp Health threshold* (on page 598).

Monitoring WhatsUp Gold server disk usage

WhatsUp Gold must be set to monitor its own disk usage to avoid disk exhaustion. Over time, accumulated log files and other data can fill up a disk. Disk exhaustion causes services to run slowly and eventually fail in which case, WhatsUp Gold may drop incoming device data and log messages.

You can avoid this condition by creating and adding a performance monitor for the systems (the devices) hosting the WhatsUp Gold components. This includes primary and secondary WhatsUp Gold servers, additional pollers, and the WhatsUp Gold database server system if it is on a machine that is separate from the WhatsUp Gold secondary machine.

You must also create an Alert Center threshold to notify a Windows administrator who can intervene and offload older collected data to an archive database.

To monitor and alert when disk utilization exceeds 90%:

- 1 Establish SNMPv3 credentials to interact with each of the WhatsUp Gold server machines.
- 2 Create the following Alert Center thresholds as applicable:
 - § WhatsUp Gold Primary Server Disk Utilization Exceeds 90%
 - § WhatsUp Gold Secondary Server Disk Utilization Exceeds 90%
 - § WhatsUp Gold Database Server Disk Utilization Exceeds 90%For more information, see *Configuring Alert Center thresholds* (on page 553).
- 3 Add the Global Disk Utilization Monitor to each system in your WhatsUp Gold deployment. This monitor is available in the performance monitor section of device properties when you right-click the device in the device list. For more information, see *Working with Performance Monitors* (on page 453).

Nightly rollups of log files and collected device data for each day facilitate offloading the oldest data to an archive for safekeeping. For more information, see Program Options - Report Data. If you receive an alert that a WhatsUp Gold server is exceeding the 90% disk usage threshold, offload some of the oldest data to an archive for safekeeping.

Backing up the WhatsUp Gold database

You must perform regular backups of the WhatsUp Gold database to ensure collected device data is preserved. You can use the WhatsUp database utilities in the Administration Console to back up and restore the database including:

- § WhatsUp SQL Database
- § WhatsUp Flow Monitor SQL Database
- § Layer 2 Discovery Database

For more information, see *Maintaining the database* (on page 967) and the related topics for steps to back up and restore the database.

Set the WhatsUp Gold server platform to use FIPS cryptography

This procedure sets the underlying Microsoft server IIS and .NET connections to use FIPS validated cryptographic algorithms. IIS (Internet Information Server) handles communications with external web users. .NET connections handle communications with additional pollers (if used) and a secondary WhatsUp Gold failover server (if used).

Setting the WhatsUp Gold server platform to use FIPS cryptography means you must set any additional poller server system or secondary WhatsUp Gold failover server system to use FIPS cryptography as well. Web user browsers automatically use the correct cryptography.

To check for and enable use of FIPS cryptography:

- 1 Log on to Windows as administrator.
- 2 Click **Start > Control Panel > Administrative Tools**.
- 3 Expand **Local Security Policy > Local Policies > Security Options**.
- 4 Scroll down to **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
- 5 Double-click to select the Local Security Setting options, then select **Enabled** if it is not already enabled.

Using FIPS 140-2 cryptography

WhatsUp Gold provides a number of protocols for communicating with external entities consisting of:

- § Remote WhatsUp Gold users accessing the web interface.
- § WhatsUp Gold external components such as a secondary failover server, additional pollers, an external LDAP, or Active Directory server, if any of these optional components are used.
- § Devices on the network that provide data to WhatsUp Gold for action and storage.

Some of these protocols are insecure such as HTTP, telnet, FTP, TFTP, SNMPv1 and SNMPv2, such that an eavesdropper could intercept or even modify content used to trigger alarms and notifications. Wherever possible, Ipswitch recommends using the most secure protocols possible that employ strong encryption while avoiding insecure protocols. Secure protocols include HTTPS (SSL and TLS), SNMPv3, and SSHv2.



Note: Some passive monitors and flow monitors receive only plain text data (flow data and event logs) from network devices. Secure protocols are not available for these monitors.

When using secure protocols you need to store device credentials within WhatsUp Gold to enable communications.

WhatsUp Gold provides a FIPS mode you can set which configures WhatsUp Gold active monitors and performance monitors to use FIPS validated cryptographic algorithms for communicating with network devices. FIPS 140-2 is the Federal Information Processing Standard that specifies security requirements for a system protecting sensitive but unclassified information.

If WhatsUp Gold is installed on an operating system that is currently running in FIPS140-2 mode, WhatsUp Gold installer detects the FIPS compliant operating system and automatically places WhatsUp Gold in FIPS 140-2 mode upon initial installation and start-up. However, if WhatsUp Gold is installed on an operating system that is not running in the FIPS compliant mode or the operating system has the FIPS compliant mode enabled after a WhatsUp Gold install occurs, then you must manually enable the Operate in FIPS 140-2 mode option in the WhatsUp Gold console application Program Options General dialog. For more information, see *Enabling FIPS 140-2 mode* (on page 905).

Note the following important considerations if you plan to operate WhatsUp Gold in FIPS 140-2 mode:

- § WhatsUp Gold does not recommend that you enable FIPS if you plan to use SNMPv1, SNMPv2, or SNMPv3 credentials that do not use encryption or authentication.
- § WhatsUp Gold recommends that SSHv2 only be used with FIPS 140-2 certified algorithms, because WhatsUp Gold in FIPS 140-2 mode does not support communications using non-certified algorithms.
- § SNMPv3 credentials using MD5 and DES56 are prohibited; you are unable to enable FIPS if SNMPv3 credentials using MD5 exist in the Credentials Library. You must modify or remove such credentials in order to enable FIPS.

The following may occur when you try to enable FIPS 140-2 mode in the Program Options dialog:

- § An error message is presented indicates that you have non-compliant SNMPv3 credentials (but you have a compliant SSL certificate):
This option is disabled because the SNMPv3 credentials are not FIPS compliant. Go to the Credentials Library to edit or remove the SNMP credentials. After editing or removing the credentials, you can enable this option in the Program Options dialog.

Setting WhatsUp Gold server to use FIPS cryptography

This procedure sets the WhatsUp Gold server to use FIPS validated cryptographic algorithms within the following protocols:

- § SNMPv3 connections for Active Monitors and Performance Monitors.
- § SSH for WhatsConfigured connections.
- § SSL communication with an LDAP or Active Directory Server if one of these optional servers is used.

As an example, if you do not enable FIPS mode and you configure SSL communication with an LDAP or Active Directory Server, the SSL protocol may use weaker algorithms like MD5 hashing. Setting FIPS mode ensures SHA hashing is used to enforce better security. Make sure that you configure credentials for these protocols. For more information, see *Using credentials* (on page 267).

To enable FIPS 140-2 mode:

- 1 Open the Administration Console. In Windows, click **Start > All Programs > Ipswitch WhatsUp Gold > WhatsUp Gold Admin Console**.
- 2 Log on using the default user name (admin) and password (admin).
- 3 From the console main menu, click **Configure > Program Options**.
- 4 Click the **General** icon.
- 5 Select **Operate in FIPS 140-2 mode** to enable FIPS 140-2 mode.

Using WhatsUp Gold password management

WhatsUp Gold has two default user accounts named Admin and Guest. After WhatsUp Gold is installed, set strong passwords for these accounts to prevent unauthorized access. Follow the password complexity requirements below.

Additionally, Ipswitch recommends requiring all users to change their passwords at least once every three months. Be sure to send reminders to users to change their passwords on a regular basis.

The password change function is available in the WhatsUp Gold web interface **Admin > Preferences** dialog. Users must have the Change Your Password user right to change their password.

Password Complexity Requirements

Minimum strength passwords:

- § are at least eight characters in length and are not based on repetition, dictionary words, usernames, relative or pet names, or biographical information including ID numbers, ancestors' names or dates.
- § include both upper-case and lower-case characters and at least one of the following
- § at least one number
- § at least one punctuation symbol

Users whose password are set (or reset) by a WhatsUp Gold authorized user must change their passwords. Users must have the Change Your Password user right to change their password.

To change your WhatsUp Gold web interface password:

- 1 From the WhatsUp Gold web interface, go to **Admin > Preferences**. The User Preferences dialog appears.
- 2 Click **Change your password**. The Change Password dialog appears.
- 3 Enter your existing password into the **Enter Current Password** box.
- 4 Enter a new password into the **Enter New Password** and **Confirm Password** boxes.
- 5 Click **OK** to save changes.

Getting Familiar with WhatsUp Gold

In This Chapter

- Using the WhatsUp Gold Web Interface 15
- Using the WhatsUp Gold Console..... 21
- Using the Discovery Console..... 24
- Using WhatsUp Gold Mobile Access..... 25

Using the WhatsUp Gold Web Interface

In This Chapter

Accessing the web interface.....	15
About the WhatsUp Gold web interface.....	15
Using Application Settings: System.....	19
Organizing devices, device groups, and maps with drag-and-drop	19
About the Status Tray (WhatsUp Gold Status Center) and Desktop Actions applications	20

Accessing the web interface

You can connect to the WhatsUp Gold web interface from any supported browser by entering the WhatsUp Gold web address. The WhatsUp Gold web interface supports both IPv4 and IPv6 addresses.

The web address consists of the hostname or IP address 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/wuginstall_163) 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 662) and *Logs* (on page 720) tabs and dashboard reports are located in the *Dashboard* (on page 42) 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 19), 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 as well as force the device into maintenance mode. From a device list or report view, hover the mouse pointer over a device name to view popup information.

The screenshot displays the 'Details View' of the WhatsUp Gold interface. A table lists various devices with columns for 'Display Name', 'Host Name', and 'Address'. A mouse cursor is hovering over the device 'JCB12Win7x64.NMDEVSQLA.com', which has triggered a detailed popup window.

The popup window for 'JCB12Win7x64.NMDEVSQLA.com (192.168.1.100)' provides the following information:

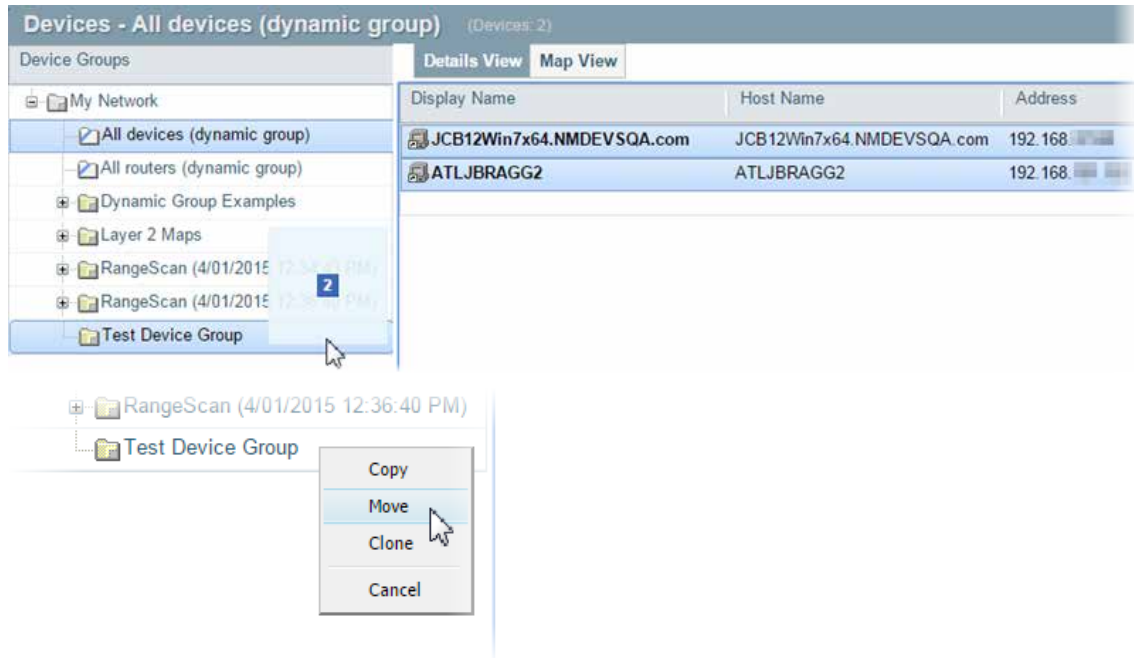
- Active Monitors - 0 Down**: Ping status is 'Up for 1 hour'.
- Performance Monitors**:
 - Ping Latency and Availability: 0 ms, Polled 6 minutes ago.
 - CPU Utilization: 7%, Polled 6 minutes ago.
 - Memory Utilization: 21.33%, Polled 6 minutes ago.
 - Disk Utilization: 65.26%, Polled 6 minutes ago.
- Group Membership**:
 - RangeScan (4/20/2015 12:30:51 PM)
 - VMware Cluster: NMDEVSQLA
 - VMware Datacenter: Atlanta
 - Layer 2 topology map
 - Virtual Infrastructure
- Put in Maintenance Mode**: A button at the bottom right of the popup.

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

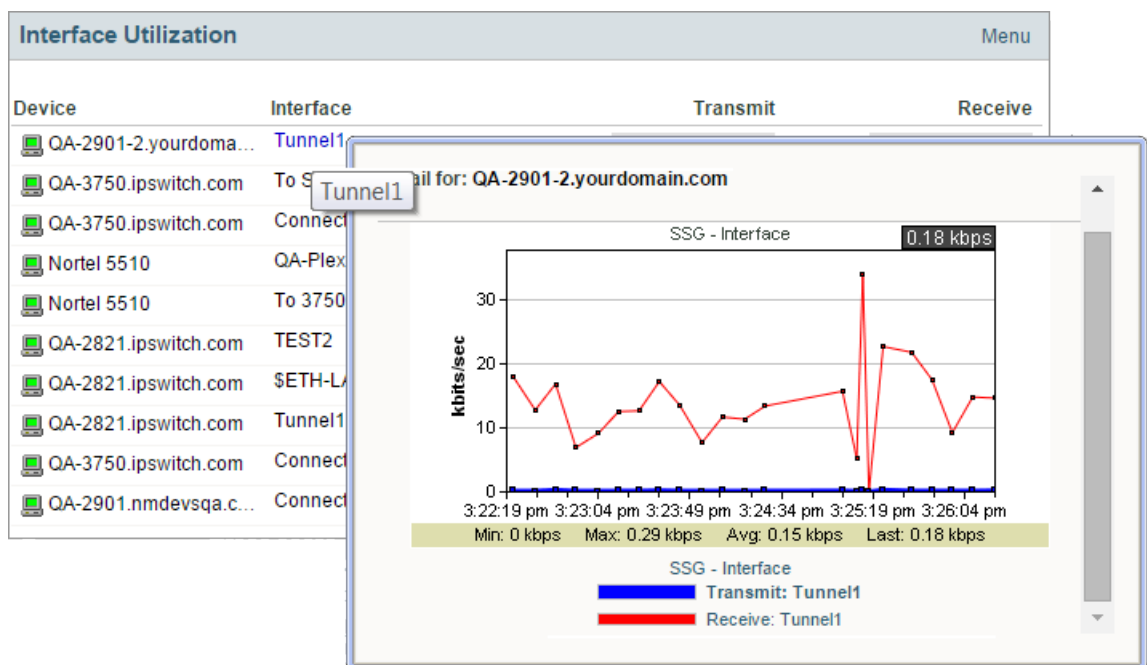
The screenshot shows a message bar at the bottom of the page. It contains the following information:

- Notification**: 'Aruba620-US set off a WebAlarm 5m ago.'
- Message**: '"This is my quiet web alarm"'
- Countdown**: '1 more WebAlarms have triggered since this alarm'
- Buttons**: 'View', 'Mute', 'Dismiss', and 'Dismiss All'.
- Checkbox**: 'Acknowledge Device with Dismissal' (checked).


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



- § **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.



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. 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 281).



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 Status Tray (WhatsUp Gold Status Center) and Desktop Actions applications

WhatsUp Gold installs two task bar icons on your computer; the Status Tray icon, now called the WhatsUp Gold Status Center, and the Desktop Actions icon.

WhatsUp Gold Status Center

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

To configure WhatsUp Gold Status Center 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

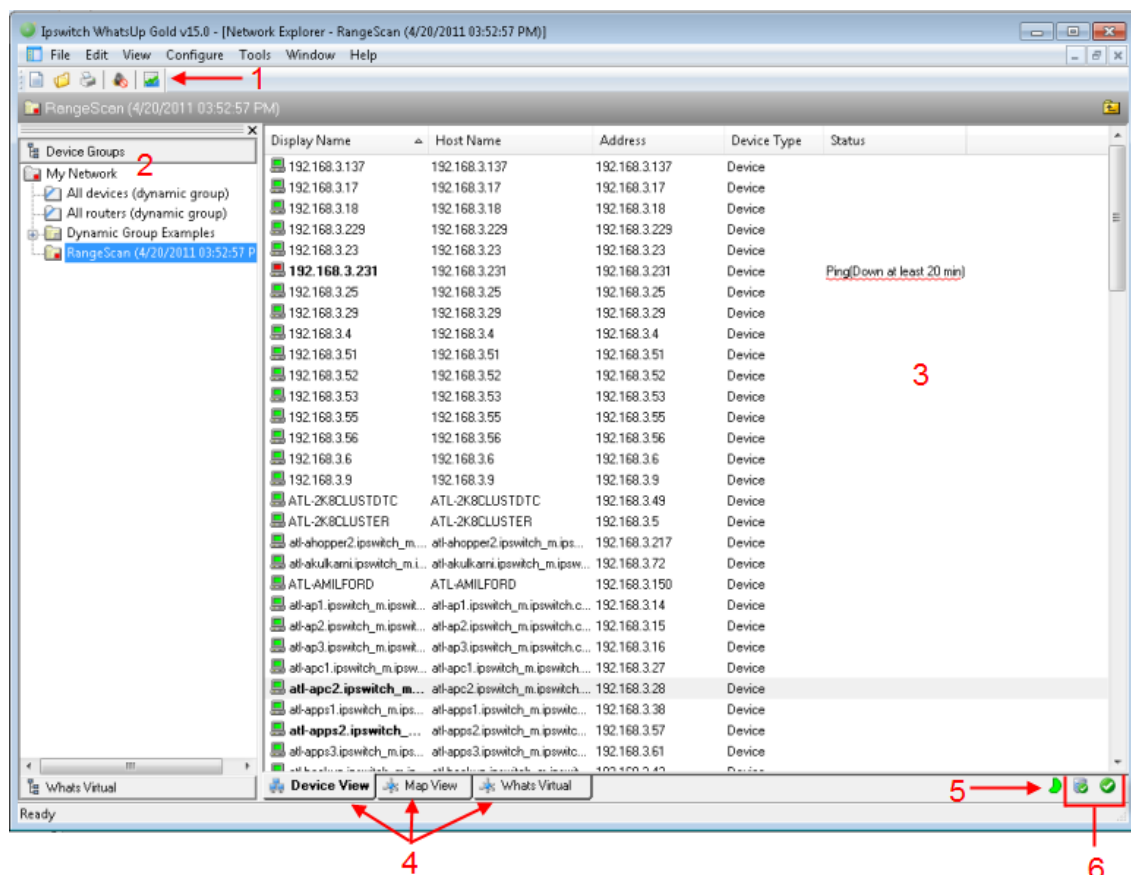
In This Chapter

About the console 21

About the Status Tray (WhatsUp Gold Status Center) and Desktop Actions applications 22

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.



- 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 Status Tray (WhatsUp Gold Status Center) and Desktop Actions applications

WhatsUp Gold installs two task bar icons on your computer; the Status Tray icon, now called the WhatsUp Gold Status Center, and the Desktop Actions icon.

WhatsUp Gold Status Center

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

To configure WhatsUp Gold Status Center 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 Discovery Console

In This Chapter

Learning about the Discovery Console 24

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 255) 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 242) 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 240) section.

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

- § *Devices Discovered* (on page 249)
- § *Progress Summary information* (on page 248)
- § *Device Information tab* (on page 253)
- § *Scheduled Discoveries tab* (on page 251)
- § *Saved Results tab* (on page 254)

Using WhatsUp Gold Mobile Access

In This Chapter

About WhatsUp Gold Mobile Access.....	25
Managing WhatsUp Gold mobile access.....	25
Accessing WhatsUp Gold from a mobile device	26
Navigating and using the WhatsUp Gold Mobile Access home screen	29

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 4.2



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/`

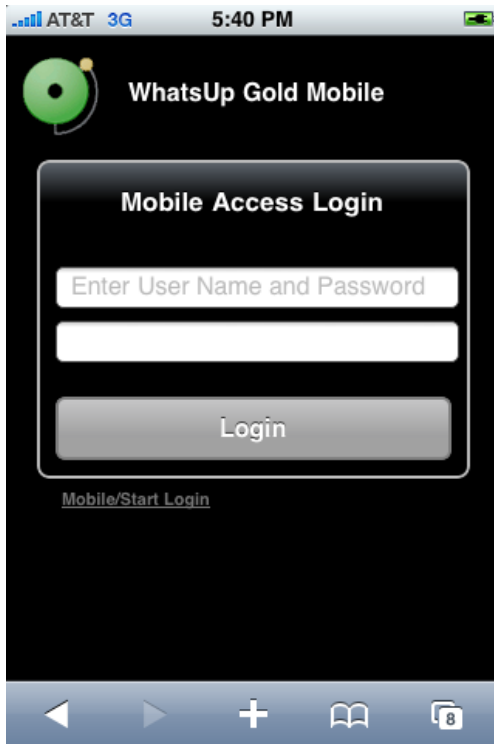


Note: When you use the default web server port (80), you do not have to include the port in the address. All ports other than 80 require that the port number follow the url in the web address.



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

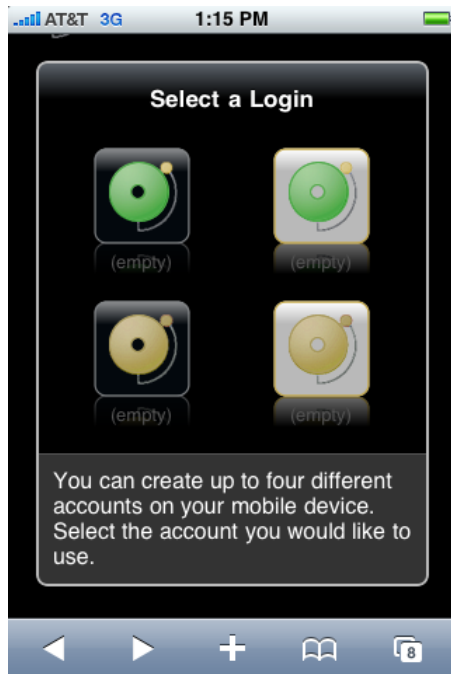
In addition to the standard login, WhatsUp Gold Mobile Access includes a one-click login feature. Because entering text in a mobile phone can be time consuming, WhatsUp Gold allows you to create up to four one-click logins per mobile device. You can bookmark each login or add to a mobile device Home 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.



- 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.



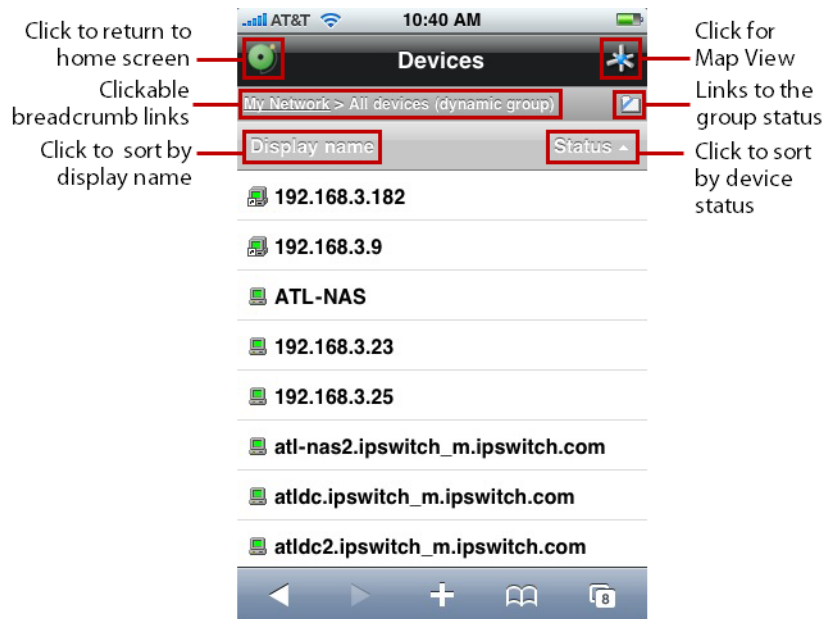
The home screen includes links to key WhatsUp Gold features so that you can view reports and monitor your network devices from remote locations:

- § 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.

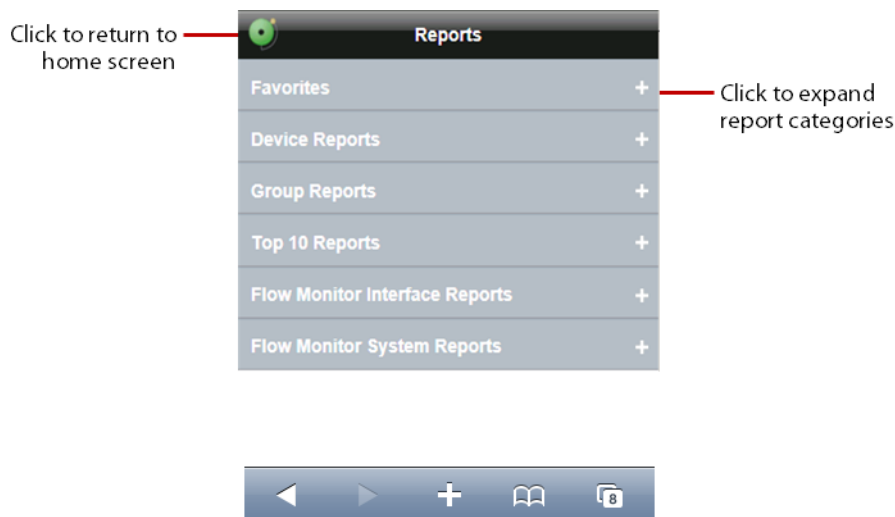


Click a device to view device reports or click a device group to view devices within a group.

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.



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:
`(123) 123-1234`

To add an email address as a Note or Attribute:

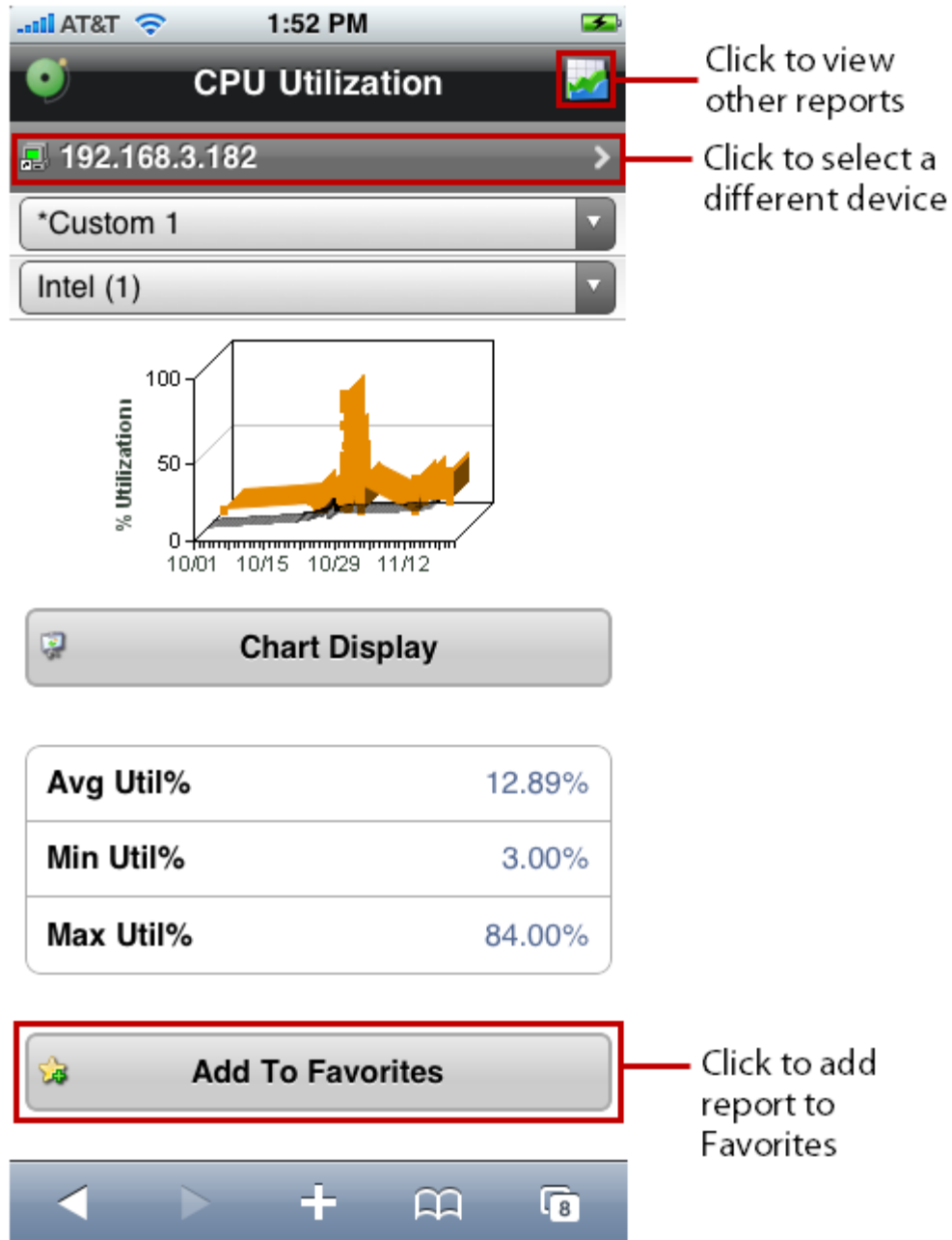
- 1 From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.
- 2 In the **Attribute** or **Note** field, use standard html code for an email link. For example:
`<a href="mailto:<John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

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

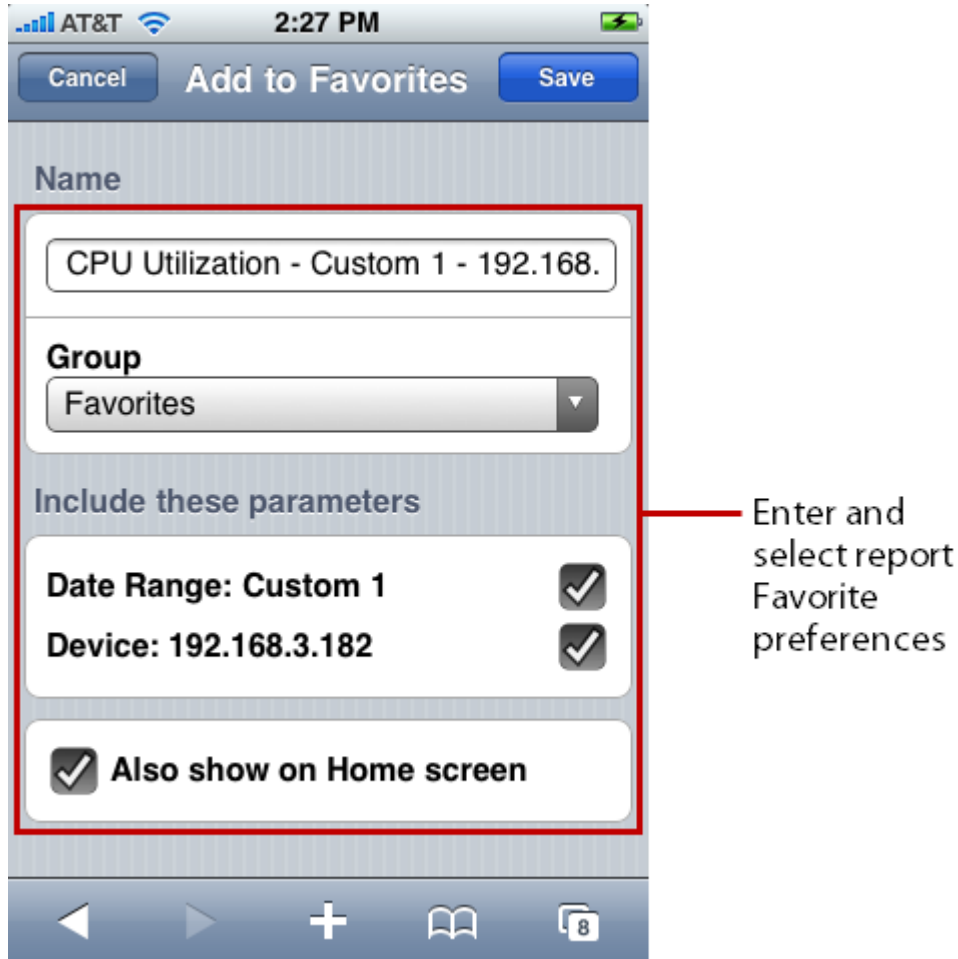
- 1 From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.
- 2 In the **Attribute** or **Note** field, use standard html code for a Google map link. Google map links can be copied 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.



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**.

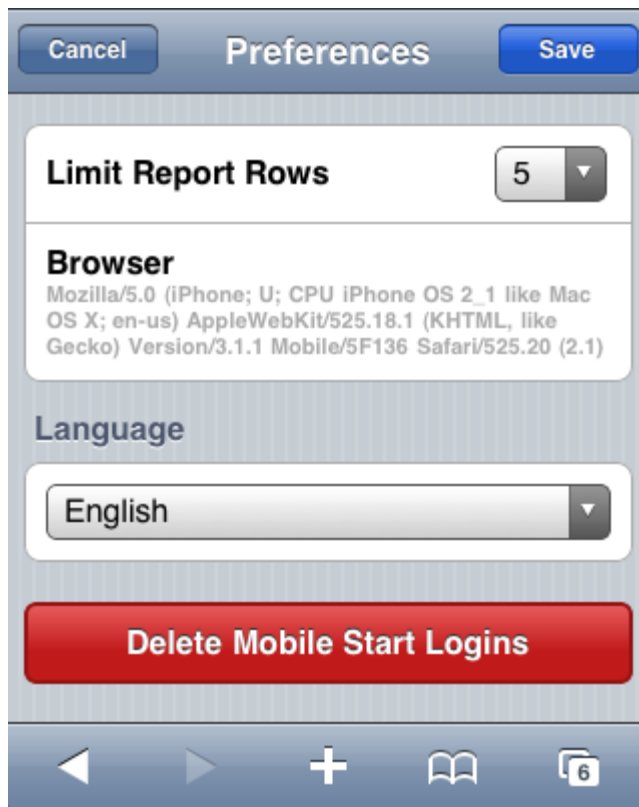


On the Home screen, click **Favorites** to expand and view your favorite reports. You can also click **Recent Reports** to view the ten most recent reports you have viewed.

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.



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	35
Poller Installation and Removal.....	37
Configuring WhatsUp Gold to use additional pollers.....	39
Poller Health Dashboard	39
Polling Performance Tuning.....	39
Using Polling with WhatsUp Gold Failover and Distributed editions	40
Poller usage in WhatsUp Gold	41

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. Using additional pollers can efficiently scale polling operations to a larger number of network devices, ultimately providing the capacity to monitor and manage larger networks.

Additional pollers are 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 WhatsUp Gold, 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 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 888).



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

In This Chapter

WhatsUp Gold Poller installation and configuration	37
WhatsUp Gold Poller Removal.....	38

WhatsUp Gold Poller installation and configuration

To install a poller on another network machine, you must obtain the install file from the **Download Now** link on the WhatsUp Gold support site (**Start > All Programs > Ipswitch WhatsUp Gold vX > Get Remote Poller** (<http://www.whatsupgold.com/products/download/wug-poller.aspx>)).

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 poller is installed on a remote machine, 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 this machine using the same user credentials used during the poller installation. You can also run the remote machine 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 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* (on page 92) 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 888).

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* (on page 48) and *Poller Health dashboard report* (on page 92).

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 below. 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 888).
- 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_163).

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 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, its 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 monitor and performance monitor data to the WhatsUp Gold server.

The following functions are supported by the WhatsUp Gold local poller and services. These features operate on the local poller only (not supported on pollers installed on remote machines):

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

Dashboard

In This Chapter

Understanding and using dashboards	43
Using Favorites.....	55
Viewing Dashboard reports.....	58

Understanding and using dashboards

In This Chapter

Learning about dashboards.....	43
About the Home Dashboard.....	44
About the Device Status dashboard.....	45
About the Top 10 dashboard.....	46
Overview of dashboard report categories.....	47
Adding dashboard reports to a dashboard view.....	48
Searching for dashboard reports.....	50
Working with dashboard views.....	50
Changing dashboard content.....	51
Using the dashboard report menu.....	52
Configuring a dashboard report.....	52
Moving dashboard reports within a dashboard view.....	53
Navigating dashboard views.....	53

Learning about dashboards

The WhatsUp Gold Home dashboard is the first screen you see after logging in to the web interface. This is your personal, customizable Home portal, or *dashboard*.

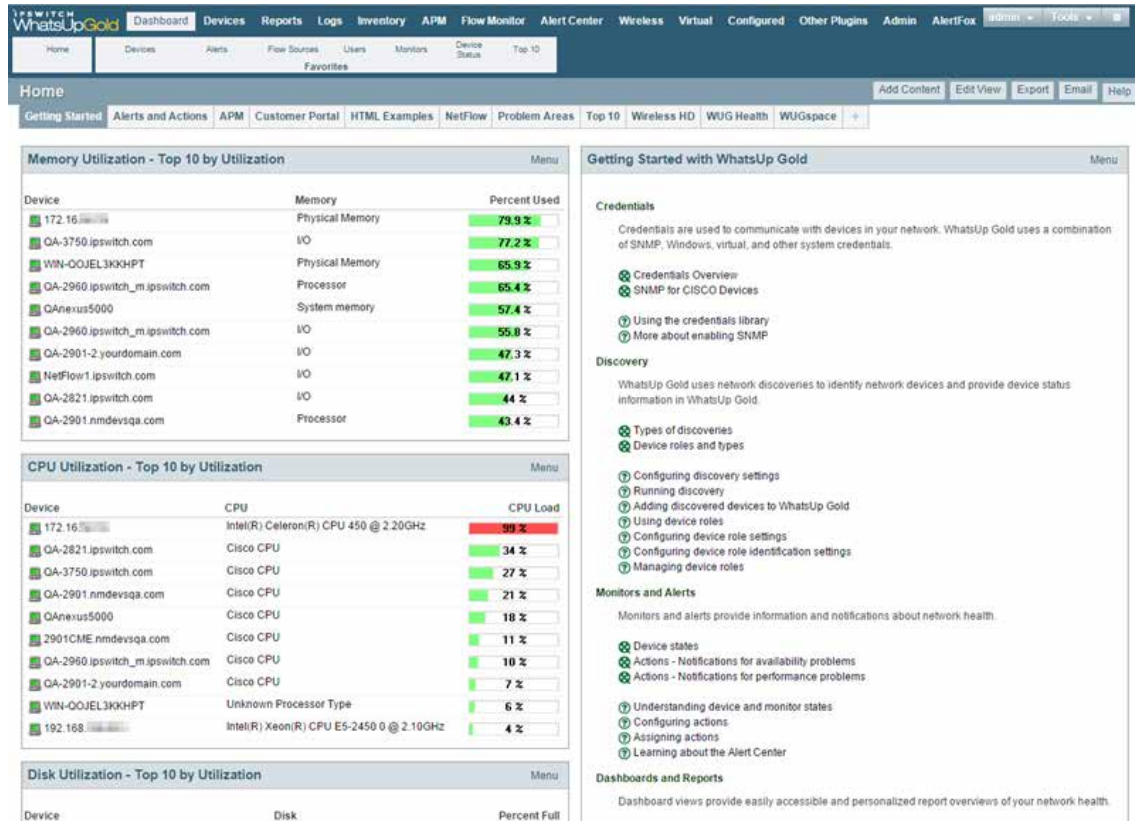
Dashboards in WhatsUp Gold are user-specific, and are configurable to include *dashboard reports* (on page 48) specific to users' needs. Dashboards contain multiple *views*, displayed as tabs, that let you organize groupings of dashboard reports according to the type of information they display. You can click on different view tabs within a dashboard to display different views within the same dashboard. For more information, see *Managing dashboard views* (on page 899)

When you begin customizing your dashboard views, consider the types of information you need to view most often, the devices to which you need to pay closest attention, and the level of detail you want to monitor through a particular dashboard view. For more information, *Adding dashboard reports to a dashboard view* (on page 48).

Changes that you make to a dashboard view affect only your user account. If you decide to completely change all of the dashboard views under your account, your user account is the only account affected by these changes.

About the Home Dashboard

The WhatsUp Gold *Home Dashboard* is the first screen that you see after you complete the initial setup of WhatsUp Gold and log in to the web interface. Referred to as Home, this universal dashboard is designed to display the network information that you need most visible.



You can place any dashboard report on a Home dashboard; including summary, group, and device-specific data.

The content of this Dashboard varies for each user. Changes that you make to a dashboard view only affect your user account. This Dashboard should contain the information about your network that is most important to you. This Dashboard comes with some stock content such as *Devices with Down Active Monitors* and *Top 10 Devices by Ping Response Time*, although these reports can and should be replaced by the reports that are most relevant to your needs.

The Home Dashboard for all versions of WhatsUp Gold displays Getting Started and Alerts and Actions starter views. Depending on your specific plug-ins, user rights, and licensing, additional starter views may be present by default.

Each dashboard view includes several default dashboard reports that you can decide to keep, alter, or remove. You can also add other dashboard reports to these views. For more information, see *Adding dashboard reports to a dashboard view* (on page 48).

You can create your own dashboard views for the Home dashboard through the *Manage Dashboard Views* (on page 899) dialog.

About the Device Status dashboard

Device Status dashboard

The Device Status dashboard is used to view information about a specific device. You can only add single device dashboard reports to the Device Status dashboard.



The Device Status dashboard presents relevant information about the health and performance of a *single* monitored device. Throughout the web interface you see links to devices, such as [HP ProCurve Switch](#). All of these links point to the Device Status dashboard for that device. If there is a potential problem with a monitored device, the Device Status dashboard is a good place to look for more information on the device status. The Device Status dashboard includes several default dashboard views:

- § Disk/CPU/Memory
- § General
- § Router/Switch/Interface
- § Virtual Current Utilization
- § Virtualization

The device name displays at the top of the Device Status report. To change the focus of the report to another device without leaving the report, select a new device from the device context in the dashboard title bar.



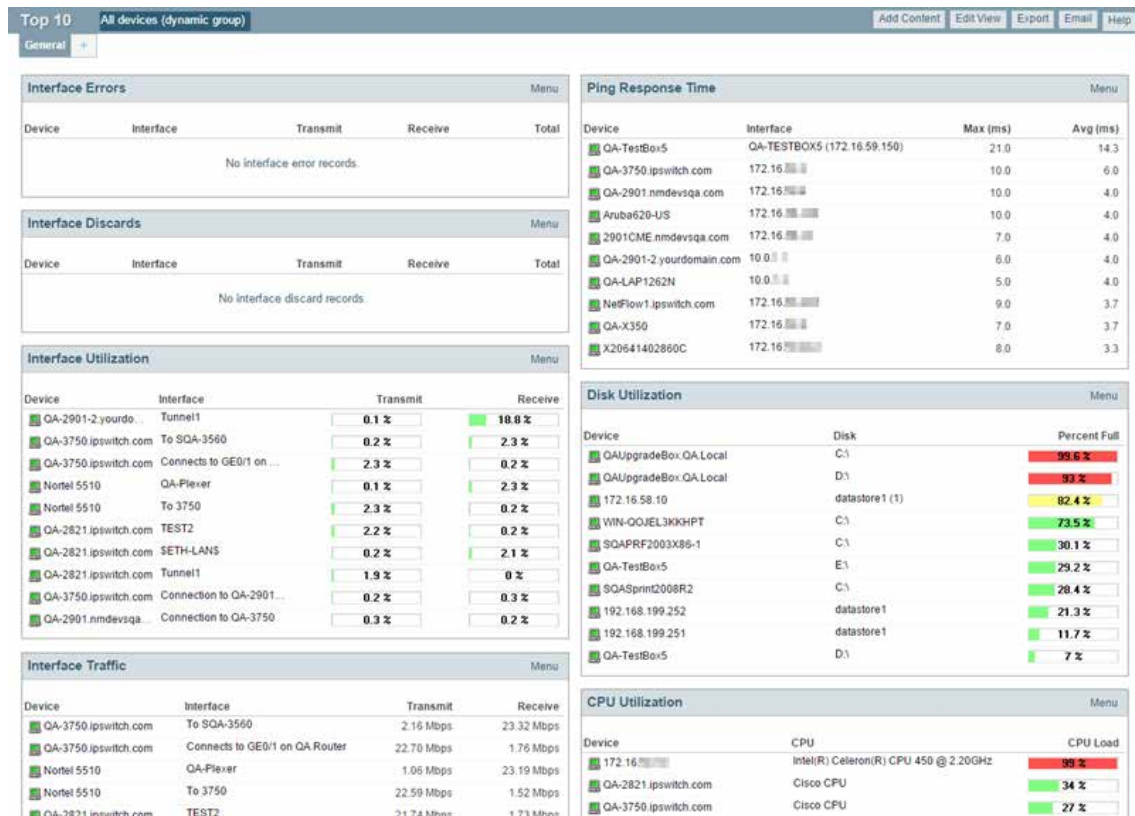
There are many different types of devices and a variety of features and services that can be monitored. The dashboard views let you select a view that is most appropriate for the individual device. Each time the report is visited, the last view selected for a device displays.

The Disk/CPU/Memory View is the most appropriate view for a Windows or UNIX host that supports the Host Resources MIB for performance monitoring. The Router/Switch/Interface View is the most appropriate view for a manageable Switch or Router that is capable of reporting Interface or Bandwidth utilization.

For more information, see *Adding dashboard reports to a dashboard* (on page 48).

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.



You can add any of the *Top 10 reports* (on page 229) 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* (on page 48).
- § 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* (on page 50).

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

Overview of dashboard report categories

WhatsUp Gold offers a collection of dashboard reports to display in a variety of ways on a dashboard and provide useful network information at a glance. These smaller reports show similar information to that found in the full reports. Because of their smaller size, multiple reports can be placed in a dashboard view, making it possible to view multiple reports simultaneously.

Dashboard reports are broken down into categories according to the type of information they display:

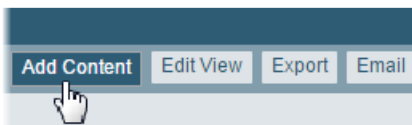
- § **Alert Center.** These dashboard reports display information that pertains to device thresholds and threshold summary information.
- § **CPU Utilization.** These dashboard reports display information that pertains to device and network CPU levels.
- § **Custom Performance Monitors.** These dashboard reports display information that pertains to your custom performance monitors.
- § **Disk Utilization.** These dashboard reports display information that pertains to device and network disk capacity levels.
- § **Flow Monitor.** Flow Monitor dashboard reports display data from Flow Monitor and can be used within Flow Monitor report views and WhatsUp Gold dashboard views.
- § **General.** These dashboard reports display information on your WhatsUp Gold settings and diagnostics, database size, as well as device-specific and user-configured details.
- § **Interface Errors and Discards.** These dashboard reports display information that pertains to device interface data errors and data discards.
- § **Interface Utilization.** These dashboard reports display information that pertains to device and network interfaces.
- § **Inventory.** These dashboard reports provide a break-down of network devices and their settings, including Actions, monitors, and policies.
- § **Memory Utilization.** These dashboard reports display information that pertains to device and network memory levels.

- § **Performance (Historic and Last Poll).** These dashboard reports display information gathered from WMI and SNMP Performance Monitors regarding your network devices' CPU, disk, interface, and memory utilization; and ping latency and availability.
- § **Ping Availability and Response Time.** These dashboard reports display information that pertains to device ping availability, response time, and packet loss.
- § **Problem Areas.** These are trouble-shooting dashboard reports that allow you to investigate network issues.
- § **Remote/Central** (included in the WhatsUp Gold Distributed, and MSP Editions). These include a variety of dashboard reports for the Remote Sites that you are monitoring with the WhatsUp Gold Central Site.
- § **Split Second Graphs Split Second Graphs** (included in the WhatsUp Gold Premium, Distributed, and MSP Editions). These are real-time graphs that display information on SNMP and WMI performance counters. These reports allow you to include the real-time information available on the *Web Performance Monitor* (on page 326) network tool and the *Web Task Manager* (on page 328) network tool in any dashboard view.
- § **Threshold.** These dashboard reports display information on your network CPU, disk, interface, and memory utilization, and ping function; at or above a specific threshold.
- § **Top 10.** These dashboard reports display the top devices on your network according to their CPU, disk, interface, and memory utilization, and ping function.
- § **Virtualization.** These dashboard reports display information about vCenter servers, virtual hosts and their associated virtual machines. You can see details about the virtual host or vCenter server, a list of the virtual machines, as well as CPU, disk, interface, and memory utilization for virtual machines.
- § **Wireless** (included in the WhatsUp Gold Premium, Distributed, and MSP Editions). These dashboard reports display information about Lightweight Access Points (Lightweight APs), Wireless Access Points (WAPs), and Wireless LAN Controllers (WLAN Controllers) devices as well as the devices connected to the WAPs, transmit and receive errors, and syslog messages.

Dashboard reports are listed multiple times in the **Add Content** pane. For example, the Disk Utilization dashboard report is listed under the Threshold, Top 10, and Performance categories.

Adding dashboard reports to a dashboard view

You can customize a dashboard by adding additional reports to the dashboard views. Click **Add Content** to add additional reports to the dashboard view.

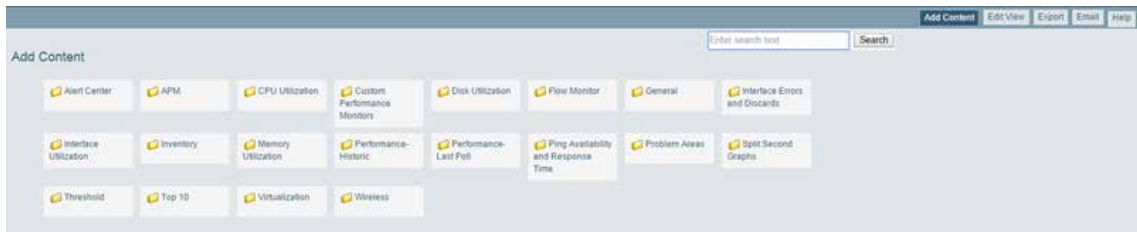


The reports available to add to the current dashboard vary, depending on the dashboard view type. Home dashboard views can include any available dashboard report, while you can only add reports which apply to a single device to a Device Status dashboard view. Reports are grouped into categories based on their function to make finding the right report easier.

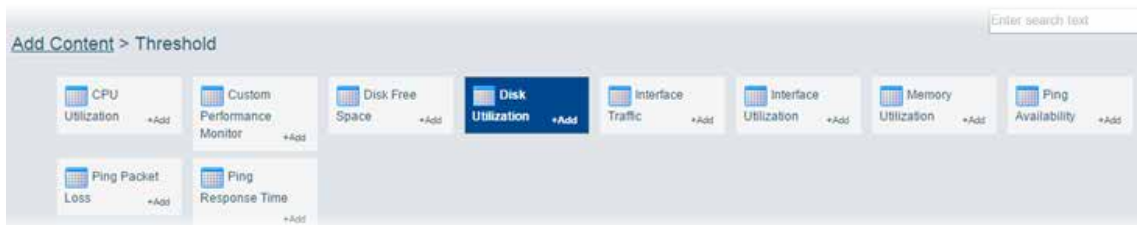
Report types include tabular, pie charts, line charts, gauges, and others, depending on the type of data displayed. When you select a report in the list, a report preview displays.

To add reports to a dashboard view:

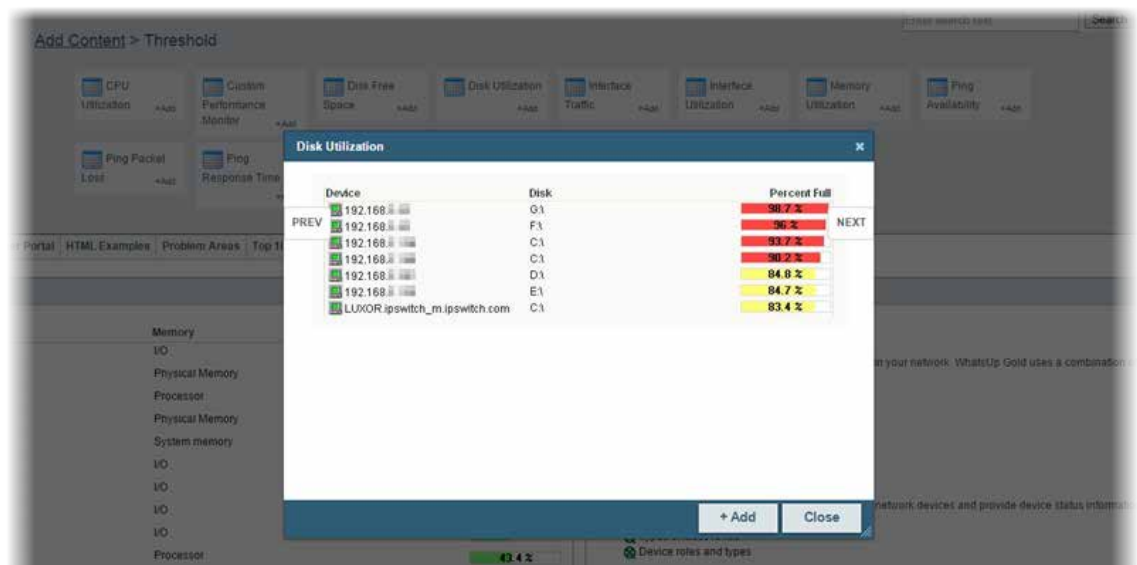
- 1 Open the dashboard and select the dashboard view where you want the report to appear.
- 2 In the title bar of the dashboard pane, click **Add Content**. The Add Content pane appears.



- 3 Select the category of report you want to add by clicking the related folder. The reports in that category display.



- 4 Click the report you want to add. A preview of the report displays.
- 5 Click the **Next** and **Prev** buttons to cycle through the next and previous reports within the category.



- 6 Click **Add**.
- 7 Continue selecting and adding reports until you have added all of the reports. You can add up to 15 reports to a single view.

- 8 When you have finished adding reports, click **Close** to close the report dialog.
- 9 Click **I'm Done** to return to the dashboard view. The newly added reports appear in the dashboard view.



- § To configure a report in your dashboard, click **Menu > Configure** in the title bar of the report.
- § To remove a report from a dashboard view, click **Menu > Close**.

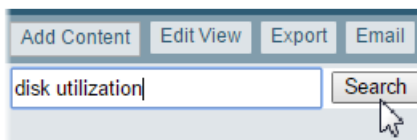
Threshold - Disk Utilization			Menu	Getting St
Device	Disk	Percent Full	Configure...	Help
QAUprgradeBox.QA.Local	C:\	99.6 %	Close	
QAUprgradeBox.QA.Local	D:\	93 %		
172.16.	datastore1 (1)	82.4 %		
WIN-QOJEL3KKHPT	C:\	73.5 %		

Searching for dashboard reports

Use the dashboard report search feature to locate specific reports that you want to add to a dashboard view.

To search for reports:

- 1 From the Home, Top 10, or Device Status dashboard, click **Add Content**. The Add Content pane appears.
- 2 Type all or part of the report name in the box at the top of the Add Content pane.
- 3 Click the **Search** button. The matching reports appear in the pane.



Working with 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 manage views for multiple users or configure dashboard views from the Admin tab, see *Managing dashboard views* (on page 899).
- § To switch to a different dashboard view, click a tab in the dashboard tabs.
- § To delete a view, click and drag the associated tab. The drag here to delete tab appears to the right of the plus sign (+).
- § Click **Add Content** to open the Add Content pane and select additional reports to add to the current view.

- § To change the order of the dashboard view tabs, click and drag a tab to a new location.

To create a new dashboard view from the dashboard:

- 1 From the dashboard where you want to add the new view, click the plus sign (+). The New Dashboard View dialog appears.
- 2 Enter or select the appropriate information:
 - § **View name.** Enter a unique name for the dashboard view.
 - § **Start with.** Select how you would like the dashboard view to begin. You may choose one 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).
- 3 Click **OK** to save changes.

To edit a dashboard view from the dashboard:

- 1 Click **Edit View** in the toolbar. The Edit Dashboard View dialog appears.
- 2 Enter the appropriate information:
 - § **View name.** Enter a unique name for the dashboard view.
 - § **Number of columns.** If it is a customized view, enter the number of columns to include in the view.
 - § **Column 1 width.** If it is a customized view, enter the width of the first column in the view (in pixels).
 - § **Column 2 width.** If it is a customized view, enter the width of the second column in the view (in pixels).
- 3 Click **OK** to save changes.

Changing dashboard content

Dashboard reports are smaller versions of the monitor reports listed on the Monitoring tab. The dashboard reports are displayed within WhatsUp Gold dashboard views. For more information, see *Understanding and using dashboards* (on page 43).

- § To add a report, click **Add Content** on the WhatsUp Gold toolbar to bring up the Add Content pane. From this pane, you can select multiple dashboard reports from multiple categories. A preview for the dashboard report displays when you select it. For more information see, *Adding dashboard reports to a Device Status dashboard* (on page 45).
- § To remove a report, click **Menu > Configure** for that dashboard report and then select **Close**. Keep in mind that when you remove a report, any customizations you have made to it are lost.

- § To move a dashboard report, click the report title bar and drag it to a new space in the dashboard view.
- § To change the settings for a dashboard report, click **Menu > Configure** in the title bar of that report.

Using the dashboard report menu

Each dashboard report has a menu on the right side of its title bar. From the Dashboard Report Menu, you can access help for a specific dashboard report, go to the configuration dialog for a report, or close the report. Closing a report removes it from the dashboard view. Keep in mind that after you remove a dashboard report from a dashboard, all customization to the dashboard report is lost.

Configuring a dashboard report

Dashboard reports can be customized to fit your specific needs. From a dashboard report menu, click **Configure** to open the configuration dialog. On this dialog, you can:

- § Change the report title
- § Select a device or device group for the report
- § Set the size of the report

Configure Report ? x

Report name:
Threshold - Disk Utilization

Device group: ☒ Every device
Every device

Threshold (%):
over 50.0

Maximum rows to return:
10

Column 2 width:
200

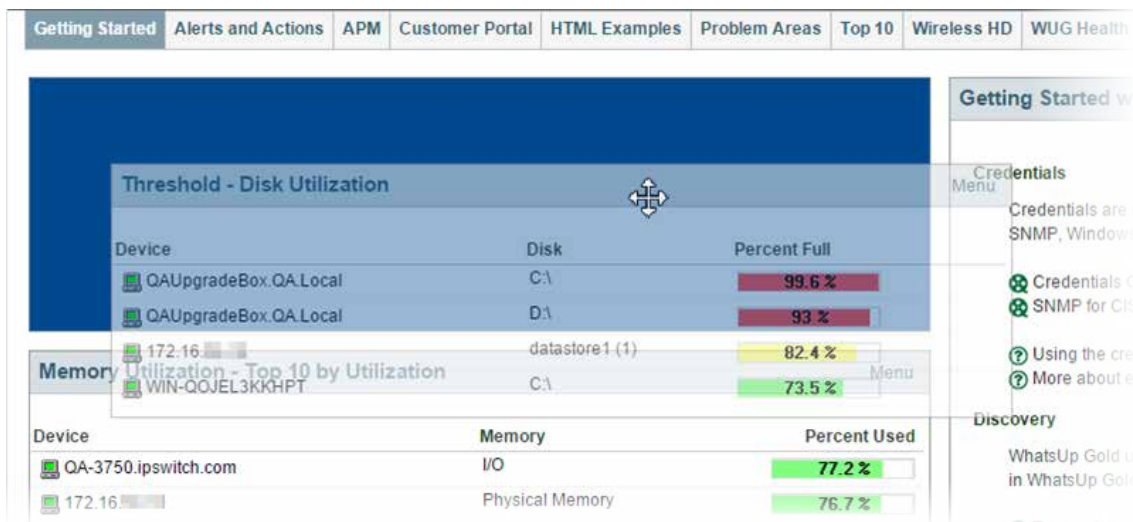
OK Cancel

Moving dashboard reports within a dashboard view

WhatsUp Gold supports drag-and-drop within the web interface. You can move a dashboard report from one column of a dashboard view to another, or position a dashboard report above or below another dashboard report, by clicking the report title bar and dragging it to another area of the dashboard view. The new dashboard configuration is saved, including after you log out from the web interface or when you move between dashboard views.

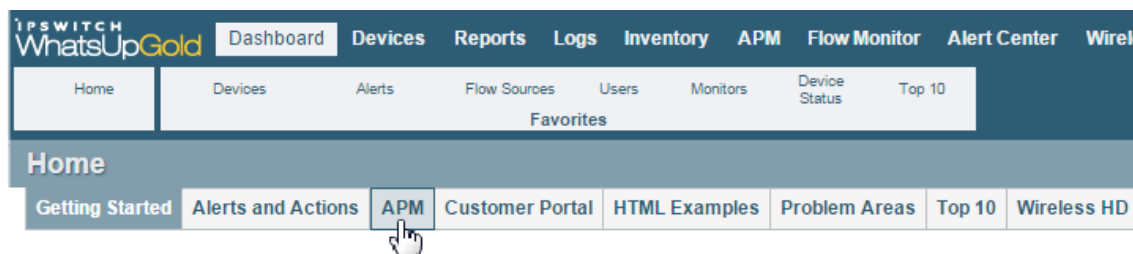
To move a dashboard report:

- 1 With the mouse pointer in the title bar of the report you want to move, click and hold the left mouse button.
- 2 Drag the pointer to the desired location. A blue box highlights the area where the report will appear.
- 3 Release the mouse button to place the report in the new page location. The report appears in the new location.



Navigating dashboard views

Navigate from one dashboard view to another by clicking the dashboard view tabs. You can also use the WhatsUp Gold toolbar to add content to a dashboard view, edit your dashboard and dashboard views, export and schedule report emails, and access the WhatsUp Gold help system.



The WhatsUp Gold Toolbar

Use the WhatsUp Gold toolbar to perform the following activities:

- § **Add Content.** Open the Add Content pane and add reports to your dashboard view.
- § **Edit View.** Edit your current dashboard view settings.
- § **Export.** Export the currently displayed data to a file.
- § **Email.** Email or schedule reports. For more information, see *Scheduling Reports* (on page 688).
- § **Help.** View online help topics for the window you are currently viewing.

Using Favorites

Understanding favorites

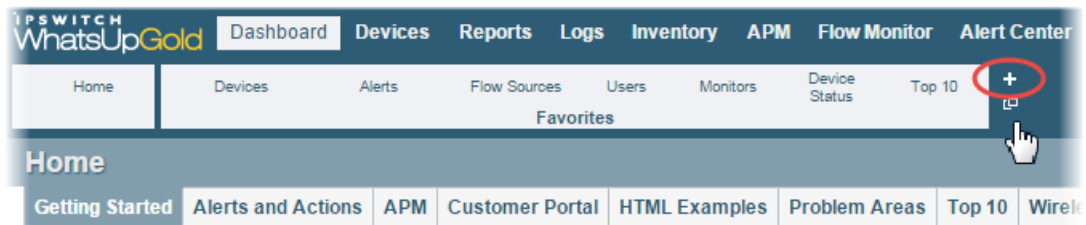
WhatsUp Gold favorites let you create your own customized toolbar by adding the WhatsUp Gold options you use most often to a single tab. You can edit and organize your favorites the way that best fits your needs. For more information, see *Adding favorites* (on page 55).

To access WhatsUp Gold Favorites, go to the **Dashboard > Favorites**.

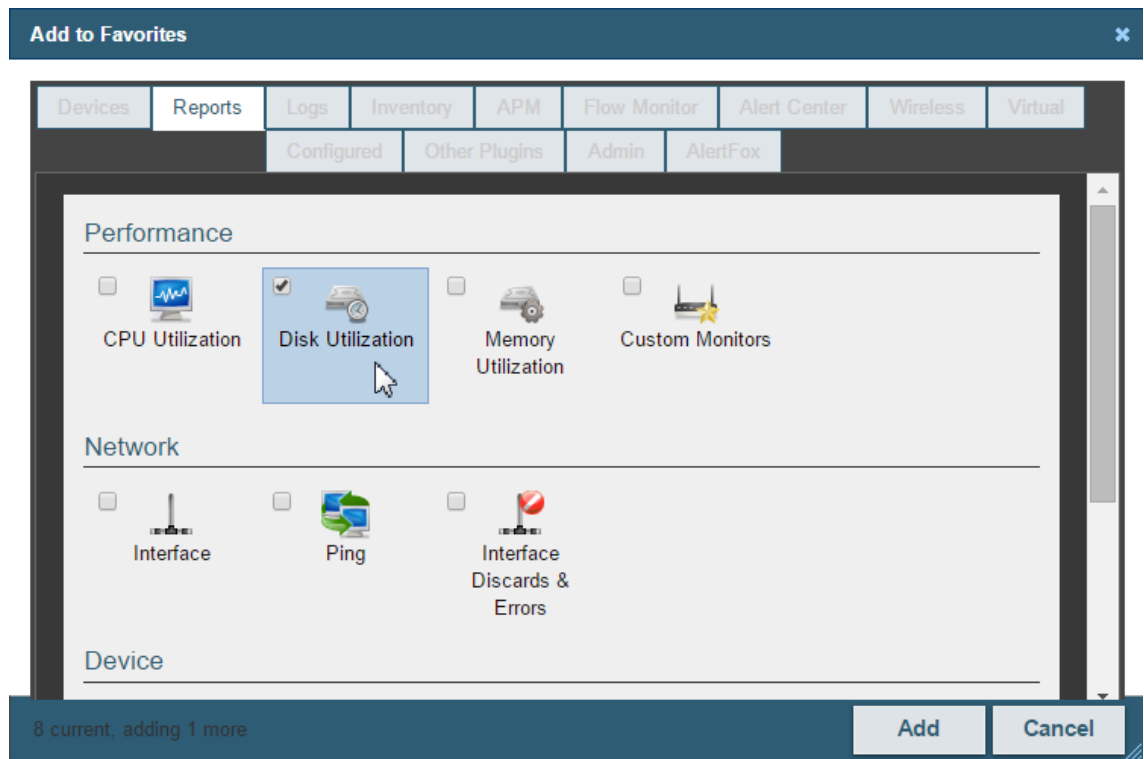
Adding favorites

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.

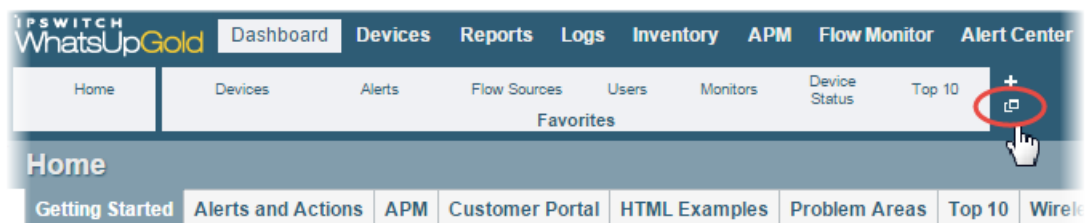


- 5 Continue clicking tabs and selecting buttons until you have added as many as you want to add.
- 6 Click **Add** to save your changes and add the selected buttons to your Favorites. The selected buttons appear in your Favorites group.

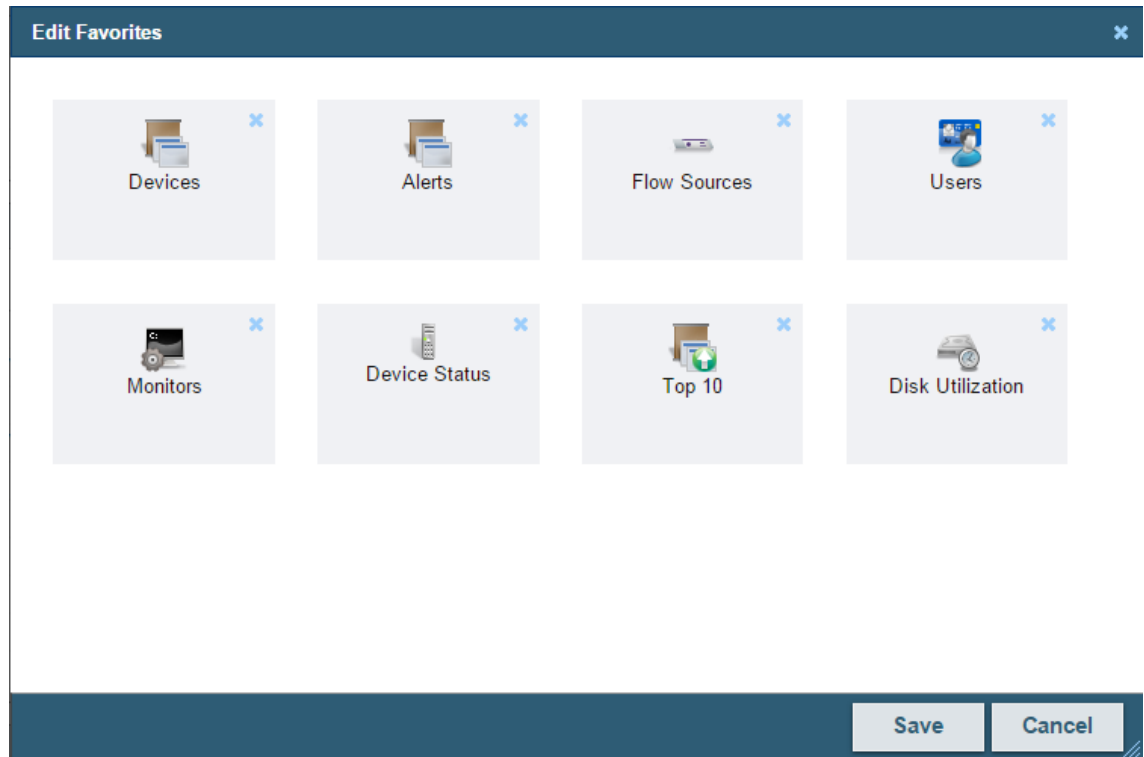
Editing favorites

To remove buttons from your Favorites group:

- 1 Click **Dashboard**.
- 2 Click the **Edit Favorites** icon.



- 3 From the dialog, click the **X** at the upper right of each button you want to remove from the toolbar.



- 4 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 Click and drag the buttons within the Edit Favorites dialog to the order you prefer.
- 2 When the buttons are in the preferred order, click **Save**. The dialog closes and the toolbar updates with the new button order.

Viewing Dashboard reports

In This Chapter

Alert Center reports	59
APM Dashboard Reports	61
CPU Utilization reports	63
Custom Performance Monitor reports	68
Disk Utilization reports	73
General reports	80
Interface Errors and Discards reports	96
Interface Utilization reports	104
Inventory reports	113
Memory Utilization reports	117
Performance-Historic reports	123
Performance-Last Poll reports	141
Ping Availability and Response Time reports	152
Problem Areas reports	161
Problem Areas Specific Device	172
Remote/Central reports	178
Split Second Graph reports	206
Threshold reports	221
Top 10 reports	229

Alert Center reports

In This Chapter

About the Alert Center: Threshold Summary report..... 59

About the Alert Center: Device Thresholds report..... 59

About the Alert Center: Threshold Summary report

This dashboard report displays the total number of unresolved items for each Alert Center threshold type.

If items have been acknowledged, they are included in parenthesis to the right of the number of unresolved items for a threshold type.



Tip: Click an unresolved items count to view the Alert Center Home page with that particular threshold type applied as a filter.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
- 3 Specify a **Name** for the report; this name appears at the dashboard report title.
- 4 Click **OK** to save changes.

For more information

Updating Alert Center items (on page 521)

About the Alert Center: Device Thresholds report

This device-level dashboard report displays Alert Center thresholds for which an aspect on the selected device is out of threshold.

For each threshold, the aspect and coinciding value is listed.

Performance thresholds:

- § Performance CPU, Disk, Interface, and Memory thresholds list the average utilization.
- § Performance ping availability lists ping packet loss.
- § Ping response time lists the average response time.

Passive thresholds:

- § Passive SNMP Trap lists the trap count.
- § Syslog lists the message count.
- § Windows Event lists the event count.



Note: This dashboard report does not display threshold data for Flow thresholds or for the WhatsUp Health threshold, as they are not device-specific thresholds.



Tip: Click a threshold name to view the Alert Center Item Details dialog.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

For more information

Updating Alert Center items (on page 521)

APM Dashboard Reports

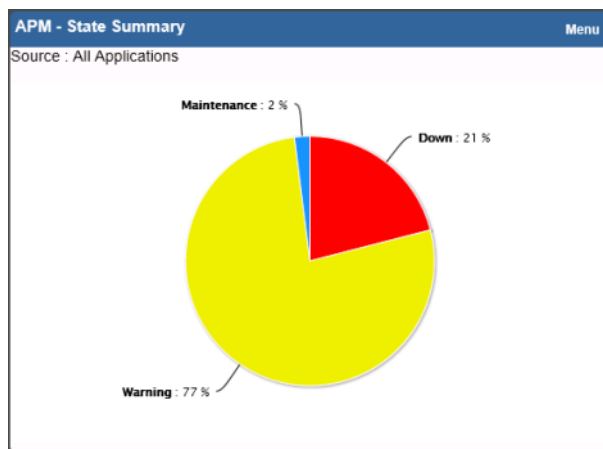
In This Chapter

About the APM: State Summary Dashboard Report 61

About the APM: Application Event Log Dashboard Report..... 62

About the APM: State Summary Dashboard Report

The State Summary dashboard report displays a pie chart depicting the application state of a selected application profile type, application profile, or application instance.



To configure the State Summary dashboard report:

- 1 From the State Summary dashboard report, click **Menu > Configure**. A Configure Menu dialog appears.
- 2 Click browse (...) to launch a dialog showing the APM navigation tree.
- 3 Select an application profile type, application profile, or application instance for display in the dashboard report.



Important: Summary data for any profile type, application profile, or application instance selected includes data for all components and groups under your selection in the navigation tree.

- 4 Click **OK**.
- 5 (Optional) Modify the **Report name**, **Width**, and/or **Height** of the dashboard report using the applicable boxes.
- 6 Click **OK**.

About the APM: Application Event Log Dashboard Report

The Application Event Log dashboard report displays state change, action activity and action resolution information for a selected application profile type, application profile, or application instance.

APM - Application Event Log			Menu
Source : All Applications			
Log Type : State Change, Action Activity, Resolved Action			
Date	Source Name	Details	
2/7/2013 1:25 PM	HP_Printer (QA Area)	Changed state to Up. Details : Com...	
2/7/2013 1:25 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Up. Details : 10 m...	
2/7/2013 1:20 PM	HP_Printer (QA Area)	Changed state to Warning. Details : ...	
2/7/2013 1:20 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Warning. Details : ...	
2/7/2013 1:15 PM	HP_Printer (QA Area)	Changed state to Up. Details : Com...	
2/7/2013 1:15 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Up. Details : 10 m...	
2/7/2013 1:10 PM	HP_Printer (QA Area)	Changed state to Warning. Details : ...	
2/7/2013 1:10 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Warning. Details : ...	
2/7/2013 1:00 PM	HP_Printer (QA Area)	Changed state to Up. Details : Com...	
2/7/2013 1:00 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Up. Details : 10 m...	
2/7/2013 12:40 PM	HP_Printer (QA Area)	Changed state to Warning. Details : ...	
2/7/2013 12:40 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Warning. Details : ...	
2/7/2013 12:35 PM	HP_Printer (QA Area)	Changed state to Up. Details : Com...	
2/7/2013 12:35 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Up. Details : 10 m...	
2/7/2013 12:30 PM	HP_Printer (QA Area)	Changed state to Warning. Details : ...	
2/7/2013 12:30 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Warning. Details : ...	
2/7/2013 12:25 PM	HP_Printer (QA Area)	Changed state to Up. Details : Com...	
2/7/2013 12:25 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Up. Details : 10 m...	
2/7/2013 12:20 PM	HP_Printer (QA Area)	Changed state to Warning. Details : ...	
2/7/2013 12:20 PM	HP_Printer (QA Area) : prtMarkerS...	Changed state to Warning. Details : ...	

To configure the Application Event Log dashboard report:

- 1 From the Application Event Log dashboard report, click **Menu > Configure**. A Configure Menu dialog appears.
- 2 Click browse (...) to launch a dialog showing the APM navigation tree.
- 3 Select an application profile type, application profile, or application instance for display in the dashboard report.



Important: Summary data for any profile type, application profile, or application instance selected includes data for all components and groups under your selection in the navigation tree.

- 4 Click **OK**.
- 5 (Optional) Modify the **Report name**, **Select Max items**, **Width**, and/or **Height** of the dashboard report using the applicable boxes.
- 6 (Optional) Enable/Disable the **Event Log Types** to be displayed within the dashboard report by clicking the applicable check boxes. Options are **State Change**, **Action Activity**, and **Resolved Action**.
- 7 (Optional) Click the **Show Source Type Column** check box to display the source of the state change or action for your selection within the dashboard report.
- 8 Click **OK**.

CPU Utilization reports

In This Chapter

CPU Utilization dashboard reports.....	63
About the CPU Utilization Last X hours/days (Single Device) report	64
About the CPU Utilization Last X hours/days (Specific CPU) report.	64
About the Last Polled CPU Utilization (Specific CPU) report.....	65
About the CPU Utilization: Last Polled Value (Single Device) report	66
About the Top 10: CPU Utilization report.....	67

CPU Utilization dashboard reports

CPU Utilization dashboard reports	Type	Description
Last Polled Values (single device)	Home	Shows the CPU utilization(s) for a specific device at the time of the last poll.
Last Polled Values (specific CPU)	Home	Shows the CPU utilization for a specific CPU at the time of the last poll.
Over 80% Utilization*	Home	Lists all network devices with a CPU utilization greater than 80%.
Over 90% Utilization	Home	Lists all network devices with a CPU utilization greater than 90%.
Top 10 by Utilization*	Home	Lists the top 10 devices based on their current CPU utilization percentage.
Top 20 by Utilization	Home	Lists the top 20 devices based on their current CPU utilization percentage.
Last 4 hours (single device)	Device	Details all CPU utilization percentages for one device over the last 4 hours.
Last 8 hours (single device)	Device	Details all CPU utilization percentages for one device over the last 8 hours.
Last 7 days (single device)	Device	Details all CPU utilization percentages for one device over the last 7 days.
Last 30 days (single device)	Device	Details all CPU utilization percentages for one device over the last 30 days.
Last 4 hours (specific CPU)	Home	Details CPU utilization percentages for a specific CPU for one device over the last 4 hours.
Last 8 hours (specific CPU)	Home	Details CPU utilization percentages for a specific CPU for one device over the last 8 hours.
Last 7 days (specific CPU)	Home	Details CPU utilization percentages for a specific CPU for one device over the last 7 days.
Last 30 days (specific CPU)	Home	Details CPU utilization percentages for a specific CPU for one device of the last 30 days.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the CPU Utilization Last X hours/days (Single Device) report

This device-level dashboard report displays multiple area graphs that detail the CPU utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor device CPUs to watch for trends, spikes, or drops in CPU utilization.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
 - § **Trend Type**. Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
 - § **Dimensions**. Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
 - § **Width**. Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: Large graph images can be used, but be aware that these larger images will refresh at slower speeds. The optimum size will depend on the speed of your network connection from your browser to your Web server.

- § **Height**. Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.
 - § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum**. Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the CPU Utilization Last X hours/days (Specific CPU) report

This home-level dashboard report displays a line graph that details the CPU utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes on one of their CPUs.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

- § **Report name.** Enter a title for the dashboard report.
- § **Device.** Select a device by clicking the browse (...) button.
- § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
- § **Graph type.** Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Width.** Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: You can use large graph images, but be aware that larger images refresh at slower speeds. The optimum size depends on the speed of your network connection from your browser to your web server.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
- § **Graph the maximum.** Select this option to graph the maximum.

3 Click **OK** to save changes.

About the Last Polled CPU Utilization (Specific CPU) report

This home-level dashboard report provides graphical illustration of a device's CPU utilization at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view a device's CPU status quickly, even from across the room.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available CPU space in green, and used space in red.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the CPU percentage used.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the CPU percentage used.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the CPU percentage used.
- § **Text.** A numerical representation of the CPU percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § **Red.** Above 90%
 - § **Yellow.** Between 80% and 90%

- § **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the CPU size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **CPU to graph.** Select the CPU that you want to monitor.
 - § **Graph type.** Select the type of graph you would like the report to display.
- 3 Click **OK** to save changes.

About the CPU Utilization: Last Polled Value (Single Device) report

This device-level dashboard report displays current CPU utilization percentages for all CPUs on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor the CPU(s) of an important device to watch for spikes in CPU utilization. The report shows:

- § **Description.** The particular CPU.
- § **CPU Load.** The percentage of the CPU currently in use. The colors displayed in the CPU Load column coincide with the WhatsUp threshold colors:
- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § To view a graphical representation of the report data, select **Use a graph to display the values**.
 - § If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types*. (on page 675)
- 3 Click **OK** to save changes.

About the Top 10: CPU Utilization report

This home-level dashboard report displays the top devices based on their current CPU utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load. Report percentages are displayed in colors that represent the CPU utilization thresholds:

- § Red. Above 90%
- § Yellow. Above 80%
- § Green. 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **CPU.** The device CPU description.
- § **CPU Load.** The percentage of CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information:
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

Custom Performance Monitor reports

In This Chapter

Custom Performance Monitor dashboard reports.....	68
About the Custom Performance Monitor Values	
Last X hours/days (Single Device) report.....	69
About the Custom Performance Monitor Values	
Last X hours/days (Specific Monitor) report.....	70
About the Last Polled Custom Performance Monitor Values	
(Single Device) report.....	71
About the Top 10: Custom Performance Monitor report.....	71
About the Threshold: Custom Performance Monitor report.....	72

Custom Performance Monitor dashboard reports

Custom Performance Monitor dashboard reports	Type	Description
Last Polled Values (single device)	Home	Details information on custom performance monitor(s) for a single device at the time of the last poll.
Last Polled Value (specific monitor)	Home	Details information on a specific custom performance monitor at the time of the last poll.
Top 10 with threshold*	Home	Lists the top 10 devices by a custom performance monitor threshold.
Top 20 with threshold	Home	Lists the top 20 devices by a custom performance monitor threshold.
Top 10 by specific monitors*	Home	Lists the top 10 devices by a specific custom performance monitor.
Top 20 by specific monitors	Home	Lists the top 20 devices by a specific custom performance monitor.
Last 4 hours (single device)	Device	Details custom performance monitors for a device over the last 4 hours.
Last 8 hours (single device)	Device	Details custom performance monitors for a device over the last 8 hours.
Last 7 days (single device)	Device	Details custom performance monitors for a device over the last 7 days.
Last 30 days (single device)	Device	Details custom performance monitors for a device over the last 30 days.
Last 4 hours (specific monitor)	Home	Details a specific custom performance monitor over the last 4 hours.

Custom Performance Monitor dashboard reports	Type	Description
Last 8 hours (specific monitor)	Home	Details a specific custom performance monitor over the last 8 hours.
Last 7 days (specific monitor)	Home	Details a specific custom performance monitor over the last 7 days.
Last 30 days (specific monitor)	Home	Details a specific custom performance monitor over the last 30 days.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the Custom Performance Monitor Values Last X hours/days (Single Device) report

This device-level dashboard report can display multiple graphs that detail custom performance monitors for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor a device's performance monitor(s) to watch for trends, spikes, or drops.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
 - § **Trend Type**. Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
 - § **Dimensions**. Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
 - § **Width**. Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: Large graph images can be used, but be aware that these larger images refresh at slower speeds. The optimum size depends on the speed of your network connection from your browser to your web server.

- § **Height**. Specify how tall, in pixels, the graph or chart should appear.
- § **Vertical Axis Scaling**. Select either auto or fixed scale.
- § **Min**. Enter a number for the lowest point on the Y axis.
- § **Max**. Enter a number for the highest point on the Y axis.

- § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Custom Performance Monitor Values Last X hours/days (Specific Monitor) report

This home-level dashboard report displays a line graph that details a custom performance monitor for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor important devices and their custom performance monitors.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Custom aspect to graph.** Select the aspect from the list.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
 - § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the web browser. Choose None, Line, or Curve.
 - § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
 - § **Width.** Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: You can use large graph images, but be aware that these larger images refresh at slower speeds. The optimum size depends on the speed of your network connection from your browser to your web server.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y axis.
 - § **Max.** Enter a number for the highest point on the Y axis.
- § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Last Polled Custom Performance Monitor Values (Single Device) report

This device-level dashboard report displays any custom performance monitors configured for a device and their last poll values. Placing this dashboard report in a device dashboard allows you to monitor important performance monitors and keep up with their latest poll values.

- § **Name.** The name of the performance monitor as listed in the Performance Monitor Library.
- § **Poll Time.** The time the last poll took place.
- § **Time Delta.** The time between the last two polls.
- § **Value.** The value of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
- 3 Click **OK** to save changes.

About the Top 10: Custom Performance Monitor report

This home-level dashboard report displays top devices in a group based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values.

- § **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.
- § **For group.** The group you selected to display in the report.
- § **Device.** The device associated with the custom performance monitor. Clicking on the device opens its Device Status dashboard.
- § **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list is empty.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

About the Threshold: Custom Performance Monitor report

This home-level dashboard report displays the top devices based on a selected custom WMI or SNMP performance monitor.

The top of the report displays the name of the selected custom performance monitor and to which device group the report applies.

Each entry in the report contains the following information:

Device. The monitored network device.

Value. The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
2. Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Performance monitor.** Choose a performance monitor from the drop-down menu. If there are no performance monitors listed in the drop-down menu, you must first configure a custom WMI or SNMP performance monitor from the Performance Monitor Library.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria from the separate list.
 - § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
3. Click **OK** to save the changes.

Disk Utilization reports

In This Chapter

Disk Utilization dashboard reports.....	73
About the Disk Utilization Last X hours/days (Single Device) report	74
About the Disk Free Space Last X hours/days (Specific Disk) report	75
About the Disk Utilization Last X hours/days (Specific Disk) report.	75
About the Disk Utilization: Last Polled Value (Specific Disk) report.	76
About the Disk Utilization: Last Polled Values (Single Device) report	77
About the Threshold: Disk Utilization report.....	77
About the Top 10: Disk Free Space report	78
About the Top 10: Disk Utilization report.....	79

Disk Utilization dashboard reports

Disk Utilization dashboard reports	Type	Description
Last Polled Values (single device)	Device	Shows the disk utilization for all disks for a specific device at the time of the last poll.
Last Polled Values (specific disk)	Home	Shows the disk utilization for a specific disk on one device at the time of the last poll.
All Disks Over 80%*	Home	Lists all network devices with disk utilization greater than 80%.
All Disks Over 90%	Home	Lists all network devices with disk utilization greater than 90%.
Top 10 by Utilization*	Home	Lists the top 10 devices based on current disk utilization percentages.
Top 20 by Utilization	Home	Lists the top 20 devices based on current disk utilization percentages.
Top 10 by Free Space*	Home	Lists the top 10 devices based on current free disk space.
Top 20 by Free Space	Home	Lists the top 20 devices based on current free disk space.
Last 4 hours (single device)	Device	Details all disk utilization percentages for one device over the last 4 hours.
Last 8 hours (single device)	Device	Details all disk utilization percentages for one device over the last 8 hours.
Last 7 days (single device)	Device	Details all disk utilization percentages for one device over the last 7 days.
Last 30 days (single device)	Device	Details all disk utilization percentages for one device over the last 30 days.
Last 4 hours (specific disk utilization)	Home	Details utilization percentages for a specific disk for one device over the last 4 hours.

Disk Utilization dashboard reports	Type	Description
Last 8 hours (specific disk utilization)	Home	Details utilization percentages for a specific disk for one device over the last 8 hours.
Last 7 days (specific disk utilization)	Home	Details utilization percentages for a specific disk for one device over the last 7 days.
Last 30 days (specific disk utilization)	Home	Details utilization percentages for a specific disk for one device over the last 30 days.
Last 4 hours (specific disk free space)	Home	Details free space for a specific disk for one device over the last 4 hours.
Last 8 hours (specific disk free space)	Home	Details free space for a specific disk for one device over the last 8 hours.
Last 7 days (specific disk free space)	Home	Details free space for a specific disk for one device over the last 7 days.
Last 30 days (specific disk free space)	Home	Details free space for a specific disk for one device over the last 30 days.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the Disk Utilization Last X hours/days (Single Device) report

This device-level dashboard report can display multiple area graphs that detail the disk utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor a device's disk(s) to watch for trends, spikes, or drops in its disk utilization.

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the appropriate information:
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.

- § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Disk Free Space Last X hours/days (Specific Disk) report

This home-level dashboard report displays a line graph that details the disk free space in GB for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes on their disk.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 2 Click **OK** to save changes.

About the Disk Utilization Last X hours/days (Specific Disk) report

This home-level dashboard report displays a line graph that details the disk utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes on their disk.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.

- § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report in pixels.
 - § **Height.** Enter a height for the report in pixels.
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y axis.
 - § **Max.** Enter a number for the highest point on the Y axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Disk Utilization: Last Polled Value (Specific Disk) report

This home-level dashboard report provides graphical illustration of disk utilization for a device at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view disk status quickly, even from across the room.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available disk space in green, and used space in red.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the disk percentage used.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the disk percentage used.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the disk percentage used.
- § **Text.** A numerical representation of the disk percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § **Red.** Above 90%
 - § **Yellow.** Between 80% and 90%
 - § **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the disk size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.

- § **Device.** Choose a device by clicking on the browse (...) button.
 - § **Disk to graph.** Select a disk to graph for devices with more than one disk.
 - § **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

About the Disk Utilization: Last Polled Values (Single Device) report

This device-level dashboard report displays current disk utilization percentages for all disks on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's disk(s) to watch for spikes in disk space. The colors displayed in the Percent Used column coincide with the WhatsUp threshold colors:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Description.** The particular disk.
- § **Size Used.** The size of disk in use at the time of the last poll.
- § **Total Size.** The total size of the disk.
- § **Percentage Used.** The percentage of the total size of the disk in use at the time of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § To view a graphical representation of the report data, select **Use a graph to display the values**.
 - § If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- 3 Click **OK** to save changes.

About the Threshold: Disk Utilization report

This home-level dashboard report displays the top devices based on their percentage of disk utilization. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their disk utilization by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Disk.** The description of the drive.
- § **Percent Full.** The amount of utilized disk space on that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold percentage and select a threshold criteria (*under, over, equals*) from the list.



Note: Though a default threshold exists, you can change this threshold. If you do so, change the report title accordingly.

- § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Disk Free Space report

This home-level dashboard report displays the top devices based on their percentage of available free disk space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk capacity by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Disk.** The device's drive description.
- § **Size.** The size of the disk in MB.
- § **Free space.** The amount of free space on the disk in MB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.

- § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the Description column in pixels.
- 3 Click **OK** to save changes.

About the Top 10: Disk Utilization report

This home-level dashboard report displays the top devices based on their percentage of utilized disk space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Disk.** The drive description.
- § **Percent Full.** The percentage of the disk currently utilized.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

General reports

In This Chapter

General dashboard reports.....	80
About the General: Custom Links report.....	82
About the General: Database Size report.....	82
About the General: Database Table Usage report.....	83
About the General: Device Active Monitor States report.....	83
About the General: Device Attributes report.....	84
About the General: Device Custom Links report.....	84
About the General: Device Dependencies report.....	85
About the General: Device Notes report.....	85
About the General: Device Performance Monitor Summary report	85
About the General: Device SNMP Details report.....	86
About the General: Device Status report.....	87
About the General: Device Toolbar report.....	87
About the General: Element Count report.....	88
About the General: Favorite Reports report.....	88
About the General: Free Form Text/HTML report.....	89
About the General: Group Status report.....	89
About the General: Interface Details (Specific Interface) report.....	90
About the General: Map View report.....	91
About the General: Monitors Applied report.....	92
About the General: Poller Health report.....	92
About the General: Search Knowledge Base report	93
About the General: Summary Counts reports.....	93
About the General: Web User Activity Log	94

General dashboard reports

General dashboard reports	Type	Description
Custom Links	Device	Displays any custom links assigned to a device in Device Properties > Custom Links .
Database Size	Home	Displays a graphical representation of the WhatsUp Gold database at the time of the last poll.

General dashboard reports	Type	Description
Database Table Usage	Home	Displays a graphical representation of the WhatsUp Gold top five database tables. If Flow Monitor is installed, Flow Monitor or Flow Monitor Archive database views can be configured to display in the dashboard report.
Device Active Monitor States	Device	Lists all of a device's Active Monitors and their current state.
Device Attributes	Device	Displays device attributes configured in Device Properties > Attributes .
Device Custom Links	Home	Displays any custom links that you add to the dashboard report.
Device Dependencies	Device	Shows the state of a device and any devices that are up or down dependent on that device.
Device Notes	Device	Displays device notes configured in Device Properties > Notes .
Device Performance Monitor Summary	Device	Displays a polling summary for the device currently in context.
Device SNMP Details	Device	Displays device SNMP details.
Device Status	Device	Displays device details, active monitors, attributes, and the device groups to which a device belongs.
Device Toolbar	Device	Displays device details configured in Device Properties > General .
Element Count	Home	Displays inventory quantity data, which can help determine the proper licensing count when purchasing upgrades and additional WhatsUp Gold plug-ins.
Favorite Reports	Home	Displays a list and link to any full report on your list of favorites
Free Form Text/HTML	Home	Displays any free form text or HTML code that you add to the dashboard report.
Group Status	Home	Displays a summary for the selected device group.
Interface Details	Home	Displays SNMP information reported by a specific network interface.
Map View	Home	Displays a smaller version of a network map.
Monitors Applied	Home	Displays a list of any Active, Passive, or Performance monitors assigned to the selected device.
Poller Health	Home	Displays the status of the local poller and all pollers installed on your network
Search Knowledge Base	Home	Allows you to search the WhatsUp Gold Knowledge Base.
Getting Started with WhatsUp Gold	Home	Displays information regarding the new the new web interface, dashboard, and dashboard reports.
Web User Activity Log	Home	Displays a log of when a user logs on or off the web interface, and the actions taken while logged on.

About the General: Custom Links report

This universal dashboard report lets you add http links to a dashboard for easy access. For example, use this dashboard report to add a link to your company's home page to easily access this page from the WhatsUp web interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.
 - § Click **Add** to add a new custom link to the dashboard report.
 - § Select an existing link and click **Edit** to change an existing link.
 - § Select an existing link and click **Remove** to remove a link from the list.
 - § Move an existing link up or down the list by first selecting it, and then clicking **Up** or **Down**.
- 3 Click **OK** to save changes.

About the General: Database Size report

This home-level dashboard report provides graphical illustration of the database size at the time of the last poll. Placing this dashboard report in a dashboard allows you to view your database size at a glance.

The graph uses color to show the current status:

- § **Red**. Above 75%
- § **Yellow**. Between 50% and 75%
- § **Green**. 50% or less

Under the graph, the database size is listed in MBs, along with the percentages for used and free space.



Note: Graphs will only show for Microsoft SQL Server Express Editions, as other editions of Microsoft SQL Server have no size limitations.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Pie**. A 3-D pie graph that displays available database space in green, and used space in red.

- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the database percentage used.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the database percentage used.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the database percentage used.
- § **Text.** A numerical representation of the database percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

- 3 Click **OK** to save changes.

About the General: Database Table Usage report

This home-level dashboard report provides bar graphs of the top five WhatsUp Gold database tables' usage. The remaining database table space usage is graphed in the *Other* category. If Flow Monitor is installed, Flow Monitor or Flow Monitor Archive database views can be configured to display the number of records for each record type in the dashboard report. Placing this dashboard report in a dashboard allows you to view the top five database table sizes and manage the database size as it grows.



Note: Graphs only show for Microsoft SQL Server Express Editions, as other editions of Microsoft SQL Server have no size limitations.



Tip: You can use the Alert Center to set database threshold alerts for WhatsUp Gold and Flow Monitor. For more information, see *Configuring a WhatsUp Health threshold* (on page 598).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Select Database.** Select the WhatsUp Gold, Flow Monitor, or Flow Monitor Archive database to display in the report.
- 3 Click **OK** to save changes.

About the General: Device Active Monitor States report

This device-level dashboard report lists all of a device's Active Monitors and their current state. Adding this report to a Device Status dashboard will update you on the health of a crucial device's Active Monitors, as well as list what Active Monitors are currently configured for the device. If you only want to see down Active Monitors, see Problem Areas: Down Active Monitors *Problem Areas Specific Device: Down Active Monitors* (on page 172).

- § **Monitor.** The type of Active Monitor.
- § **State.** The state of the Monitor after the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Click browse (...) to add a device.
- 3 Click **OK** to save changes.

About the General: Device Attributes report

This device-level dashboard report displays device attributes that are configured/added to a device in **Device Properties > Attributes**. By adding this dashboard report to a device dashboard, you can keep important identification information visible. For example, you can include the location of a device, to whom a workstation belongs, or other identification indicators.



Tip: Clicking the device icon brings up its Device Status Report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
- 3 Click **OK** to save changes.

About the General: Device Custom Links report

This dashboard report displays a customizable list of web links for a single device. Although the report can be displayed from the dashboard, in order to create the customizable list of web links, you must perform this task through Device Properties. For more information, see *Using Device Properties - Custom Links* (on page 313).

Each entry in the report contains the following information:

- § **Device**. The name of the selected device.
- § **Custom Links**. The customizable list of web links.

To configure the report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Graph dialog appears.
- 2 Modify the appropriate information.
 - § **Report name**. Change the title for the dashboard report, if applicable.
 - § **Device**. Click the browse (...) icon to select the device that you want the report to include.
- 3 Click **OK**. The selected device name and the custom links will display below the report name on the main report page.

About the General: Device Dependencies report

This device-level dashboard report shows the state of a device and any devices that are up or down dependent upon it. In addition, the states of these dependent devices are listed along with any down Active Monitors.

This dashboard report contains the following boxes:

- § **Dependencies for:** The selected device's name or IP address.
- § **The selected device is Up dependent on:** any device(s) the selected device is Up dependent on. If none are listed, the selected device is not Up dependent on any other device(s).
- § **The selected device is Down dependent on:** any device(s) the selected device is Down dependent on. If none are listed, the selected device is not Down dependent on any other device(s).

For more information on setting dependencies, please see the Dependencies Overview and Setting Dependencies.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
- 3 Click **OK** to save changes.

About the General: Device Notes report

This device-level dashboard report displays device notes configured in **Device Properties > Notes**. You may want to add this dashboard report to the dashboard of a device to help differentiate it from other devices you are monitoring, or to keep up with important reminders for a specific device.



Tip: Clicking on the device icon opens its Device Status Report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Click browse (...) to select the device this report applies to.
- 3 Click **OK** to save changes.

About the General: Device Performance Monitor Summary report

This device-level dashboard report summarizes all Performance Monitors configured for a single device.

The dashboard report includes the following boxes:

- § **Performance Monitor Type.** The type of Performance Monitor, for example, CPU Utilization.
- § **Polling Collection.** What the application is polling, for example, "All," "Default," or "Active Interfaces."
- § **Polling Interval.** How often the Performance Monitor is being polled.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Column 1 width.** Enter a width for column 1 in pixels.
- 3 Click **OK** to save the changes.

About the General: Device SNMP Details report

This device-level dashboard report displays a device's SNMP details. You can use this dashboard report to display a variety of device-specific SNMP details to assist in monitoring important devices. For example, you can use it to monitor how long a device has been up and to pin-point its down time.

Click on the device to bring up its Device Status Report.

- § **Property.** The OID label.
- § **Value.** The information returned from the poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § Click **Add** to add another OID to the SNMP value list from the MIB Browser.
 - § Select an existing OID, then click **Edit** to make a change.
 - § Select an existing OID, then click **Remove** to delete it from the list.
 - § Move an OID up or down the list by selecting it and clicking either **Move Up** or **Move Down**.
- 3 Click **OK** to save changes.

About the General: Device Status report

The Device Status dashboard report displays a snapshot of a specific device. You can change the device-in-context, but the dashboard reports within the Device Status Dashboard remain the same. The Device Status dashboard report displays the following information for a device:

Display name. The name that displays in WhatsUp Gold for the device.

Device type. The type of device.

Host name. The host name for the device.

Address. The address of the device.

Active Monitors. A list of any active monitors applied to the device and their current state.

Attributes. Any additional information about the device.

Group membership. The WhatsUp Gold groups to which the device belongs.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Click browse (...) to select a device.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the General: Device Toolbar report

This device-level dashboard report displays a device's details configured in **Device Properties > General**. You may want to add this dashboard report to a device's dashboard to help differentiate it from other devices you are monitoring.



Tip: Clicking on the device icon brings up its Device Status Report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Click browse (...) to select the device this report applies to.
- 3 Click **OK** to save changes.

About the General: Element Count report

The Element Count report displays inventory quantity data, which can help determine the proper licensing count when purchasing upgrades and additional WhatsUp Gold plug-ins. The following items are displayed:

- § **Device Count.** Displays the number of devices currently monitored by WhatsUp Gold.
- § **Monitored Interfaces.** Displays the number of unique interfaces for which WhatsUp Gold has data in the database.
- § **Monitored Disk Volumes.** Displays the number of unique volumes for which WhatsUp Gold has data in the database.
- § **Flow Source Count.** Displays the number of flow sources observed by WhatsUp Gold.



Important: Flow Source Count only lists the number of sources currently being received. It does not reflect the number of sources for which you are licensed.

- § **VMWare VM Count.** Displays the number of virtual machines observed by WhatsUp Gold.
- § **VMWare Host Count.** Displays the number of virtual hosts observed by WhatsUp Gold.
- § **Wireless Infrastructure Devices.** Displays the number of wireless access points and wireless LAN controllers currently monitored by WhatsUp Gold.
- § **Whats Configured Device Task Count.** Displays the number of devices to which WhatsConfigured tasks have been assigned.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Modify the **Report name** as desired.
- 3 Click **OK** to save changes.

About the General: Favorite Reports report

This general workspace report displays a list and link to any full report on your list of favorites.

To go to a report displayed in the workspace report, click on a report name.

This list is populated on the Reports tab by adding a report to your list of favorites.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.

About the General: Free Form Text/HTML report

This universal level dashboard report allows you to write any HTML text for display within a dashboard view. Displaying this dashboard report offers you the ability to keep important information in view.

This free-form dashboard report supports:

- § Any HTML text
- § Standard HTML formatting - bold, italic, and underline
- § Tables and
 tags

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Type a title for the report.
 - § **Free form text/HTML**. Type your HTML code or text in this box.
- 3 Click **OK** to save changes.

About the General: Group Status report

This home-level dashboard report displays a summary for the selected device group by the *current* count of its:

- § Monitored devices
- § Up devices



Note: All active monitors on a device must be up to be shown in the Up devices list.

- § Down devices



Note: All active monitors on a device must be down to be shown in the Down devices list.

- § Devices with down active monitors
- § Enabled active monitors
- § Devices with up active monitors
- § Down active monitors
- § Up interfaces
- § Down interfaces
- § Unacknowledged devices
- § Actions fired in the last 4 hours



Note: The Group Status dashboard report only reports on the first child of any group. It does not show recursive report data for devices in sub-groups.



Note: When you click a link to the reports, the devices included in the full report are all devices that have exhibited the status behavior during the selected date and time periods of the report. The dashboard report, however, only displays the number of devices that are *currently* exhibiting the selected status.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the General: Interface Details (Specific Interface) report

This General Dashboard report displays SNMP information reported by a specific interface. To gather this data, you must have the *SNMP Credentials* (on page 267) configured for the device in its Device Properties.

Device Information

The top section of the Dashboard report shows the current state of the device, as well as the display name and device type. Click the device name to go to that device's *Device Status* (on page 45) report.

Interface Information

The lower section of the Dashboard report is the information reported by SNMP:

- § **Interface name.** The name and IP address of the interface. Click the interface name to access the *Interface Utilization* (on page 700) report for this interface.
- § **Type.** The type code of the interface as defined in the MIB file for the interface.
- § **Index.** The SNMP index of the interface.
- § **Description.** Usually the interface or port name on the device.

Polling Information

- § **Status.** The current status of the device as reported through SNMP. Click the status code to access the Router/Switch/Interface view of the Device Status report.
 - § 1 - up
 - § 2 - down
 - § 3 - testing
 - § 4 - unknown

- § 5 - dormant
- § 6 - notPresent
- § 7 - lowerLayerDown
- § **Last poll time.** The date and time of the last successful poll.
- § **Last poll time interval.** The time (in seconds) between the last two successful polls.

Received octets

- § **Rx speed.** The maximum bandwidth (in Mbps) that the interface allows for received octets..
- § **Last rx octets.** The bandwidth (in Kbps) used by the interface during the last polling period for received octets.
- § **Rx octets total.** The total number of octets received (in KB) during the last polling cycle.
- § **Rx utilization.** The percent of the total bandwidth used by the interface for received octets during the last polling cycle.

Transmitted octets

- § **Tx speed.** The maximum bandwidth (in Mbps) that the interface allows for transmitted octets.
- § **Last tx octets.** The bandwidth (in Kbps) used by the interface during the last polling period for transmitted octets.
- § **Tx octets total.** The total number of octets transmitted (in KB) during the last polling cycle.
- § **Tx utilization.** The percent of the total bandwidth used by the interface for transmitted octets during the last polling cycle.

Configuration

Use the Configure Interface Details page to select an interface on a specific device. You can also change the title of the Dashboard report by entering a new name in the **Report name** box.

About the General: Map View report

This dashboard report displays a smaller version of a network map.

- § Clicking a device in the map takes you to the Device Status dashboard for that device.
- § Clicking the device group name at the bottom of the map dashboard report takes you to the Devices list.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button.

§ **Width.** Enter a width for the map boundary box in pixels.

§ **Height.** Enter a height for the map boundary box in pixels.

You can select these optional items:

§ **Draw device type icons.** This includes device type icons in the map. Devices are represented by dots when this option is not selected.

§ **Show unconnected links.** This displays links unconnected links in the map.

§ **Show dependency arrows.** This displays arrows that indicating up and down dependencies on group devices in the map.

§ **Clip device labels.** This removes device labels from the map.

§ **Wrap device labels.** This wraps device labels in the map.

3 Click **OK** to save changes.

About the General: Monitors Applied report

This home or device-level dashboard report displays any Active, Passive, or Performance monitors configured for and assigned to the selected device.

The report body displays:

§ A listing of monitors by type and name.



Tip: Click the **Reports** link next to a monitor name to view a list of any associated full reports.

To configure this dashboard report in WhatsUp Gold:

1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

§ **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.

§ **Device.** Select a device for the report by clicking the browse (...) button.

3 Click **OK** to save changes.

About the General: Poller Health report

This home-level dashboard report displays the status of the local poller and all pollers installed on your network. Placing this dashboard report in a dashboard allows you to ascertain at a glance if one or more pollers are down.

Each entry in the report contains the following information:

§ **Status.** A color-coded indicator of poller status.

§ **Name.** Displays the name of the poller.

§ **Lag Time.** The amount of time in seconds the poller is behind its scheduled time to poll devices; indicates poller overloaded.

§ **Lag Time Status.** Indicates if lag time is causing a polling issue.

To the left of each poller name is a circular icon that serves as a visual indicator of poller status:

- § **Red.** Indicates the listed poller is not active or status is unknown.
- § **Yellow.** Indicates the poller is starting up or beginning to fail.
- § **Green.** Indicates the listed poller is active and functioning properly.



Note: A yellow status icon is rare and is only seen as an automatic intermediary between red and green when a poller starts up or is failing.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Lag thresholds.** Enter time in seconds for Good, Fair, and Poor.
- 3 Click **OK** to save changes.

About the General: Search Knowledge Base report

This home-level dashboard report allows you to search the WhatsUp Gold Knowledge Base.

To perform a Knowledge Base search from this dashboard report:

- 1 Enter an alphanumeric phrase in the box provided.
- 2 Click **Search**. A new WhatsUp Gold Knowledge Base web page that contains the results of the search appears.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- 3 Click **OK** to save changes.

About the General: Summary Counts reports

This general dashboard report gives a summary of a group by the total number of:

- § Monitored devices
- § Up devices
- § Down devices
- § Devices with down Active Monitors
- § Devices in Maintenance
- § Active Monitors
- § Down Active Monitors

- § Up interfaces
- § Down interfaces
- § Actions fired in the last 4 hours

Each entry in the report contains the following information:

- § **Count.** The total number of that specific type of passive monitor on the network.
- § **Total number of.** The device status types.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- 3 Click **OK** to save changes.

About the General: Web User Activity Log

This home-level dashboard report displays a log of when a user logs on or off the web interface, and the actions taken while logged on.

- § **Web user.** The specific WhatsUp Web user to which the message pertains.
- § **Date.** The date of the message.
- § **Category.** The type of message. Possible categories and example details:
- § **Devices.** Indicates a change to a device or device group, for example, "'Created device' %1"
- § **Action.** Indicates changes made to action types, for example, "'Modified action type' %1"
- § **Device Properties.** Indicates changes made to device properties, for example, "'Removed passive monitor type '%1' from '%2'"
- § **Active Monitor.** Indicates changes made to active monitor types, for example, "'Modified active monitor type '%1'"
- § **Action.** Indicates changes made to action types, for example, "'Deleted action type '%1'"
- § **Action Policy.** Indicates changes made to action policies, for example, "'Created action policy type '%1'"
- § **System.** Indicates changes to the overall system, for example, "'Modified 'ip security settings'"
- § **Bulk Field Change operations.** Indicates that a Bulk Field change successfully executed, for example, "'Maintenance Bulk Field changes' for %1"
- § **Login.** A record of user logins and logouts, for example, "Logged in"
- § **User.** Indicates changes made to user accounts, for example, "Deleted user '%1'"

- § **Credentials.** Indicates changes made to credentials, for example, "Changed credentials '%1'"
- § **Passive Monitor.** Indicates changes made to passive monitors, for example, "Modified passive monitor type '%1'"
- § **Performance Monitor.** Indicates changes made to performance monitors, for example, "Modified performance monitor type '%1'"
- § **Dashboards.** Indicates changes made to dashboards, for example, "Modified dashboard 'General'"
- § **Flow.** (available with Flow Monitor only) Indicates changes made to Flow Interface Details, for example, "Modified Flow dashboard report: 'General'"
- § **Details.** The details of the activity.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Date range.** Select a date range for the dashboard report from the drop-down menu.
 - § **Maximum rows to return.** Enter a number for the number of rows displayed in the dashboard report.
 - § **Column 4 width.** Enter a width for the Details column (in pixels).
- 3 Click **OK** to save changes.

Interface Errors and Discards reports

In This Chapter

Interface Errors and Discards dashboard reports	96
About the Interface Discards Last X hours/days (Single Device) report	97
About the Interface Discards Last X hours/days (Specific Interface) report	98
About the Interface Errors Last X hours/days (Single Device) report	99
About the Interface Errors Last X hours/days (Specific Interface) report	100
Interface Errors and Discards - Last Poll (Single Device) report.....	101
About the Top 10: Interface Discards report.....	102
Top 10: Interface Errors report.....	102

Interface Errors and Discards dashboard reports

Interface Errors and Discards dashboard reports	Type	Description
Interface Errors and Discards - Last Polled Values (single device)	Home / Device	Shows the interface errors and discards for the selected device network interfaces at the time of the last poll.
Top 10 by Number of Errors	Home	Lists the top 10 device interfaces with packet errors for inbound and outbound data during a selected time period.
Top 10 by Number of Discards	Home	Lists the top 10 device interfaces with packet discards for inbound and outbound data during a selected time period.
Top 20 by Number of Errors	Home	Lists the top 20 device interfaces with packet errors for inbound and outbound data during a selected time period.
Top 20 by Number of Discards	Home	Lists the top 20 device interfaces with packet discards for inbound and outbound data during a selected time period.
Interface Errors - Last 4 Hours (single device)	Home / Device	Displays graphs that detail the percentage of interface errors for inbound and outbound packet data for all interfaces on a device during the last 4 hours.
Interface Errors - Last 8 Hours (single device)	Home / Device	Displays graphs that detail the percentage of interface errors for inbound and outbound packet data for all interfaces on a device during the last 8 hours.
Interface Errors - Last 7 Days (single device)	Home / Device	Displays graphs that detail the percentage of interface errors for inbound and outbound packet data for all interfaces on a device during the last 7 days.
Interface Errors - Last 30 Days (single device)	Home / Device	Displays graphs that detail the percentage of interface errors for inbound and outbound packet data for all interfaces on a device during the last 30 days.

Interface Errors and Discards dashboard reports	Type	Description
Interface Discards - Last 4 Hours (single device)	Home / Device	Displays graphs that detail the percentage of interface discards for inbound and outbound packet data for all interfaces on a device during the last 4 hours.
Interface Discards - Last 8 Hours (single device)	Home / Device	Displays graphs that detail the percentage of interface discards for inbound and outbound packet data for all interfaces on a device during the last 8 hours.
Interface Discards - Last 7 Days (single device)	Home / Device	Displays graphs that detail the percentage of interface discards for inbound and outbound packet data for all interfaces on a device during the last 7 days.
Interface Discards - Last 30 Days (single device)	Home / Device	Displays graphs that detail the percentage of interface discards for inbound and outbound packet data for all interfaces on a device during the last 30 days.
Interface Errors - Last 4 Hours (specific interface)	Home	Displays a graph that details the percentage of interface errors for inbound and outbound packet data for a specific interface on a device during the last 4 hours.
Interface Errors - Last 8 Hours (specific interface)	Home	Displays a graph that details the percentage of interface errors for inbound and outbound packet data for a specific interface on a device during the last 8 hours.
Interface Errors - Last 7 Days (specific interface)	Home	Displays a graph that details the percentage of interface errors for inbound and outbound packet data for a specific interface on a device during the last 7 days.
Interface Errors - Last 30 Days (specific interface)	Home	Displays a graph that details the percentage of interface errors for inbound and outbound packet data for a specific interface on a device during the last 30 days.
Interface Discards - Last 4 Hours (specific interface)	Home	Displays a graph that details the percentage of interface discards for inbound and outbound packet data for a specific interface on a device during the last 4 hours.
Interface Discards - Last 8 Hours (specific interface)	Home	Displays a graph that details the percentage of interface discards for inbound and outbound packet data for a specific interface on a device during the last 8 hours.
Interface Discards - Last 7 Days (specific interface)	Home	Displays a graph that details the percentage of interface discards for inbound and outbound packet data for a specific interface on a device during the last 7 days.
Interface Discards - Last 30 Days (specific interface)	Home	Displays a graph that details the percentage of interface discards for inbound and outbound packet data for a specific interface on a device during the last 30 days.

About the Interface Discards Last X hours/days (Single Device) report

This device-level dashboard report displays graphs that detail the percentage of interface discards for inbound and outbound packet data for all interfaces on a device during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing problems.

To display a single interface, use the *Performance: Interface Discards Last X hours/days - Specific Interface* (on page 98) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface discards, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface discard values that are of real concern.

- § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw**. Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Discards Last X hours/days (Specific Interface) report

This device-level dashboard report displays a line graph that details the percentage of interface utilization discards for inbound and outbound packet data for a specific device interface during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing packet discard problems.

To display more than one interface, use the *Interface Discards (last X hours/days - Single Device)* (on page 97) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.

- § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Errors Last X hours/days (Single Device) report

This device-level dashboard report displays graphs that detail the percentage of interface errors for inbound and outbound data packets for all interfaces on a device during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing packet error problems.

To display a single interface, use the *Performance: Interface Errors (Last X hours/days - Specific Interface)* (on page 100) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.

- § **Device.** Select a device by clicking the browse (...) button.
- § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
- § **Graph type.** Select the type of graph you would like the report to display.
- § **Trend type.** Select the type of trend you would like the report to use.
- § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
- § **Vertical Axis Scaling.** Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.

- § **Min.** Enter a number for the lowest point on the Y-axis.
- § **Max.** Enter a number for the highest point on the Y-axis.
- § **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
- § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.

3 Click **OK** to save changes.

About the Interface Errors Last X hours/days (Specific Interface) report

This device-level dashboard report displays a line graph that details the percentage of interface utilization errors for inbound and outbound packet data for a specific device interface during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing packet error problems.

To display more than one interface, use the *Interface Errors (last X hours/days - Single Device)* (on page 99) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.

- § **Graph type.** Select the type of graph you would like the report to display.
- § **Trend type.** Select the type of trend you would like the report to use.
- § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report in pixels.
 - § **Height.** Enter a height for the report in pixels.
- § **Vertical Axis Scaling.** Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.

- § **Min.** Enter a number for the lowest point on the Y axis.
- § **Max.** Enter a number for the highest point on the Y axis.
- § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.

3 Click **OK** to save changes.

Interface Errors and Discards - Last Poll (Single Device) report

This device-level dashboard report provides details for the number of interface transmit (outbound) and receive (inbound) errors, and transmit and receive discards for the specified device. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot devices that are experiencing interface errors and discard problems.

Each entry in the report contains the following information:

- § **Description.** The selected device interface.
- § **Transmit Errors.** The number of packets transmitted through the device interface with errors.
- § **Receive Errors.** The number of packets received through the device interface with errors.
- § **Transmit Discards.** The number of packets transmitted through the device interface that were discarded.
- § **Receive Discards.** The number of packets received through the device interface that were discarded.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.

- § **Column 1 width.** The width of the column in the dashboard in pixels.
- 3 Click **OK** to save changes.

About the Top 10: Interface Discards report

This home-level dashboard report displays the top device interfaces with packet discards for inbound and outbound data during a selected time period.

- § **Device.** The network device name.
- § **Interface.** The interface description.
- § **Transmit.** The number of discarded packets transmitted from each interface.
- § **Receive.** The number of discarded packets received from each interface.
- § **Total.** Provides the number of packets discarded for each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select all devices or a specific device group for the dashboard report. Select **Every device** or clear **Every device** if you want to select a specific device group, then click the browse (...) button to select the device group you want to include in this dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Top 10: Interface Errors report

This home-level dashboard report displays the top device interfaces with packet errors for inbound and outbound data during a selected time period.

- § **Device.** The network device name.
- § **Interface.** The interface description.
- § **Transmit.** The number of packets transmitted from each interface.
- § **Receive.** The number of packets received from each interface.
- § **Total.** Provides the number of packet errors for each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select all devices or a specific device group for the dashboard report. Select **Every device** or clear **Every device** if you want to select a specific device

group, then click the browse (...) button to select the device group you want to include in this dashboard report.

§ **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.

§ **Column 2 width.** Enter a width for the column (in pixels).

3 Click **OK** to save changes.

Interface Utilization reports

In This Chapter

Interface Utilization dashboard reports	104
About the Interface Utilization:	
Interface Traffic Last X hours/days (Single Device) report.....	105
About the Interface Utilization (Specific Interface Traffic) report ...	106
About the Interface Utilization	
Last X hours/days (Single Device) report.....	107
About the Interface Utilization	
Last X hours/days (Specific Interface Utilization) report.....	108
About the Last Polled Interface Utilization	
Value (Specific Interface) report.....	109
Interface: Last Polled Values (Single Device) report	109
About the Threshold: Interface Utilization report	110
About the Top 10: Interface Utilization report.....	111
About the Top 10: Interface Traffic report.....	111
About the Threshold: Interface Traffic report.....	112

Interface Utilization dashboard reports

Interface Utilization dashboard reports	Type	Description
Last Polled Interface (single device)	Device	Shows the interface utilization for all network interfaces at the time of the last poll.
Last Polled Interface (specific interface)	Home	Shows the interface utilization for a specific network interface at the time of the last poll.
All Interfaces over 80% Bandwidth Utilization*	Home	Lists all network interfaces with a utilization greater than 80%.
All Interfaces over 90% Bandwidth Utilization	Home	Lists all network interfaces with a utilization greater than 90%.
Top 10 with Traffic Threshold*	Home	Lists the top 10 devices based on their current interface traffic.
Top 10 by Bandwidth Utilization*	Home	Lists the top 10 devices based on their current interface utilization.
Top 20 by Bandwidth Utilization	Home	Lists the top 20 devices based on their current interface utilization.
Top 10 by Traffic*	Home	Lists the top 10 devices based on their current interface traffic.

Interface Utilization dashboard reports	Type	Description
Top 20 by Traffic	Home	Lists the top 20 devices based on their current interface traffic.
Last 4 hours (single device)	Device	Details all interface utilization percentages for one device over the last 4 hours.
Last 8 hours (single device)	Device	Details all interface utilization percentages for one device over the last 8 hours.
Last 7 days (single device)	Device	Details all interface utilization percentages for one device over the last 7 days.
Last 30 days (single device)	Device	Details all interface utilization percentages for one device over the last 30 days.
Last 4 hours (specific interface utilization)	Home	Details utilization for a specific interface for one device over the last 4 hours.
Last 8 hours (specific interface utilization)	Home	Details utilization for a specific interface for one device over the last 8 hours.
Last 7 days (specific interface utilization)	Home	Details utilization for a specific interface for one device over the last 7 days.
Last 30 days (specific interface utilization)	Home	Details utilization for a specific interface for one device over the last 30 days.
Last 4 hours (specific traffic interface)	Home	Details traffic for a specific interface for one device over the last 4 hours.
Last 8 hours (specific traffic interface)	Home	Details traffic for a specific interface for one device over the last 8 hours.
Last 7 days (specific traffic interface)	Home	Details traffic for specific interface for one device over the last 7 days.
Last 30 days (specific traffic interface)	Home	Details traffic for a specific interface for one device over the last 30 days.
Interface Traffic - Last 4 Hours (single device)	Device	Details traffic for all interfaces for one device over the last four hours.
Interface Traffic - Last 8 hours (single device)	Device	Details traffic for all interfaces for one device over the last eight hours.
Interface Traffic - Last 7 days (single device)	Device	Details traffic for all interfaces for one device over the last seven days.
Interface Traffic - Last 30 days (single device)	Device	Details traffic for all interfaces for one device over the last 30 days.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the Interface Utilization: Interface Traffic Last X hours/days (Single Device) report

This device-level dashboard report displays a line graph that details the interface traffic for a device during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

You can control the number of graphs appearing in the dashboard by changing the **Maximum number of graphs to draw** setting. Some devices have numerous interfaces, and displaying all of them can be too resource-intensive for WhatsUp Gold. Displayed interfaces are selected based on the order they are received from the database when the number of interfaces present exceeds the **Maximum number of graphs to draw** setting.



Note: The Interface Traffic report updates the units of measure displayed based on the traffic received over the interface. Units are determined per interface, however, and both outgoing and incoming traffic are evaluated to determine the unit of measure displayed. The smallest unit of measure is used in the report. For example, if the incoming traffic is measured in Kbps, but the outgoing traffic is measured in bps, then the dashboard report uses bps as the unit of measure for the graph for that interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Utilization (Specific Interface Traffic) report

This home-level dashboard report displays a line graph that details the number of packets transmitted and received by a device during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § Vertical Axis Scaling. Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Utilization Last X hours/days (Single Device) report

This device-level dashboard report displays graphs that detail the interface utilization percentages for all interfaces on a device during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

To display a single interface, use the *Interface Utilization (Last 4 Hours - Specific Interface)* (on page 108) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).

- § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Utilization Last X hours/days (Specific Interface Utilization) report

This device-level dashboard report displays a line graph that details the interface utilization percentage during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

To display more than one interface, use the *Interface Utilization (All Interfaces)* (on page 107) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Last Polled Interface Utilization Value (Specific Interface) report

This home-level dashboard report provides graphical illustration of an interface utilization at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view an interface status quickly, even from across the room.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available interface space in green, and used space in red.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the interface percentage used.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the interface percentage used.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the interface percentage used.
- § **Text.** A numerical representation of the interface percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § **Red.** Above 90%
 - § **Yellow.** Between 80% and 90%
 - § **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the interface size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device for the report by clicking on the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

Interface: Last Polled Values (Single Device) report

This device-level dashboard report displays current interface utilization percentages for all interfaces on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's interface(s) to keep up with the number of packets they are currently transmitting and receiving. The colors in the second Transmit and Received columns coincide with the WhatsUp Threshold colors:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Description.** The particular interface.
- § **Speed.** The interface speed.
- § **Transmit (kbps).** The number of packets transmitted in kbps.
- § **Receive (kbps).** The number of packets received in kbps.
- § **Transmit.** The percentage of packets transmitted.
- § **Receive.** The percentage of packets received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
- 3 Click **OK** to save changes.

About the Threshold: Interface Utilization report

This home-level dashboard report displays the top devices based on their percentage of transmitted and received packets. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their interface utilization by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Transmit.** The percentage of packets transmitted by a device.
- § **Receive.** The percentage of packets received by a device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.

- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Interface Utilization report

This home-level dashboard report displays the top devices in a group based on their interface utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial interfaces and their current utilization by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Interface.** The interface description.
- § **Transmit.** The percentage of packets transmitted from each interface.
- § **Receive.** The percentage of packets received from each interface.

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the appropriate information.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Interface Traffic report

This home-level dashboard report displays the top devices in a group based on their current interface traffic as a total of packets transmitted and received.

- § **Device.** The network device.
- § **Interface.** The device's interface description.
- § **Transmit.** The number of packets transmitted from each interface.
- § **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width**. Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Threshold: Interface Traffic report

This home-level dashboard report displays interface traffic information for a specified device group based on the number of packets both sent and received. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current interface traffic rates by glancing at the numbers in the transmit and receive columns for each device.

- § **Device**. The network device.
- § **Interface**. The interface description.
- § **Transmit**. The number of packets sent.
- § **Receive**. The number of packets received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device group**. Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold**. Enter a number for the threshold and select a threshold criteria symbol from the list.
 - § **Maximum rows to return**. Enter the number of records to display in the dashboard report.
 - § **Column 2 width**. Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Inventory reports

In This Chapter

Inventory dashboard reports	113
About the Inventory: Total Actions Applied by Type report	113
About the Inventory: Total Active Monitors by Type report.....	114
About the Inventory: Total Devices by Type report.....	114
About the Inventory: Devices with a Specific Attribute report	115
About the Inventory: Total Passive Monitors by Type report.....	115
About the Inventory: Total Performance Monitors by Type report	116

Inventory dashboard reports

Inventory dashboard reports	Type	Description
Total Devices by Type	Home	Lists all monitored network devices by type and number.
Total Active Monitors by Type	Home	Lists all Active Monitors on the network by type and number.
Total Passive Monitors by Type	Home	Lists all Passive Monitors on the network by type and number.
Total Performance Monitors by Type	Home	Lists all Performance Monitors on the network by type and number.
Total Actions Applied by Type	Home	Lists all Actions on the network by type and number.
Total Devices with Specific Attributes	Home	Lists all devices with a specific attribute.

About the Inventory: Total Actions Applied by Type report

This home-level dashboard report gives a summary of actions on the network by type. This can be useful for gathering statistical information as well as general knowledge about the type of monitoring currently in use for your network. If you notice a particularly useful or successful action isn't used extensively, you can apply more of this type of action to other crucial devices on the network. You can also remove less successful actions.

- § **Action Type.** The type of action.
- § **Percentage.** The percentage accounted for on the network by that specific type of action.
- § **Count.** The total number of that specific type of action on the network.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

About the Inventory: Total Active Monitors by Type report

This home-level dashboard report gives a summary of active monitors on the network by type. This can be useful for gathering statistical information as well as general knowledge about the type of monitoring currently in use for your network. If you see that a typically useful or successful active monitor isn't used extensively, you can apply more of this type of monitor to other crucial devices on the network. Inversely, you can decrease less successful monitors.

- § **Active Monitor**. The type of active monitor.
- § **Percentage**. The percentage accounted for on the network by that specific type of active monitor.
- § **Count**. The total number of that specific type of active monitor on the network.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

About the Inventory: Total Devices by Type report

This home-level dashboard report lists network devices by type. This can be useful for gathering statistical information as well as general knowledge about the type of devices currently in use on your network.

- § **Device Type**. The type of device.
- § **Percentage**. The percentage accounted for of the total by a particular type of device.
- § **Count**. The total number of that particular type of device.
- § **Total**. The total number of devices on the network.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.

- § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

About the Inventory: Devices with a Specific Attribute report

This home-level dashboard report displays information on devices with specific attributes. This can be useful for gathering statistical information as well as general knowledge about the type of devices currently in use on your network.

- § **Attribute Name.** Contact, Description, or Location
- § **Percentage.** The percentage accounted for of the total by an attribute.
- § **Count.** The total number of a specific attribute for a specific device.
- § **Total.** The total number of the attribute.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Column 1 width.** Enter a width for the Attribute column (in pixels).
 - § **Attribute Name.** Select Contact, Description, or Location.
- 3 Click **OK** to save changes.

About the Inventory: Total Passive Monitors by Type report

This universal-level dashboard report gives a summary of passive monitors on the network by type. This can be useful for gathering statistical information as well as general knowledge about the type of monitoring currently in use for your network. If you notice a particularly useful or successful action isn't used extensively, you can apply more of this type of action to other crucial devices on the network. You can also remove less successful actions.

- § **Passive Monitor Type.** The type of passive monitor.
- § **Percentage.** The percentage accounted for on the network by that specific type of passive monitor.
- § **Count.** The total number of that specific type of passive monitor on the network.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

About the Inventory: Total Performance Monitors by Type report

This home-level dashboard report gives a summary of performance monitors on the network by type. This can be useful for gathering statistical information as well as general knowledge about the type of monitoring currently in use for your network. If you notice a particularly useful or successful action isn't used extensively, you can apply more of this type of action to other crucial devices on the network. You can also remove less successful actions.

- § **Performance Monitor Type.** The type of performance monitor.
- § **Polls Per Min.** The total number of polls per minute by performance monitor type.
- § **Count.** The total number of a particular performance monitor on the network.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

Memory Utilization reports

In This Chapter

Memory Utilization dashboard reports	117
About the Memory Utilization Last X hours/days (Single Device) report	118
About the Memory Utilization Last X hours/days (Specific Aspect) report	118
About the Memory Utilization: Last Polled Value (Specific Aspect) report	119
About the Memory Utilization: Last Polled Value (Single Device) report	120
About the Threshold: Memory Utilization report	121
About the Top 10: Memory Utilization report	121

Memory Utilization dashboard reports

Memory Utilization dashboard reports	Type	Description
Last Polled Values (single device)	Device	Shows the memory utilization for all device memory at the time of the last poll.
Last Polled Value (specific aspect)	Home	Shows the memory utilization for a specific network device at the time of the last poll.
Over 80% Utilization*	Home	Lists all network devices with a memory utilization greater than 80%.
Over 90% Utilization	Home	Lists all network devices with a memory utilization greater than 90%.
Top 10 by Utilization*	Home	Lists the top 10 devices based on their current memory utilization.
Top 20 by Utilization	Home	Lists the top 20 devices based on their current memory utilization.
Last 4 hours (single device)	Device	Details all memory utilization percentages for one device over the last 4 hours.
Last 8 hours (single device)	Device	Details all memory utilization percentages for one device over the last 8 hours.
Last 7 days (single device)	Device	Details all memory utilization percentages for one device over the last 7 days.
Last 30 days (single device)	Device	Details all memory utilization percentages for one device over the last 30 days.
Last 4 hours (specific aspect)	Home	Details utilization of a specific memory type for one device over the last 4 hours.
Last 8 hours (specific aspect)	Home	Details utilization of a specific memory type for one device over the last 8 hours.
Last 7 days (specific aspect)	Home	Details utilization of a specific memory type for one device over the last 7 days.

Memory Utilization dashboard reports	Type	Description
Last 30 days (specific aspect)	Home	Details utilization of a specific memory type for one device over the last 30 days.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the Memory Utilization Last X hours/days (Single Device) report

This device-level dashboard report displays an area graph that details the memory utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes in memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.
 - § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Memory Utilization Last X hours/days (Specific Aspect) report

This home-level dashboard report displays a line graph that details the memory utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes in memory.

To display more than one memory, use the Memory Utilization (All Memories) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.
 - § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Memory Utilization: Last Polled Value (Specific Aspect) report

This home-level dashboard report provides graphical illustration of device memory utilization at the time of the last poll. Placing this dashboard report in a dashboard allows you to view device memory status quickly.

There are five types of graphs to choose from:

- § **Pie**. A 3-D pie graph that displays available memory space in green, and used space in red.
- § **Gauge**. A semi-circle graph (much like a car speedometer) with a pointer that indicates the memory percentage used.
- § **Horizontal bar**. A horizontal bar graph (much like a ruler) with a pointer that indicates the memory percentage used.
- § **Vertical bar**. A vertical bar graph (much like a thermometer) with a pointer that indicates the memory percentage used.
- § **Text**. A numerical representation of the memory percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § **Red**. Above 90%
 - § **Yellow**. Between 80% and 90%
 - § **Green**. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the memory size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device for the report by clicking the browse (...) button.
 - § **Memory aspect to graph**. For devices with more than one memory aspect, select a memory aspect to graph.
 - § **Graph type**. Choose the type and size of the graph.
- 3 Click **OK** to save changes.

About the Memory Utilization: Last Polled Value (Single Device) report

This device-level dashboard report displays current memory utilization percentages for all memories on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's memory(s) to watch for spikes in memory utilization. The colors displayed in the Percent Used column coincide with the WhatsUp threshold colors:

- § **Red**. Above 90%
- § **Yellow**. Between 80% and 90%
- § **Green**. 80% or less

Each entry in the report contains the following information:

- § **Description**. The particular memory.
- § **Size Used**. The size of memory in use at the time of the last poll.
- § **Total Size**. The total size of the memory.
- § **Percentage Used**. The percentage of the total size of the memory in use at the time of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § To view a graphical representation of the report data, select **Use a graph to display the values**.

- § If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- 3 Click **OK** to save changes.

About the Threshold: Memory Utilization report

This home-level dashboard report displays the top devices based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory capacity by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- § **Percent Used.** The percentage of utilized memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though a default threshold exists, you can change this threshold. If you do, change the report title accordingly.

- § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Memory Utilization report

This home-level dashboard report displays the top devices based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%

§ **Green.** 80% or less

Each entry in the report contains the following information:

§ **Device.** The network device.

§ **Memory.** The memory type. For example, Physical Memory or Virtual Memory.

§ **Percent Used.** The percentage of utilized memory.

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the appropriate information into the following boxes:
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

Performance-Historic reports

In This Chapter

Performance-Historic dashboard reports.....	124
About the CPU Utilization	
Last X hours/days (Single Device) report.....	125
About the CPU Utilization	
Last X hours/days (Specific CPU) report.....	126
About the Custom Performance Monitor Values	
Last X hours/days (Single Device) report.....	127
About the Custom Performance Monitor Values	
Last X hours/days (Specific Monitor) report.....	128
About the Disk Free Space	
Last X hours/days (Specific Disk) report.....	129
About the Disk Utilization	
Last X hours/days (Single Device) report.....	129
About the Disk Utilization	
Last X hours/days (Specific Disk) report.....	130
About the Interface Discards	
Last X hours/days (Single Device) report.....	131
About the Interface Discards	
Last X hours/days (Specific Interface) report	131
About the Interface Errors	
Last X hours/days (Single Device) report.....	132
About the Interface Errors	
Last X hours/days (Specific Interface) report	133
About the Interface Utilization:	
Interface Traffic Last X hours/days (Single Device) report.....	134
About the Interface Utilization	
(Specific Interface Traffic) report	135
About the Interface Utilization	
Last X hours/days (Single Device) report.....	136
About the Interface Utilization	

Last X hours/days (Specific Interface Utilization) report.....	137
About the Memory Utilization	
Last X hours/days (Single Device) report.....	137
About the Memory Utilization	
Last X hours/days (Specific Aspect) report.....	138
About the Ping:	
Last X hours/days (Single Device Availability) report	139
About the Ping Response Time	
Last X hours/days (Single Device) report.....	139

Performance-Historic dashboard reports

Performance - Historic dashboard reports	Type	Description
Custom Performance Monitor Values (last 4 hours - single device)	Device	Details custom Performance Monitor values for one device over the last 4 hours.
Interface Utilization (last 4 hours - single device)	Device	Details all interface utilization percentages for one device over the last 4 hours.
CPU Utilization (last 4 hours - single device)	Device	Details all CPU utilization percentages for one device over the last 4 hours.
Memory Utilization (last 4 hours - single device)	Device	Details all memory utilization percentages for one device over the last 4 hours.
Disk Utilization (last 4 hours - single device)	Device	Details all disk utilization percentages for one device over the last 4 hours.
Ping Response Time (last 4 hours - single device)	Device	Details all ping response times for device interfaces over the last 4 hours.
Ping Availability (last 4 hours - single device)	Device	Details all ping availability for a device interfaces over the last 4 hours.
Interface Traffic (last 4 hours - specific interface)	Home	Details interface traffic for a specific device interface over the last 4 hours.
Custom Performance Monitor Values (last 4 hours - specific monitor)	Home	Details a device's specific custom Performance Monitor values over the last 4 hours.

Performance - Historic dashboard reports	Type	Description
Interface Utilization (last 4 hours - specific interface)	Home	Details utilization percentages for a specific interface for one device over the last 4 hours.
CPU Utilization (last 4 hours - specific CPU)	Home	Details utilization percentages for a specific CPU for one device over the last 4 hours.
Disk Utilization (last 4 hours - specific disk)	Home	Details utilization percentages for a specific disk for one device over the last 4 hours.
Disk Free Space - Last 4 Hours (specific disk)	Home	Details the percentage of available disk space over the last four hours for one disk on one device.
Memory Utilization - Last 4 Hours (specific aspect)	Device	Details utilization percentages for a specific memory type for one device over the last 4 hours.
Interface Traffic - Last 4 Hours (single device)	Device	Details traffic for all interfaces for one device over the last four hours.
Interface Errors - Last 4 Hours (single device)	Device	Details the percentage of interface errors for outbound and inbound traffic on one device over the last four hours.
Interface Discards - Last 4 hours (single device)	Device	Details the percentage of interface discards for inbound and outbound traffic for all interfaces on a specific device. over the last four hours.
Interface Errors - last 4 hours (specific interface)	Device	Details the percentage of interface errors for outbound and inbound traffic on one device interface over the last four hours.
Interface Discards - Last 4 hours (specific interface)	Device	Details the percentage of interface discards for inbound and outbound traffic for one interface on a specific device over the last four hours.

About the CPU Utilization Last X hours/days (Single Device) report

This device-level dashboard report displays multiple area graphs that detail the CPU utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor device CPUs to watch for trends, spikes, or drops in CPU utilization.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.

- § **Device.** Select a device by clicking the browse (...) button.
- § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
- § **Graph type.** Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Width.** Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: Large graph images can be used, but be aware that these larger images will refresh at slower speeds. The optimum size will depend on the speed of your network connection from your browser to your Web server.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the CPU Utilization Last X hours/days (Specific CPU) report

This home-level dashboard report displays a line graph that details the CPU utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes on one of their CPUs.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
 - § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the web browser. Choose None, Line, or Curve.

- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Width.** Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: You can use large graph images, but be aware that larger images refresh at slower speeds. The optimum size depends on the speed of your network connection from your browser to your web server.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Custom Performance Monitor Values Last X hours/days (Single Device) report

This device-level dashboard report can display multiple graphs that detail custom performance monitors for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor a device's performance monitor(s) to watch for trends, spikes, or drops.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
 - § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
 - § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
 - § **Width.** Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: Large graph images can be used, but be aware that these larger images refresh at slower speeds. The optimum size depends on the speed of your network connection from your browser to your web server.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y axis.
 - § **Max.** Enter a number for the highest point on the Y axis.
 - § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Custom Performance Monitor Values Last X hours/days (Specific Monitor) report

This home-level dashboard report displays a line graph that details a custom performance monitor for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor important devices and their custom performance monitors.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Custom aspect to graph.** Select the aspect from the list.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph to display the data in the report. Select from the following: Bar, Line, Area, Spline, or Stepline.
 - § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the web browser. Choose None, Line, or Curve.
 - § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
 - § **Width.** Enter a width (in pixels) for the graph portion of this dashboard report. The default is 500 pixels.



Note: You can use large graph images, but be aware that these larger images refresh at slower speeds. The optimum size depends on the speed of your network connection from your browser to your web server.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Vertical Axis Scaling.** Select either auto or fixed scale.

- § **Min.** Enter a number for the lowest point on the Y axis.
 - § **Max.** Enter a number for the highest point on the Y axis.
 - § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Disk Free Space Last X hours/days (Specific Disk) report

This home-level dashboard report displays a line graph that details the disk free space in GB for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes on their disk.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 2 Click **OK** to save changes.

About the Disk Utilization Last X hours/days (Single Device) report

This device-level dashboard report can display multiple area graphs that detail the disk utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard allows you to monitor a device's disk(s) to watch for trends, spikes, or drops in its disk utilization.

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the appropriate information:
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.

- § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to graph the maximum.
- 3 Click **OK** to save changes.

About the Disk Utilization Last X hours/days (Specific Disk) report

This home-level dashboard report displays a line graph that details the disk utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes on their disk.

To configure this dashboard report in WhatsUp Gold:


- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report in pixels.
 - § **Height.** Enter a height for the report in pixels.
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y axis.
 - § **Max.** Enter a number for the highest point on the Y axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Discards Last X hours/days (Single Device) report

This device-level dashboard report displays graphs that detail the percentage of interface discards for inbound and outbound packet data for all interfaces on a device during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing problems.

To display a single interface, use the *Performance: Interface Discards Last X hours/days - Specific Interface* (on page 98) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
 - 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.
-  **Tip:** WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface discards, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface discard values that are of real concern.
- § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw**. Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
 - 3 Click **OK** to save changes.

About the Interface Discards Last X hours/days (Specific Interface) report

This device-level dashboard report displays a line graph that details the percentage of interface utilization discards for inbound and outbound packet data for a specific device

interface during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing packet discard problems.

To display more than one interface, use the *Interface Discards (last X hours/days - Single Device)* (on page 97) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.

- § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Errors Last X hours/days (Single Device) report

This device-level dashboard report displays graphs that detail the percentage of interface errors for inbound and outbound data packets for all interfaces on a device during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing packet error problems.

To display a single interface, use the *Performance: Interface Errors (Last X hours/days - Specific Interface)* (on page 100) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.

- § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw**. Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Errors Last X hours/days (Specific Interface) report

This device-level dashboard report displays a line graph that details the percentage of interface utilization errors for inbound and outbound packet data for a specific device interface during a selected time period. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot interfaces experiencing packet error problems.

To display more than one interface, use the *Interface Errors (last X hours/days - Single Device)* (on page 99) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.

- § **Report name.** Enter a title for the dashboard report.
- § **Device.** Select a device by clicking the browse (...) button.
- § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
- § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
- § **Graph type.** Select the type of graph you would like the report to display.
- § **Trend type.** Select the type of trend you would like the report to use.
- § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report in pixels.
 - § **Height.** Enter a height for the report in pixels.
- § **Vertical Axis Scaling.** Select either auto or fixed scale.



Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.

- § **Min.** Enter a number for the lowest point on the Y axis.
- § **Max.** Enter a number for the highest point on the Y axis.
- § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.

3 Click **OK** to save changes.

About the Interface Utilization: Interface Traffic Last X hours/days (Single Device) report

This device-level dashboard report displays a line graph that details the interface traffic for a device during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

You can control the number of graphs appearing in the dashboard by changing the **Maximum number of graphs to draw** setting. Some devices have numerous interfaces, and displaying all of them can be too resource-intensive for WhatsUp Gold. Displayed interfaces are selected based on the order they are received from the database when the number of interfaces present exceeds the **Maximum number of graphs to draw** setting.



Note: The Interface Traffic report updates the units of measure displayed based on the traffic received over the interface. Units are determined per interface, however, and both outgoing and incoming traffic are evaluated to determine the unit of measure displayed. The smallest unit of measure is used in the report. For example, if the incoming traffic is measured in Kbps, but the outgoing traffic is measured in bps, then the dashboard report uses bps as the unit of measure for the graph for that interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.
 - § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw**. Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Utilization (Specific Interface Traffic) report

This home-level dashboard report displays a line graph that details the number of packets transmitted and received by a device during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).

- § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Utilization Last X hours/days (Single Device) report

This device-level dashboard report displays graphs that detail the interface utilization percentages for all interfaces on a device during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

To display a single interface, use the *Interface Utilization (Last 4 Hours - Specific Interface)* (on page 108) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Interface Utilization Last X hours/days (Specific Interface Utilization) report

This device-level dashboard report displays a line graph that details the interface utilization percentage during a selected time period. Adding this dashboard report to a dashboard allows you to easily monitor interfaces experiencing problems.

To display more than one interface, use the *Interface Utilization (All Interfaces)* (on page 107) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Date range**. Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type**. Select the type of graph you would like the report to display.
 - § **Trend type**. Select the type of trend you would like the report to use.
 - § **Dimensions**. Select the dimension in which you would like the graph to display.
 - § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling**. Select either auto or fixed scale.
 - § **Min**. Enter a number for the lowest point on the Y-axis.
 - § **Max**. Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum**. Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Memory Utilization Last X hours/days (Single Device) report

This device-level dashboard report displays an area graph that details the memory utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes in memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.

- § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Memory Utilization Last X hours/days (Specific Aspect) report

This home-level dashboard report displays a line graph that details the memory utilization percentage for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing spikes in memory.

To display more than one memory, use the Memory Utilization (All Memories) dashboard report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.

- § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.

- 3 Click **OK** to save changes.

About the Ping: Last X hours/days (Single Device Availability) report

This device-level dashboard report displays an area graph that details the ping availability percentages for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing ping problems.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
- 3 Click **OK** to save changes.

About the Ping Response Time Last X hours/days (Single Device) report

This device-level dashboard report displays an area graph that details the ping response times for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing ping response delays.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.

- § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

Performance-Last Poll reports

In This Chapter

Performance-Last Poll dashboard reports	141
About the CPU Utilization:	
Last Polled Value (Single Device) report	142
About the Last Polled CPU Utilization (Specific CPU) report	143
About the Last Polled Custom	
Performance Monitor Values (Single Device) report	144
About the Last Polled Custom	
Performance Monitor Values (Specific Monitor) report	144
About the Disk Utilization:	
Last Polled Values (Single Device) report	145
About the Disk Utilization:	
Last Polled Value (Specific Disk) report	146
Interface Errors and Discards - Last Poll (Single Device) report	147
Interface: Last Polled Values (Single Device) report	147
About the Last Polled Interface Utilization	
Value (Specific Interface) report	148
About the Memory Utilization: Last Polled	
Value (Single Device) report	149
About the Memory Utilization: Last Polled	
Value (Specific Aspect) report	149
About the Performance:	
Last Polled Ping Response Time (Specific Interface) report	150

Performance-Last Poll dashboard reports

Performance - Last Poll dashboard reports	Type	Description
Custom Performance Monitor Values (single device)	Device	Shows the values for all custom Performance Monitors for a single device at the time of the last poll.
Interface Utilization (single device)	Device	Shows the interface utilization for all device interfaces for a single device at the time of the last poll.
CPU Utilization (single device)	Device	Shows the CPU utilization for all CPUs for a single device at the time of the last poll.

Performance - Last Poll dashboard reports	Type	Description
Memory Utilization (single device)	Device	Shows the memory utilization for all memory types for a single device at the time of the last poll.
Disk Utilization (single device)	Device	Shows the disk utilization for all of disks for a single device at the time of the last poll.
Custom Performance Monitor Values (specific monitor)	Home	Shows the values for a specific device custom Performance Monitor.
Interface Utilization (specific interface)	Home	Shows the utilization of a specific device interface at the time of the last poll.
CPU Utilization (specific CPU)	Home	Shows the utilization of a specific device CPU at the time of the last poll.
Memory Utilization (specific aspect)	Home	Shows the utilization of a specific device memory type at the time of the last poll.
Disk Utilization (specific disk)	Home	Shows the utilization of a specific device disk at the time of the last poll.
Ping Response Time (specific interface)	Home	Shows the ping response time of a specific device interface at the time of the last poll.
Interface Errors and Discards (single device)	Device	Shows the number of interface errors on all interfaces for inbound and outbound traffic for a single device.

About the CPU Utilization: Last Polled Value (Single Device) report

This device-level dashboard report displays current CPU utilization percentages for all CPUs on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor the CPU(s) of an important device to watch for spikes in CPU utilization. The report shows:

- § **Description.** The particular CPU.
- § **CPU Load.** The percentage of the CPU currently in use. The colors displayed in the CPU Load column coincide with the WhatsUp threshold colors:
- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.

- § **Device.** Select a device by clicking the browse (...) button.
 - § To view a graphical representation of the report data, select **Use a graph to display the values.**
 - § If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types*. (on page 675)
- 3 Click **OK** to save changes.

About the Last Polled CPU Utilization (Specific CPU) report

This home-level dashboard report provides graphical illustration of a device's CPU utilization at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view a device's CPU status quickly, even from across the room.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available CPU space in green, and used space in red.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the CPU percentage used.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the CPU percentage used.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the CPU percentage used.
- § **Text.** A numerical representation of the CPU percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the CPU size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **CPU to graph.** Select the CPU that you want to monitor.
 - § **Graph type.** Select the type of graph you would like the report to display.
- 3 Click **OK** to save changes.

About the Last Polled Custom Performance Monitor Values (Single Device) report

This device-level dashboard report displays any custom performance monitors configured for a device and their last poll values. Placing this dashboard report in a device dashboard allows you to monitor important performance monitors and keep up with their latest poll values.

- § **Name.** The name of the performance monitor as listed in the Performance Monitor Library.
- § **Poll Time.** The time the last poll took place.
- § **Time Delta.** The time between the last two polls.
- § **Value.** The value of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
- 3 Click **OK** to save changes.

About the Last Polled Custom Performance Monitor Values (Specific Monitor) report

This home-level dashboard report provides graphical illustration of a device custom performance monitor at the time of the last poll. Placing this dashboard report in a dashboard allows you to view the performance status of a device quickly.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays the custom performance monitor value.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the custom performance monitor value.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the custom performance monitor value.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the custom performance monitor value.
- § **Text.** A numerical representation of the custom performance monitor value. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less



Note: If you do not select the **Define custom min and max values** option on the report configuration dialog, the text value will be displayed in black.

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § **Custom aspect to graph**. Select the custom performance monitor configured for the device to display in the report. If you have not yet, you must configure a custom performance monitor for this device. First configure the monitor in the Performance Monitor Library, and then add it to the device in Device Properties.
 - § **Define custom min and max values**. Selecting this option allows you to choose from all of the graph types listed above. Not selecting this option only allows you to use the text graph.
 - § **Minimum value**. Enter the minimum value to graph.
 - § **Maximum value**. Enter the maximum value to graph.
 - § **Graph type**. Choose the type and size of the graph.



Note: If you choose the gauge graph, selecting the **Define custom min and max values** allows you to reverse the high and low values on the gauge. For example, you could have the 100% available memory as green on the gauge instead of red which would signify a problem.

- § **Width**. Enter a width for the report (in pixels).
 - § **Height**. Enter a height for the report (in pixels).
- 3 Click **OK** to save changes.

About the Disk Utilization: Last Polled Values (Single Device) report

This device-level dashboard report displays current disk utilization percentages for all disks on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's disk(s) to watch for spikes in disk space. The colors displayed in the Percent Used column coincide with the WhatsUp threshold colors:

- § **Red**. Above 90%
- § **Yellow**. Between 80% and 90%
- § **Green**. 80% or less

Each entry in the report contains the following information:

- § **Description**. The particular disk.
- § **Size Used**. The size of disk in use at the time of the last poll.
- § **Total Size**. The total size of the disk.
- § **Percentage Used**. The percentage of the total size of the disk in use at the time of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
 - § To view a graphical representation of the report data, select **Use a graph to display the values**.
 - § If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- 3 Click **OK** to save changes.

About the Disk Utilization: Last Polled Value (Specific Disk) report

This home-level dashboard report provides graphical illustration of disk utilization for a device at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view disk status quickly, even from across the room.

There are five types of graphs to choose from:

- § **Pie**. A 3-D pie graph that displays available disk space in green, and used space in red.
- § **Gauge**. A semi-circle graph (much like a car speedometer) with a pointer that indicates the disk percentage used.
- § **Horizontal bar**. A horizontal bar graph (much like a ruler) with a pointer that indicates the disk percentage used.
- § **Vertical bar**. A vertical bar graph (much like a thermometer) with a pointer that indicates the disk percentage used.
- § **Text**. A numerical representation of the disk percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § **Red**. Above 90%
 - § **Yellow**. Between 80% and 90%
 - § **Green**. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the disk size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.
 - § **Device**. Choose a device by clicking on the browse (...) button.

- § **Disk to graph.** Select a disk to graph for devices with more than one disk.
- § **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

Interface Errors and Discards - Last Poll (Single Device) report

This device-level dashboard report provides details for the number of interface transmit (outbound) and receive (inbound) errors, and transmit and receive discards for the specified device. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot devices that are experiencing interface errors and discard problems.

Each entry in the report contains the following information:

- § **Description.** The selected device interface.
- § **Transmit Errors.** The number of packets transmitted through the device interface with errors.
- § **Receive Errors.** The number of packets received through the device interface with errors.
- § **Transmit Discards.** The number of packets transmitted through the device interface that were discarded.
- § **Receive Discards.** The number of packets received through the device interface that were discarded.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Column 1 width.** The width of the column in the dashboard in pixels.
- 3 Click **OK** to save changes.

Interface: Last Polled Values (Single Device) report

This device-level dashboard report displays current interface utilization percentages for all interfaces on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's interface(s) to keep up with the number of packets they are currently transmitting and receiving. The colors in the second Transmit and Received columns coincide with the WhatsUp Threshold colors:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Description.** The particular interface.
- § **Speed.** The interface speed.
- § **Transmit (kbps).** The number of packets transmitted in kbps.

- § **Receive** (kbps). The number of packets received in kbps.
- § **Transmit**. The percentage of packets transmitted.
- § **Receive**. The percentage of packets received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name**. Enter a title for the dashboard report.
 - § **Device**. Select a device by clicking the browse (...) button.
- 3 Click **OK** to save changes.

About the Last Polled Interface Utilization Value (Specific Interface) report

This home-level dashboard report provides graphical illustration of an interface utilization at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view an interface status quickly, even from across the room.

There are five types of graphs to choose from:

- § **Pie**. A 3-D pie graph that displays available interface space in green, and used space in red.
- § **Gauge**. A semi-circle graph (much like a car speedometer) with a pointer that indicates the interface percentage used.
- § **Horizontal bar**. A horizontal bar graph (much like a ruler) with a pointer that indicates the interface percentage used.
- § **Vertical bar**. A vertical bar graph (much like a thermometer) with a pointer that indicates the interface percentage used.
- § **Text**. A numerical representation of the interface percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § **Red**. Above 90%
 - § **Yellow**. Between 80% and 90%
 - § **Green**. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the interface size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.

- § **Device.** Select a device for the report by clicking on the browse (...) button.
 - § **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - § **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

About the Memory Utilization: Last Polled Value (Single Device) report

This device-level dashboard report displays current memory utilization percentages for all memories on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's memory(s) to watch for spikes in memory utilization. The colors displayed in the Percent Used column coincide with the WhatsUp threshold colors:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Description.** The particular memory.
- § **Size Used.** The size of memory in use at the time of the last poll.
- § **Total Size.** The total size of the memory.
- § **Percentage Used.** The percentage of the total size of the memory in use at the time of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § To view a graphical representation of the report data, select **Use a graph to display the values**.
 - § If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- 3 Click **OK** to save changes.

About the Memory Utilization: Last Polled Value (Specific Aspect) report

This home-level dashboard report provides graphical illustration of device memory utilization at the time of the last poll. Placing this dashboard report in a dashboard allows you to view device memory status quickly.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available memory space in green, and used space in red.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the memory percentage used.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the memory percentage used.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the memory percentage used.
- § **Text.** A numerical representation of the memory percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the memory size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Memory aspect to graph.** For devices with more than one memory aspect, select a memory aspect to graph.
 - § **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

About the Performance: Last Polled Ping Response Time (Specific Interface) report

This home-level dashboard report provides graphical illustration of a device's ping response time. Placing this dashboard report in a dashboard will allow you to view device ping response time status quickly.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available ping response time in green.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the the ping response time.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the ping response time.

- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the ping response time.
- § **Text.** A numerical representation of the ping response time. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
- § Red. Above 90%
- § Yellow. Between 80% and 90%
- § Green. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes:
 - § **Name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Interface.** Select the interface that you want to monitor.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Maximum ping response time.** Enter a value (in milliseconds) for the maximum ping response time.
- 3 Click **OK** to save changes.

Ping Availability and Response Time reports

In This Chapter

Ping Availability and Response Time dashboard reports	152
About the Threshold: Ping Availability report.....	153
About the Threshold: Ping Packet Loss report.....	154
About the Threshold: Ping Response Time report	155
About the Ping:	
Last X hours/days (Single Device Availability) report	155
About the Ping Response Time	
Last X hours/days (Single Device) report.....	156
About the Performance:	
Last Polled Ping Response Time (Specific Interface) report.....	156
About the Ping -	
Last Poll (Single Device Response Time) report.....	157
Top 10: Ping Availability report.....	158
About the Top 10: Ping Packet Loss report.....	159
About the Top 10: Ping Response Time report.....	159

Ping Availability and Response Time dashboard reports

Ping Availability and Response Time dashboard reports	Type	Description
Last 4 hours (single device response time)	Device	Shows the ping response time for all interfaces for a specific device over the last 4 hours.
Last 8 hours (single device response time)	Device	Shows the ping response time for all interfaces for a specific device over the last 8 hours.
Last 7 days (single device response time)	Device	Shows the ping response time for all interfaces for a specific device over the last 7 days.
Last 30 days (single device response time)	Device	Shows the ping response time for all interfaces for a specific device over the last 30 days.
Last 4 hours (single device availability)	Device	Shows the ping availability for all interfaces for a specific device over the last 4 hours.
Last 8 hours (single device availability)	Device	Shows the ping availability for all interfaces for a specific device over the last 8 hours.
Last 7 days (single device availability)	Device	Shows the ping availability for interfaces for a specific device over the last 7 days.
Last 30 days (single device availability)	Device	Shows the ping availability for all interfaces for a specific device over the last 30 days.

Ping Availability and Response Time dashboard reports	Type	Description
availability)		over the last 30 days.
Last Polled Response Time (specific interface)	Home	Shows the last ping response time of a specific device interface at the time of the last poll.
Top 10 by Ping Response Time*	Home	Lists the top 10 devices based on current ping response time.
Top 20 by Ping Response Time	Home	Lists the top 20 devices based on current ping response time.
Top 10 by Ping Packet Loss*	Home	Lists the top 10 devices based on current ping packet loss.
Top 20 by Ping Packet Loss	Home	Lists the top 20 devices based on current ping packet loss.
Top 10 by Ping Availability*	Home	Lists the top 10 devices based on their current ping availability.
Top 20 by Ping Availability	Home	Lists the top 20 devices based on their current ping availability.
Devices with Ping Response Time over 100 msec	Home	Lists all devices with a ping response time greater than 100 msec.
Devices with Ping Response Time over 500 msec	Home	Lists all devices with a ping response time greater than 500 msec.
Devices with Ping Packet Loss over 50%	Home	Lists all devices with a ping packet loss greater than 50%.
Devices with Ping Packet Loss over 75%	Home	Lists all devices with a ping packet loss greater than 75%.
Devices with Ping Availability over 50%*	Home	Lists all devices with a ping availability greater than 50%.
Devices with Ping Availability over 75%	Device	Lists all devices with a ping availability greater than 75%.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the Threshold: Ping Availability report

This home-level dashboard report displays ping availability information for a specific device. A graph displays in the dashboard, charting the device response time to pings (in msec) over the amount of time defined by the specific report type.

§ **Device.** The network device.

§ **Interface.** The network interface.

§ **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device group**. Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold**. Enter a number for the threshold and select a threshold criteria symbol from the list.
 - § **Maximum rows to return**. Enter the number of records to display in the dashboard report.
 - § **Column 2 width**. Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Ping Packet Loss report

This home-level dashboard report displays packet loss information and percentages for devices in a specific group, based on the latest poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their ping packet loss by glancing at the colors associated with each percentage level:

- § **Red**. Above 90%
- § **Yellow**. Between 80% and 90%
- § **Green**. 80% or less

Each entry in the report contains the following information:

- § **Device**. The network device.
- § **Interface**. The network interface.
- § **Sent**. The number of packets sent from the device.
- § **Lost**. The total number of packets lost from the device
- § **% Lost**. The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device group**. Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold**. Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.

- § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Ping Response Time report

This home-level dashboard report displays ping response times for devices in a specific device group. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at the Max and Avg columns for each device.

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Max (ms).** The maximum response time in milliseconds.
- § **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Ping: Last X hours/days (Single Device Availability) report

This device-level dashboard report displays an area graph that details the ping availability percentages for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing ping problems.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - § **Graph type.** Select the type of graph you would like the report to display.

- § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
- 3 Click **OK** to save changes.

About the Ping Response Time Last X hours/days (Single Device) report

This home-level dashboard report displays ping availability information for devices in a specific group. This dashboard report charts device response time to pings (in msec) over the length of time defined by the specific report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Date range.** Select a date range from the drop-down menu.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Trend type.** Select the type of trend you would like the report to use.
 - § **Dimensions.** Select the dimension in which you would like the graph to display.
 - § **Width.** Enter a width for the report (in pixels).
 - § **Height.** Enter a height for the report (in pixels).
 - § **Vertical Axis Scaling.** Select either auto or fixed scale.
 - § **Min.** Enter a number for the lowest point on the Y-axis.
 - § **Max.** Enter a number for the highest point on the Y-axis.
 - § **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

About the Performance: Last Polled Ping Response Time (Specific Interface) report

This home-level dashboard report provides graphical illustration of a device's ping response time. Placing this dashboard report in a dashboard will allow you to view device ping response time status quickly.

There are five types of graphs to choose from:

- § **Pie.** A 3-D pie graph that displays available ping response time in green.
- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the the ping response time.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the ping response time.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the ping response time.
- § **Text.** A numerical representation of the ping response time. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - § Red. Above 90%
 - § Yellow. Between 80% and 90%
 - § Green. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes:
 - § **Name.** Enter a title for the dashboard report.
 - § **Device.** Select a device by clicking the browse (...) button.
 - § **Interface.** Select the interface that you want to monitor.
 - § **Graph type.** Select the type of graph you would like the report to display.
 - § **Maximum ping response time.** Enter a value (in milliseconds) for the maximum ping response time.
- 3 Click **OK** to save changes.

About the Ping - Last Poll (Single Device Response Time) report

This device-level dashboard report gives a graphical representation of a device's ping response time at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view a device's ping status quickly, even from across the room.

There are four types of graphs to choose from:

- § **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the ping response time.
- § **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the ping response time.
- § **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the ping response time.
- § **Text.** A numerical representation of the disk percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Graph type.** Select a type and size of graph to display within the dashboard report.
 - § **Maximum ping response time (ms).** Enter a maximum for the dashboard report.
3. Click **OK** to save changes.

Top 10: Ping Availability report

This home-level dashboard report displays the top devices in a group based on their ping availability percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level.

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the *Ping Availability* (on page 704) report.
- § **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- § **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Ping Packet Loss report

This home-level dashboard report displays the top devices in a group based on their ping packet loss percentages at the time of the last poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at the colors associated with each packet loss percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Sent.** The number of packets sent.
- § **Lost.** The number of packets lost.
- § **% Loss.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
 - § **Top count.** Enter the number of records to display in the dashboard report.
- 3 Click **OK** to save changes.

About the Top 10: Ping Response Time report

This home-level dashboard report displays the top devices in a group based on their ping response times. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at each device's Max and Avg columns.

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width**. Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas reports

In This Chapter

Problem Areas dashboard reports.....	161
About the Problem Areas:	
Actions Fired in the Last X Hours report	162
About the Problem Areas:	
All Completely Down Devices report	163
About the Problem Areas: All Down Interfaces report.....	163
About the Problem Areas: Device Group Mini Status report.....	164
About the Problem Areas:	
Devices with Down Active Monitors report	165
About the Problem Areas:	
Devices with Down Critical Monitors report.....	165
About the Problem Areas: General Error Log report.....	166
About the General: Summary Counts reports.....	166
About the Problem Areas: Tail of Action Activity Log report.....	167
About the Problem Areas:	
Tail of Passive Monitor Error Log report.....	167
About the Problem Areas: Tail of SNMP Trap Log report.....	168
About the Problem Areas: Tail of State Change Log report.....	169
About the Problem Areas: Tail of Syslog report.....	169
About the Problem Areas: Tail of Windows Event Log report	170
About the Problem Areas: Unacknowledged Devices report.....	170
About the Problem Areas: Web Alarms report.....	171

Problem Areas dashboard reports

Problem Areas dashboard reports	Type	Description
Devices with Down Active Monitors	Device	Displays down Active Monitors for a device.
All Down Interfaces	Device	Displays down interfaces for a device.
Tail of State Change Log	Device	Displays the tail of the State Change Log for a specified device.
Tail of Syslog	Device	Displays the tail of the Syslog full report for a specified device.
Tail of Windows Event Log	Device	Displays the tail of the Windows Event Log for a specified device.

Problem Areas dashboard reports	Type	Description
Tail of SNMP Trap Log	Device	Displays the tail of the SNMP Trap Log for a specified device.
Tail of Action Activity Log*	Device	Displays the tail of the Action Activity Log for a specified device.
Tail of Passive Monitor Error Log	Device	Displays the tail of the Passive Monitor Error Log for a specified device.
Web Alarms	Device	Displays any web alarms fired for a specified device.
All Completely Down Devices	Home	Displays down devices for a specified device group.
All Down Interfaces	Home	Displays down interfaces for a specified device group.
Devices with Down Active Monitors	Home	Displays devices with down Active Monitors within a specified device group.
Unacknowledged Devices	Home	Displays unacknowledged devices within a specified device group.
Tail of State Change Log	Home	Displays a tail of the State Change Log for your network.
Summary Counts*	Home	Displays a summary of a specified device group.
Tail of Syslog	Home	Displays the tail of the Syslog full report for your network.
Tail of Windows Event Log	Home	Displays the tail of the Windows Event Log for your network.
Tail of SNMP Trap Log	Home	Displays the tail of the SNMP Trap Log for your network.
Tail of Action Activity Log*	Home	Displays the tail of the Action Activity Log for your network.
Tail of Passive Monitor Error Log	Home	Displays the tail of the Passive Monitor Error Log for your network.
Device Group Mini Status	Home	Lists all devices in a device group and displays their status by color.
Web Alarms	Home	Shows a snap shot of the most recent web alarms fired on your network.
General Error Log	Home	Displays the tail of the General Error Log for your network.
Actions Fired in the Last 4 Hours	Home	Displays all devices that have fired an action in the last four hours.

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

About the Problem Areas: Actions Fired in the Last X Hours report

This dashboard report displays devices that have fired an action over a selected period of time. Placing this dashboard report in a dashboard can give you a snapshot of the health and success of actions on your network.

- § **Date.** The date the action was fired. Click a date to bring up the Action Log.
- § **Source.** The device from which the action was fired. Click a device to bring up the Device Status Report.
- § **Action Name.** The name of the action as listed in the Active Monitor Library.

- § **Trigger.** The trigger for the action, either Up or Down. Click a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices.
 - § **Last hours.** Enter the number of hours from which you would like information displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the column in pixels.
 - § **Maximum rows to return.** Enter a value for the number of rows of data displayed within the report.
- 3 Click **OK** to save changes.

About the Problem Areas: All Completely Down Devices report

This dashboard report displays down devices for a specified group. Adding this dashboard report to a dashboard helps you monitor your network status by displaying which devices are down.

- § **Device.** The network device.
- § **Status.** The status of the device after the last poll.

You can maximize your available monitor space by limiting the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for column 2 in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: All Down Interfaces report

This dashboard report displays down interfaces for a specified group. Adding this dashboard report to a dashboard allows you to monitor network status by displaying all interfaces that are down.

- § **Device.** The network device.
- § **Status.** The status of the interface after the last poll.

You can maximize your available monitor space by limiting the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select Every device to select all devices regardless of their subgroups.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for column 2 in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: Device Group Mini Status report

This dashboard report lists all devices in a group and displays their status by color, allowing you to quickly scan and observe the statuses of devices in a group. Displaying multiple mini status reports within a dashboard view allows you to watch more than one group on your network at once, and can help you monitor important or problem areas more efficiently. You can also optionally display active monitors associated with the devices in a selected group, which is helpful in identifying which services on your network are down.

To help maximize the available viewing area on your monitor, you can change the size of each mini status report. Even if the font size is too small to read at first glance, you can use the mouse over text to find out the identity of a device. The static rows of the mini status also aid in device recognition, as devices always stay in the same row regardless of their current state.

Status icon colors are the same as the WhatsUp Gold state colors:

- § **Green** is Up
- § **Red** is Down
- § **Gray** is Unknown

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. To select every device on the network, select Every device.
 - § **Every device.** Select this option to display every device in the system. However, only devices that you have permissions to view display.

- § **Style.** Select the style and size in which you would like the mini status displayed.
 - § **Normal.** Displays device and active monitor status with icons.
 - § **High Contrast.** Displays device and active monitor status with bright colors.
 - § **Show Active Monitors.** Select this option to display the active monitors associated with the group devices.
 - § **Active Monitors per Row.** Select the number of active monitors displayed per row.
 - § **Active Monitors Cell Width.** Enter a cell width in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: Devices with Down Active Monitors report

This dashboard report displays devices with down active monitors for a select group. Adding this dashboard report to a dashboard view helps you watch your network status by showing you which devices are down, and the status of active monitors.

- § **Device.** The network device.
- § **Status.** The status of the device active monitor after the last poll.

To help maximize the available viewing area on your monitor, you can limit the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select Every device to select all devices.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for column 2 in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: Devices with Down Critical Monitors report

This home-level dashboard report displays devices with down critical monitors for a specified device group. Adding this dashboard report to a dashboard allows you to easily keep-up with your network's status by showing you which devices are down, and the status of critical monitors.

- § **Device.** The network device.
- § **Status.** The status of device's critical monitor after the last poll.

You can maximize your screen real-estate by limiting the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device group**. Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum rows to return**. Enter the number of records to display in the dashboard report.
 - § **Column 2 width**. Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas: General Error Log report

This dashboard report displays any error received by WhatsUp Gold. Displaying this dashboard report within a dashboard view helps you keep tabs on all of your network errors.

This dashboard report includes the following boxes:

- § **Date**. The date the error took place.
- § **Category**. The type of error.
- § **Source**. Where the error originated.
- § **Details**. The details of the error.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
 - § **Column 4 width**. Enter a width for column 4 (in pixels).
- 3 Click **OK** to save changes.

About the General: Summary Counts reports

This general dashboard report gives a summary of a group by the total number of:

- § Monitored devices
- § Up devices
- § Down devices
- § Devices with down Active Monitors
- § Devices in Maintenance
- § Active Monitors
- § Down Active Monitors

- § Up interfaces
- § Down interfaces
- § Actions fired in the last 4 hours

Each entry in the report contains the following information:

- § **Count.** The total number of that specific type of passive monitor on the network.
- § **Total number of.** The device status types.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of Action Activity Log report

This dashboard report shows the tail (last 10 records) of the Action Log. Placing this dashboard report in a dashboard lets you see the success rate of actions fired. This enables you to monitor important devices easily and to quickly address any issues. The dashboard report is linked to the full Action Log, which shows all of the actions that WhatsUp Gold has attempted to fire based on the configuration of the action.

- § **Date.** The date the action was fired. Click a date to bring up the Action Log.
- § **Source.** The source of the action. Click a source to bring up the Device Status report.
- § **Action Name.** The name of the Action.
- § **Trigger.** The trigger for the action (either Up or Down). Click a trigger to open the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the column (in pixels).
 - § **Column 3 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of Passive Monitor Error Log report

This universal problem areas dashboard report shows any passive monitor errors that have occurred for the specified devices.

- § **Date.** The date the error occurred.
- § **Device.** The network device.
- § **Category.** The category code of the error. Possible values include Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error).
- § **Details.** Text that describes the error that was received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. To select every device on the network, select **Every device**.
 - § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - § **Column 4 width.** Enter a width for the Details column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of SNMP Trap Log report

This dashboard report displays the tail (last 10 records) of the SNMP Trap Log. Placing this dashboard report in a dashboard displays system-wide SNMP traps. For more information, the dashboard report is linked to the full SNMP Trap Log, which provides a history of SNMP traps that have occurred during the time period displayed at the bottom of the report.

- § **Date.** The date and time the trap occurred.
- § **Device.** The device from which the trap was sent.
- § **SNMP Trap Type.** The type of trap.
- § **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.



Note: In order for entries to be added to this report, the SNMP Trap listener must be enabled, and either a SNMP trap passive monitor must be added to a device or unsolicited SNMP traps must be accepted. For more information, see *Enabling the SNMP Trap Listener* (on page 903).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the Source column in pixels.
 - § **Column 4 width.** Enter a width for the Payload column in pixels.

- 3 Click **OK** to save changes.

About the Problem Areas: Tail of State Change Log report

This dashboard report shows the tail (last 10 records) of the State Change Timeline. Placing this dashboard report in a dashboard can help you visualize the monitor health for a device and also decrease the monitoring of crucial devices. For more information, see the full State Change Timeline, which is linked to this dashboard report. The State Change Log shows a time line of when each monitor changed from one state to another during the displayed time period.

- § **Start time.** The date and time of the state change. Click a time to bring up the State Change Timeline for a single device.
- § **Device.** The device on which the action is configured. Click a device to bring up the Device Status report.
- § **Monitor.** The active monitor by type. Click an active monitor to bring up the Active Monitor Availability report for that monitor.
- § **State.** The state of the condition at the time of the poll. Click a state to bring up the State Change Timeline for that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 3 width.** Enter a width for the Monitor column (column 3) in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of Syslog report

This dashboard report displays the tail (last 10 records) of the Syslog Entries Report. Placing this dashboard report in a dashboard grants visual access to Syslog log entries for the system. For more information, this dashboard report is linked to the Syslog Entries report, which shows Syslog events logged for the system during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Syslog listener must be enabled, and either a Syslog passive monitor must be added to a device or unsolicited messages must be accepted. For more information, see *Enabling the Syslog listener* (on page 904).

- § **Date.** The date and time the Syslog entry was received by WhatsUp Gold.
- § **Device.** The device for which the message was configured.
- § **Syslog Type.** The type of message.
- § **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.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width**. Enter a width for the Device column in pixels.
 - § **Column 4 width**. Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of Windows Event Log report

This dashboard report displays the tail (last 10 records) of the Windows Event Log. Placing this dashboard report in a dashboard displays system-wide Windows events. For more information, this dashboard report is linked to the Windows Event Log, which shows Windows events logged during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Windows Event Log listener must be enabled. For more information on the Windows Event Log listener, see [Enabling the Windows Event Log Listener \(on page 904\)](#).

- § **Date**. The date and time the event was received by WhatsUp Gold.
- § **Device**. The device or program that originated the entry.
- § **WinEvent Type**. The type of Windows Event.
- § **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 with the event message.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width**. Enter a width for the Device column in pixels.
 - § **Column 4 width**. Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

About the Problem Areas: Unacknowledged Devices report

This home-level dashboard report displays unacknowledged devices in a specific group. Adding this dashboard report to a dashboard alerts you of unacknowledged devices in a group at a glance, allowing you to quickly resolve issues.

- § **Device**. The network device.

- § **Device Type.** The type of device.
- § **Unacknowledged For.** The amount of time the device has gone unacknowledged.
- § **In Maintenance.** Either Yes or No.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 3 width.** Enter a width for column 3 (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas: Web Alarms report

This dashboard report shows a snapshot of the most recent web alarms fired on your network. Add this dashboard report to a highly visible dashboard so that recent issues can be noted and addressed if needed.

- § **Date.** The date the alarm was fired. Click on a date to bring up the Web Alarms Report.
- § **Source.** The source of the alarm, such as a device or active monitor. Click on a source to bring up the Device Status report. The icon next to the display name of the item shows the current state of that item.
- § **Message.** The message produced by the web alarm.
- § **Trigger.** This is the state that caused the web alarm to trigger. Click on a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the Source column in pixels.
 - § **Column 3 width.** Enter a width for the Message column in pixels.
- 3 Click **OK** to save changes.

Problem Areas Specific Device

In This Chapter

About the Problem Areas:

Down Active Monitors (Single Device) report.....172

About the Problem Areas:

Device Down Interfaces (Single Device) report.....173

About the Problem Areas:

Tail of Action Activity Log (Single Device) report173

About the Problem Areas Specific Device:

Tail of Passive Monitor Error Log (Single Device) report174

About the Problem Areas Specific Device:

Tail of SNMP Trap Log (Single Device) report.....174

About the Problem Areas Specific Device:

Tail of State Change Log (Single Device) report.....175

About the Problem Areas: Tail of Syslog (Single Device) report.....176

About the Problem Areas Specific Device:

Tail of Windows Event Log (Single Device) report176

About the Problem Areas Specific Device:

Web Alarms (Single Device) report.....177

About the Problem Areas: Down Active Monitors (Single Device) report

This device-level dashboard report displays the down active monitors for a device and their current state. The Down Active Monitors dashboard report displays the following information for a device:

§ **Monitor.** The type of Active Monitor.

§ **State.** The state of the Monitor after the last poll.

Adding this report to a Device Status dashboard keeps you updated on the health of the active monitors for an important device. If no active monitors appear in the report, none are currently down.

To see all Active Monitors on a device regardless of down state, see *General: Device Active Monitors* (on page 83).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Click browse (...) to select a device.
- 3 Click **OK** to save changes.

About the Problem Areas: Device Down Interfaces (Single Device) report

This dashboard report displays down interfaces for a specific device.

- § **Interface.** The network interface.
- § **Status.** The status of the interface after the last poll.

Adding this dashboard report to a dashboard lets you quickly view the status of a particular device by showing you what interfaces are down on a device.

To help maximize the available viewing area on your monitor, limit the number of rows displayed in the report or decrease the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the Status column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of Action Activity Log (Single Device) report

This device-level dashboard report shows the tail (last 10 records) from the Action Log for a specified device. Placing this dashboard report in a device dashboard grants visual access to the success rate of actions fired for a particular device. Crucial devices can be monitored easily, and problems can be dealt with swiftly. For more information, the dashboard report is linked to the full Action Log, which shows all of the actions that WhatsUp Gold has attempted to fire on the device, based on the configuration of the action.

- § **Date.** The date the action was fired. Click on a date to bring up the Action Log.
- § **Source.** The source of the action. Click on a source to bring up the Device Status report.
- § **Trigger.** The action's trigger. Either Up or Down. Click on a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.

- § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Top count.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas Specific Device: Tail of Passive Monitor Error Log (Single Device) report

This dashboard report shows any performance monitor error logs that have occurred for a specified device.

- § **Date.** The date the error occurred.
- § **Category.** The category code of the error. Either Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error.)
- § **Details.** Text that describes the error that was received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device.** Click Browse (...) to select a device.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 3 width.** Enter a width for the Details column.
- 3 Click **OK** to save changes.

About the Problem Areas Specific Device: Tail of SNMP Trap Log (Single Device) report

This device-level dashboard report displays the tail (last 10 records) of the SNMP Trap Log for a specified device. Placing this report report in a device report grants visual access to SNMP traps for a particular device. For more information, the report report is linked to the full SNMP Trap Log, which provides a history of SNMP traps that have occurred for a device during the time period displayed at the bottom of the report.

- § **Date.** The date and time the trap occurred.
- § **Device.** The device where the trap originated.
- § **SNMP Trap Type.** The type of trap.
- § **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.



Note: In order for entries to be added to this report, the SNMP Trap listener must be enabled and an SNMP Trap passive monitor must be added to the device. For more information, see *Enabling the SNMP Trap Listener* (on page 903).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** Enter the number of rows you would like displayed in the report.
 - § **Column 2 width.** Enter a width for the Device column (in pixels).
 - § **Column 4 width.** Enter a width for the Payload column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas Specific Device: Tail of State Change Log (Single Device) report

This device-level dashboard report shows the tail (last 10 records) from the State Change Timeline for a specified device. Placing this dashboard report in a device dashboard can visualize a device's monitor health and help ease the task monitoring crucial devices. For more information, the dashboard report is linked to the full State Change Log, which shows a time line of when each monitor on a device changed from one state to another during the displayed time period.

- § **Start time.** The date and time of the state change. Click on a time to bring up the Device List.
- § **Device.** The device the action is configured on. Click on a device to bring up the Device Status dashboard.
- § **Monitor.** The active monitor by type.
- § **State.** The state of the condition at the time of the poll. Click on a state to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Name.** Enter a title for the dashboard report.
 - § **Top count.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the Device column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas: Tail of Syslog (Single Device) report

This device-level dashboard report displays the tail (last 10 records) from the Syslog Entries Report for a specified device. Placing this dashboard report in a device dashboard grants visual access to Syslog log entries for a particular device. For more information, this dashboard report has been linked to the Syslog Entries report, which shows Syslog events logged for the selected device during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Syslog listener must be enabled, and a Syslog passive monitor must be added to a device. For more information, see *Enabling the Syslog Listener* (on page 904).

- § **Date.** The date and time the Syslog entry was received by WhatsUp Gold.
- § **Syslog Type.** The type of message.
- § **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.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Click browse (...) to select a device.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 3 width.** Enter a width for the Payload column (in pixels).
- 3 Click **OK** to save changes.

About the Problem Areas Specific Device: Tail of Windows Event Log (Single Device) report

This dashboard report displays the tail (last 10 records) of the Windows Event Log for a specific device. Placing this dashboard report in a dashboard displays system-wide Windows events. For more information, this dashboard report is linked to the Windows Event Log, which shows Windows events logged during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Windows Event Log listener must be enabled. For more information on the Windows Event Log listener, see *Enabling the Windows Event Log Listener* (on page 904).

- § **Date.** The date and time the event was received by WhatsUp Gold.
- § **WinEvent Type.** The type of Windows Event.
- § **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 with the event message.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device**. Click browse (...) to select a device.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
 - § **Column 3 width**. Enter a width for the Payload column (in pixels).
- 3** Click **OK** to save changes.

About the Problem Areas Specific Device: Web Alarms (Single Device) report

This dashboard report shows a snapshot of the most recent web alarms fired on a particular device.

The following boxes appear in this dashboard report:

- § **Date**. The date the alarm was fired. Click a date to bring up the Web Alarms Report.
- § **Message**. The message produced by the web alarm.
- § **Trigger**. This is the state that caused the web alarm to trigger. Click a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the report.
 - § **Device**. Browse for the device to display web alarms for.
 - § **Maximum rows to return**. Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width**. Enter a width for the column in pixels.
 - § **Column 3 width**. Enter a width for the Payload column in pixels.
- 3** Click **OK** to save changes.

Remote/Central reports

In This Chapter

Remote/Central dashboard reports.....	179
About the Remote Reports: Remote Group List report.....	180
About the Remote Reports: Remote Site List report.....	180
About the Remote Reports: Remote Sites Overview report	181
About the Remote Reports: Tail of Remote Site Log report.....	182
About the Remote Reports: Active Monitor States report.....	183
About the Remote Reports: Device Status report	183
About the Remote Reports: Monitor Status report.....	184
About the Remote Reports: Summary Counts report.....	184
About the Remote Reports: Tail of Action Activity Log report	185
About the Remote Reports: Top 10 Ping Response Time report.....	186
About the Remote Reports:	
Top 10 Ping Response Time over 1ms report.....	186
Remote Reports: Top 10 Ping Packet Loss	187
Remote Reports: Top 10 Ping by Packet Loss over 50%	189
About the Remote Reports: Top 10 CPU by Utilization report	190
About the Remote Reports:	
Top 10 CPU by Utilization over 80% report	191
About the Remote Reports: Top 10 Memory by Utilization report.....	192
About the Remote Reports:	
Top 10 Memory by Utilization over 80% report	192
About the Remote Reports: Top 10 Disk Utilization report.....	193
About the Remote Reports:	
Top 10 Disk Utilization over 80% report.....	194
About the Remote Reports: Top 10 Disk Free Space report	195
About the Remote Reports:	
Top 10 Disk Free Space Over 1024 MB report	196
About the Remote Reports: Top 10 Interface Utilization report.....	197
About the Remote Reports:	
Top 10 Interface Utilization Over 80% report.....	198

About the Remote Reports:

Top 10 Interface Traffic Utilization Over 80% report.....199

About the Remote Reports:

Top 10 Interface with Traffic Over 50 Kbps report.....200

Remote Reports:

Top 10 Custom Performance Monitor dashboard report201

About the Remote Reports:

Top 10 Custom Performance Monitor with Threshold report202

About the Remote Reports: Top 10 Ping Availability report203

About the Remote Reports:

Top 10 Ping Availability Over 50% report204

Remote/Central dashboard reports

Remote/Central dashboard reports	Type	Description
(Only available in distributed editions)		
Summary Counts (Remote)	Home	Provides a summary for a remote site by the total number of its monitored devices, up devices, down devices, devices with down active monitors, devices in maintenance, active monitors, down active monitors, up interfaces, down interfaces, actions fired in the last four hours.
Active Monitor States (Remote)	Home	Displays Active Monitor states for a remote site at the time of the last refresh.
Tail of Action Activity Log (Remote)	Home	Provides the tail (last 10 records) of the Action Log for a device group on a remote site.
Device Status (Remote)	Home	Displays a status summary for devices on a remote site at the time of the last refresh.
Monitor Status (Remote)	Home	Displays a status summary for monitors on a remote site at the time of the last refresh.
Remote Site List	Home	Lists all sites configured for use in WhatsUp Gold Remote and Central Site Editions.
Tail of Remote Site Log	Home	Provides the tail (last 10 records) of the Remote Site Log.
Remote Site Overview	Home	Displays an overview of information on a remote site configured for use in your WhatsUp Gold Distribute Solution.

Remote/Central dashboard reports	Type	Description
Group List (Remote)	Home	Lists all subgroups in a remote site's My Network Group and their status at the time of the last refresh.

About the Remote Reports: Remote Group List report

This remote reports dashboard report lists all groups configured in a remote server's WhatsUp Gold My Network group and their status at the last refresh time. For more information, see Using the Remote/Central dashboard reports.

The report displays the following information:

- § **Remote server.** The remote server selected for the report.
- § **Last run.** The last time discovery ran.
- § **Group name.** The name of the remote server's My Network group.
- § **Display name.** The names of all subgroups configured on the selected remote server.
- § **Status.** The status of the groups at the time of the last run.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- 3 Click **OK** to save changes.

About the Remote Reports: Remote Site List report

This Remote Report dashboard report lists all sites configured for use with WhatsUp Gold Remote and Central Site Editions. For more information, see Using the Remote/Central dashboard reports.

This report displays the following information:

- § **Display Name.** The Remote Site's display name.
- § **Local device.** The device associated with the Remote Site. This device is often the computer that is running the WhatsUp software to monitor a Remote Site.
- § **Last connect time.** The last time WhatsUp Gold connected to the Remote Site.
- § **Last refresh time.** The last time data gathered from the Remote Site was refreshed.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Column 3 width**. Enter a width (in pixels) for the Last connect time column.
 - § **Column 4 width**. Enter a width (in pixels) for the Last refresh time column.
- 3 Click **OK** to save changes.

About the Remote Reports: Remote Sites Overview report

This remote reports dashboard report displays an overview of information on a Remote Site configured for use in your WhatsUp Gold Distributed Solution. For more information, see Using the Remote/Central dashboard reports.

The name of the Remote Site is displayed in the upper-left side of the report. The **Last snapshot** is the time information gathered from the Remote Site was refreshed to display in this dashboard report.

The dashboard report displays the following information about the Remote Site:

- § **Http address**. The Http address specified for the site at **Configure > Program Options > Central Site Configuration**.
- § **Last connect time**. The last time WhatsUp Gold connected to the Remote Site.
- § **Last refresh time**. The last time data gathered from the Remote Site was refreshed to display updated data.
- § **# of devices**. The number of devices on the Remote Site.
- § **# of monitors**. The number of monitors configured for the devices on the Remote Site.
- § **# of queries**. The number of queries running on the Remote Site.
- § **Display name**. The Remote Site device's display name.
- § **Device type**. The Remote Site device's type.
- § **Host name**. The Remote Site device's host name.
- § **Address**. The Remote Site device's address.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - § **Remote site**. Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Local device.** Allows users, with rights, the ability to select a local device to associate the Remote Site with. 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.

- 1 Click **OK** to save changes.

About the Remote Reports: Tail of Remote Site Log report

This home-level Remote Reports dashboard report displays the tail (last 10 records) of the Remote Site Log. The report displays information for both a WhatsUp Gold Client and a Server, depending on which version of WhatsUp Gold you are running. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Date.** The date the error took place.
- § **Type.** The type of the error message received.
- § **Message.** The error message received.
- § **Remote Site.** The Remote Site on which the failed connection took place.



Note: The Remote site column is only displayed when you are running the Server Distributed version of WhatsUp Gold.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - § **Column 1 width.** Enter a width for the column in pixels.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Active Monitor States report

This remote report dashboard report lists all Active Monitors assigned to devices on the selected Remote Site. For more information, see Using the Remote/Central dashboard reports.

The table included in the dashboard report lists each device by display name, and the state of all Active Monitors assigned to each device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site**. Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Remote active monitor type**. Select a remote active monitor type for the report. The default is All active monitor types.
 - § **Internal monitor state**. Select an internal monitor state (All states, Up, Maintenance, Down, Unknown) for the report.
- 3 Click **OK** to save changes.

About the Remote Reports: Device Status report

This remote dashboard report provides a status summary of all monitored devices on a Remote Site according to the last refresh time. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Display name**. The display name for the monitored device.
- § **Devices up**. The number of monitored devices on the Remote Site in the Up state at the last connect time.
- § **Devices down**. The number of monitored devices on the Remote Site in the Down state at the last connect time.
- § **In maintenance**. The number of monitored devices on the Remote Site in the maintenance at the last connect time.
- § **Last refresh time**. The last time data gathered from the Remote Site was refreshed to display updated data.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:

- § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- 3 Click **OK** to save changes.

About the Remote Reports: Monitor Status report

This remote dashboard report provides a status summary of all monitors configured for the monitored devices on a Remote Site according to the last refresh time. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Display name.** The monitored device's display name.
- § **Monitors up.** The total number of monitors on the Remote Site in the Up state at the last connect time.
- § **Monitors down.** The total number of monitors on the Remote Site in the Down state at the last connect time.
- § **Last refresh time.** The last time data gathered from the Remote Site was refreshed to display updated data.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- 3 Click **OK** to save changes.

About the Remote Reports: Summary Counts report

This remote reports dashboard report provides a summary for a Remote Site by the total number of:

- § Monitored devices
- § Up devices
- § Down devices
- § Devices with down Active Monitors
- § Devices in Maintenance
- § Active Monitors
- § Down Active Monitors
- § Up interfaces
- § Down interfaces
- § Actions fired in the last 4 hours

For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains these pieces of information:

- § **Count.** The total number of that specific type of passive monitor on the network.

§ **Total number of.** The device status types.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- 3 Click **OK** to save changes.

About the Remote Reports: Tail of Action Activity Log report

This remote reports dashboard report shows the tail (last 10 records) of the Action Log for a device group on a Remote Site. Placing this dashboard report in a dashboard grants visual access to the success rate of actions fired for a particular device group on a Remote Site. Crucial devices can be monitored easily, and problems can be dealt with swiftly. For more information, the dashboard report is linked to the full Action Log, which shows all of the actions that WhatsUp Gold has attempted to fire on the group, based on the configuration of the action. For more information, see Using the Remote/Central dashboard reports.

The dashboard report displays the following information about the Remote Site:

- § **Date.** The date the action was fired. Click on a date to bring up the Action Log.
- § **Source.** The source of the action. Click on a source to bring up the Device Status report.
- § **Action Name.** The name of the Action.
- § **Trigger.** The trigger for the action. Either Up or Down. Click on a trigger to open the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.
 - § **Note:** The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the hostname report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.

- § **Column 2 width.** Enter a width for the column in pixels.
- § **Column 3 width.** Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Ping Response Time report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their ping response times. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at each device's Max and Avg columns. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Ping Response Time over 1ms report

This home-level dashboard report displays ping response times by threshold for devices in a specific device group on a Remote Site. Placing this dashboard report in a dashboard allows

you to keep tabs on crucial devices and their current ping response times by glancing at devices with ping response times over 1ms. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Max (ms).** The maximum response time in milliseconds.
- § **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though the default threshold is 1ms, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Ping Packet Loss

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their ping packet loss percentages at the last poll. Placing this dashboard report in a

dashboard allows you to keep tabs on crucial devices by glancing at the colors associated with each packet loss percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Sent.** The number of packets sent.
- § **Lost.** The number of packets lost.
- § **% Loss.** The percentage of sent packets that have been lost.



Note: All of the data displayed in this dashboard report is based on the latest poll.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Ping by Packet Loss over 50%

This home-level dashboard report displays packet loss information and percentages for devices in a specific group from a Remote Site based on the latest poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their ping packet loss by glancing at each device's ping packet loss over 50%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Sent.** The number of packets sent from the device.
- § **Lost.** The total number of packets lost from the device
- § **% Lost.** The percentage of sent packets that have been lost.



Note: All of the data displayed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 50%, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 CPU by Utilization report

This home-level dashboard report displays the top devices in a group from a Remote Site based on their current CPU utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains these pieces of information.

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **CPU.** The device's CPU description.
- § **CPU Load.** The percentage of CPU currently in use.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 CPU by Utilization over 80% report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their current CPU utilization percentage thresholds. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load by glancing at each device's current CPU utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Description.** The device description.
- § **CPU Load.** The percentage of the CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Memory by Utilization report

This home-level dashboard report displays the top devices in group on a Remote Site, based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- § **Percent Used.** The percentage of utilized memory.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Memory by Utilization over 80% report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their memory utilization percentages. Placing this dashboard report in a dashboard

allows you to keep tabs on crucial devices and their current memory capacity by glancing at each device's current memory utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- § **Percent Used.** The percentage of utilized memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Disk Utilization report

This home-level dashboard report displays the top devices based on their percentage of utilized disk space on a Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Disk.** The device's drive description.
- § **Percent Full.** The percentage of the disk currently utilized.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Disk Utilization over 80% report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their percentage of disk utilization. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their disk utilization by glancing at each device's current disk utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.

- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Disk.** The device's drive description.
- § **Percent Full.** The amount of utilized disk space on that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Disk Free Space report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their percentage of available free space on the Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current level of disk free space by glancing at the current disk percentage level for each device. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.

- § **Device.** The network device.
- § **Disk.** The device's drive description.
- § **Size.** The size of the disk in GB.
- § **Free space.** The amount of free space on the disk in GB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.
 - § **Note:** The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.
 - § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Disk Free Space Over 1024 MB report

This home-level dashboard report displays the top devices based on their available free space over 1024 MB on a Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current level of disk free space by glancing at each device's current disk space level over 1024 MB.

For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Disk.** The device drive description.
- § **Size.** The size of the disk in GB.
- § **Free space.** The amount of free space on the disk in GB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site**. Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group**. Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display**. Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
- § **Threshold**. Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 1024MB, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width**. Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Interface Utilization report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface utilization percentages. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site**. The remote server for which the report is configured.
- § **Last snapshot**. The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device**. The network device.
- § **Interface**. The device's interface description.
- § **Transmit**. The number of packets transmitted from each interface.
- § **Receive**. The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Interface Utilization Over 80% report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The device's interface description.
- § **Transmit.** The number of packets transmitted from each interface.
- § **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Interface Traffic Utilization Over 80% report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface utilization percentages. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The device interface description.
- § **Transmit.** The number of packets transmitted from each interface.
- § **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.

- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the *'Others'* category, and display when **Include 'Others'** is selected.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Interface with Traffic Over 50 Kbps report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface with traffic over 50 Kbps. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The device's interface description.
- § **Transmit.** The number of packets transmitted from each interface.
- § **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the *'Others'* category, and will be displayed when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though the default threshold is 50Kbps, you can change this threshold. If you do so, you should change the report title accordingly.

- § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Custom Performance Monitor dashboard report

This home-level dashboard report displays top devices in a remote group based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.
- § **For group.** The group you selected to display in the report.
- § **Device.** The device associated with the custom performance monitor. Clicking on the device will bring up its Device Status dashboard.
- § **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list will be empty.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the

category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.

§ **Column 2 width.** Enter a width for the column in pixels.

3 Click **OK** to save changes.

About the Remote Reports: Top 10 Custom Performance Monitor with Threshold report

This home-level dashboard report displays top devices in a group from a Remote Site, based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.
- § **For group.** The group you selected to display in the report.
- § **Device.** The device associated with the custom performance monitor. Clicking on the device will bring up its Device Status dashboard.
- § **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list will be empty.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the

category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.

§ **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.

§ **Column 2 width.** Enter a width for the column in pixels.

3 Click **OK** to save changes.

About the Remote Reports: Top 10 Ping Availability report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their ping availability percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

§ **Remote Site.** The remote server for which the report is configured.

§ **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.

§ **Device.** The network device.

§ **Interface.** The network interface.

§ **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the Ping Availability report.

§ **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.

§ **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

§ **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.

§ **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

§ **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.

§ **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.

- § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Remote Reports: Top 10 Ping Availability Over 50% report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their ping availability percentage over 50%. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- § **Remote Site.** The remote server for which the report is configured.
- § **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the Ping Availability report.
- § **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- § **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- § **Device Group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
- § **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 50%, you can change this threshold. If you do so, you should change the report title accordingly.

§ **Column 2 width.** Enter a width for the column (in pixels).

3 Click **OK** to save changes.

Split Second Graph reports

In This Chapter

Split Second Graph dashboard reports	206
Using Split Second Graph dashboard reports	207
About the Split Second Graph: CPU report	207
About the Split Second Graph: CPU Gauge report	209
About the Split Second Graph: Disk report	210
About the Split Second Graph: Interface report	211
About the Split Second Graph: Memory report	212
About the Split Second Graph: Performance Monitor report	213
About the Split Second Graph: Ping report	214
About the Split Second Graph: Ping Gauge report	215
About the Split Second Graph: Task Manager CPU report	216
About the Split Second Graph: Task Manager CPU Bar report	217
About the Split Second Graph: Task Manager Memory report	218
About the Split Second Graph: Task Manager Memory Bar report	219

Split Second Graph dashboard reports

Split Second Graph dashboard reports (not available in Standard Edition)	Type	Description
Performance Monitor	Home	Displays custom real-time graphs for an SNMP or WMI enabled device.
Interface	Home	Displays real-time interface utilization for an SNMP-enabled device.
CPU	Home Or Device	Displays real-time cpu utilization for all CPUs on an SNMP-enabled device.
CPU gauge	Home or device	Displays real-time cpu utilization for all CPUs on an SNMP-enabled device.

Split Second Graph dashboard reports	Type	Description
Ping	Home Or Device	Displays real-time ping response time for all network interfaces on a device.
Ping gauge	Home or device	Displays real-time ping response time for all network interfaces on a device.
Disk	Home or device	Displays real-time disk utilization for all disks on an SNMP-enabled device.
Memory	Home or Device	Displays real-time memory utilization for an SNMP enabled-device.
Task Manager CPU Line Graph	Home or Device	Displays the CPU usage of a WMI-enabled device as a line graph.
Task Manager Memory Usage Line Graph	Home or Device	Displays the memory usage of a WMI-enabled device as a line graph.
Task Manager CPU Bar Graph	Home or Device	Displays a bar graph of the CPU usage of a WMI-enabled device in real time.
Task Manager Memory Bar Graph	Home or Device	Displays a bar graph of the memory usage of a WMI-enabled device in real time.

Using Split Second Graph dashboard reports

Split Second Graph dashboard reports allow you to embed real-time data available from InstantInfo popups, the Web Task Manager, and the Web Performance Monitor into any dashboard view.

For information on how to add a dashboard report to a dashboard view, see *Adding dashboard reports to a dashboard view* (on page 48).

About the Split Second Graph: CPU report

This dashboard report displays real-time CPU utilization for all CPUs on an SNMP-enabled device. The device must have SNMP credentials specified in **Device Properties > Credentials**. This report queries the specified device for a list of all CPUs and then polls and graphs each of them for the duration that the report is loaded in the web browser.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - § **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - § **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- § **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

About the Split Second Graph: CPU Gauge report

This dashboard report displays real-time CPU utilization for all CPUs on an SNMP-enabled device. The device must have SNMP credentials specified in Device **Properties > Credentials**. This report queries the specified device for a list of all CPUs and then polls and graphs each of them for the duration that the report is loaded in the web browser.



Note: The transparent dial indicates the CPU minimum or maximum utilization percentage and the solid dial indicates the current CPU utilization percentage. If there are two CPUs on a device, only data for one CPU displays on the gauge at a time. Click a CPU in the legend (Intel 1 or Intel 2) to place focus on a particular CPU gauge.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the dashboard report title bar, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Graph type.** Select a graph size for the gauge, either Small, Medium, or Large.
 - § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** This value determines the amount of time that WhatsUp Gold uses to determine the gauge's average value. For example, if the gauge's data interval is set to 60 seconds, the value reported on the gauge is calculated by averaging the minimum value and the maximum value reported over that 60 second timeframe.
- 3 Click **OK** to save changes.

About the Split Second Graph: Disk report

This dashboard report displays real-time disk utilization for all disks on a SNMP enabled device. The device must have SNMP credentials specified in **Device Properties > Credentials**. This report queries the specified device for a list of all disks and then polls and graphs each of them for the duration that the report is loaded in the Web browser.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - § **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - § **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- § **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

About the Split Second Graph: Interface report

This dashboard report displays real-time interface utilization for an SNMP enabled device. The device must have SNMP credentials specified in **Device Properties > Credentials**.



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: This dashboard report is only available on Home dashboard views.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Interface name.** For devices with more than one interface, select a device by click the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - § **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - § **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- § **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 675).

- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

About the Split Second Graph: Memory report

This dashboard report displays real-time memory utilization for a SNMP enabled device. The device must have SNMP credentials specified in **Device Properties > Credentials**. This report queries the specified device to determine if it can report memory utilization and then polls and graphs it for the duration that the report is loaded in the web browser.



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 configure this dashboard report in WhatsUp Gold:

- 1 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - § **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.

§ **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- § **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 2 Click **OK** to save changes.

About the Split Second Graph: Performance Monitor report

For more information on building custom graphs, please see the Web Performance Monitor help.



Note: This dashboard report is only available on Home dashboard views.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Click browse (...) and select the device you want to monitor.
 - § **Interface to graph.** Select the device interface to graph from the list.

- § **Width.** Specify how wide, in pixels, the graph or chart should appear.
- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - § **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - § **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- § **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 675).
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

About the Split Second Graph: Ping report

This dashboard report displays real-time Ping response time for all network interfaces on a device. This report queries the database for a list of all configured network interfaces and then polls and graphs each of them for the duration that the report is loaded in the web browser.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information in the following boxes.

- § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- § **Device.** Select a device for the report by clicking the browse (...) button.
- § **Interface to graph.** Select which interface to ping.
- § **Width.** Specify how wide, in pixels, the graph or chart should appear.
- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - § Auto Scale adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - § Fixed Scale shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- § **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see Graph Types.
- § **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- § **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

3 Click **OK** to save changes.

About the Split Second Graph: Ping Gauge report

This dashboard report displays real-time Ping response time for all network interfaces on a device. This report queries the database for a list of all configured network interfaces and

then polls and graphs each of them for the duration that the report is loaded in the Web browser.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following boxes.
 - § **Report name**. Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device**. Select a device for the report by clicking the browse (...) button.
 - § **Interface to graph**. For devices with more than one interface, select an interface to graph by clicking the browse (...) button.
 - § **Graph type**. Select a graph size for the gauge, either Small, Medium, or Large.
 - § **Maximum ping response time (ms)**. The maximum number displayed on the gauge. Enter a number (in ms) for this maximum time.
 - § **Refresh interval (seconds)**. Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds)**. This value determines the amount of time that WhatsUp Gold uses to determine the gauge's average value. For example, if the gauge's data interval is set to 60 seconds, the value reported on the gauge is calculated by averaging the minimum value and the maximum value reported over that 60 second timeframe.
- 3 Click **OK** to save changes.

About the Split Second Graph: Task Manager CPU report

This dashboard report displays the CPU usage of specific device as a line graph. The device must have Windows credentials specified in **Device Properties > Credentials**. This dashboard report shows current real-time data as well as historical data plotted on the line graph. The graph shows up to x seconds of historical data.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following boxes.

- § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- § **Device.** Select a device for the report by clicking the browse (...) button.
- § **Width.** Specify how wide, in pixels, the graph or chart should appear.
- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

About the Split Second Graph: Task Manager CPU Bar report

This dashboard report displays a bar graph of the CPU usage of a specific device in real time. The device must have Windows credentials specified in **Device Properties > Credentials**. You must configure this dashboard report and select a device before any data is reported.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.

- § **Height.** Specify how tall, in pixels, the graph or chart should appear.
- § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

About the Split Second Graph: Task Manager Memory report

This dashboard report displays the memory usage of specific device as a line graph. The device must have Windows credentials specified in **Device Properties > Credentials**. This dashboard report shows current real-time data as well as historical data plotted on the line graph. The graph shows up to x seconds of historical data.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

About the Split Second Graph: Task Manager Memory Bar report

This dashboard report displays a bar graph of the memory usage of a specific device in real time. The device must have Windows credentials specified in **Device Properties > Credentials**. You must configure this dashboard report and select a device before any data is reported.



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 configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information:
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device.** Select a device for the report by clicking the browse (...) button.
 - § **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - § **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - § **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- § **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

Threshold reports

In This Chapter

Threshold dashboard reports.....	221
About the Threshold: CPU Utilization report.....	222
About the Threshold: Custom Performance Monitor report.....	222
About the Top 10: Disk Free Space report	223
About the Threshold: Disk Utilization report.....	224
About the Threshold: Interface Traffic report.....	224
About the Threshold: Interface Utilization report	225
About the Threshold: Memory Utilization report	226
About the Threshold: Ping Availability report.....	226
About the Threshold: Ping Packet Loss report.....	227
About the Threshold: Ping Response Time report	228

Threshold dashboard reports

Threshold dashboard reports	Type	Description
Ping Response Time*	Home	Displays the top devices based on their current ping response time thresholds.
Ping Packet Loss	Home	Displays the top devices based on their current ping packet loss thresholds.
CPU Utilization	Home	Displays the top devices based on their current CPU utilization percentage thresholds.
Memory Utilization	Home	Displays the top devices based on their current memory utilization percentage thresholds.
Disk Utilization	Home	Displays the top devices based on their current disk utilization percentage thresholds.
Disk Free Space*	Home	Displays the top devices based on their current disk free space thresholds.
Interface Utilization	Home	Displays the top devices based on their current interface utilization percentage thresholds.
Interface Traffic*	Home	Displays the top devices based on their current interface traffic thresholds.
Ping Availability	Home	Displays the top devices based on their current ping availability thresholds.
Custom Performance Monitor	Home	Displays the value for performance monitors on devices over, under or equal to a configured threshold value.

About the Threshold: CPU Utilization report

This home-level dashboard report displays the top devices based on their current CPU utilization percentage thresholds. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Description.** The description of the device.
- § **CPU Load.** The percentage of the CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though a default threshold exists, you can change this threshold. If you do, change the report title accordingly.

- § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Custom Performance Monitor report

This home-level dashboard report displays the top devices based on a selected custom WMI or SNMP performance monitor.

The top of the report displays the name of the selected custom performance monitor and to which device group the report applies.

Each entry in the report contains the following information:

Device. The monitored network device.

Value. The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device group**. Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Performance monitor**. Choose a performance monitor from the drop-down menu. If there are no performance monitors listed in the drop-down menu, you must first configure a custom WMI or SNMP performance monitor from the Performance Monitor Library.
 - § **Threshold**. Enter a number for the threshold and select a threshold criteria from the separate list.
 - § **Maximum rows to return**. Enter the number of records to display in the dashboard report.
- 3 Click **OK** to save the changes.

About the Top 10: Disk Free Space report

This home-level dashboard report displays the top devices based on their percentage of available free disk space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk capacity by glancing at the colors associated with each percentage level:

- § **Red**. Above 90%
- § **Yellow**. Between 80% and 90%
- § **Green**. 80% or less

Each entry in the report contains the following information:

- § **Device**. The network device.
- § **Disk**. The device's drive description.
- § **Size**. The size of the disk in MB.
- § **Free space**. The amount of free space on the disk in MB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Device group**. Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold**. Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.

- § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- § **Column 2 width.** Enter a width for the Description column in pixels.
- 3 Click **OK** to save changes.

About the Threshold: Disk Utilization report

This home-level dashboard report displays the top devices based on their percentage of disk utilization. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their disk utilization by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Disk.** The description of the drive.
- § **Percent Full.** The amount of utilized disk space on that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold percentage and select a threshold criteria (*under, over, equals*) from the list.



Note: Though a default threshold exists, you can change this threshold. If you do so, change the report title accordingly.

- § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report.
- § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Interface Traffic report

This home-level dashboard report displays interface traffic information for a specified device group based on the number of packets both sent and received. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current interface traffic rates by glancing at the numbers in the transmit and receive columns for each device.

- § **Device.** The network device.
- § **Interface.** The interface description.
- § **Transmit.** The number of packets sent.
- § **Receive.** The number of packets received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Interface Utilization report

This home-level dashboard report displays the top devices based on their percentage of transmitted and received packets. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their interface utilization by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Transmit.** The percentage of packets transmitted by a device.
- § **Receive.** The percentage of packets received by a device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.

- § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
- § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Memory Utilization report

This home-level dashboard report displays the top devices based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory capacity by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- § **Percent Used.** The percentage of utilized memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (*under, equals, over*) from the list.



Note: Though a default threshold exists, you can change this threshold. If you do, change the report title accordingly.

- § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report.
- § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Ping Availability report

This home-level dashboard report displays ping availability information for a specific device. A graph displays in the dashboard, charting the device response time to pings (in msec) over the amount of time defined by the specific report type.

- § **Device.** The network device.
- § **Interface.** The network interface.

§ **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

§ **Report name.** Enter a title for the dashboard report.

§ **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.

§ **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.

§ **Maximum rows to return.** Enter the number of records to display in the dashboard report.

§ **Column 2 width.** Enter a width for the Description column (in pixels).

3 Click **OK** to save changes.

About the Threshold: Ping Packet Loss report

This home-level dashboard report displays packet loss information and percentages for devices in a specific group, based on the latest poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their ping packet loss by glancing at the colors associated with each percentage level:

§ **Red.** Above 90%

§ **Yellow.** Between 80% and 90%

§ **Green.** 80% or less

Each entry in the report contains the following information:

§ **Device.** The network device.

§ **Interface.** The network interface.

§ **Sent.** The number of packets sent from the device.

§ **Lost.** The total number of packets lost from the device

§ **% Lost.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

§ **Report name.** Enter a title for the dashboard report.

§ **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.

- § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

About the Threshold: Ping Response Time report

This home-level dashboard report displays ping response times for devices in a specific device group. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at the Max and Avg columns for each device.

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Max (ms).** The maximum response time in milliseconds.
- § **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - § **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - § **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - § **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Top 10 reports

In This Chapter

Top 10 dashboard reports	229
About the Top 10: CPU Utilization report.....	230
About the Top 10: Custom Performance Monitor report.....	230
About the Top 10: Disk Free Space report	231
About the Top 10: Disk Utilization report.....	232
About the Top 10: Interface Discards report.....	232
Top 10: Interface Errors report.....	233
About the Top 10: Interface Traffic report.....	233
About the Top 10: Interface Utilization report.....	234
About the Top 10: Memory Utilization report.....	234
Top 10: Ping Availability report	235
About the Top 10: Ping Packet Loss report.....	236
About the Top 10: Ping Response Time report.....	236
Wireless Top 10 Bandwidth.....	237
Wireless Top 10 Client Count	237
Wireless Top 10 Rogue Count	238
Wireless Top 10 RSSI.....	238

Top 10 dashboard reports

Top 10 dashboard reports	Type	Description
Ping Response Time	Home	Displays the top devices based on their current ping response time.
Ping Packet Loss	Home	Displays the top devices based on their current ping packet loss.
CPU Utilization	Home	Displays the top devices based on their current CPU utilization.
Memory Utilization	Home	Displays the top devices based on their current memory utilization.
Disk Utilization	Home	Displays the top devices based on their current disk utilization.
Disk Free Space	Home	Displays the top devices based on their current disk free space.
Interface Utilization	Home	Displays the top devices based on their current interface utilization.
Interface Traffic	Home	Displays the top devices based on their current interface traffic.
Custom Performance	Home	Displays the value for performance monitors on devices over,

Top 10 dashboard reports	Type	Description
Monitor		under or equal to a configured threshold value.
Ping Availability	Home	Displays the top devices based on their current ping availability.
Interface Errors	Home	Displays the top devices based on total interface errors.
Interface Discards	Home	Displays the top devices based on total interface discards.

About the Top 10: CPU Utilization report

This home-level dashboard report displays the top devices based on their current CPU utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load. Report percentages are displayed in colors that represent the CPU utilization thresholds:

- § Red. Above 90%
- § Yellow. Above 80%
- § Green. 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **CPU.** The device CPU description.
- § **CPU Load.** The percentage of CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information:
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Custom Performance Monitor report

This home-level dashboard report displays top devices in a group based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values.

- § **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.

- § **For group.** The group you selected to display in the report.
- § **Device.** The device associated with the custom performance monitor. Clicking on the device opens its Device Status dashboard.
- § **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list is empty.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

About the Top 10: Disk Free Space report

This home-level dashboard report displays the top devices based on their percentage of available free space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current level of disk free space by glancing at the current disk percentage level for each device.

- § **Device.** The network device.
- § **Disk.** The drive description.
- § **Size.** The size of the disk in GB.
- § **Free space.** The amount of free space on the disk in GB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices.
 - § **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Disk Utilization report

This home-level dashboard report displays the top devices based on their percentage of utilized disk space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Disk.** The drive description.
- § **Percent Full.** The percentage of the disk currently utilized.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Interface Discards report

This home-level dashboard report displays the top device interfaces with packet discards for inbound and outbound data during a selected time period.

- § **Device.** The network device name.
- § **Interface.** The interface description.
- § **Transmit.** The number of discarded packets transmitted from each interface.
- § **Receive.** The number of discarded packets received from each interface.
- § **Total.** Provides the number of packets discarded for each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select all devices or a specific device group for the dashboard report. Select **Every device** or clear **Every device** if you want to select a specific device

group, then click the browse (...) button to select the device group you want to include in this dashboard report.

§ **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.

§ **Column 2 width.** Enter a width for the column (in pixels).

3 Click **OK** to save changes.

Top 10: Interface Errors report

This home-level dashboard report displays the top device interfaces with packet errors for inbound and outbound data during a selected time period.

§ **Device.** The network device name.

§ **Interface.** The interface description.

§ **Transmit.** The number of packets transmitted from each interface.

§ **Receive.** The number of packets received from each interface.

§ **Total.** Provides the number of packet errors for each interface.

To configure this dashboard report in WhatsUp Gold:

1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

§ **Report name.** Enter a title for the dashboard report.

§ **Device group.** Select all devices or a specific device group for the dashboard report. Select **Every device** or clear **Every device** if you want to select a specific device group, then click the browse (...) button to select the device group you want to include in this dashboard report.

§ **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.

§ **Column 2 width.** Enter a width for the column (in pixels).

3 Click **OK** to save changes.

About the Top 10: Interface Traffic report

This home-level dashboard report displays the top devices in a group based on their current interface traffic as a total of packets transmitted and received.

§ **Device.** The network device.

§ **Interface.** The device's interface description.

§ **Transmit.** The number of packets transmitted from each interface.

§ **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following boxes.

§ **Report name.** Enter a title for the dashboard report.

- § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

About the Top 10: Interface Utilization report

This home-level dashboard report displays the top devices in a group based on their interface utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial interfaces and their current utilization by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Interface.** The interface description.
- § **Transmit.** The percentage of packets transmitted from each interface.
- § **Receive.** The percentage of packets received from each interface.

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the appropriate information.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Memory Utilization report

This home-level dashboard report displays the top devices based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory load by glancing at the colors associated with each percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- § **Percent Used.** The percentage of utilized memory.

To configure this dashboard report:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the appropriate information into the following boxes:
 - § **Report name.** Enter a title for the dashboard report.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

Top 10: Ping Availability report

This home-level dashboard report displays the top devices in a group based on their ping availability percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level.

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the *Ping Availability* (on page 704) report.
- § **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- § **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

About the Top 10: Ping Packet Loss report

This home-level dashboard report displays the top devices in a group based on their ping packet loss percentages at the time of the last poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at the colors associated with each packet loss percentage level:

- § **Red.** Above 90%
- § **Yellow.** Between 80% and 90%
- § **Green.** 80% or less

Each entry in the report contains the following information:

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Sent.** The number of packets sent.
- § **Lost.** The number of packets lost.
- § **% Loss.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name.** Enter a title for the dashboard report.
 - § **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - § **Maximum rows to return.** This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width.** Enter a width for the column (in pixels).
 - § **Top count.** Enter the number of records to display in the dashboard report.
- 3 Click **OK** to save changes.

About the Top 10: Ping Response Time report

This home-level dashboard report displays the top devices in a group based on their ping response times. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at each device's Max and Avg columns.

- § **Device.** The network device.
- § **Interface.** The network interface.
- § **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following boxes.
 - § **Report name**. Enter a title for the dashboard report.
 - § **Maximum rows to return**. This column deems how many devices appear in the report. Enter the number of device records you want displayed in the report. For example, if you want a top 10 report, enter 10 records; if you want a top 20 report, enter 20 records.
 - § **Column 2 width**. Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Wireless Top 10 Bandwidth

The Top 10 Bandwidth dashboard report displays the ten wireless elements (Client Groups, Clients, SSIDs, or APs) on your network with the highest aggregate bandwidth. For each device displayed, the following data is displayed:

- § **Client Group/Client/SSID/AP**. Displays the Client Group, Client, SSID, or access point depending on how the table is grouped.
- § **Min**. Displays the minimum speed of data traffic during the selected time interval in kilobytes per second. Min. is only displayed when the Top 10 Bandwidth Report is viewed in tabular format.
- § **Max**. Displays the maximum speed of data traffic during the selected time interval in kilobytes per second. Max. is only displayed when the Top 10 Bandwidth Report is viewed in tabular format.
- § **Average Bytes Received/Sent**. Displays the aggregate average amount of data received (under Traffic In) or sent (under Traffic Out) by the client, SSID, or access point during the selected time interval in kilobytes per second.



Important: For important information regarding traffic in, traffic out, and how bandwidth data is reported by Wireless, see Bandwidth.

Wireless Top 10 Client Count

The Top 10 Client Count dashboard report displays the ten wireless elements (Client Groups, Clients, SSIDs, or APs) on your network with the highest number of clients connected. For each device listed, the following data is displayed:

- § **Client Group/SSID/AP**. Displays the Client Group, SSID, or access point depending on how the table is grouped.
- § **Min**. Displays the lowest number of clients the device connected to at one time within the specified time interval. Min. is only displayed when the Top 10 Client Count Report is viewed in tabular format.
- § **Max**. Displays the highest number of clients the device connected to at one time within the specified time interval. Max. is only displayed when the Top 10 Client Count Report is viewed in tabular format.

- § **Average Count.** Displays the aggregate average number of clients the device connected to within the specified time interval.

Wireless Top 10 Rogue Count

The Top 10 Rogue Count dashboard report displays a listing of the ten access points on your network with the highest number of rogues detected. For each device listed, the following data is displayed:

- § **Device.** Displays the device name or IP address of the access point.
- § **Rogue Count.** Displays the number of times the device was polled and returned data within the selected time interval.

Wireless Top 10 RSSI

The Top 10 RSSI dashboard report displays a the ten wireless infrastructure devices on your network with the lowest RSSI percentage. For each device listed, the following data is displayed:

- § **Device.** Displays the client group name or access point.
- § **Min%.** Displays the lowest signal transmission strength received from the device within the selected time interval.
- § **Max%.** Displays the highest signal transmission strength received from the device within the selected time interval.
- § **Average%.** Displays the average signal strength from the selected device within the selected time interval.

Devices

In This Chapter

Discovery Console	240
Using Devices	264
Using Maps	271
Managing devices.....	281
Using Device Properties.....	304
Using Network Tools	316
Monitoring Devices.....	340

Discovery Console

In This Chapter

Discovering network devices	240
Using Device Roles	255
Managing device roles	262

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 24).

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 240) and *Preparing WhatsUp Gold for discovery* (on page 241).

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; SNMP v2/v2c credentials are preferred. For information about how to enable SNMP on a specific device, see *Enabling SNMP on Windows devices* (on page 479) in the *WhatsUp Gold Online Help* (<http://www.whatsupgold.com/wug163webhelp>) or consult the network device documentation.

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 972) 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 255) 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 267) 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 656) in the help.

Configuring and running discovery

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

- § *Configuring discovery settings* (on page 242)
- § *Running discovery* (on page 247)
- § *Adding discovered devices to WhatsUp Gold* (on page 250)

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

Configuring 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 246).
- § **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 246).
- § **Hosts File Scan.** WhatsUp Gold imports devices from a hosts file. For more information, see *Using Hosts File Scan* (on page 246).



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, Windows (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 in WhatsUp Gold. For more information, see *Using Credentials* (on page 267).



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

- § **SNMP Timeout (seconds).** Enter the time, in seconds, for an SNMP device to respond. 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.
- § **SNMP Retries.** Enter the number of times to try to attempt to discover a device at a given IP address before continuing on to the next device. The default is 1 retry.
- § **WMI Timeout (seconds).** Enter the time, in seconds, for a WMI device to respond. If it does not respond to the scan within this time, the scan continues on to the next IP address. The default is 10 seconds.
- § **Merge Level** allows you to adjust the device discovery merge level from an existing device in WhatsUp Gold with a newly discovered device in WhatsUp Gold on a per session basis. This Merge Level option applies to devices that have multiple IP addresses assigned to it. The Primary IP, during a discovery session, refers to the first IP found on the device. The Primary IP of a device that has been saved to the WhatsUp Gold database can be viewed and set in the device's Device Property dialog. The following options are available for discovery merge levels:
 - § **Any to Any.** Any IP of an incoming device merges to Any IP of a device previously discovered and included in the WhatsUp Gold database. This is the default discovery

behavior in v16.0 and 16.1.0. 16.1 SP1 and later use Primary to Primary as the default merge level.

- § **Any to Primary.** Any IP of an incoming device merges to the Primary IP of a device previously discovered and included in the WhatsUp Gold database.
- § **Primary to Any.** Primary IP of an incoming device merges to Any IP of a device previously discovered and included in the WhatsUp Gold database.
- § **Primary to Primary.** Primary IP of an incoming device to Primary IP of a device previously discovered and included in the WhatsUp Gold database. This is the default discovery behavior in 16.1 SP1 and later.
- § **Always Create.** Always create a new device with no merging for previously discovered devices that are included in the WhatsUp Gold database.



Note: Scheduled discovery does not have a concept of merge level and always uses the Primary to Primary merge method.

- § **Resolve host names.** Select this option to have WhatsUp Gold attempt to populate the list of discovered devices with host names. 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 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).
- § **Autoscan virtual environments.** Select this option to automatically scan virtual machine devices after WhatsUp Gold detects a vCenter server or VMware host. If you do not want WhatsUp Gold to scan for the virtual machines hosted by discovered VMware servers, clear **Auto scan virtual environments**.



Note: When the **Autoscan virtual environments** option is selected and a vCenter server is being discovered, the scan will first scan the vCenter server, then it will scan each of the VMware hosts and virtual machines managed by the vCenter server.



Note: When the **Autoscan virtual environments** option is selected and only a VMware host is being discovered, the scan will first scan the VMware host, then it will scan each of the virtual machines hosted by the VMware host.



Note: In order for WhatsUp Gold to successfully scan a virtual machine device, VMware Tools must be installed on the device.

- § **Use layer 2 discovery and generate layer 2 topology map.** By default, WhatsUp Gold automatically uses layer 2 discovery to generate layer 2 topology maps and inventory information available in the Device Viewer. This information is used to create graphical representations of network connections between discovered devices.
- § **Gather information for wireless topology and performance.** Select this option to enable wireless device discovery using the Wireless plug-in.

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.

The screenshot shows the 'Discovery Console' window. On the left, the 'Progress Summary' pane includes:

- Device Summary:** Device Limit (5000), Existing Devices (299), Discovered Devices (122).
- Network Traffic:** SNMP Bytes (1047672 / 841066), PDU (in/out) (13337 / 14015), Scanned (255 of 255).
- Session Metrics:** Scan Start (3/9/2015 10:58:39 AM), Scan End (3/9/2015 11:06:19 AM), Elapsed Time (00:07:46).
- Session Settings:** Scan Type (IP Range Scan), Layer 2 scan (enabled), SNMP Credentials (3 / 3), SSH Credentials (1 / 1), Windows Credentials (3 / 3), VMware Credentials (3 / 3).

The main 'Devices Discovered' table lists several devices, all with a Status of 'complete'. The bottom of the console shows a progress bar at 100.00% and tabs for 'Device Information', 'Scheduled Discoveries (0)', and 'Saved Results (0)'.

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 255).

- § **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 255) 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 255) 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.



- 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 242).
- 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 259) (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 259) 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 251).

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 250).

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*.

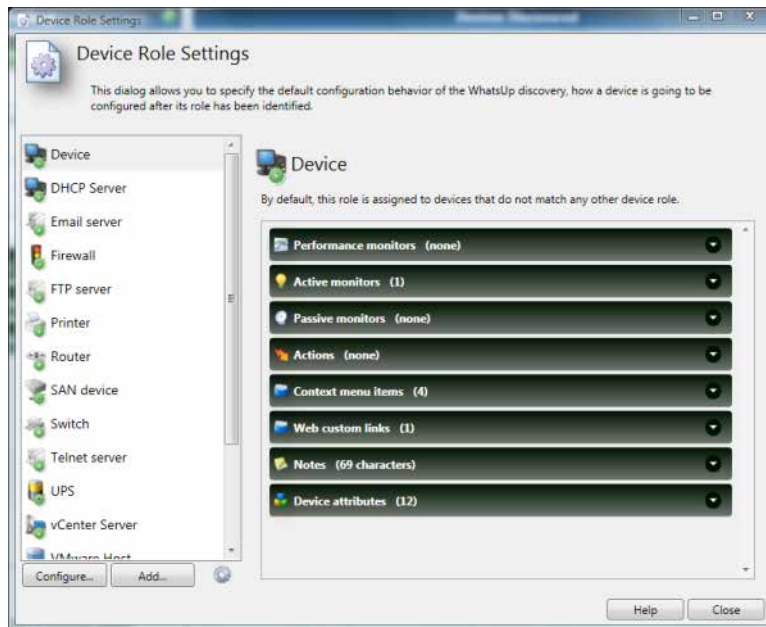
Device roles do two things:

- § 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.



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

To configure device role settings:

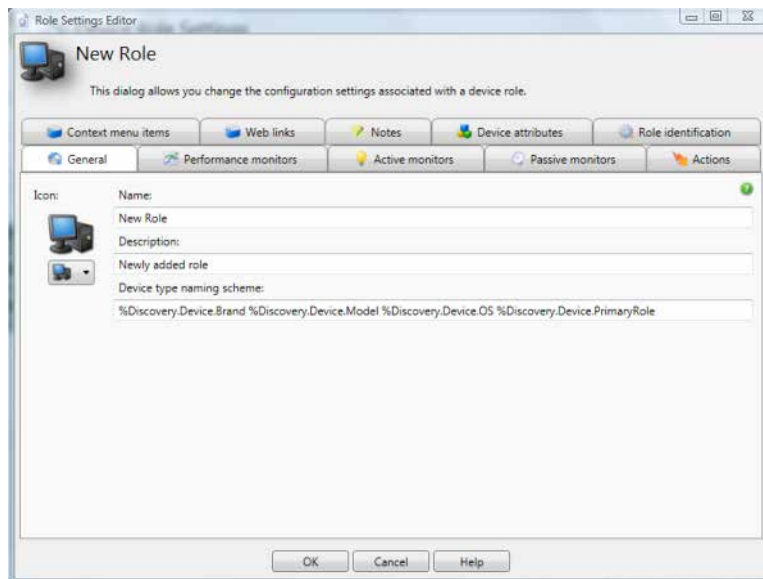
- 1 Open the Discovery console from the WhatsUp Gold console.
- 2 Click **Advanced > Device role settings**. The Device Role Settings dialog appears.
- 3 Select the device role you want to modify, then click **Configure**.

- 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.

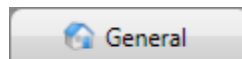


- 4 Configure the device properties. The following table lists the device properties that can be configured to be automatically added to discovered devices that match a device role.

To configure this property

The device's icon and informational overlay text, as seen on the device map

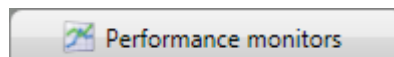
Use this tab



Notes

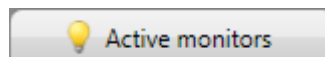
Supports discovery percent variables (on page 259). For more information, see the General tab console Help.

Performance monitors applied to the device



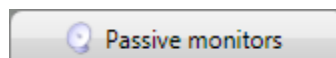
For more information, see the Performance monitors tab console Help.

Active monitors applied to the device, including which active monitors are critical


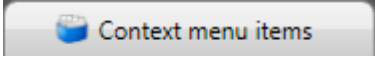
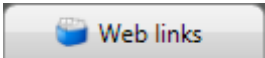
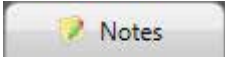
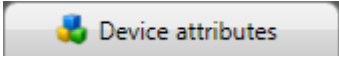
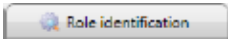


To make an active monitor critical, click the checkbox in the **Critical** column of that monitor. For more information, see About critical active monitors (on page 432) and the Active monitors tab console Help.

Passive monitors associated with the device



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.

To configure this property	Use this tab	Notes
Action policy applied to the device		For more information, see the Passive monitors tab console Help.
Context menu items available when right-clicking on the device in the console		For more information, see the Actions tab console Help.
Web links available for the device in the web interface		Supports discovery percent variables (on page 259). For more information, see the Context menu items tab console Help.
The initial content of the device's Notes box		Supports discovery percent variables (on page 259). For more information, see the Web links tab console Help.
Attributes added to the device		Supports discovery percent variables (on page 259). For more information, see the Notes tab console Help.
The criteria a discovery scan uses to determine whether a device fits a specific role		Supports discovery percent variables (on page 259). For more information, see the Device attributes tab console Help.
-		For more information, see Configuring device role identification settings (on page 257).

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 1.3.6.1.2.1.1.0 (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 1.3.6.1.2.1.1.0, 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.

<code>%Discovery.Device.VMware.Host.NumberCPUCores</code>	Returns the number of CPU cores on the VMware host server.
<code>%Discovery.Device.VMware.Host.NumberCPUPkgs</code>	Returns the number of CPU packages on the VMware host server.
<code>%Discovery.Device.VMware.Host.NumberCPUThreads</code>	Returns the number of CPU threads on the VMware host server.
<code>%Discovery.Device.VMware.Host.CPUFrequency</code>	Returns the CPU clock frequency of the VMware host server in Hz.
<code>%Discovery.Device.VMware.Host.CPUModel</code>	Returns the CPU model used by the VMware host server.
<code>%Discovery.Device.VMware.Host.MemorySize</code>	Returns the amount of memory in the VMware host server.
<code>%Discovery.Device.VMware.Host.NumberVMsTotal</code>	Returns the total number of virtual machines hosted by the VMware server.
<code>%Discovery.Device.VMware.Host.NumberVMsPoweredOn</code>	Returns the number of virtual machines hosted by the VMware server that are in the powered on state.
<code>%Discovery.Device.VMware.Host.NumberVMsSuspended</code>	Returns the number of virtual machines hosted by the VMware server that are in the suspended state.
<code>%Discovery.Device.VMware.Host.NumberVMsPoweredOff</code>	Returns the number of virtual machines hosted by the VMware server that are in the powered off state.

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

<code>%Discovery.Session.ElapsedTime</code>	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 262)
- § *Duplicate existing device roles* (on page 262)
- § *Modify device roles* (on page 263)
- § *Enable or disable device roles* (on page 263)
- § *Restore device roles to their original settings* (on page 263)
- § *Delete device roles* (on page 263)

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.....	264
Understanding device and monitor states.....	265
Understanding state changes.....	266
About device icons.....	266
Using Credentials.....	267
Searching for devices.....	267
Understanding group access and user rights for Find Device.....	268
Searching for devices with interface traffic	269

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.

Active Monitors

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 341).

Passive Monitors

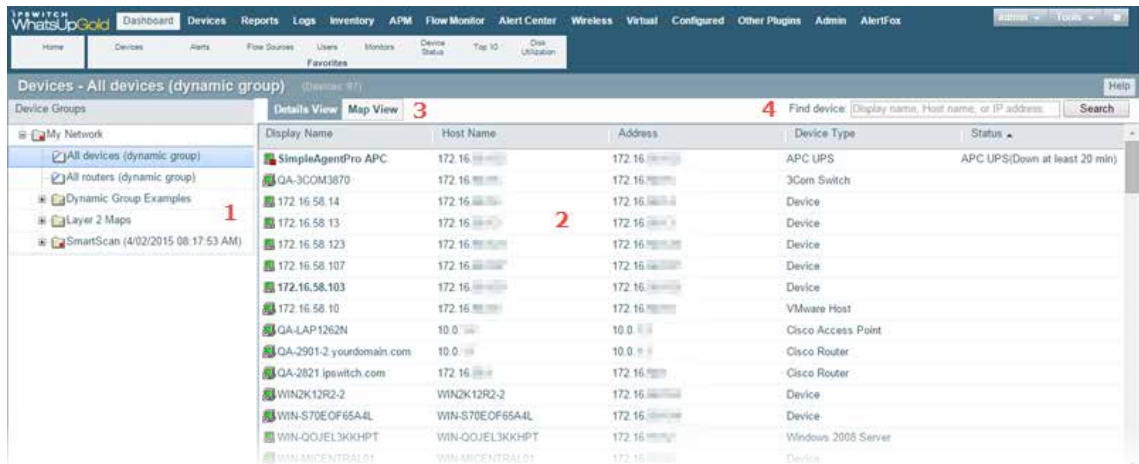
You can also configure passive monitors, which listen for specified events to occur on a device and when the event occurs, notifies you or takes other actions. For more information, see the *Passive Monitors overview* (on page 436).

Performance Monitors

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*.

To view network devices:

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



- 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*.
- 2 Details View** (shown). Lists network devices as a list of devices in a group.
- 3 Map View.** 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 271).
- 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 267).

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.

Understanding device and monitor states

In WhatsUp Gold devices are classified by *states*, or the condition of the device at the time it was last polled. Device states are determined by the status of the device and any passive or active monitors assigned to the device.

WhatsUp Gold device states:

- § **Up** - The device and all of its monitors were up at the time of its last poll. It is possible for a device to be partially up if one of the device's monitors is up, but others are down.
- § **Down** - The device and all of its monitors were down at the time of its last poll. It is possible for a device to be partially down if one of the device's monitors is down, but others remain up. Keep in mind that in some cases, a down device may not necessarily be physically down. Down means that WhatsUp Gold is unable to gather the information it needs to consider the device up. For example, if a device is behind a slow DSL connection, it is difficult for WhatsUp Gold to quickly gather responses from

queries. As such, the device could be considered down although the device is in fact powered on and running as expected. If unexpected down statuses are issued for devices, be sure to check connections, firewalls, and the like to ensure that WhatsUp Gold is able to query devices for status information.

§ *Maintenance* - The device was in maintenance mode at the time of its last poll.

§ *Unknown* - The device has not yet been polled; this status most typically displays immediately following discovery.

For information about the icons that indicate a device's status, see [About device icons](#).



Tip: The *State Summary* (on page 740) log displays a summary of device states for devices in a device group.

Understanding state changes

Device and monitor state changes occur when after a poll, the status of the device or a monitor assigned to the device has changed from the status found on the poll preceding the most recent poll.

In the Device List or Map View, a bold device name indicates 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**.





For more information, see *Using Acknowledgments* (on page 301).



Tip: The *State Change Acknowledgment* (on page 716) report gives a list of devices in a device group whose state changes need acknowledgment.

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 271).

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

It is important to set up credentials for network devices before discovering new devices with WhatsUp Gold. The Credentials system stores the applicable login, community string, or connection string information for network devices such as routers, switches, servers, virtual hosts, and other devices. Use the device credential library to add the following devices and application credential types to WhatsUp Gold:

- § 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.

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 268).

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 305) 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 305).
- § 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 Maps

In This Chapter

Using Map View	271
About Map View device limitations.....	274
Using Map Options commands.....	274
Creating Layer 2 Groups.....	275

Using Map View

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

- § Organize devices into user-specified groups, for example, all HTTP servers, or devices in a certain location.
- § Configure Layer-2 maps for device groups to illustrate the network topology of the particular device group.
- § 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 -

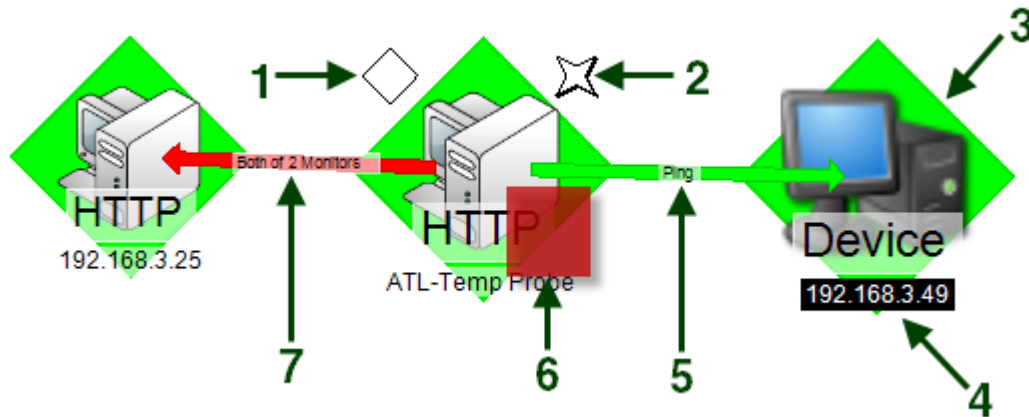
From the WhatsUp Gold console, go to **View > Map View**.

Interpreting Map View

Map View consists of device icons, annotations, and graphical indicators which are used to represent the state of your network. Device icons are a graphical representation of network devices and provide the hostname or IP address of each device. These icons can be modified by adding annotations, which you can add manually in the WhatsUp Gold admin console, and by graphical indicators that 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 865) 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.

Using Map Options commands

You can configure network maps using the following commands, accessible from the Map Options right-click menu:

- § **Add Devices.** Click this command to add network devices to the map using the Select Devices to Add dialog.
- § **Remove Devices.** Click this command to remove from the map using the Select Devices to Remove dialog.
- § **Add Connected.** Click this command to add connected devices to the map using the following sub-menu commands.



Note: The following commands cannot be undone; ensure that you want to add the number of devices listed in parenthesis before clicking a command.

- § **Network Devices.** Click this command to add connected network devices, such as routers and switches.
- § **Servers.** Click this command to to add connected servers.
- § **Workstations.** Click this command to add connected workstations.
- § **Printers.** Click this command to click this command to add connected printers.
- § **Virtual Servers.** Click this command to add connected virtual servers.
- § **Virtual Machines.** Click this command to to add connected virtual machines.
- § **Wireless LAN Controllers.** Click this command to add connected wireless LAN controllers.
- § **Wireless Access Points.** Click this command to add connected wireless access points.
- § **Devices.** Click this command to add connected devices to the map using the Select Connected Devices to Add dialog.
- § **Add Associated.** Click this command to add associated devices to the map using the following sub-menu commands.



Note: The following commands cannot be undone; ensure that you want to add the number of devices listed in parenthesis before clicking a command.

- § **Virtual Machines.** Click this command to add associated virtual machines.
- § **Wireless Access Points.** Click this command to add associated wireless access points.
- § **Devices.** Click this command to add associated devices.
- § **Set as root device.** Select a device, then right-click to view this command to make the selected device the root device for the map. The root device is the parent device, then all connected devices are assigned as children. The map layouts are based on the parent/child relationship set by the root device.
- § **Auto-select root device.** Click this command to have the root device for the map chosen automatically.
- § **Remove Up Dependencies.** Select a device, then right-click this command remove any up dependencies from the selected device. For more information, see *Dependencies overview* (on page 295).
- § **Group/Layout Settings.** Click this command to add and configure a new device group map using the Layer-2 Map Properties dialog. For more information, see *Creating Layer-2 Groups* (on page 275).

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 278).

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.

Managing devices

In This Chapter

Learning about devices.....281

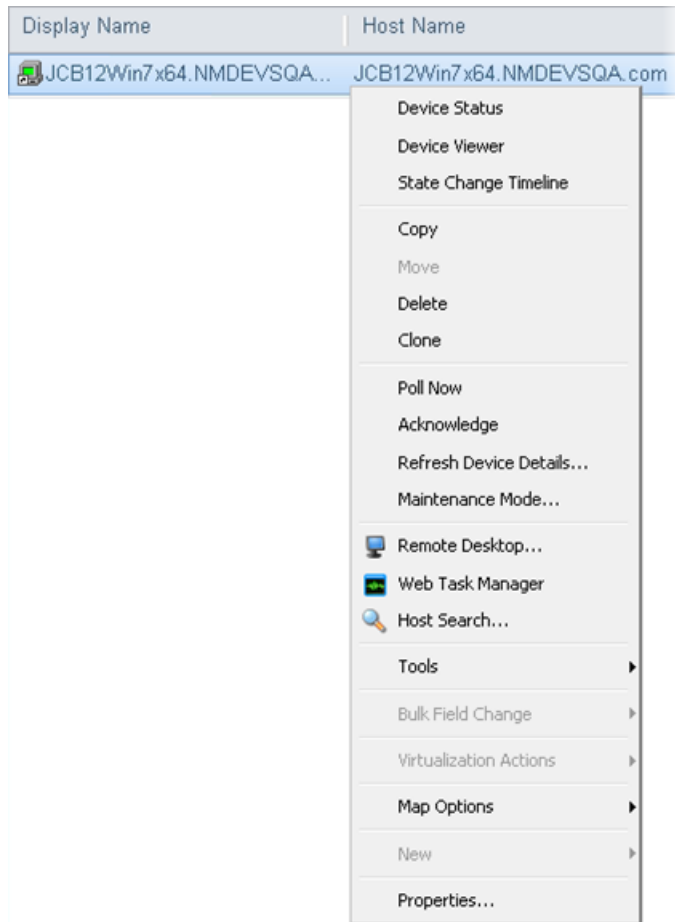
Learning about devices

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 24)
- § 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 255).

- 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 283).
- 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 **Devices** 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 **Devices** 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 **Devices** 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 **Devices** 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.

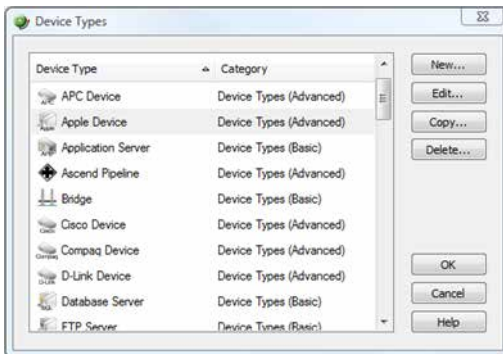
Using device types



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 240).

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.



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 or group details using layer 2:

Right-click a single device or device group, then click **Refresh Device Details** or **Refresh Group 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** or **Refresh Group 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 setup 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 289).

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 289).

Cloning a device using drag-n-drop

To clone a device using drag-and-drop:

- 1 From the WhatsUp Gold web interface, click the **Devices** 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 with 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 accomplished 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. WhatsUp Gold considers a device is down when it does not send the data back.

Tuning polling intervals

It's important to note that polling interval settings affect how WhatsUp Gold determines a specific device state. For example, if a user has specified that she only wants to poll a device every 5 minutes, WhatsUp Gold will only recognize device state changes at the 5 minute polling intervals. If a device has been down 2 minutes, it will be recognized as down when the 5 minute polling interval occurs. Corresponding Up actions will be triggered after the 5 minute poll occurs rather than when the device went down at the two minute point.

The device polling interval affects the way WhatsUp Gold determines the specific device state. When a device transitions from Up to Down, it checks to determine the last time the device was Up. For example, with the default polling interval of 60 seconds, when a device goes down it looks back and determines that the last time it was up was 63 seconds ago so it goes from "Up at least 5" to "Down." In the next polling interval when the device still returns down, WhatsUp Gold looks backward and determines that the last Up time was 125 seconds ago so it now is "Down at least 2 minutes."

If a 5 minute polling interval is set, the first time that a device returns down, WhatsUp Gold looks back and determines that the last time the device was up was 304 seconds ago so it transitions directly from "Up at least 5 minutes" to "Down at least 5 minutes" (skipping the Down and Down 2 states). Similarly, when the device comes back up, WhatsUp Gold looks back to determine the last time the device was Down and it registers that it was 301 seconds ago so it transitions directly from "Down at least 5" to "Up at least 5 minutes."

In short, if you plan to use polling intervals longer than the default of 60 seconds, we recommend that you associate actions with device states that will not be skipped because of the extended polling interval.

Changing how you poll devices

After a device is added to the database, WhatsUp Gold begins monitoring the 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 **Devices** 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



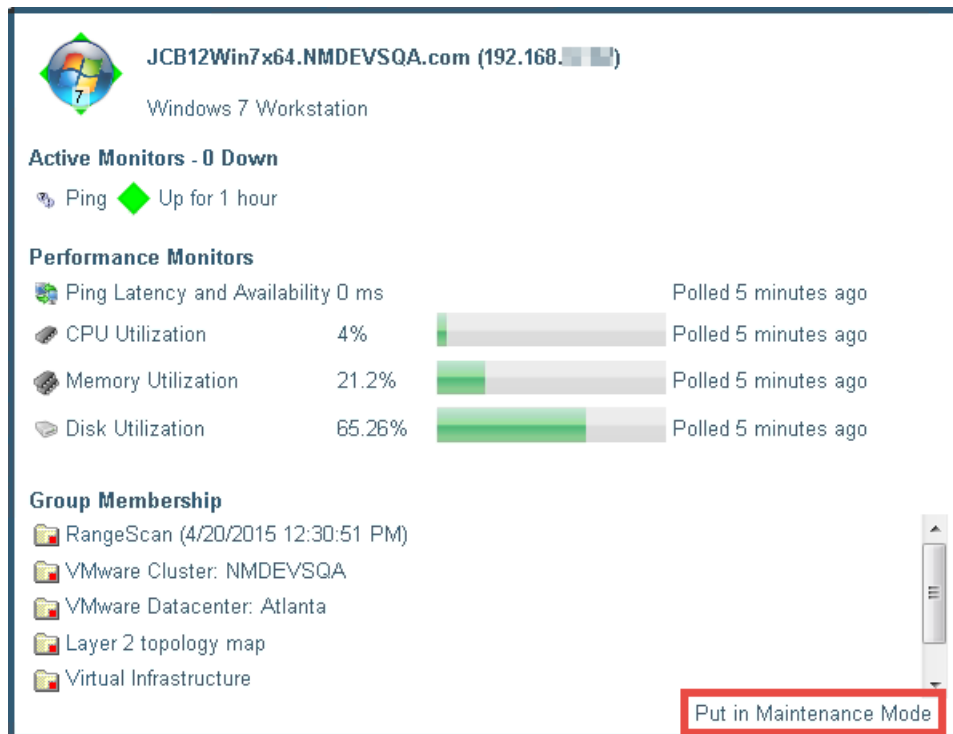
Map View

To put a device into maintenance mode:

Method 1

- 1 From the WhatsUp Gold web interface, click the Devices tab, then click Devices.
- 2 In the Details View or Map View, hover over a device to view the device details pop-up dialog.

3 Click **Put in Maintenance Mode**.



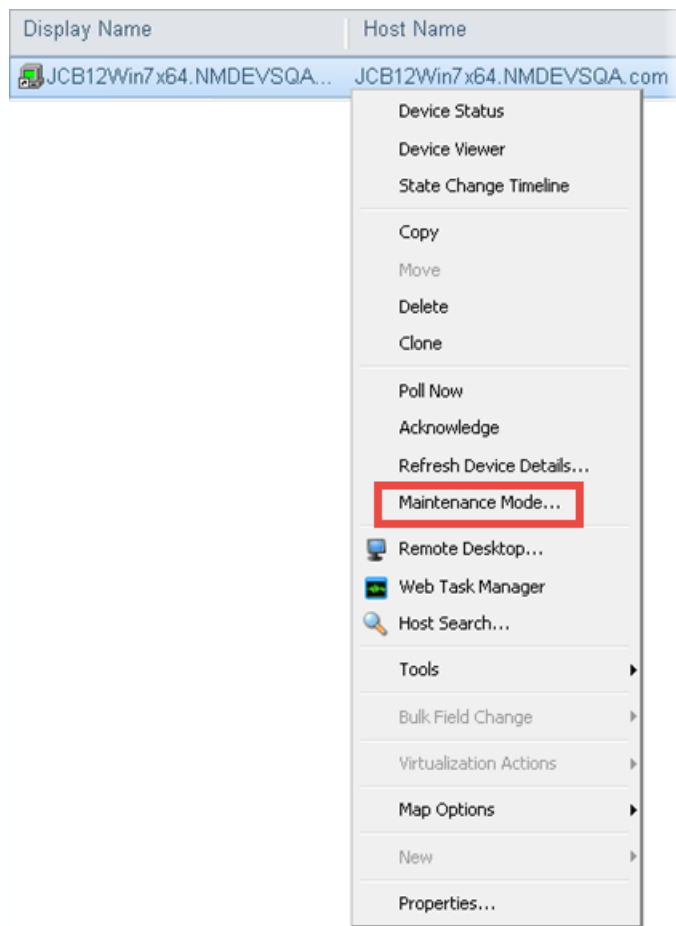
4 Ensure **Force (Device Name) into maintenance mode now** is enabled.

5 Click **OK**.

Method 2

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

- 2 In the Details View or Map View, right-click a device, then click **Maintenance Mode**.

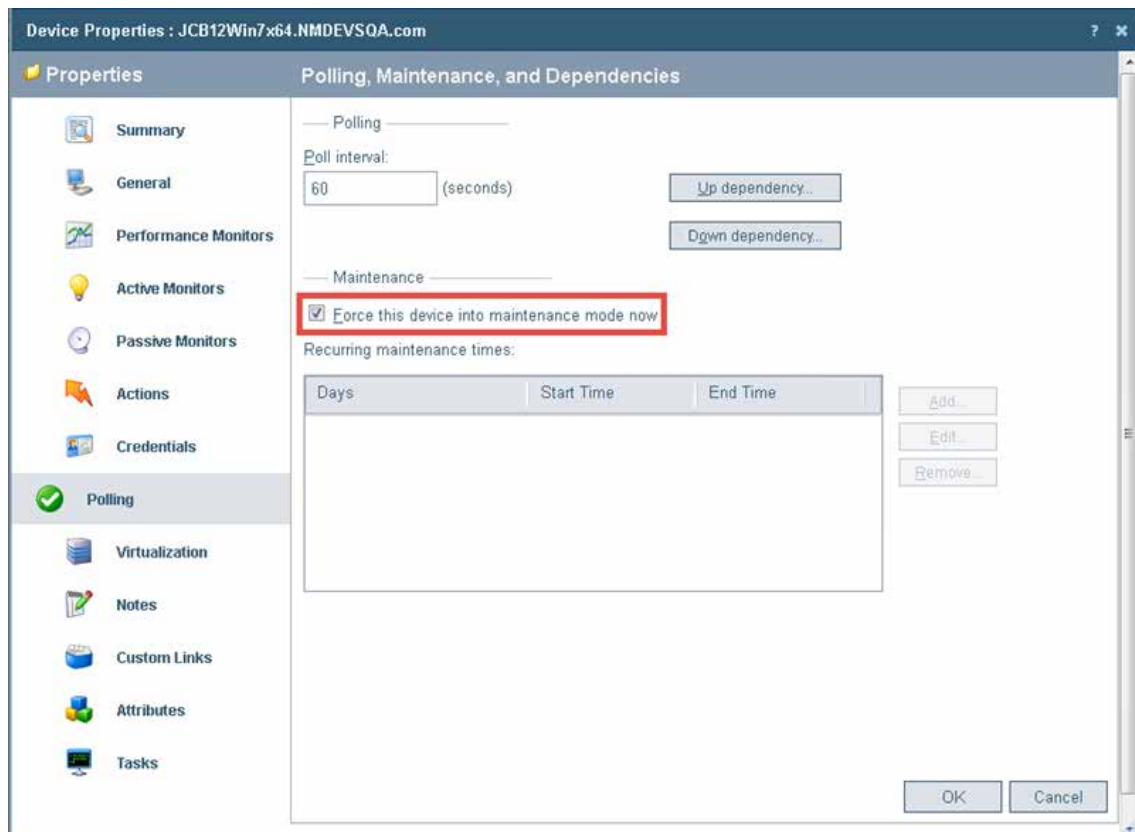


- 3 Ensure **Force Device into maintenance mode now** is enabled.
- 4 Click **OK**.

Method 3

- 1 From the WhatsUp Gold web interface, click the Devices 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 Select the **Polling** tab.



- 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 for each device.

To change the polling frequency for a device:

- 1 From the WhatsUp Gold web interface, click the **Devices** 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 **Devices** 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.

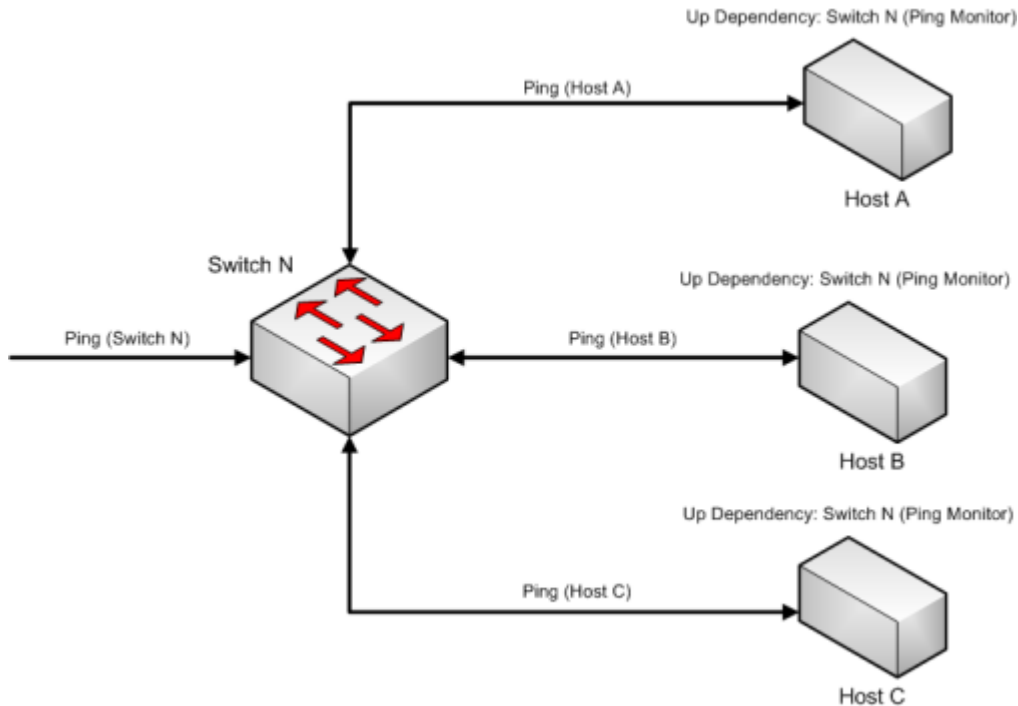
Up Dependencies

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.



Down Dependencies



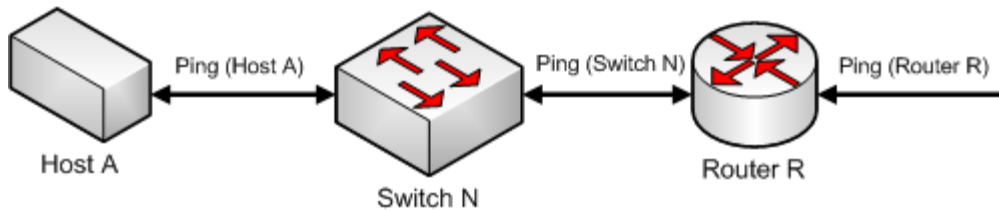
Important: If you use the APM plug-in and have APM components that include WhatsUp Gold devices with dependencies, be aware that APM components honor both WhatsUp Gold Unknown and Maintenance device states as Unknown states. Therefore, if a WhatsUp Gold device goes into an Unknown or Maintenance state, the APM component will change to an Unknown state. For more information about how device states roll up from individual APM component status to the overall APM instance state, see [Learning about APM component's instance state precedence](#).

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.

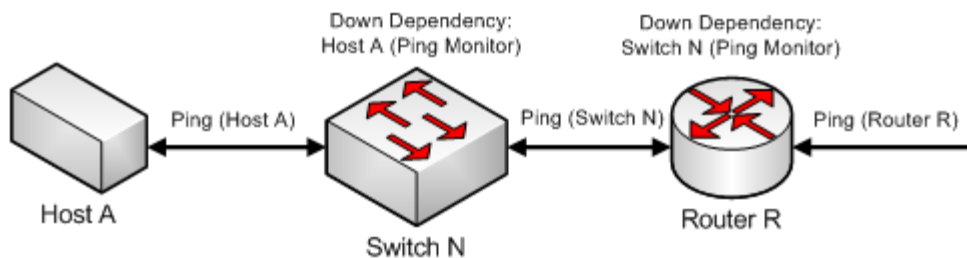
Example

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.



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.

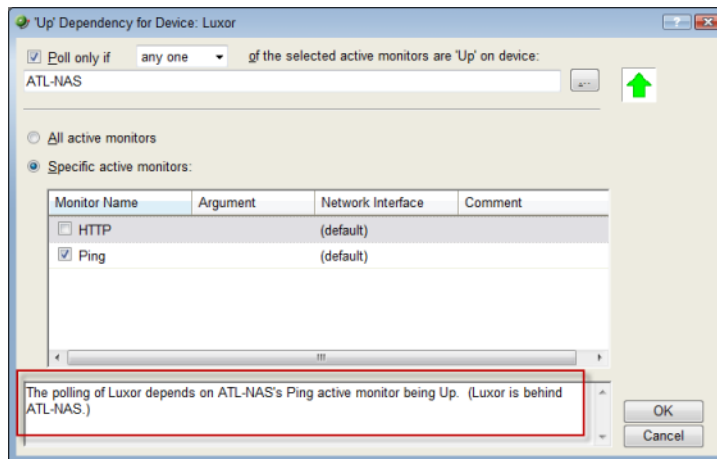
This condition occurs when the dependent device is in an inactive state, and is able to respond to an echo request from a ping of the device. Because of the down dependency, the dependent device is not being polled and is "assumed up", yet the actual state of the monitored service or process is unknown,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

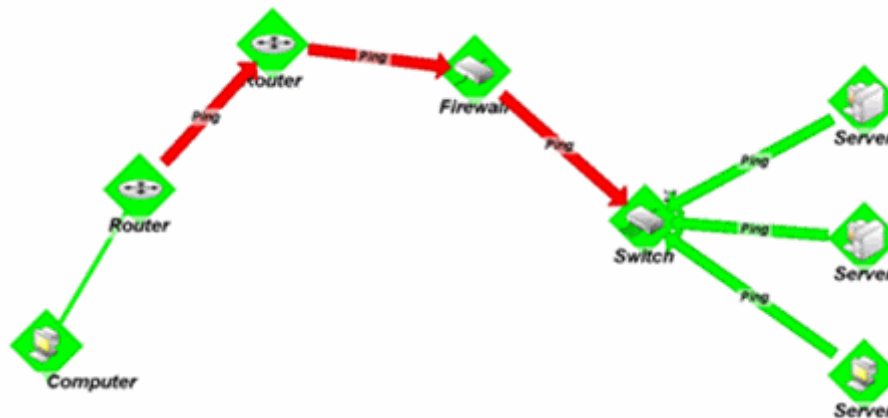
Reading dependencies

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.



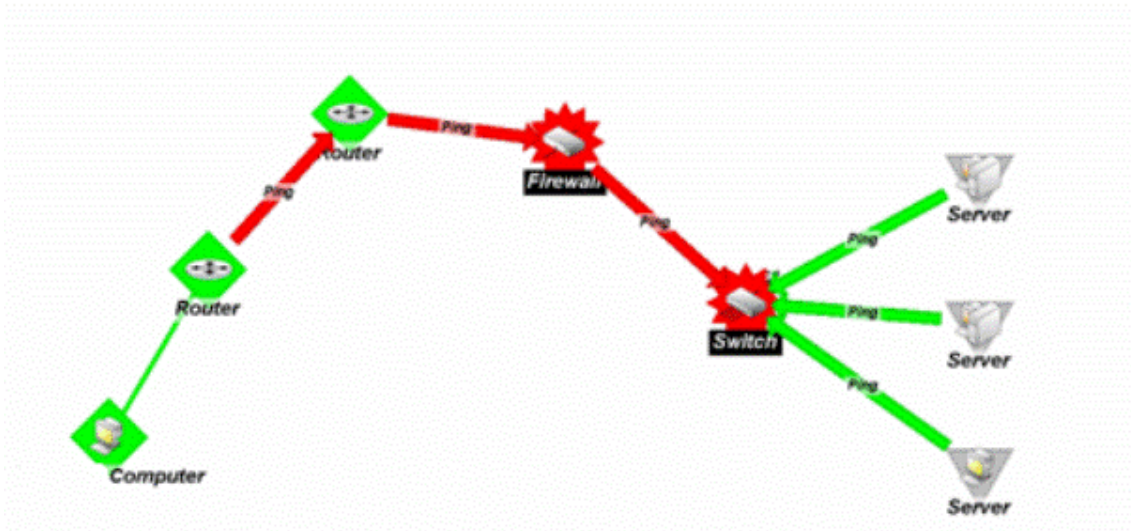
- 2 Read the dependency arrows in the Map View.



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.



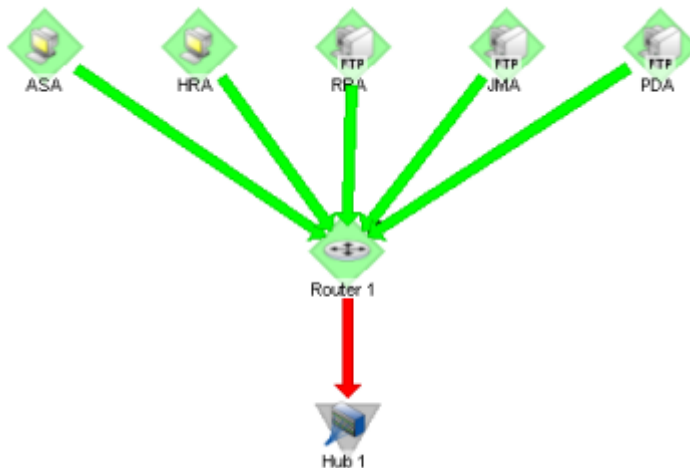
Note: You cannot set a dependency across groups. However, you can make shortcuts to the devices you want to set a dependency on in a group, then set the dependency to the shortcut.



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

Viewing Dependencies

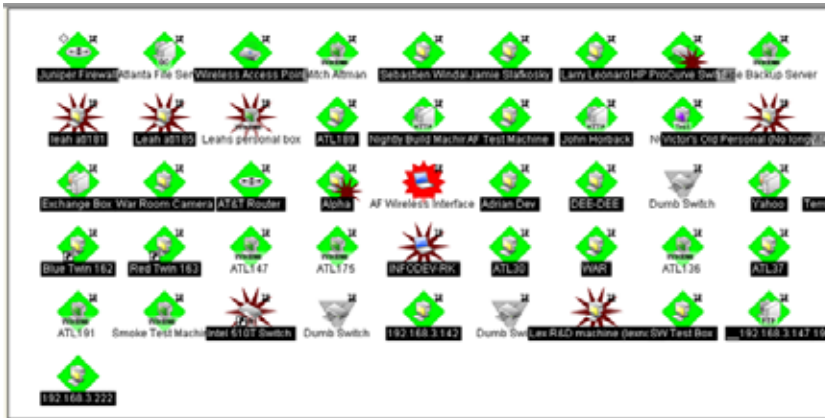
After you have set up your dependencies, you can view dependency lines in the Map view, as long as the devices appear in the same group. If the devices are not in the same group, you can refer to the Polling, Maintenance, and Dependencies dialog (**Device Properties > Polling**) to view the dependencies.



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 Acknowledgments

When a device state changes, regardless of any action that has been placed on the device, WhatsUp Gold uses the Acknowledgment 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 Acknowledgment 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 **Devices** 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 **Devices** 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.

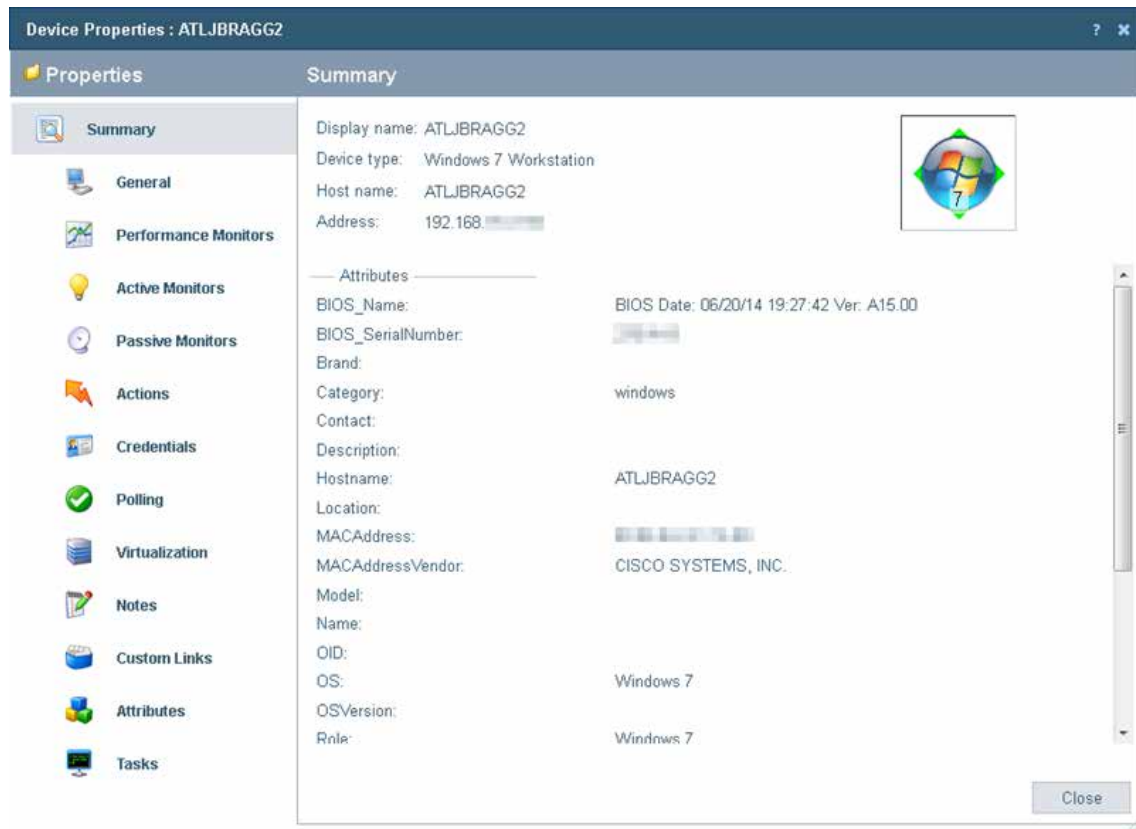
Using Device Properties

In This Chapter

Working with Device Properties	305
Using Device Properties - Summary.....	306
Using Device Properties - General	307
Device Properties - Performance Monitors.....	307
Using Device Properties - Active Monitors	308
Using Device Properties - Passive Monitors	309
Using Device Properties - Actions.....	309
Using Device Properties - Credentials.....	310
Using Device Properties - Polling	310
Using Device Properties - Virtualization.....	311
Using Device Properties - Notes	313
Using Device Properties - Custom Links	313
Using Device Properties - Attributes.....	313
Using the DeviceIdentifier attribute	314
Using Device Property - Menu.....	314
Using WhatsConfigured Device Properties - Tasks.....	315
Using Device Properties - Wireless	316

Working with Device Properties

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



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 451).



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 452), 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 343).



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 341).

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 436).

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 611).

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 267).

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 290) and *Dependencies overview* (on page 295).

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* (on page 48).

- § 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 Devicelidentifier attribute

When a Beeper Action fires, it looks for and returns a device attribute called `Devicelidentifier`. You can add this attribute to a device via its Properties (**Device Properties > Attributes**).

If the Beeper Action does not find the `Devicelidentifier` 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 Devicelidentifier 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 `Devicelidentifier`.
- 4 In **Attribute value**, enter the desired numeric value.



Note: The `Devicelidentifier` 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 - Menu

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 649) 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 317)
- § *Traceroute Tool* (on page 318)
- § *Lookup Tool* (on page 318)
- § Telnet Tool

The following tools help you identify information about MIB objects that network devices support:

- § *SNMP MIB Walker Tool* (on page 319)
- § *SNMP MIB File Explorer Tool* (on page 323)

The following tools help you identify problems with network devices so you can take corrective action to resolve issues:

- § *MAC Address Tool* (on page 324)
- § Diagnostic Tool
- § *Web Performance Monitor* (on page 326)
- § *Web Task Manager* (on page 328)

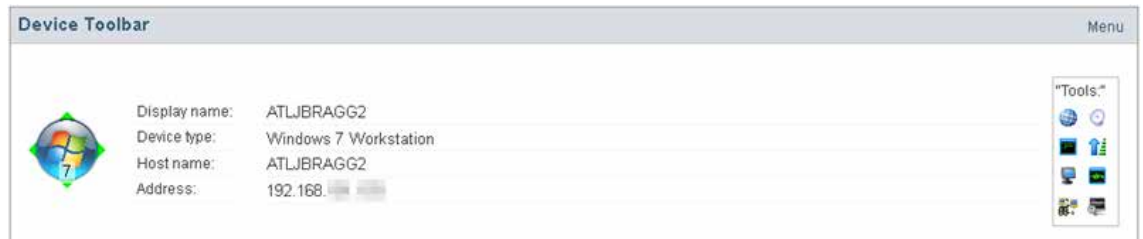


Note: The Web Performance Monitor and Web Task Manager tools are not available in WhatsUp Gold Standard Edition.

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.



- 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 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:

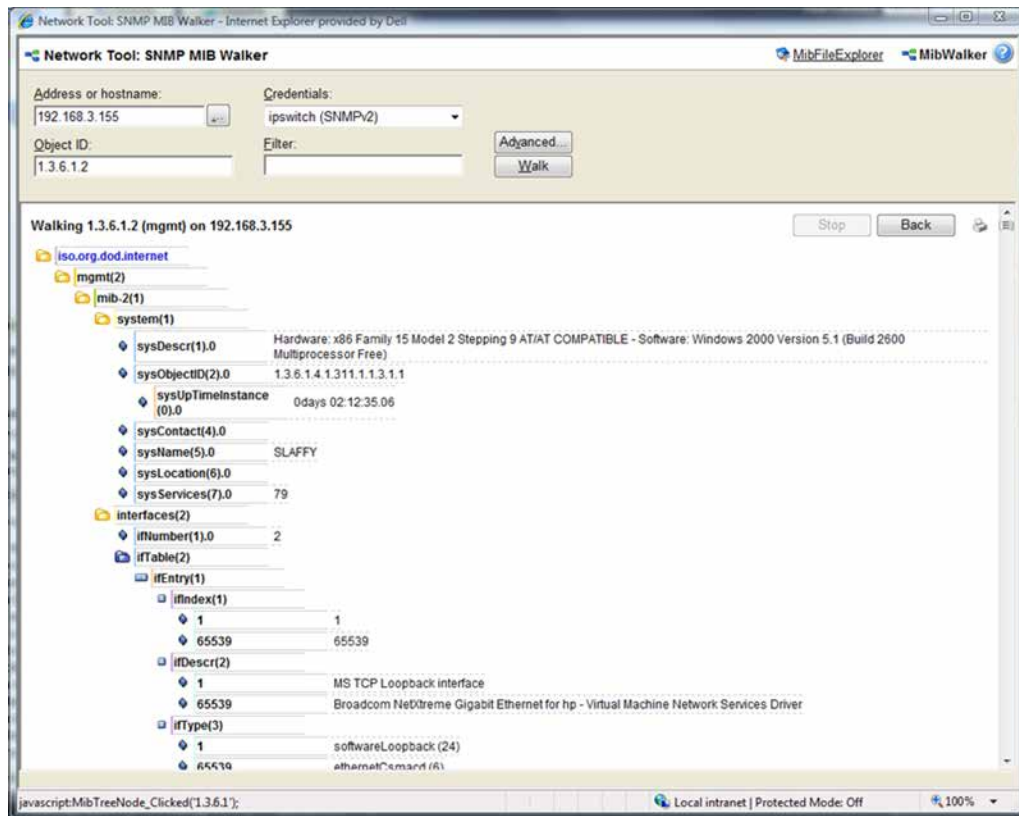
- § **Address or hostname.** Enter an IP address hostname for the device.
- § **Credentials.** Select the appropriate credentials for the device from the list. For more information, see *Using Credentials* (on page 267).
- § **Object ID.** Enter the numeric or label ID for the object for which you want 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 364).

- § 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.

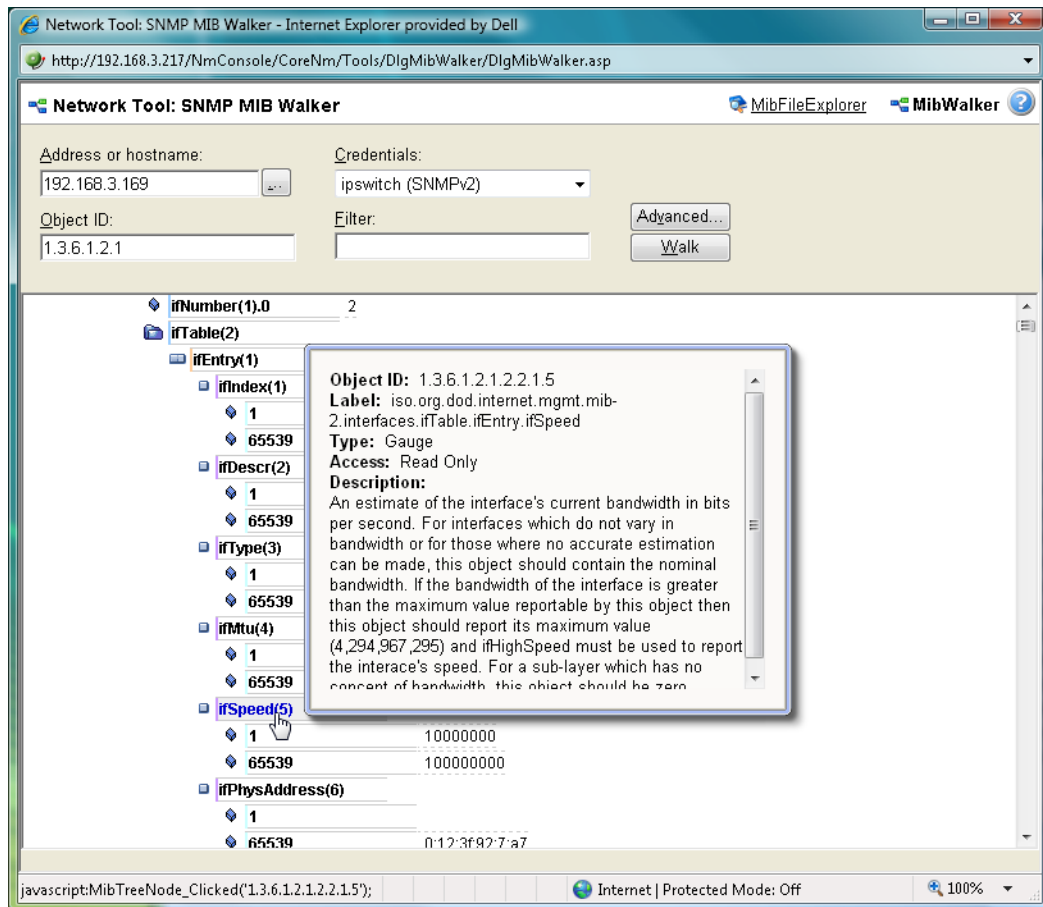
- 2 After you have entered all of the information, click **Walk** to perform the search. The SNMP MIB Walker returns a list of SNMP objects that are available on the selected device.



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 480).

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.



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 Performance 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:

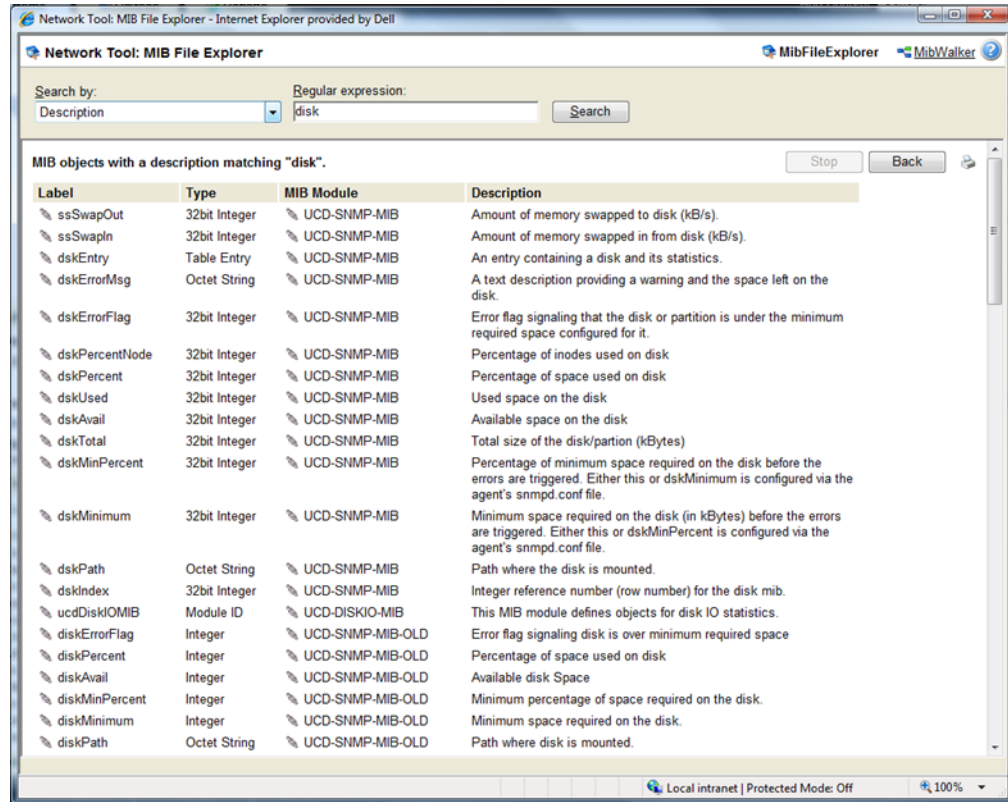
Select a module from the **MIB Module** list, then click **Display**.

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 364). After entering the description in the box, click **Find**.



- § 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 480).



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.



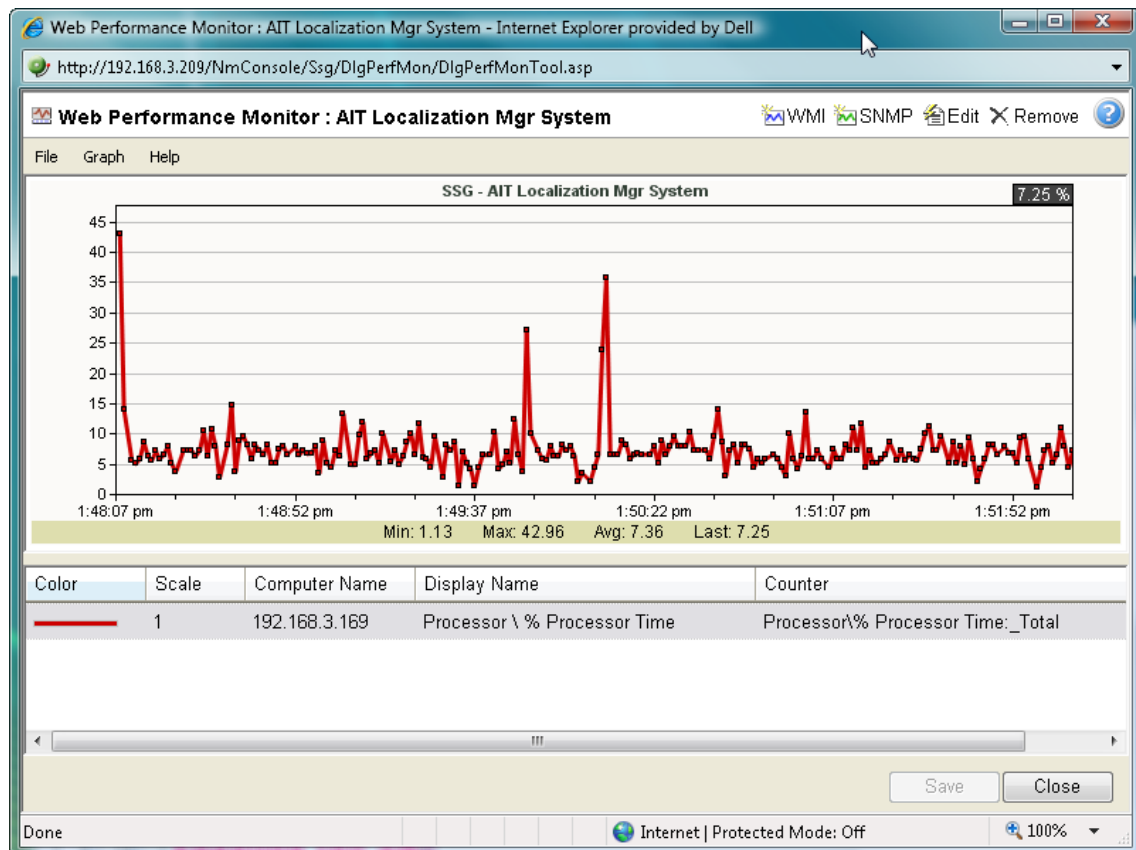
Note:: WhatsUp Gold allows you to search for MAC addresses within your network, but since Layer 2 MAC address information is only visible to local networks, only local networks can be probed for MAC address information. Therefore, only the local networks to which the WhatsUp Gold computer is connected 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.



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.

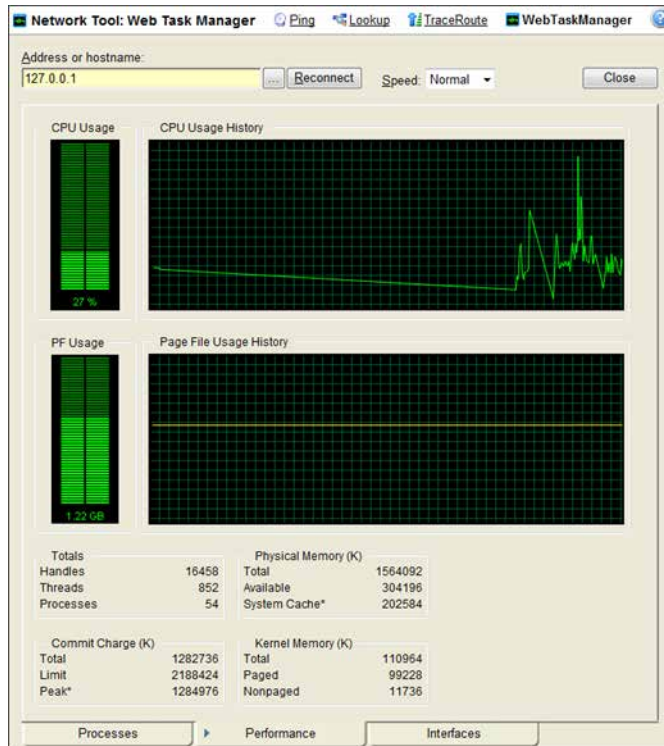
Button	Function
 WMI	Opens the Add WMI Performance Counter dialog.
 SNMP	Opens the Add SNMP Performance Counter dialog.
 Edit	Opens the appropriate dialog for editing the selected WMI or SNMP performance counter.
 Remove	Removes the selected graph item from the list and graph.
	Opens the help topic for the Web Performance Monitor

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 972).

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.



There are three tabs that provide device information:

- § **Processes** (on page 331). 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 333). 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 336). 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 330) 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 972).



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.

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
ccExtMgr.exe	SYSTEM	0	3,580 K	4,116 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**).

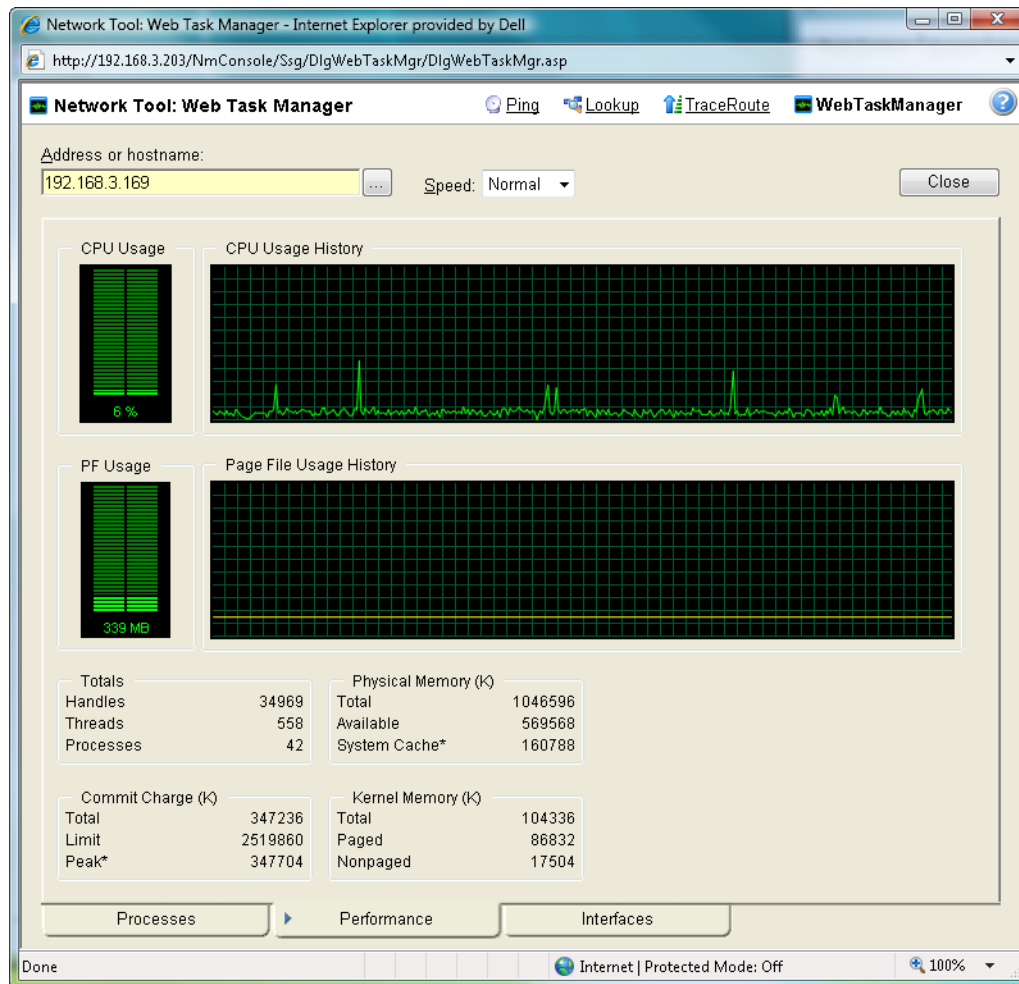
For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 972).



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.



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 330) 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**).
- 5 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 972).

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.

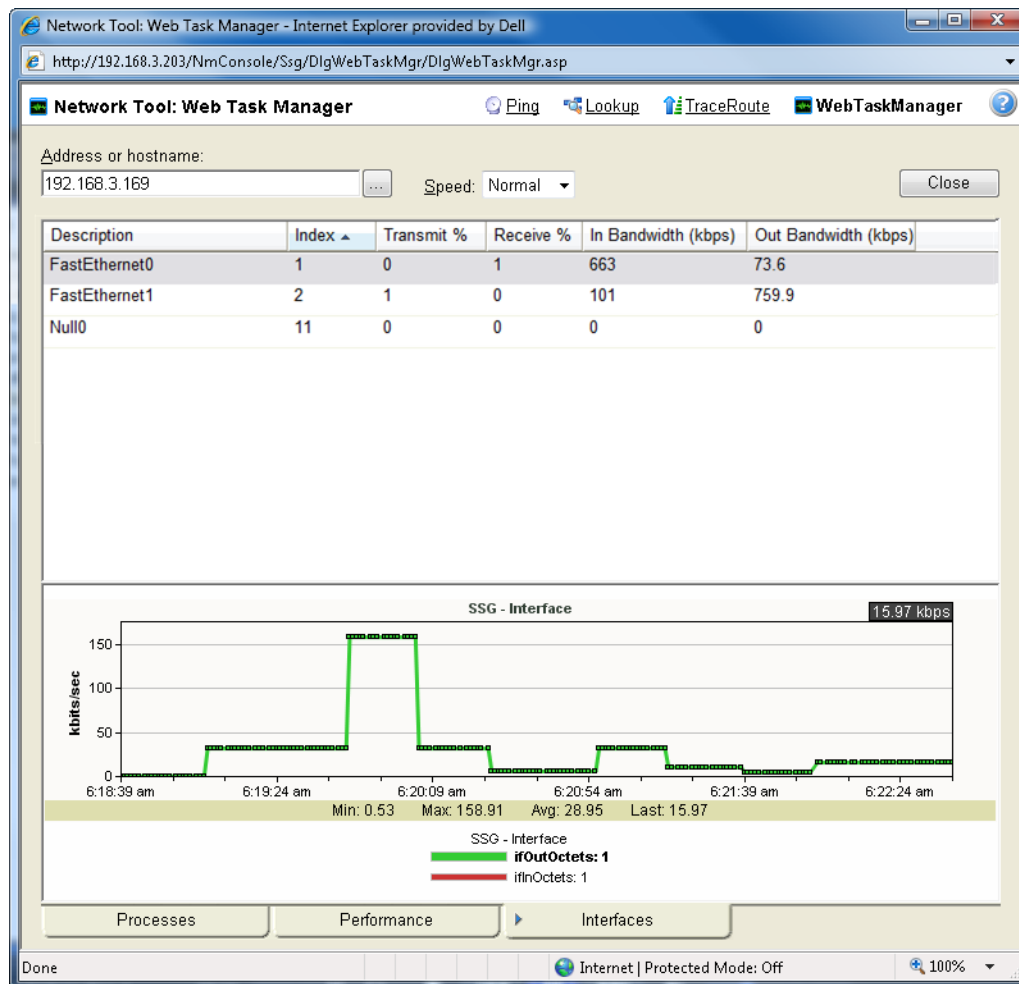
The following information are examples of the information that is provided when you connect to and view a SNMP enabled device. Note, this information varies by operating system:

- § **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 972).

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.



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 330) 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**).
- 5 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 972).

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 boxes.
 - § **IP Address.** Enter the IP address of a device for which you want to find sightings on the network. Leave this box 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 box 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 Chapter

Using Active Monitors	341
Using Passive Monitors.....	436
Using Performance Monitors	451
Enabling global performance monitors.....	475
Creating custom performance monitors.....	480
Using the Active Script Performance Monitor.....	496

Using Active Monitors

In This Chapter

Active Monitors overview	341
About the Active Monitor Library	341
Selecting an Active Monitor Type	342
Configuring Active Monitors	343
Using Premium active monitors	368

Active Monitors overview

Active monitors poll target devices for important information such as ping accessibility, device services, device files and folders, 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 various 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 343).

In addition to configuring relevant monitors, you must assign monitors to the devices you want to monitor. For more information, see *Assigning active monitors* (on page 430).

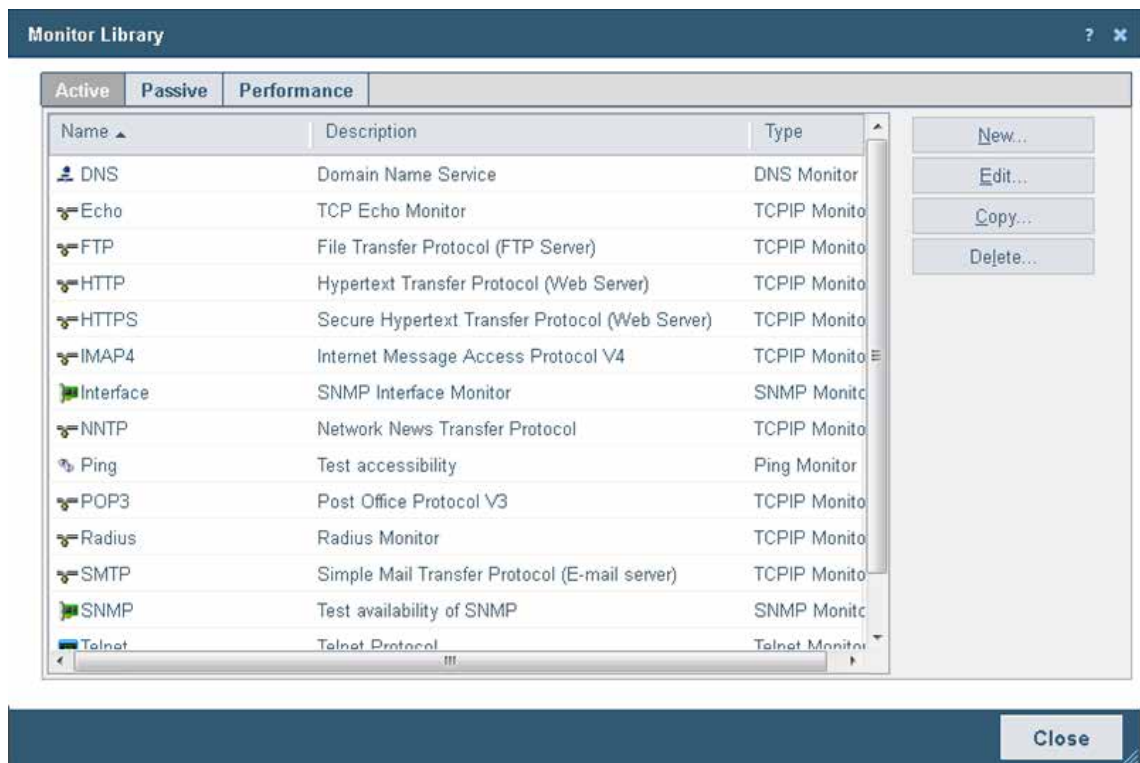
About the Active Monitor Library

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.



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 343)
- § *APC UPS Monitor* (on page 369)
- § *DNS Monitor* (on page 345)
- § *Email Monitor* (on page 372)
- § *Exchange 2003 Monitor* (on page 377)
- § *Exchange Monitor* (on page 381)
- § *Fan Monitor* (on page 385)

- § File Properties Monitor
- § Folder Monitor
- § *FTP Monitor* (on page 392)
- § *HTTP Content* (on page 395)
- § *Network Statistics Monitor* (on page 400)
- § *NT Service Monitor* (on page 346)
- § *Ping Monitor* (on page 348)
- § *Power Supply Monitor*
- § PowerShell Monitor
- § *Printer Monitor*
- § *Process Monitor* (on page 409)
- § *SNMP Monitor* (on page 350)
- § *SQL Query Monitor* (on page 413)
- § *SQL Server 2000 Monitor* (on page 418)
- § SSH Monitor
- § *TCP/IP Monitor* (on page 356)
- § *Telnet Monitor* (on page 355)
- § *Temperature Monitor* (on page 422)
- § *VoIP Monitor (available with the VoIP Monitor plug-in)* (on page 423)
- § *WAP Radio Monitor* (on page 367)
- § *WMI Formatted Monitor* (on page 424)
- § *WMI Monitor* (on page 426)

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 920).

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 SMTP server. 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.
 - § **Use the Direct Data Access execution model**. Select this option to use the Active Script Monitor execution model that was available prior to the WhatsUp Gold 16.2 SP3 release. This option may be more susceptible to Active Script monitor script errors; however, it allows you to use the `Context.GetDB` context object in scripts for direct interaction with the WhatsUp Gold database.
 - § **Use the Isolated Process execution model**. Select this option to use the Active Script Monitor execution model that became available in the WhatsUp Gold 16.2 SP3 release. This option may be less susceptible to Active Script monitor script errors, therefore providing more protection and stability for the WhatsUp Gold poller engine (nmsservice.exe); however, it DOES NOT allow you to use the `Context.GetDB` context object in scripts for direct interaction with the WhatsUp Gold database.
 - § **Script text**. Enter your monitor code in this box.
- 6 Click **OK** to save changes.
- 7 After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 430).

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 SMTP server. 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 in this box.
- 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 SMTP server. 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 430).

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 SMTP server. 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 a Service Monitor

The 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 Service Monitor to work properly. Windows 2000 Service Pack 2 or higher, XP, and 2003 and later 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 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 **Service Monitor**, then click **OK**. The 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 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 430).

To edit an existing 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 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 973)?

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 SMTP server. 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 430).

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 SMTP server. 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 430).

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 430).

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 920).

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. You can either embed the script in the monitor or place a script file on the remote machine (making sure it's executable) and enter a command in the monitor to run the script. The success or failure of the monitor is dependent 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. The command or script must return a string 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.

- § **Line end character.** Select the appropriate character type; either *None*, *Linefeed*, *Carriage return*, or *Carriage return linefeed*. Multiline scripts are entered and persisted on a Windows operating system, and include line-ending characters that may not be recognized on the target device. This configuration feature instructs WhatsUp Gold to replace the line-ending characters with the selected characters prior to connection and command execution.
 - § **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, make sure that the output contains the 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 apply the target string as a regular expression as it searches the output from the command and considers the match criteria (contains, does not contain). If unchecked, the target string is evaluated as simple text.
 - § **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, 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 430).

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. The command or script must return a string 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.

- § **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, make sure that the output contains the 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 apply the target string as a regular expression as it searches the output from the command and considers the match criteria (contains, does not contain). If unchecked, the target string is evaluated as simple text.
 - § **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, 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 SMTP server. 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 430).

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 SMTP server. 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 lmail 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 **TCPIP 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 SMTP server. 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 360)
- 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 430).

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 SMTP server. 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 360).
- 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 the commands to send to the service and the 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.

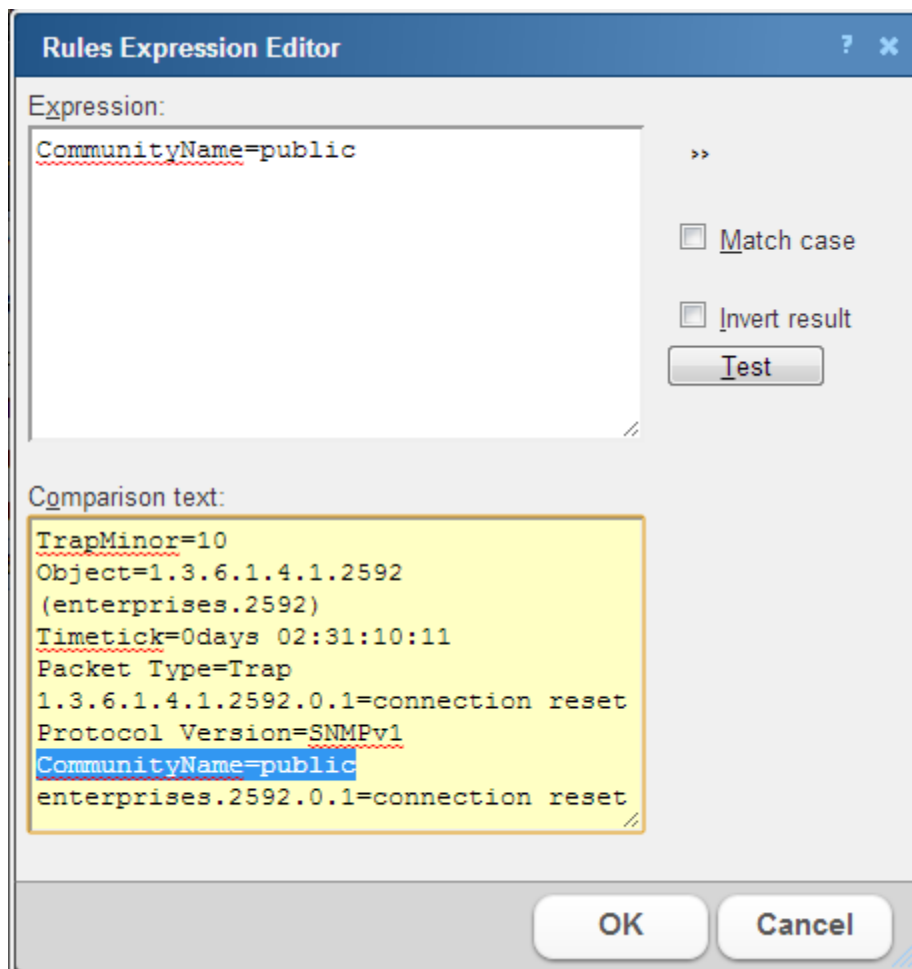
§ Enter an expression in the **Expression** box. Use the **>>**, **Match case**, and **Invert result** options to the right of the **Expression** box to help build the expression.

§ 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.

For example:





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 361)= keyword.
- § To expect a string from a port, use the `SimpleExpect` (on page 360)= or the `Expect` (on page 360)= keyword.
- § To receive a conditional response for an error or success, use *Flow Control Keywords* (on page 363).

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 360) 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 364) 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
<code>\\x##</code>	Binary value in Hexadecimal. For example, <code>\\x1B</code> is escape
<code>\\</code>	The "\" character
<code>\\t</code>	The tab character (<code>\\x09</code>)
<code>\\r</code>	The return character (<code>\\x0D</code>)
<code>\\n</code>	The new line character <code>\\x0A</code>)

WhatsUp Gold versions 7 and 8 users: The `%###` decimal syntax for specifying binary octets has been replaced with the `\\x##` hexadecimal 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 360) 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
<code>.</code> 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: colour?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: <code>^[45]</code> will only match input that begins with "4" or "5"
<code>\$</code> dollar	At the end of a regular expression, this character matches the end of the input. Example: <code>>\$</code> matches a ">" at the end of the input.

Other

Meta-character	Matches
<code> </code> alternation	Matches either expression it separates. Example: <code>H Cat</code> matches either "Hat" or "Cat"
<code>(...)</code> parentheses	Provides grouping for quantifiers, limits scope of alternation via precedence. Example: <code>(abc)*</code> matches 0 or more occurrences of the the string <code>abc</code> Example: <code>WhatsUp (Gold) (Professional)</code> matches "WhatsUp Gold" or "WhatsUp Professional"
<code>\0, \1, ...</code> backreference	Matches text previously matched within first, second, etc, match group (starting at 0). Example: <code><{head}>.*?</\0></code> matches " <code><head>xxx</head></code> ".
<code>!</code> negation	The expression following <code>!</code> does not match the input Example: <code>a!b</code> matches "a" not followed by "b".

Abbreviations

Abbreviations are shorthand Meta-characters.

Abbreviation	Matches
<code>\a</code>	Any alphanumeric character: <code>([a-zA-Z0-9])</code>
<code>\b</code>	White space (blank): <code>([\t])</code>
<code>\c</code>	Any alphabetic character: <code>([a-zA-Z])</code>
<code>\d</code>	Any decimal digit: <code>[0-9]</code>
<code>\D</code>	Any non decimal digit: <code>[^0-9]</code>
<code>\h</code>	Any hexadecimal digit: <code>([0-9a-fA-F])</code>
<code>\n</code>	Newline: <code>(\r (\r?\n))</code>
<code>\p</code>	Any punctuation character: <code>.,/\';"!@#\$\$%^&*(){}- _=+ <>!\~</code>
<code>\P</code>	Any non-punctuation character
<code>\q</code>	A quoted string: <code>(\"[^\"]*" '[^']*')</code>
<code>\s</code>	WhatsUp Gold style white space character: <code>[\t\n\r\f\v]</code>
<code>\S</code>	WhatsUp Gold style non-white space character: <code>[^ \t\n\r\f\v]</code>
<code>\w</code>	Any word characters (letters and digits): <code>([a-zA-Z0-9_])</code>
<code>\W</code>	Non-word character: <code>([^a-zA-Z0-9_])</code>
<code>\z</code>	An integer: <code>([0-9]+)</code>

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 356) 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 430).

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 430).

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 430).

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.

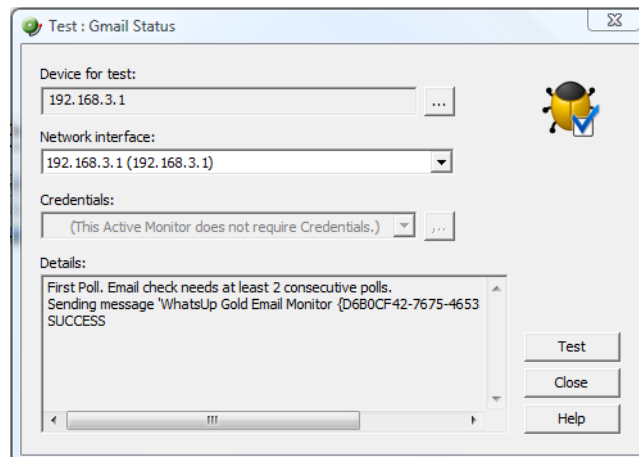
To create an Email monitor for a Gmail account:

- 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.

The screenshot shows the 'Add Email Monitor' dialog box. The 'Name' field is filled with 'Gmail Status'. The 'Description' field is filled with 'Checks Gmail status'. The 'Outgoing Mail' section is expanded, showing 'SMTP server' as 'smtp.gmail.com', 'Port' as '587', 'Mail to: (Email address)' as 'youraccount@gmail.com', and 'Mail from: (Email address)' as 'youraccount@gmail.com'. The 'Incoming Mail' section is also expanded, showing 'Mail server' as 'pop.gmail.com', 'Account type' as 'POP3', 'Username' as 'youraccount@gmail.com', and 'Password' as a masked field. At the bottom, there are three buttons: 'Advanced', 'OK', and 'Cancel'.

- 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**.



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 see the email sent by WhatsUp Gold via the Email Monitor.

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 378) to monitor.
- 2 Determine which *Exchange 2003 services* (on page 378) 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 377) 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 430).

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 613).
- 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 2010, 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 382) to monitor.
- 2 Determine which *Exchange services* (on page 382) 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 381) 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 2010, 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 430).

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 (<code>MSExchangeServiceHost</code>). 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 (<code>MSExchangeTransport</code>). 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 (<code>MSExchangeTransportLogSearch</code>). Provides message tracking and transport log searching. This service has no dependencies.
Speech Engine Service	Monitor the Speech Engine service (<code>MSSpeechService</code>). Provides speech processing services for Unified Messaging. This service is dependent upon the Windows Management Instrumentation service.
Unified Messaging	Monitor the Unified Messaging service (<code>MSExchangeUM</code>). 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), 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 430).

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. The File Properties active monitor supports %variables (%Device.Address or %Device.HostName), allowing you to use a macro for applying multiple devices to a monitor.



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**. 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 for a file on a single device.
If you provide the value for File size, File checksum using, or File modified within options, you can also use percent variables for the path of the file to monitor. For example, \\%Device.Address\website\product\index.htm or

\\%Device.HostName\website\product\index.htm for a file located on multiple machines with the same file path name.



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.
- § **File was last modified (exactly on | before | after).** (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, select the list option date of **exactly on | before | after**, then click the calendar icon 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.



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.

- § **File ____ modified within ____ before polling time.** Select this option to monitor whether the the date of the file changes withing a specific interval before polling time. Note that the expectation is that the monitor is up, so be sure the set your parameters with this in mind.
- 7** Click **OK** to save changes.
- 8** After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 430).

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.** 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 for a file on a single device.
If you provide the value for File size, File checksum using, or File modified within options, you can also use percent variables for the path of the file to monitor. For example, \\%Device.Address\website\product\index.htm or \\%Device.HostName\website\product\index.htm for a file located on multiple machines with the same file path name.



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.
File was last modified (exactly on | before | after). (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, select the list option date of **exactly on | before | after**, then click the calendar icon 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.



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.

- § **File ____ modified within ____ before polling time.** Select this option to monitor whether the the date of the file changes withing a specific interval before polling time. Note that the expectation is that the monitor is up, so be sure the set your parameters with this in mind.
- 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. The Folder active monitor supports %variables (%Device.Address or %Device.HostName), allowing you to use a macro for applying multiple devices to a monitor.



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.** The Universal Naming Convention (UNC) path that WhatsUp Gold uses to access the folder. For example:
\\192.168.3.1\website\product for a folder on a single device.
If you provide the value for File size, File checksum using, or File modified within options, you can also use percent variables for the path of the folder to monitor. For example, \\%Device.Address\website\product or
\\%Device.HostName\website\product for a folder located on multiple machines with the same folder path name.
 - § **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 430).

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**. The Universal Naming Convention (UNC) path that WhatsUp Gold uses to access the folder. For example:
\\192.168.3.1\website\product for a folder on a single device.
If you provide the value for File size, File checksum using, or File modified within options, you can also use percent variables for the path of the folder to monitor. For example, \\%Device.Address\website\product or \\%Device.HostName\website\product for a folder located on multiple machines with the same folder path name.
 - § **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 SMTP server. 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 430).

To edit an existing 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 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 SMTP server. 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 SMTP server. 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 430).

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 SMTP server. 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/rmconsole/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 SMTP server. 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 616).
 - 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 430).

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 431).

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 404).



Important: WhatsUp Gold uses a 32-bit (i.e. x86) PowerShell engine. Therefore, only 32-bit PowerShell snap-ins are supported and 64-bit only snap-ins will not function properly. Snap-ins usable in both 32-bit and 64-bit operating systems are configured for 64-bit systems by default and must be manually configured for 32-bit PowerShell engine to function properly with WhatsUp Gold.



If you are using *additional pollers* (on page 35) with WhatsUp Gold, PowerShell must be installed and any desired snap-ins must be registered identically on all poller machines for any PowerShell performance monitors, active monitors, and actions to function properly. Associated errors resulting from failed monitors will appear in the *WhatsUp Gold Status Center* (on page 20). Errors resulting from failed actions will appear in the WhatsUp Gold Event Viewer.



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 SMTP server. 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.

- § **Run under device credentials.** Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see Using the Credentials Library.
 - § **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 430).

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 SMTP server. 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.

- § **Run under device credentials.** Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see Using the Credentials Library.
 - § **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
- § Address
- § 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 430).

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 on 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 430).

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.

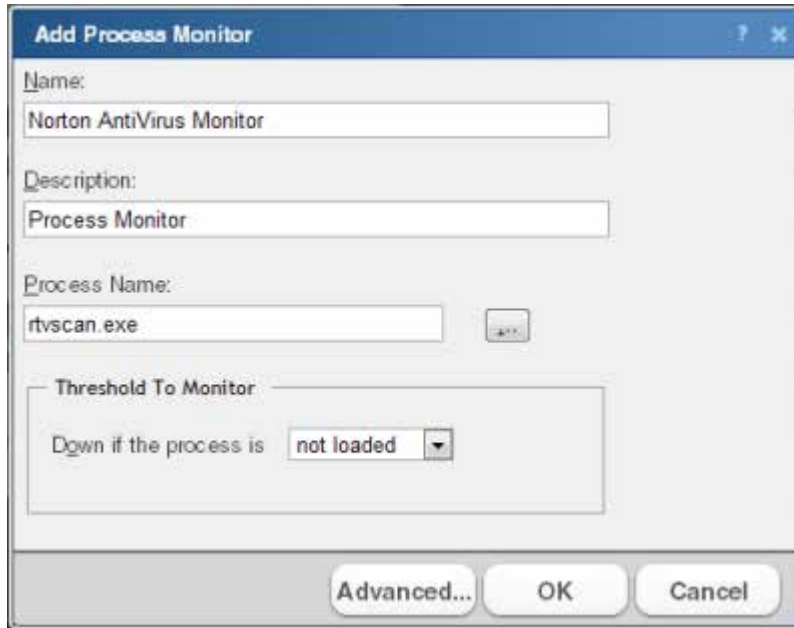
Example: Using the Process Monitor to check for antivirus software

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.



- 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 431).

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.

- 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 420).
- 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 430).

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 420).
- 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 613).



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 430).

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 Opinion 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 430).

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 430).

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 430).

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 973)?

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 613).

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 267).

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 653) 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.

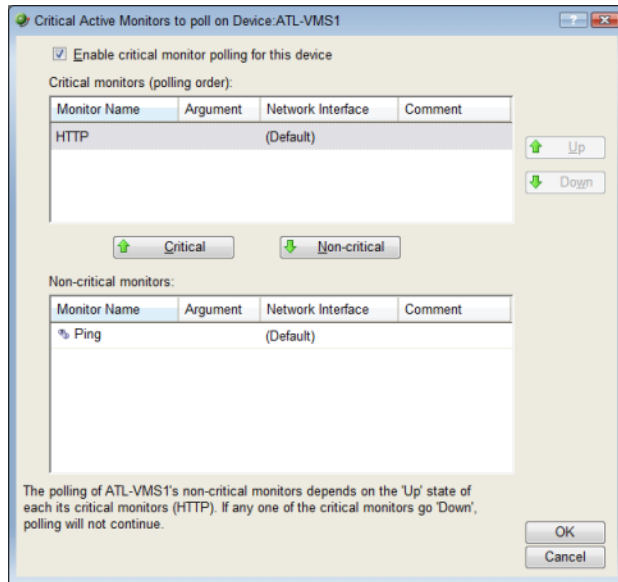
When critical monitoring is enabled, and you specify a critical polling order, you now receive only one alert when a device loses its network connectivity.



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 308) dialog.



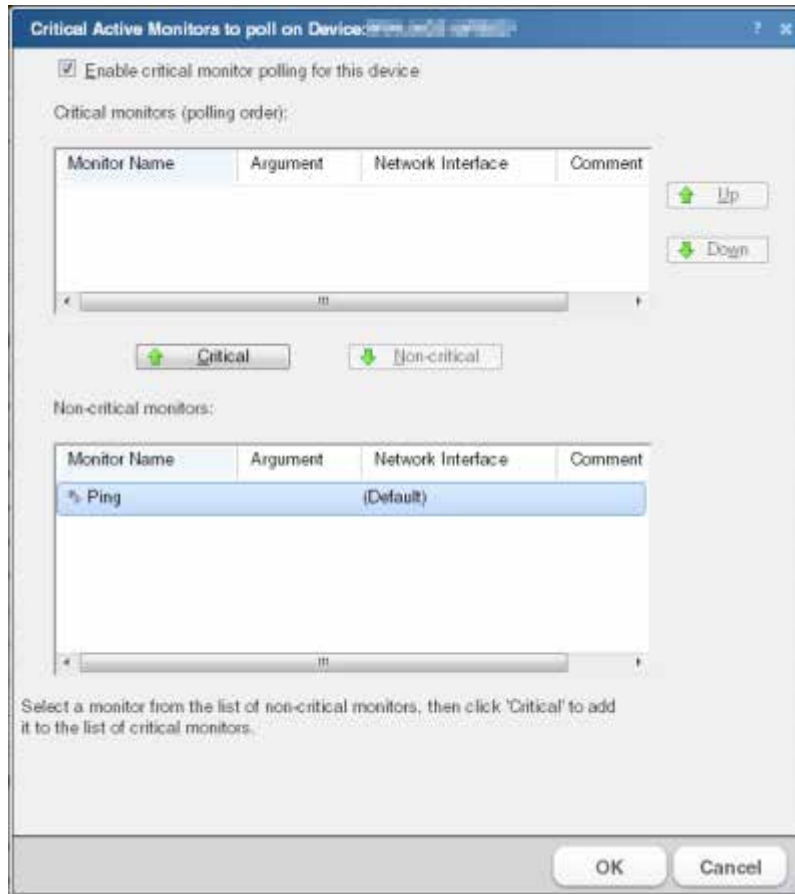
Note: Independent poll frequency for all monitors is ignored when a monitor is specified as critical.

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.



- 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

Using Passive Monitors

In This Chapter

Passive monitors overview	436
Passive Monitor Icon	437
Using the Passive Monitor Library	438
Understanding Passive Monitor Listeners.....	439
Configuring passive monitors.....	443
Assigning passive monitors	448
Group and device passive monitor reports	449

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 Authentication Failure 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.

- § The SNMP Trap monitor listens for any (all) or specific SNMP traps. SNMP traps enable an SNMP device agent to notify on significant events through unsolicited SNMP messages, or traps. For more information, see *Cisco's Understanding SNMP Traps* (<http://www.whatsupgold.com/CiscoSNMPTraps>).
- § The Windows Event Log monitor listens for any (all) or specific event messages. Windows event logs record events that happen on devices. For more information about the information the type of information that is gathered and reported in Windows logs, see the *Microsoft support site* (<http://technet.microsoft.com/en-us/library/cc722385%28v=WS.10%29.aspx>).

- § The Syslog monitor listens for any (all) or specific Syslog event messages. Syslog messages refer to a facility (the type of program that logged the message) and are assigned a severity by the sender of the message. For more information about Syslog facilities and levels of severity, see *RFC5424* (<http://tools.ietf.org/html/rfc5424>) (page 9 for facilities and page 10 for levels of severity).

After the monitor types are configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog. For more information, see *Assigning passive monitors* (on page 448).

Passive Monitors are configured and stored in the Passive Monitor Library. 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.

For more information, see *Configuring passive monitors* (on page 443).

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 439).
- 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. For more information, see *Actions overview* (on page 611).

Passive Monitor Icon

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.

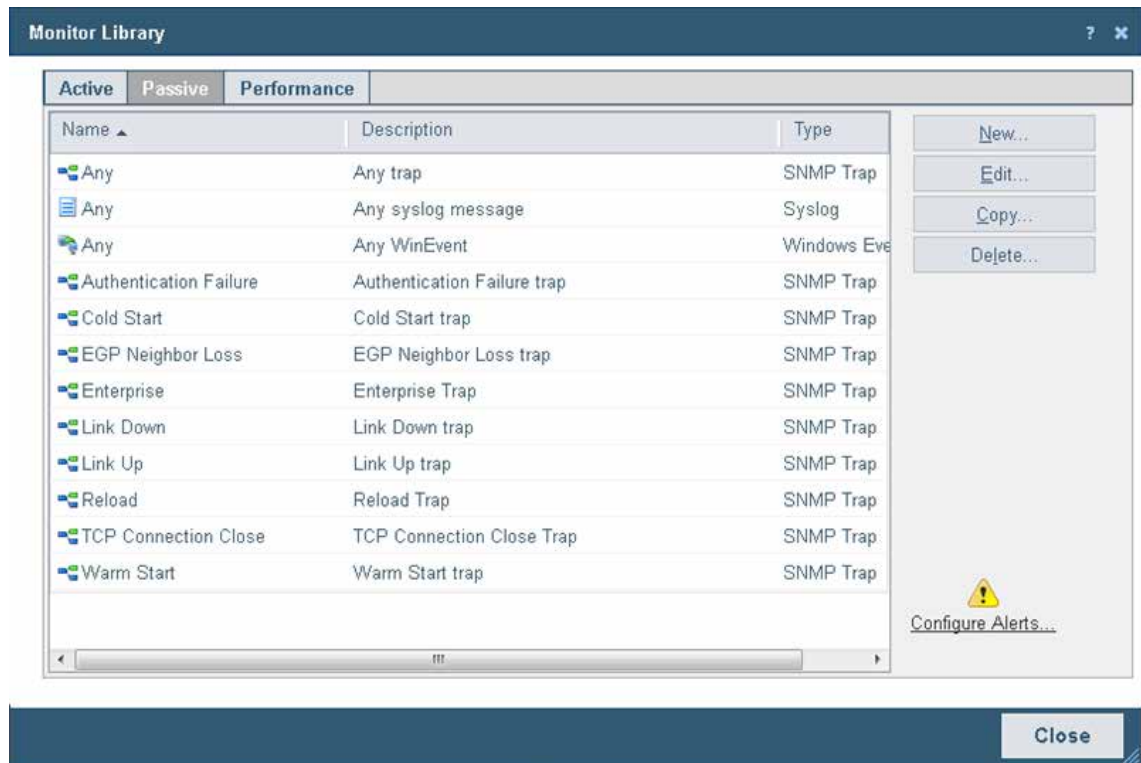
SNMP Trap passive monitors in the library

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.



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 is 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* (on page 903), *Enabling the Syslog listener* (on page 904), and *Enabling the Windows Event Log listener* (on page 904).

Configuring the SNMP Trap Listener

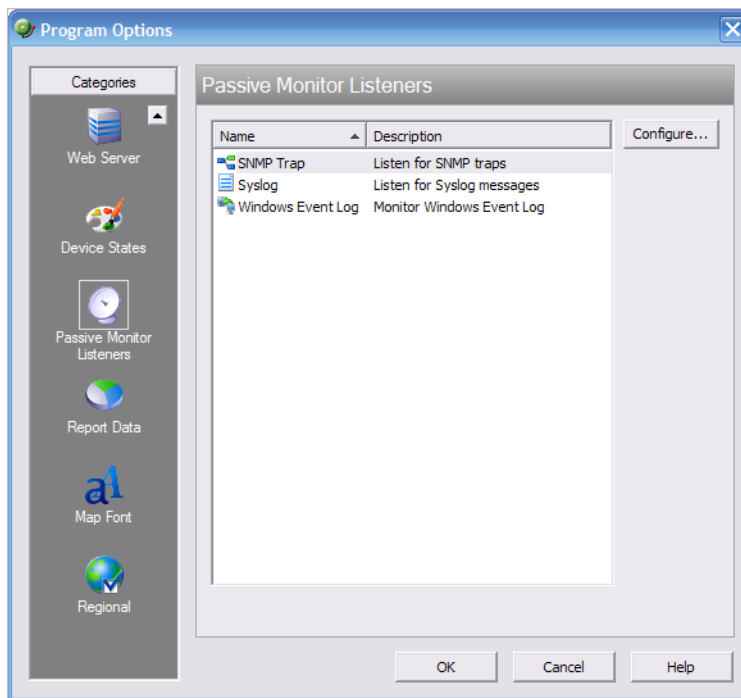
To configure the SNMP Trap Listener:

- 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.



- 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 boxes:
 - § **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 boxes:
 - § **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.

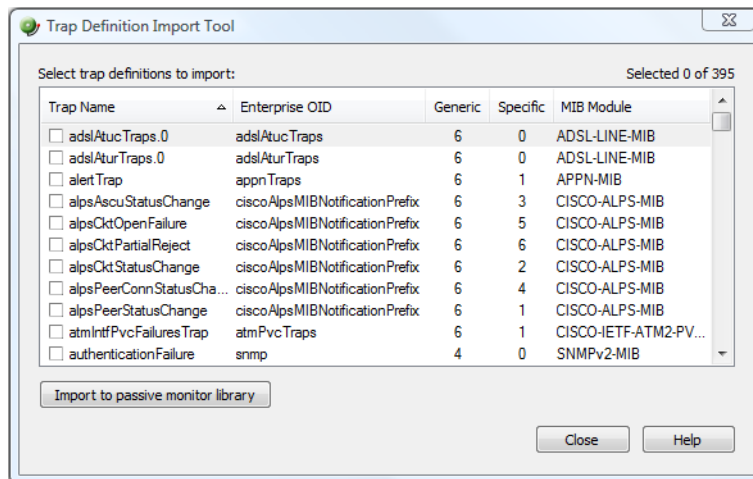
While using the Trap Definition Import Tool or any of the pre-configured passive monitors are two easy ways to configure SNMP Trap passive monitors, you still have the option to manually configure all passive monitor types via the Passive Monitor Library.

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.



- 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

The SNMP Trap monitor listens for any (all) or specific SNMP traps. SNMP traps enable an SNMP device agent to notify on significant events through unsolicited SNMP messages, or traps. For more information, see *Cisco's Understanding SNMP Traps* (<http://www.whatsupgold.com/CiscoSNMPTraps>).

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 448).

Adding and Editing a Syslog Monitor

The Syslog Passive Monitor listens for Syslog messages on the devices to which it is assigned.

Syslog is a standard for computer data logging that separates the software that generates messages from the system that stores them and the software that reports and analyzes them.

Syslog messages refer to a facility (the type of program that logged the message) and are assigned a severity by the sender of the message. For more information about Syslog facilities and levels of severity, see *RFC5424* (<http://tools.ietf.org/html/rfc5424>) (page 9 for facilities and page 10 for levels of severity).

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 359), 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 448).

For an example of why you might create a Syslog Event, see *Sample of a Syslog Monitor Event* (on page 446).

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

The Windows Event Log listens for Windows events on the devices to which it is assigned.

Windows event logs record events that happen on devices. For more information about the information the type of information that is gathered and reported in Windows logs, see the *Microsoft support site* (<http://technet.microsoft.com/en-us/library/cc722385%28v=WS.10%29.aspx>).

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 359), 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 448).

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 448).

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 267).
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 267).

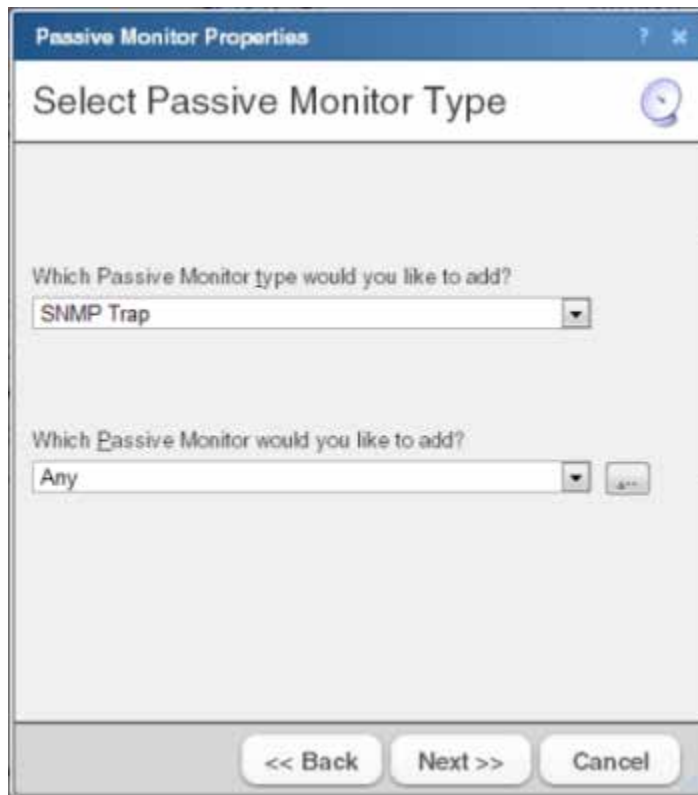


Note: When you assign a passive monitor to a device, an instance of the monitor is added to the device. Changes that you make to the monitor's configuration via the Passive Monitor Library affect all instances of the monitor. For example, if you assign a monitor to four separate devices and then make 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.



- 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	451
Using the Performance Monitor Library.....	452
Working with Performance Monitors.....	453
Adding and editing an Active Script Performance Monitor	455
Adding and editing an APC UPS Performance Monitor.....	457
Adding and editing a PowerShell Scripting performance monitor.....	458
Example - PowerShell performance monitor scripts.....	460
Adding and editing a Printer performance monitor	463
Adding and editing an SNMP Performance Monitor	465
Adding and editing a SQL Query performance monitor	466
SQL Query Builder.....	469
Adding and editing an SSH performance monitor	469
Adding and editing a Windows Performance Counter Monitor.....	471
Adding and editing a WMI Formatted Performance Monitor.....	473
Adding and editing a WMI Performance Monitor	474

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, Windows Performance Counter, WMI Formatted, and WMI performance counters.

Performance Monitors are configured in the *Performance Monitor Library* (on page 452) and are added to individual devices through the Device Properties dialog. From the Device Properties Performance Monitor dialog, you can add:

- § Pre-configured (standard) Performance Monitors
- § Device-specific (custom) Performance Monitors

For more information, see *Enabling global performance monitors* (on page 475) and *Creating custom performance monitors* (on page 480).



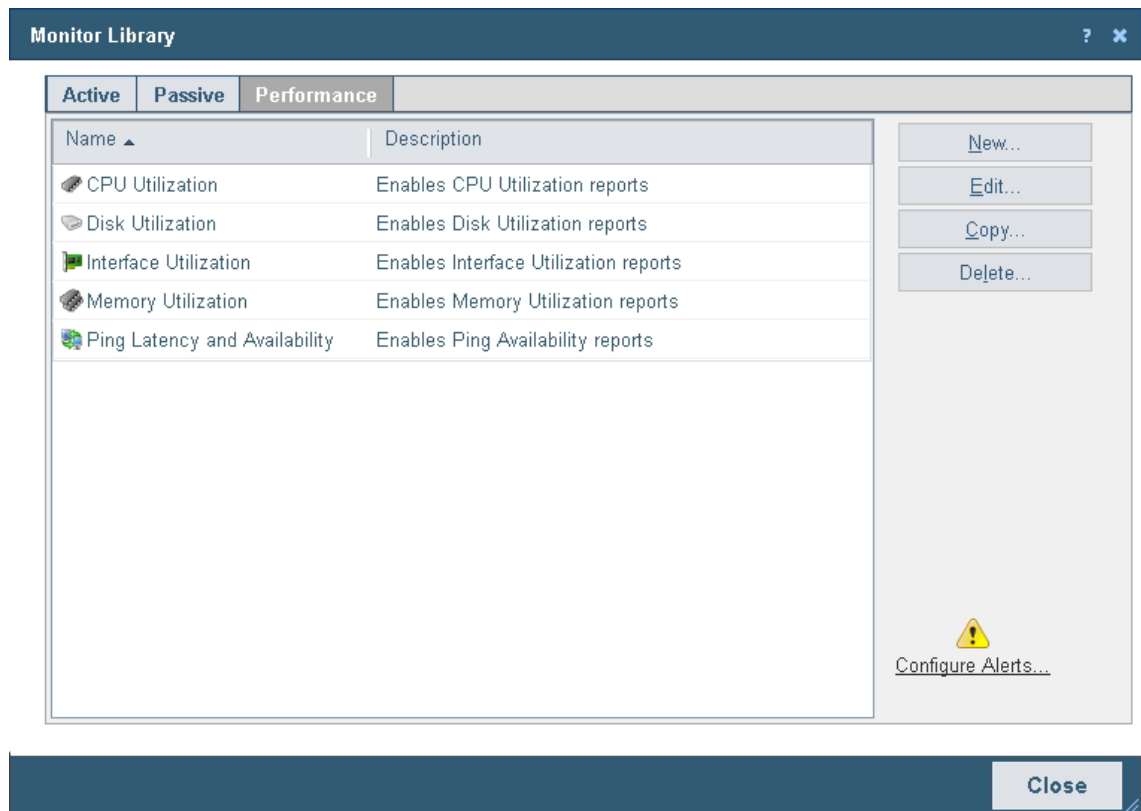
Note: Printer monitors are specific to individual printer devices; as such, the Printer Performance Monitor can only be added as an individual performance monitor in the Device Properties Performance Monitor dialog.

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.



- 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 685).

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 692) 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.



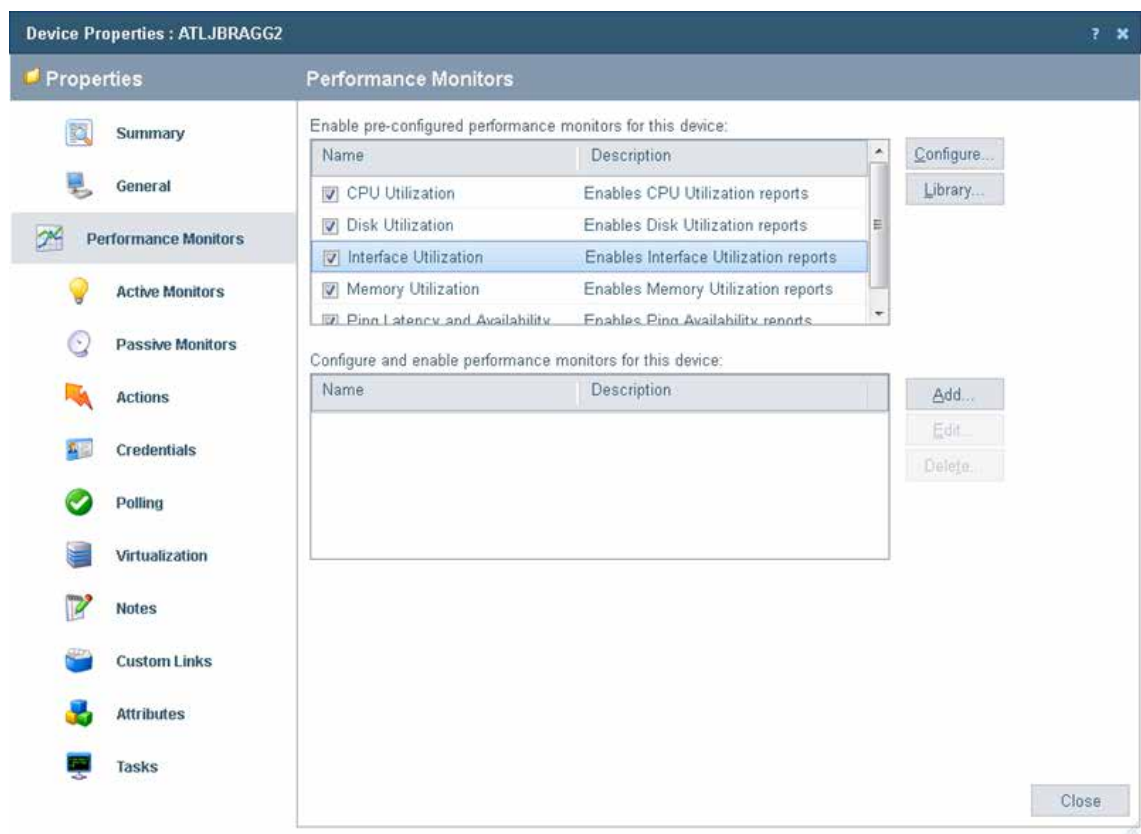
Tip: Click **Configure Alerts** to view the Alert Center Threshold Library.



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.



- 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 937).

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 > Monitors**. 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 SMTP server. 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 475).



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 973)?

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 SMTP server. 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 > Monitors**. 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 475).

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 460).



Important: WhatsUp Gold uses a 32-bit (i.e. x86) PowerShell engine. Therefore, only 32-bit PowerShell snap-ins are supported and 64-bit only snap-ins will not function properly. Snap-ins usable in both 32-bit and 64-bit operating systems are configured for 64-bit systems by default and must be manually configured for 32-bit PowerShell engine to function properly with WhatsUp Gold.



If you are using *additional pollers* (on page 35) with WhatsUp Gold, PowerShell must be installed and any desired snap-ins must be registered identically on all poller machines for any PowerShell performance monitors, active monitors, and actions to function properly. Associated errors resulting from failed monitors will appear in the *WhatsUp Gold Status Center* (on page 20). Errors resulting from failed actions will appear in the WhatsUp Gold Event Viewer.



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 > Monitors**. 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 SMTP server. 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*.

- § **Run under device credentials**. Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see *Using the Credentials Library*.
 - § **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 475).

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 SMTP server. 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.

- § **Run under device credentials.** Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see Using the Credentials Library.
 - § **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 475).

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 > Monitors**. 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.
 - § **Plot raw values**. Select this check box to monitor the current polled value instead of tracking the rate of change over time.



Note: Enable **Plot raw values** when you want to graph the current value of the SNMP object, as one would a gauge such as a vehicle's speedometer or temperature sensor, for example. Disable this option when graphing objects that measure a rate of change over time such as an odometer.

- 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 475).

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.
 - § **Plot raw values**. Select this check box to monitor the current polled value instead of tracking the rate of change over time.



Note: Enable **Plot raw values** when you want to graph the current value of the SNMP object, as one would a gauge such as a vehicle's speedometer or temperature sensor, for example. Disable this option when graphing objects that measure a rate of change over time such as an odometer or the number of times an engine's RPM exceeded a certain threshold.

- 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 > Monitors**. 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 469) 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 475).

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 469) 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. You can either embed the script in the monitor or place a script file on the remote machine (making sure it's executable) and enter a command in the monitor to run the script. Each monitor returns a single numeric value that is recorded in the database, then is used later by different WhatsUp Gold functions such as reporting or to compare against a threshold in Alert Center.

To add a new 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 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. Select one of the following script options:

§ **Numeric.** The command or script must return a single numeric value. The script can be as complex as required, but **MUST** only return a numeric value. For example, old, single-line unix-style:

```
free -m | awk 'NR==2{print $3}'
```

This is the script format required prior to WhatsUp Gold 16.2.3.

§ **Shell Interactive.** This script is not constrained to only returning single numeric values; however, the output **MUST** contain the string 'Result=xxxx' where xxxx represents a numeric value. For example, new multi-line linux-style:

```
echo Result=$(free -m | awk 'NR==2{print $3}')
```

This new script format, available in WhatsUp Gold 16.2.3 and later, supports all the features of the target script interpreters without burdening the script developer to limit the output to 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.

§ **Line end character.** Select the appropriate character type; either *None*, *Linefeed*, *Carriage return*, or *Carriage return linefeed*. Multiline scripts are entered and persisted on a Windows operating system, and include line-ending characters that may not be recognized on the target device. This configuration feature instructs WhatsUp Gold to replace the line-ending characters with the selected characters prior to connection and command execution.

§ **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 475).

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. The command or script must return a single numeric value.

As of WhatsUp Gold 16.2.3 and following releases, SSH performance monitors require that a value be returned in a specific 'Result=xxxx' format. The output **MUST** contain the string 'Result=xxxx' where xxxx represents a numeric value. For example:

Old, single-line unix-style: `free -m | awk 'NR==2{print $3}'`

New linux-style with required format: `echo Result=$(free -m | awk 'NR==2{print $3}')`



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.

§ **Line end character.** Select the appropriate character type; either *None*, *Linefeed*, *Carriage return*, or *Carriage return linefeed*. Multiline scripts are entered and persisted on a Windows operating system, and include line-ending characters that may not be recognized on the target device. This configuration feature instructs WhatsUp Gold to replace the line-ending characters with the selected characters prior to connection and command execution.

§ **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 Windows Performance Counter Monitor

The Windows Performance Counter Monitor enables data collection from performance counters exposed by various Windows applications. This monitor can only monitor Windows applications and requires Windows credentials on the device for which you want to monitor Windows applications. Additionally, devices for which you want to monitor Windows applications must have the *Remote Procedure Call* and *Remote Registry* services enabled and running.



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 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 **Windows Performance Counter Monitor**, then click **OK**. The Add Windows Performance Counter Monitor dialog appears.
- 5 Enter or select the appropriate information:
 - § **Name**. Enter a unique name for the monitor. This name displays in the Performance Monitor Library.
 - § **Description**. Enter additional information for the monitor. This description displays next to the monitor name in the Performance Monitor Library.
 - § **Category**. Enter the category to which the Windows performance counter you want to monitor belongs, such as *Processor*. Click browse (...) to select the Windows Performance Counter you would like to use in the monitor.
 - § **Counter**. Enter the specific performance counter in the category specified above for which you want to monitor, such as *% Processor Time*.
 - § **Instance**. (Optional) If applicable, enter the specific instance of the performance counter specified above for which you want to monitor, such as *_Total*. Not all counters have specific instances, so this box may be left blank.
- 6 After the monitor is added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling performance monitors* (on page 475).

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 Windows Performance Counter Monitor dialog appears.
- 4 Enter or select the appropriate information:
 - § **Name**. Enter a unique name for the monitor. This name displays in the Performance Monitor Library.
 - § **Description**. Enter additional information for the monitor. This description displays next to the monitor name in the Performance Monitor Library.
 - § **Category**. Enter the category to which the Windows performance counter you want to monitor belongs, such as *Processor*.
 - § **Counter**. Enter the specific performance counter in the category specified above for which you want to monitor, such as *% Processor Time*.
 - § **Instance**. Enter the specific instance of the performance counter specified above for which you want to monitor, such as *_Total*.
- 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 > Monitors**. 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 475).

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 > Monitors**. 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 475).

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 475) through the Device Properties dialog, or *enable a monitor on multiple devices* (on page 476) 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 267).

- 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* (on page 593).



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 302).

- § **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 911).

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 If necessary, click **Next** to install the components.
- 7 If necessary, after the install wizard completes, 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 267) 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 937).

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 SMTP server. 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 SMTP server. 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 460).



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 SMTP server. 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.
 - § **Plot raw values**. Select this check box to monitor the current polled value instead of tracking the rate of change over time.



Note: Enable **Use raw value** when you want to graph the current value of the SNMP object, as one would a gauge such as a vehicle's speedometer or temperature sensor, for example. Disable this option when graphing objects that measure a rate of change over time such as an odometer.

- 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 469) 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 SMTP server. 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 > Monitors**. 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. 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 479).

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 700).

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 920).

Alerting and actions

In This Chapter

Getting started with WhatsUp Gold alerting498

Working with Alert Center reports.....520

Using the Alerts Home reports.....526

Configuring notifications.....540

Configuring thresholds.....553

Using Actions.....611

Getting started with WhatsUp Gold alerting

In This Chapter

Step 1: Identify important devices.....	499
Step 2: Ensure monitors are configured for important devices	499
Step 3: Configure alerts for important devices.....	499
Step 4: Configure action policies.....	514

Your web server goes down over the weekend. When you get to work on Monday, you are bombarded with emails from resellers, employees, and user forum members from all over the world notifying you that they can't access your organization's website. If you had known about this problem as soon as it occurred, you could have resolved it immediately. WhatsUp Gold's alerting functions notify you of this type of problem as well as other crucial network information through various types of alerts.

WhatsUp Gold's alerting system is comprised of actions and the WhatsUp Gold Alert Center. Actions notify you on active and passive monitors; Alert Center alerts you on performance monitors, the WhatsUp Gold system, Wireless features, and Flow Monitor plug-in.

The table below shows the part of the alerting system you use to receive alerts of a particular type.

	Actions	Alert Center
Alerts on active monitors	●	
Alerts on passive monitors	●	●
Alerts on performance monitors		●
Alerts on the WhatsUp Gold database		●
Alerts on WhatsUp Gold services		●
Alerts on Wireless features		●
Alerts on WhatsUp Gold Flow Monitor		●

Together, actions and Alert Center provide you with a 360-degree notification system for your network.

For more information on alerting through actions, see *Using Actions* (on page 611).

For more information on alerting through Alert Center, see *Using Notification Policies*.

Step 1: Identify important devices

Some network administrators may only want to receive alerts for devices that are crucial to their network. In the case of smaller networks, others may want to receive alerts for all devices. No matter the strategy you choose for receiving alerts for your network, identifying the devices that are most important to your network is smart. After you identify these devices, you can design an alerting strategy to highlight their status.

For illustration purposes, we follow Nick, a network administrator for a company that develops software. Nick wants to receive alerts for the devices his colleagues and software customers need to be running everyday. Nick has decided that he wants to receive alerts on the mail server, the web server, and all servers that store product code and company information. Total, there are six servers for which Nick would like to receive alerts.

Step 2: Ensure monitors are configured for important devices

In order for you to receive alerts on monitor events, you must first have monitors configured on the devices for which you want to receive alerts. Be sure to create monitors to collect the types of information for which you want to be alerted. For example, Nick, the network administrator from Step 1, has created a Domain Service (DNS) active monitor for his web server, and an SNMP Trap passive monitor for his mail server. He has also enabled the Disk Utilization performance monitor for his four storage servers.

For information about configuring and assigning DNS active monitors, see *Using active monitors* (on page 341).

For information about configuring and assigning Windows Event Log passive monitors, see *Using passive monitors* (on page 436).

For information about configuring and enabling memory performance monitors, see *Using performance monitors* (on page 451).

Step 3: Configure alerts for important devices

Alerts can be configured for and assigned to devices, performance monitors, passive monitors, and active monitors. Alerts for performance monitors are configured and assigned in the Alert Center. Alerts for devices, active, and passive monitors are configured in the Action Library and are assigned either during the configuration process or from the Device Properties dialog.

In addition to alerts for devices and monitors, you can configure alerts for WhatsUp Gold system aspects, and the Flow Monitor and Wireless plug-ins. These alerts are configured and enabled in the Alert Center.

For example, Nick, the network administrator from Step 1, has created a Domain Service (DNS) active monitor for his web server, and an SNMP Trap passive monitor for his mail server. He has also enabled the Disk Utilization performance monitor for his four storage servers.

For the DNS active monitor assigned to the web server, Nick wants to be notified immediately if the DNS port is unavailable. An SMS Direct message sent to his cell phone will alert him immediately following the monitor's issuance of a down state.

For the SNMP Trap passive monitor assigned to the mail server, Nick wants to be alerted if Authentication Failure traps are observed by the SNMP Listener.

For the Disk Utilization performance monitors enabled for the 4 storage servers, Nick creates thresholds in Alert Center and configures a Notification Policy to alert him when the servers reach certain levels of fullness.

Nick also assigns an SMS Direct action to each of the storage servers so that he is notified immediately if a device goes down, causing the information stored on the servers to be unavailable to colleagues and software customers.

Each of the example procedures are outlined in the following sections.

Configuring alerts for active monitors

In this example, you create and assign an SMS Direct action to a DNS active monitor. SMS Direct actions send user-configured text messages to cell phones or other texting capable devices through GSM modems.

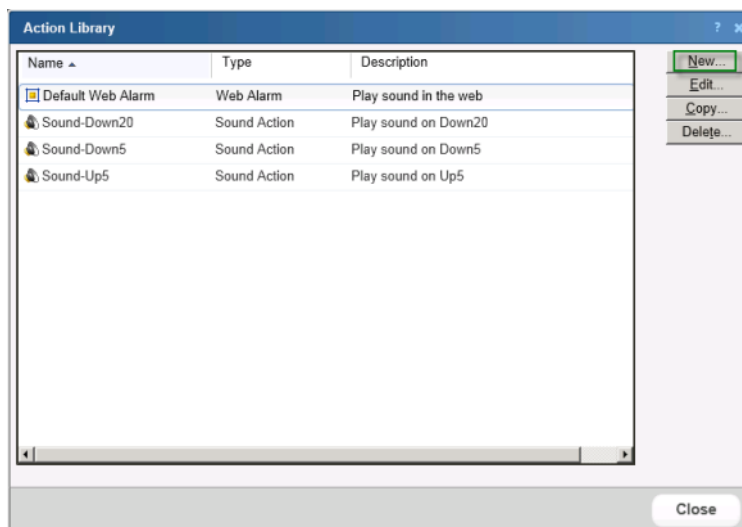
You must have the following before attempting to configure an SMS Direct action:

- § 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

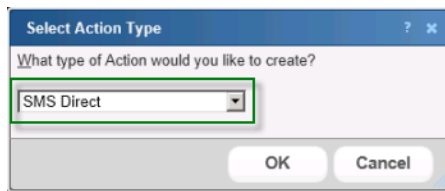
To configure an SMS Direct alert for a DNS active monitor:

First, create the SMS Direct action.

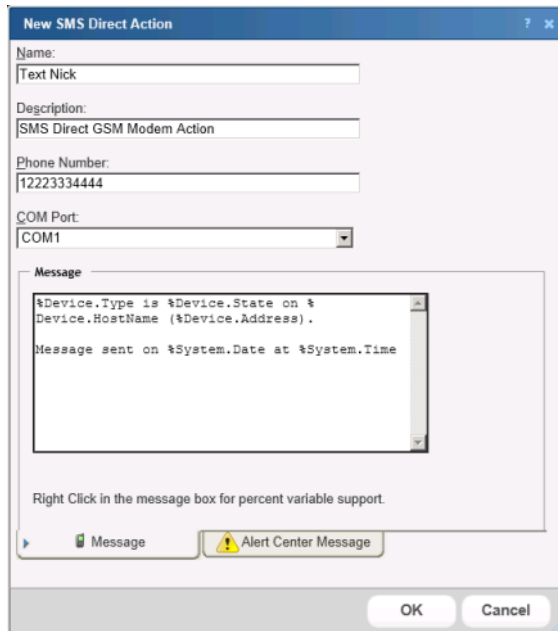
- 1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.



- 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 the appropriate information in the dialog boxes:
 - § **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.

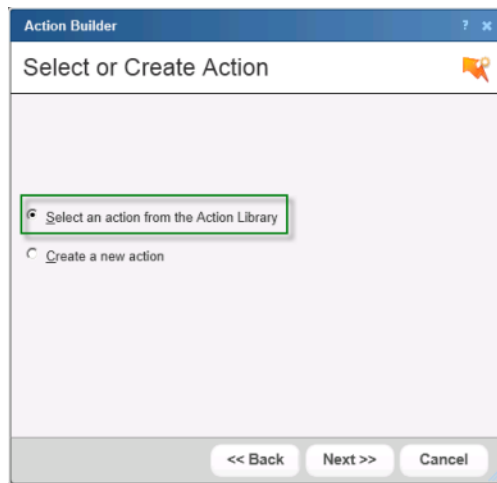
After configuring the action, assign it to the appropriate device. In this example, Nick assigns it to his web server device.

- 1 In the Details or Map View, right-click the appropriate device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Select the DNS active monitor, then click **Edit**. The Set Polling Properties dialog appears.

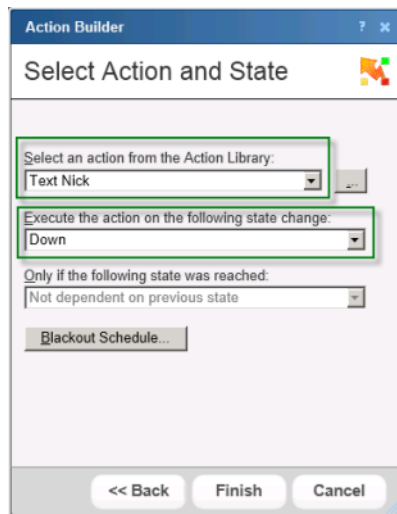
- 4 Make any adjustments to polling selections, then click **Next**. The Setup Actions for Monitor State Change dialog appears.

The **Apply individual actions** option is selected by default; keep this selection.

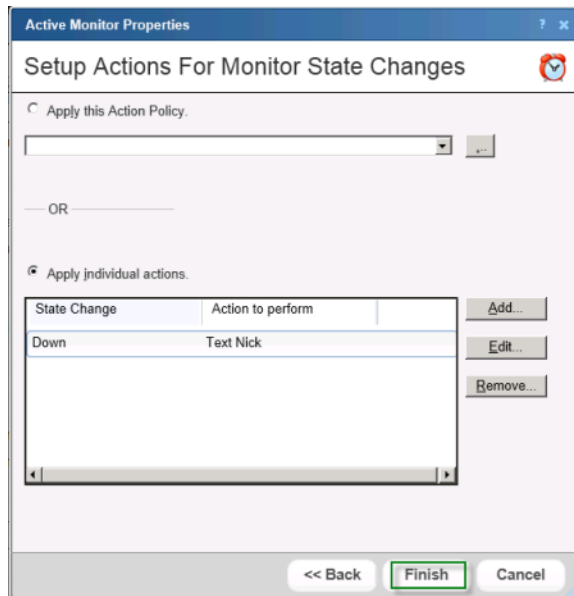
- 5 Click **Add**. The Action Builder appears.



- 6 Select the **Select an action from the Action Library** option, then click **Next**. The Select Action and State dialog appears.



- 7 Select the **SMS Direct** action from the list, select **Down** as the state change, then click **Finish**. The Setup Actions for Monitor State Changes dialog appears.



- 8 Click **Finish**. The Device Properties dialog appears.
- 9 On the Device Properties dialog, click **OK** to save changes.

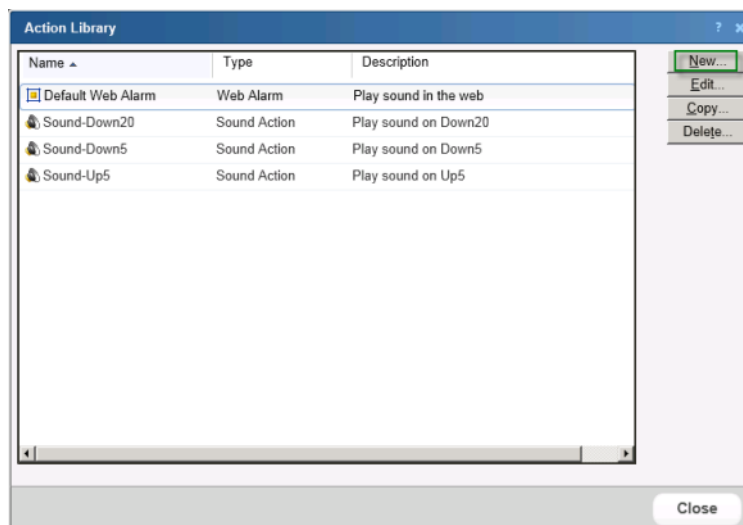
Configuring alerts for passive monitors

In this example, you create and assign an E-mail action to a SNMP Trap passive monitor. The SNMP Trap monitor listens for any (all) or specific SNMP traps. SNMP traps enable an SNMP device agent to notify on significant events through unsolicited SNMP messages, or traps.

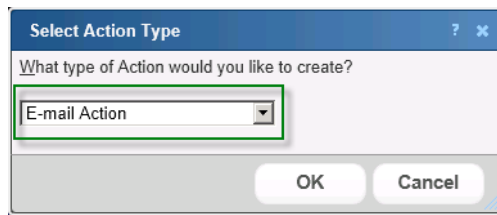
To configure an E-mail alert for an SNMP Trap passive monitor:

First, create the E-mail action.

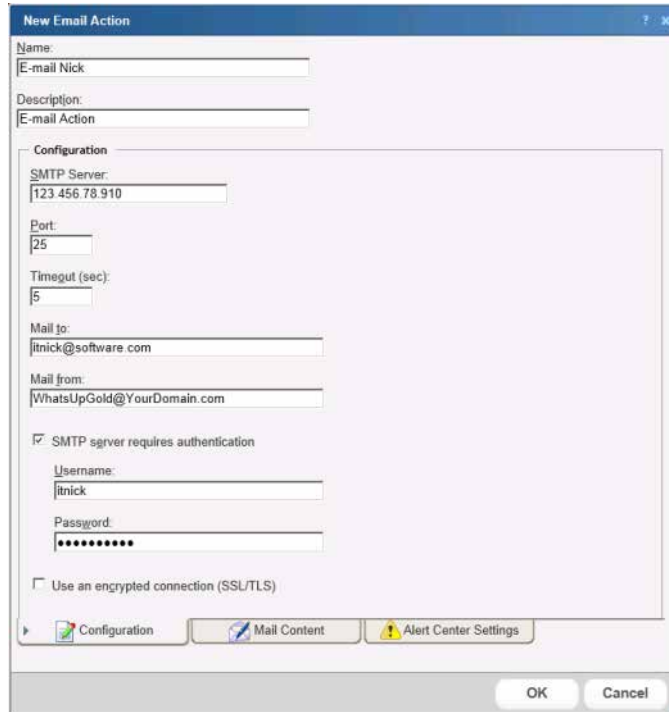
- 1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library appears.



- 2 Click **New**. The Select Action Type dialog appears.



- 3 Select **E-mail Action**, then click **OK**. The New Email Action dialog appears.

The image shows the "New Email Action" dialog box. It has a "Name:" field with "E-mail Nick" and a "Description:" field with "E-mail Action". Below these is a "Configuration" section with fields for "SMTP Server:" (123.456.78.910), "Port:" (25), "Timeout (sec):" (5), "Mail to:" (itnick@software.com), and "Mail from:" (WhatsUpGold@YourDomain.com). There is a checked checkbox for "SMTP server requires authentication" with "Username:" (itnick) and "Password:" (masked with dots) fields. An unchecked checkbox for "Use an encrypted connection (SSL/TLS)" is also present. At the bottom are tabs for "Configuration", "Mail Content", and "Alert Center Settings", and "OK" and "Cancel" buttons.

- 4 Enter the appropriate information in the dialog boxes:
 - § **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.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 listening.
 - § **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 SMTP server. This is considered a failed connection.
 - § **Mail To.** Enter the email addresses to which you want to send the alert. Email addresses must be fully qualified. You can enter multiple addresses, separated by a

semi-colon (;), comma (,), or the [SPACE] character. The address should not contain brackets, braces, quotes, or parentheses.

§ **Mail From.** Enter the email address you want to appear in the From field of the e-mail that is sent by the Email 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).

Complete the information on the **Mail Content** tab. This tab contains options pertaining to the action email message content.

The screenshot shows the 'New Email Action' dialog box with the 'Mail Content' tab selected. The 'Name' field contains 'E-mail Nick' and the 'Description' field contains 'E-mail Action'. The 'Mail Content' section has a 'Subject' field with the text '%Device.Type is %Device.State (%Device.HostName)'. Below it, the 'Message body' section has radio buttons for 'Plain text' (selected) and 'Html'. The message body text area contains the following content: '%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', a separator line, and 'This mail was sent on %System.Date at %System.Time Ipswitch WhatsUp Gold'. Below the text area, there is a note: 'Right Click in the Subject or Message body field for percent variable support.' and two buttons: 'Device Status' and 'Mobile Device Status'. At the bottom, there are three tabs: 'Configuration' (selected), 'Mail Content', and 'Alert Center Settings'. The 'OK' and 'Cancel' buttons are at the bottom right.

§ **Subject.** Enter a text message or edit the default message. You can use percent variable codes to display specific information in the subject.

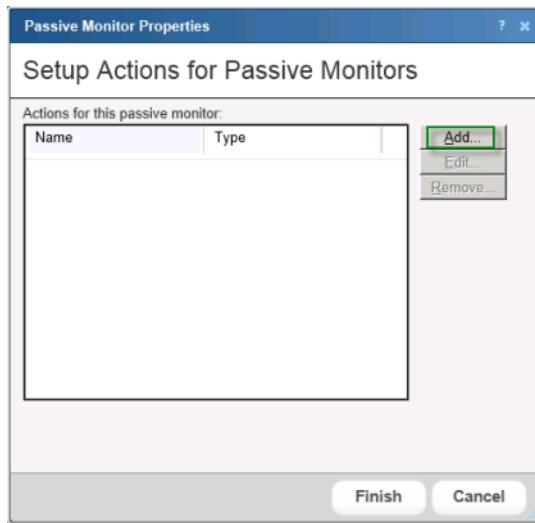
§ **Message body.** Enter a text message or edit the default message. You can use percent variable codes to display specific information in the message body.

For the purpose of this example, we are not using the dialog's Alert Center tab. Click **OK** to save the E-mail action configuration.

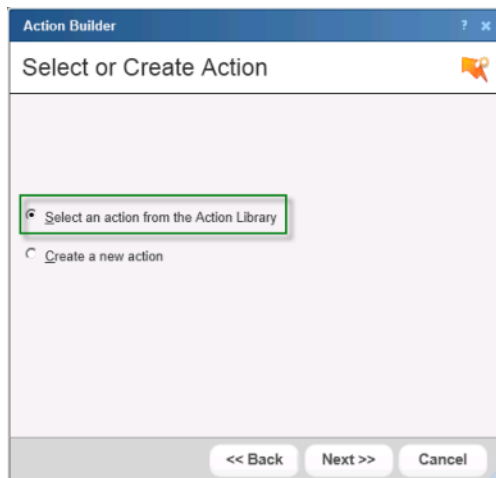
- 5 After configuring the action, assign it to the appropriate device. In this example, Nick assigns it to his mail server device.

After configuring the action, assign it to the appropriate device. In this example, Nick assigns it to his mail server device.

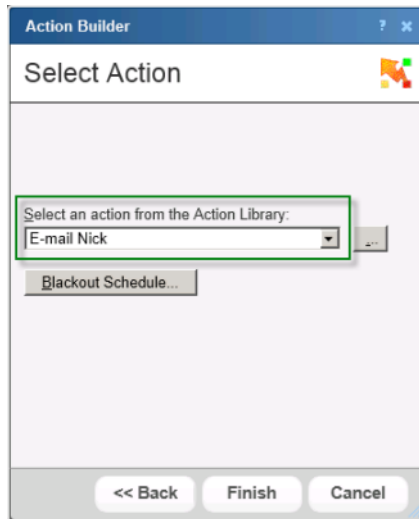
- 1 In the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Passive Monitors**. The Device Properties - Passive Monitors dialog appears.
- 3 Select the SNMP Trap passive monitor, then click **Edit**. The monitor properties dialog appears.



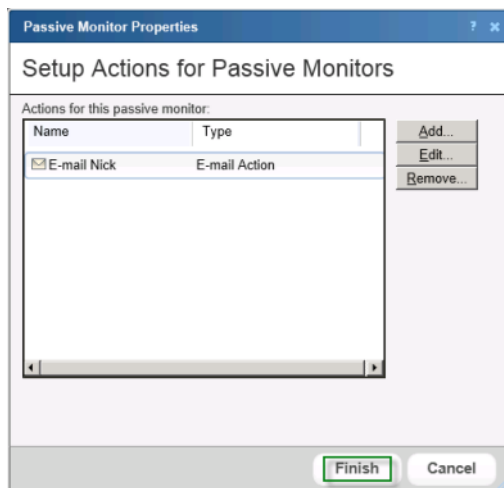
- 4 Click **Add**. The Action Builder appears.



- 5 Select the **Select an action from the Action Library** option, then click **Next**. The Select Action dialog appears.



- 6 Select the E-mail Action, then click **Finish**. The Setup Actions for Passive Monitors dialog appears.



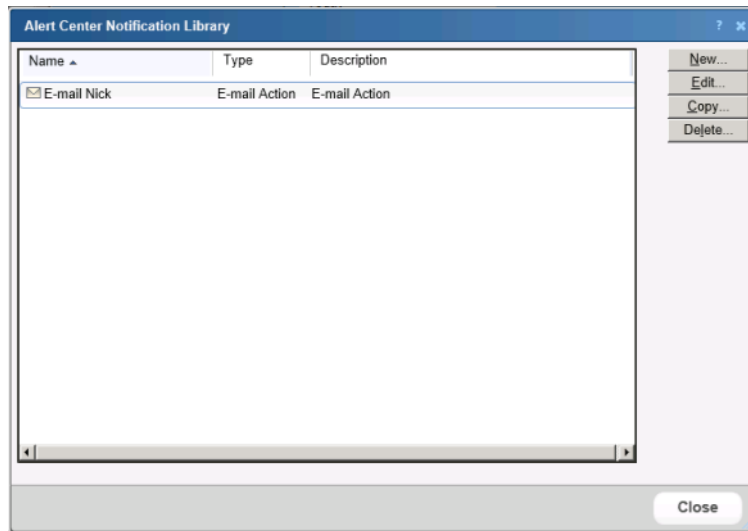
- 7 Click **Finish**. The Device Properties dialog appears.
- 8 On the Device Properties dialog, click **OK** to save changes.

Configuring alerts for performance monitors

In this example, you create performance thresholds and configure the notifications and notification policy to notify you when disk thresholds are reached or exceeded. Nick wants to receive emails when a storage server exceeds its disk utilization threshold, this example creates an E-mail action for use in the notification policy.

In order for disk thresholds to work, you must have enabled the Disk Utilization performance monitor for the devices for which you want collect disk data. Nick has enabled the Disk Utilization performance monitor on each of his storage servers.

If you have already configured E-mail actions, you can use them as notifications in Alert Center notification policies. All currently configured E-mail actions are listed in the Notification Library.

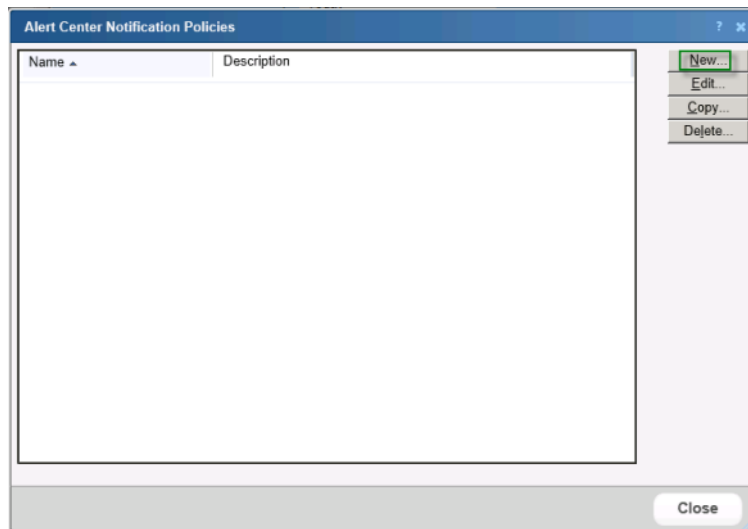


In this example, Nick created an E-mail action for his SNMP Trap passive monitor. Nick can use this same E-mail action in his notification policy.

Because an E-mail action already exists, the first thing Nick must do to configure alerts for his Disk Utilization performance monitors is create a notification policy.

To configure a notification policy:

- 1 From the WhatsUp Gold web interface, click **Alert Center > Notification Policies**. The Alert Center Notification Policies dialog appears.



- 2 Click **New**. The New Alert Center Notification Policy dialog appears.

New Alert Center Notification Policy

Name:

Description:

Select which notifications will be delivered by each step of this policy:

Notification	Type	Step 1	Step 2	Step 3
E-mail Nick	E-mail Action	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Escalation Steps

Step 2 begins after the notification starts

Step 3 begins after the notification starts

☒ Repeat step 3 every until the notification is stopped

☐ Show me a graph of this notification policy in action

OK Cancel

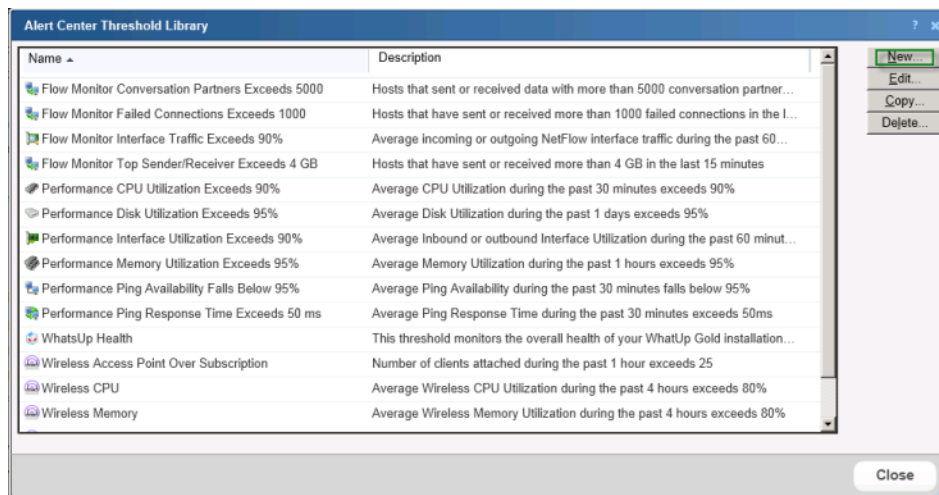
- 3 Configure the identifying information for the policy:
 - § **Name**. Enter a name for the notification policy.
 - § **Description**. Enter a description of the policy.
- 4 Select the notifications you would like delivered for each of the 3 steps of the policy. To select a notification, click the boxes for the step of the policy that you would like the notification to be sent. For example, Nick clicks the **Step 1** box for the Email Nick notification. He continued the same for Step 3.
- 5 Select how the policy notification proceed after Step 1 in the Escalation Steps section of the dialog.
 - § Specify a start time for steps 2 and 3 of the policy. By default, step 2 is set to begin 1 hour after the first notification occurs, and step 3 is set to begin 2 hours after the first notification.
 - § You can choose to repeat step 3 of the policy at a regular interval until the notification is stopped. By default, the policy is set to repeat step 3 every hour until the notification is stopped.

For this example, Nick chose to start Step 3 1 day after the notification starts. He kept the other two default selections for Step 2 and the repetition of Step 3.
- 6 Click **OK** to save changes.

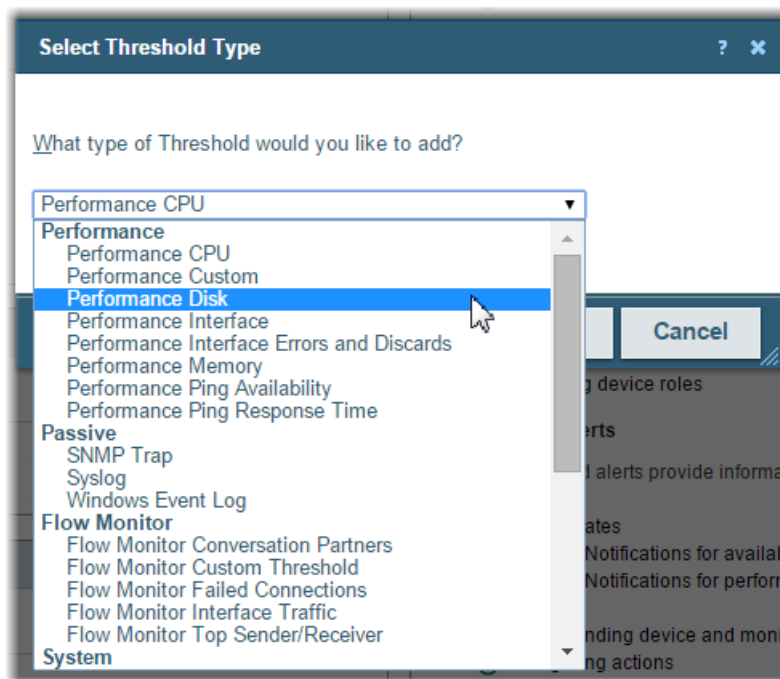
Last, configure the disk utilization thresholds.

To configure a disk utilization threshold:

- 1 From the WhatsUp Gold web interface, click **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.



- 2 Click **New**. The Select Threshold Type dialog appears.



- 3 Select *Performance Disk*, then click **OK**. The New Disk Utilization dialog appears.

New Disk Utilization Threshold

Name: Storage server disk utilization

Threshold

The threshold will alert when:

disk utilization exceeds 90 %

for more than 1 days

Devices to Monitor

Monitor all devices with disk performance data by default

Select...

Notification

E-mail Nick

Threshold Check

Check threshold every 60 minutes.

☒ Automatically resolve items no longer out of threshold

OK Cancel

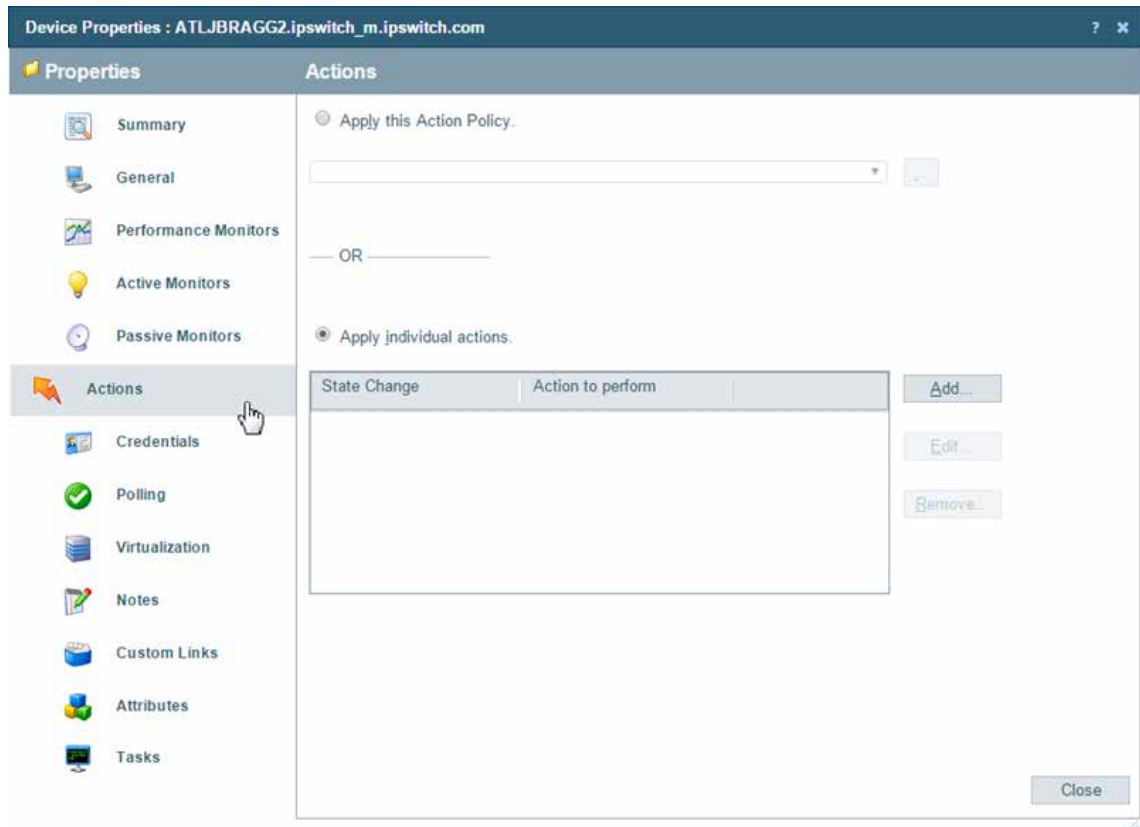
- 4 Enter the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria. For this example, select the *Utilization* option from the **disk** list. The default threshold triggers an alert when disk utilization exceeds 95% for more than 1 day. Nick changes the threshold to alert when the disk utilization exceeds 90%.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled. For this example, Nick selects his storage servers.
 - § **Notification.** Select the *E-mail Nick* policy to apply to this threshold. This policy begins sending notifications when a disk utilization item is outside the configured threshold limits.
 - § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database for items that are outside the threshold parameters. Nick kept the default of 60 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK** to save the threshold.

Configuring alerts for devices

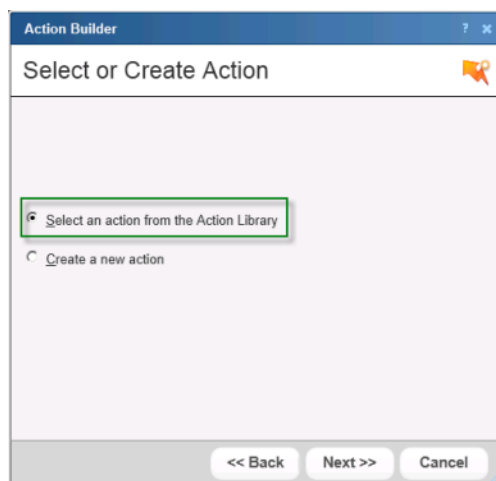
In this example, you assign an SMS Direct action to a device. Nick assigns this action to each of the storage servers so that he is notified immediately if a device goes down. The SMS Direct action was created when Nick configured it for the DNS active monitor; he can use the same action for his storage servers' status.

To assign an action to a device:

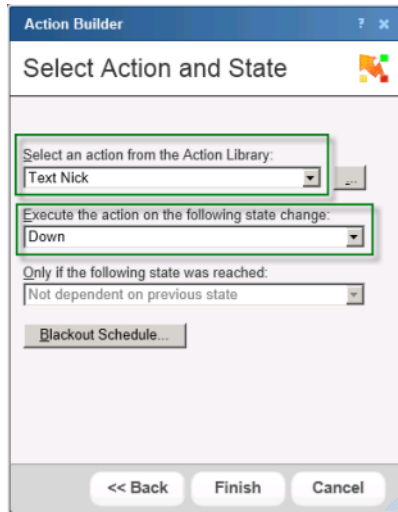
- 1 In the Details or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Device Properties - Actions dialog appears; the **Apply individual actions** option is selected by default.



- 3 Click **Add**. The Action Builder appears.



- 4 Select the **Select an Action from the Action Library** option, then click **Next**. The Select Action and State dialog appears.



- 5 Select the SMS Direct (Text Nick) action and the Down state, then click **Finish**. The Device Properties - Actions dialog appears.
- 6 On the Device Properties dialog, click **OK** to save changes.

Step 4: Configure action policies

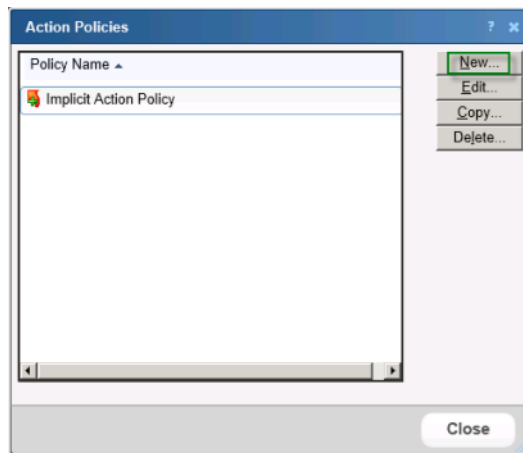
Similar to Alert Center notification policies, action policies allow you to group or sequence multiple actions together for use on any device, active, or passive monitor state change. Alert Center notification policies alert on thresholds, while action policies alert on state changes. The implicit action policy adds actions to every single device in your database; single devices can not opt out of an implicit action policy. As such, be sure to consider the types of actions you apply after implying an implicit action policy, so as to not create redundant actions which can cause double-alerts.

In this example, Nick creates an action policy to alert him by e-mail when his storage servers are initially down, and then to alert him by SMS text message when they are down for at least 20 minutes.

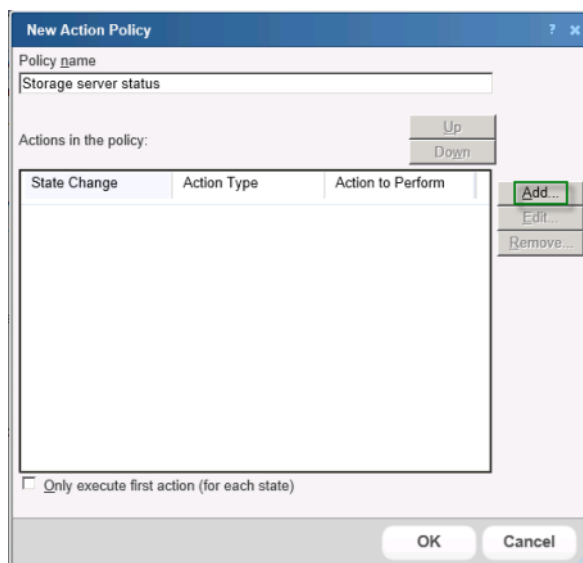
First, configure the policy.

To create an action policy:

- 1 From the WhatsUp Gold web interface, click **Admin > Action Policies**. The Action Policies dialog appears.

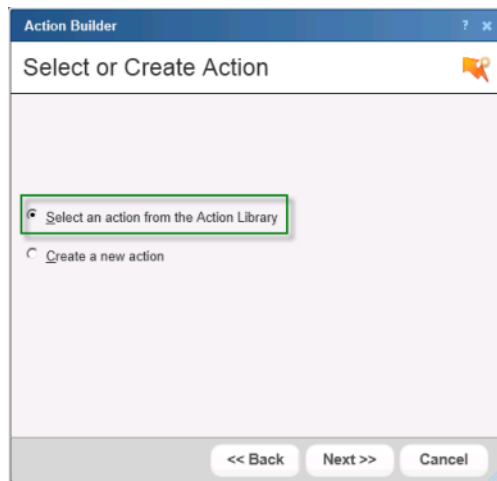


- 2 Click **New**. The New Action Policy dialog appears.

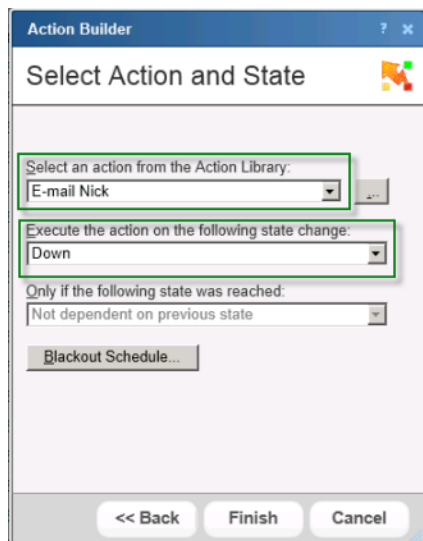


- 3 Enter a **Policy name**.

- 4 Click **Add**. The Action Builder wizard appears.

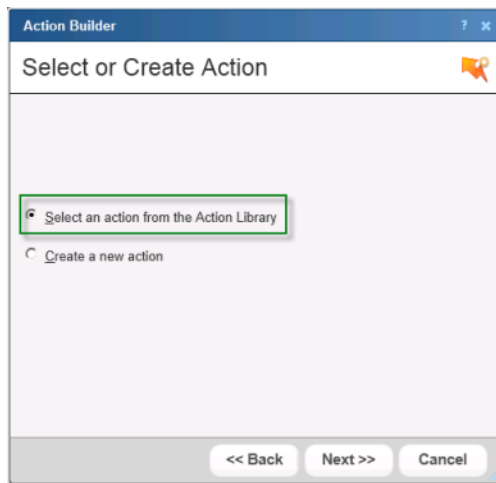


- 5 Select the **Select an action from the Action Library** option, then click **Next**. The Select Action and State dialog appears.

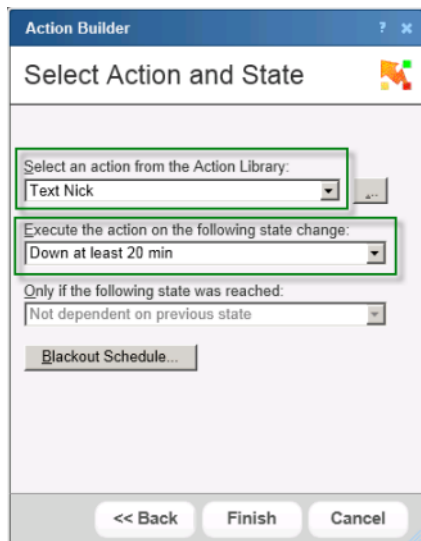


- 6 Select the E-mail action and the Down state, then click **Finish**. The New Action Policy dialog appears.

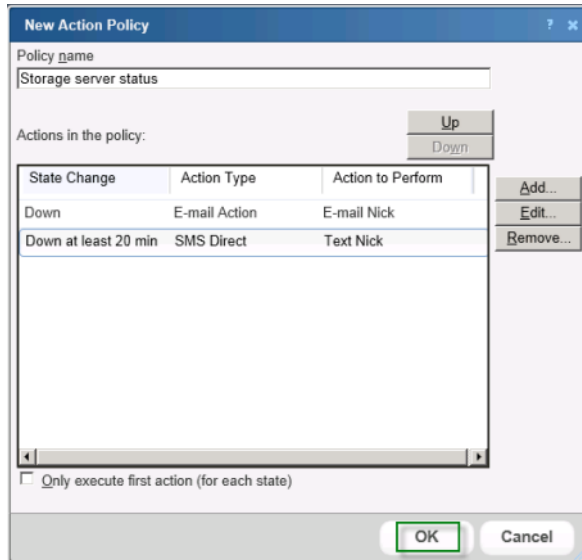
- 7 Click **Add**. The Select or Create Action Policy dialog appears.



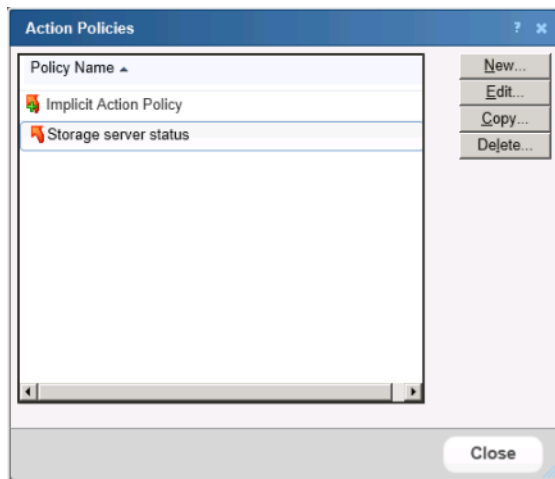
- 8 Select the **Select an action from the Action Library** option, then click **Next**. The Select Action and State dialog appears.



- 9 Select the SMS Direct action and the Down at least 20 min state, then click **Finish**. The New Action Policy dialog appears, listing the actions to be performed when each state change occurs.



- 10 Click **OK** to save the action policy. The policy is added to the Action Policies dialog.

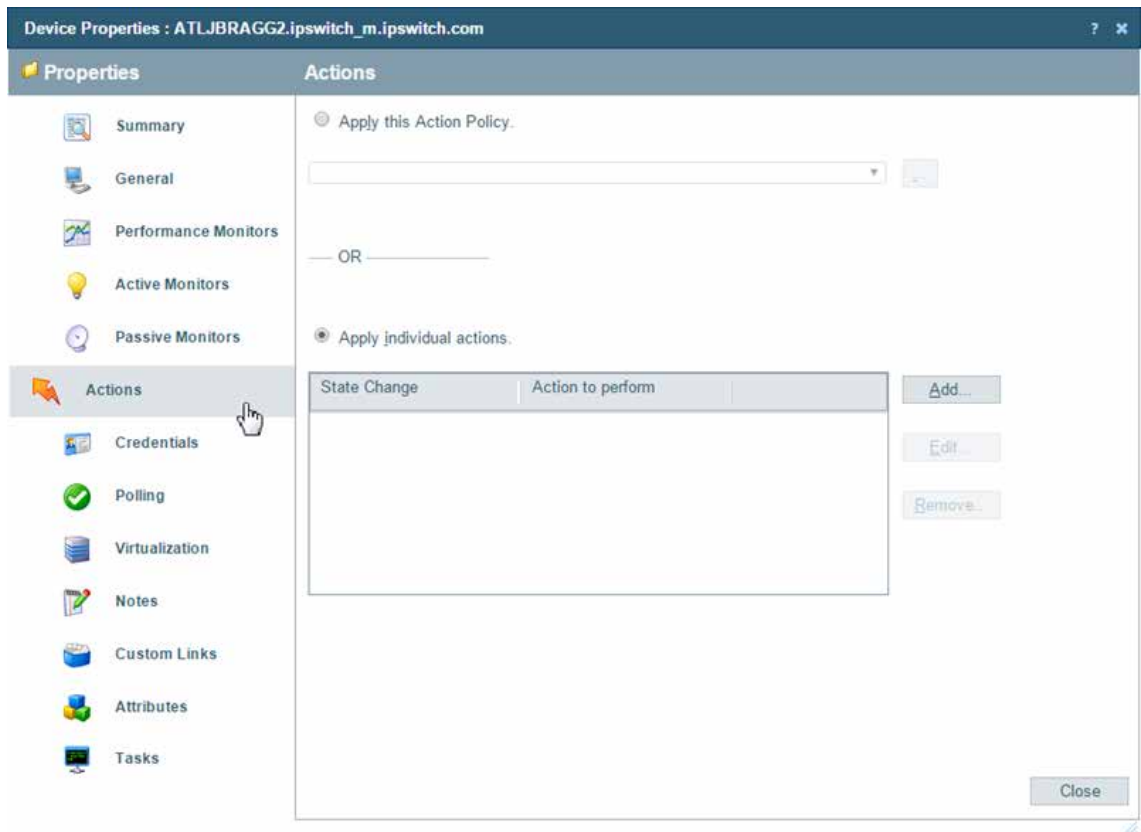


Next, assign it to the appropriate device(s). In this example, Nick assigns the policy to his storage servers.

To assign an action policy to a device:

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

- 2 Click **Actions**. The Actions dialog appears.



- 3 Select **Apply this Action Policy**, then select the appropriate action policy from the list of action policies.
- 4 Click **OK** to save changes.

Working with Alert Center reports

In This Chapter

Using Alert Center reports.....	520
Filtering the Items report	520
Using the Item History report	521
Updating Alert Center items.....	521
A note about notifications.....	523
Understanding resolving items - examples.....	523
Filtering the Log report.....	524
Configuring Alert Center records to expire	525

Using Alert Center reports

Alert Center reports are used to troubleshoot and monitor Alert Center data.

There are three Alert Center reports:

- § Running Notifications Policies
- § Log Report
- § Items Report

Filtering the Items report

Filter the Items Report by threshold and/or state.

To filter by threshold:

Using the **Filter by threshold** list, select the desired threshold(s).



Note: This list is populated with thresholds currently configured in the Threshold Library.

- § To view items for all thresholds, select **No Filter**.
- § To view items for a specific threshold, select that threshold.
- § To view items for specific threshold type, such as Flow, select that threshold type.

To filter by state:

Using the Filter by state list, select the desired item state(s).

- § To view items in all states, select **No Filter**.

To view items that have been updated to a specific state, select that state. You can select Acknowledged, Resolved, or Acknowledged and Resolved.

To filter by date:

Use the *date/time picker* (on page 669) at the top of the report to select a date range and time frame.

In the **Date range** list, many reports also allow you to specify and customize the business hour report times for reports to display. This allows you to view the network activity only for specified business hours. The date and time format for the date on this report matches the format specified in **Program Options > Regional** set in the WhatsUp Gold console.



Note: The Business Hours setting is available for group reports only.

Using the Item History report

To access the Item History report, click an item in the first column in the Items Report. The history of the selected item displays.

The Items report tracks an item through the system from creation to completion.

The report heading displays the item name, the threshold that triggered the item, the monitored device activity, and the threshold description.

Report body

Below the heading, the report displays the following information for the selected item:

- § **State.** Displays the current state of the item. Possible states include *Out of threshold*, *In threshold*, or *Disabled*.
- § **Notification progress.** Displays the progress status of an assigned notification policy. Possible progress statuses include *Pending*, *Step 1*, *Step 2*, *Step 3*, *Done*, *Acknowledged*, *Resolved*, or *Repeating Step 3*.
- § **Value.** Displays the logged value that caused the item to go out of threshold.
- § **Comment.** Displays any comments entered by the user or the system at the time the item was updated.
- § **Entry time.** Displays the time the item was updated.
- § **Duration.** Displays how long the item spent in the displayed state after it went out of threshold.

Updating Alert Center items

When a monitored device property begins to operate outside of the defined threshold, it appears as an item in a threshold dashboard report on the Alerts Home page. You can update items to either indicate that the issue is known, or remove them from the dashboard report.

To update an item:

- 1 In a threshold dashboard report, click a device name. The Alert Center Item Details dialog appears.

The dialog box is titled "Alert Center Item Details" and contains two main sections: "Item details" and "Update item(s)".

Item details:

- Item icon: A small icon representing a device or server.
- Item name: [Redacted]
- Created by: Performance Disk Utilization Exceeds
- Value: 95%
- Aspect: C:\
- Value: 99.6 %
- Current state: Out of threshold
- Notification progress: Pending
- Created on: April 02, 2015 11:08 PM

Update item(s):

At the top of this section is a dropdown menu set to "Acknowledge". To its right, a note states: "Acknowledged items are being dealt with. Notifications will continue to be sent. The items still appear in the report."

Below the dropdown are four radio button options:

- ☒ Apply to this item.
- ☐ Apply to any items created at the same time as this item
- ☐ Apply to any items older than hours
- ☐ Apply to all items in this threshold

At the bottom of the "Update item(s)" section is a text area labeled "Update comments:".

The dialog box has "OK" and "Cancel" buttons at the bottom right.

- 2 In the Update Items area, select how you would like to update the item(s).
 - § **Acknowledge.** Select to indicate that the issue with the item is known. Alert Center continues to send any related notifications regarding the item. The item continues to appear in the dashboard report.
 - § **Resolve.** Select to indicate that any actions required to address the item are complete. Notifications regarding the item stop. The item is removed from the dashboard report.
- 3 Select the item(s) to which you would like to apply the update. Options include:
 - § **Apply to this item.** Select this option to update only the currently viewed item.
 - § **Apply to any items created at the same time as this item.** Select this option to apply the update to any matching items that were created during the same poll.
 - § **Apply to any items older than ____ hours/minutes/days.** Select this option to apply the update to all alerts older than the time you select. This option is useful when one device fails and impacts numerous other devices, such as when attempting to ping devices on the other side of a failed router. Selecting to resolve all items that were

added at the same time as the router failure saves the time it would otherwise take to acknowledge each item individually.

§ **Apply to all items in this threshold.** Select this option to update any items that currently exist for this threshold.


- 4 After selecting the appropriate update, enter a brief comment in the **Update comment** boxes explaining the actions taken to address the issue.



Note: Comments are optional but recommended for your records.

- 5 Click **OK** to save changes.



Note: Items that have been acknowledged display a green check mark  next to their name on Alert Center Home threshold dashboard reports.

A note about notifications

Notifications are affected depending upon how you choose to acknowledge items. There are two basic scenarios when resolving items:

Single-item threshold

One item exists in a threshold and you acknowledge or resolve that item. The corresponding notification is also deleted and no more notifications for the item are sent.

Multiple-item threshold

Several items fall out of threshold at the same time and one notification is sent for the group of items. If you acknowledge or resolve only one item, a corresponding notification persists for all other unacknowledged and unresolved items.

However, if you select one item from the group, acknowledge or resolve it, and then select **Apply to any items created at the same time as this item**, the corresponding notification stops for all items that were created at the same time as the selected item.

Understanding resolving items - examples

When you mark an out-of-threshold item as resolved, the Alert Center ignores the item until the sample period does not include the time the item was resolved. This gives you one full sample period to fix the problem.

Example #1 - Marking an item as resolved without fixing the underlying problem will cause the item to appear again during the next sampling interval

Threshold: Disk Utilization exceeds 90%

Sample period: 1 day

Polling interval: 1 hour

Scenario:

Tuesday, 1:00 pm - Device exceeds disk utilization threshold and appears in the Items Report.

Tuesday, 1:05 pm - Item is marked as resolved, but no additional resources are provided to the device to solve the disk utilization issue.

Wednesday, 2:00 - During the next sample period, WhatsUp Gold checks the database and finds the device is out-of-threshold again. The device appears in the Items Report a second time.

Example #2 - Marking an item as resolved and fixing the issue before the next poll causes Alert Center to ignore the device during the next poll

Threshold: SNMP Trap exceeds 500 traps per hour

Sample period: 1 day

Polling interval: 30 minutes

Scenario:

Tuesday, 1:00 pm - Alert Center checks the WhatsUp Gold database for the previous 30 minutes and finds a device exceeding the threshold for SNMP traps.

Tuesday, 1:10 pm - You see the device listed as out-of-threshold, and you mark it resolved.

Tuesday, 1:30 pm - Alert Center checks the WhatsUp Gold database. The device is marked "resolved," so Alert Center ignores the device.

Tuesday, 1:35 pm - You turn off the SNMP trap agent on the device that is sending so many messages to the receiving device.

Tuesday, 2:00 pm - The device does not appear in the out of threshold items list.



Note: If you did not address the SNMP agent before the next poll, the device would again appear in the list of out of threshold devices.



Note: This method of resolving items does not apply to the WhatsUp Health threshold.

Filtering the Log report

You can filter the log report using the following methods:

Filter by date:

Use the **Date range** list at the top of the report to select a time frame for the report. By default, the report displays log entries for the previous hour.

Filter by severity level:

Use the **Filter by severity level** list to select a logging level for the report.

- § **No Filter** displays messages for every entry level.
- § **Critical** displays only critical messages.
- § **Error** displays only error messages.
- § **Warning** displays only warning messages.
- § **Information** displays only information messages.

Configuring Alert Center records to expire

You can configure the length of time to keep Alert Center data in your database on the Configure Database Record Expiration dialog.

To configure Alert Center data expiration settings:

- 1 From the Alert Center tab, click **Record Maintenance**. The **Configure Database Record Expiration** dialog appears.
- 2 Specify expiration settings:
 - § **Alert Center Log**. Enter a number of days and/or hours after which you would like to expire data for this report. Data that is expired is deleted from the database.
 - § **Alert Center Items**. Enter a number of days and/or hours after which you would like to expire data for this report.
- 3 Click **OK** to save changes.

Using the Alerts Home reports

In This Chapter

Using the Performance CPU threshold report.....	528
Using the Performance Custom threshold report.....	528
Using the Performance Disk threshold report.....	529
Using the Performance Interface threshold report.....	529
Using the Interface Errors and Discards threshold report.....	530
Using the Performance Memory threshold report.....	530
Using the Performance Ping Availability threshold report	530
Using the Ping Response Time threshold report	531
Using the SNMP Trap threshold report.....	531
Using the Syslog threshold report.....	532
Using the Windows Event Log threshold report.....	532
Using the Flow Monitor Conversation Partners threshold report..	532
Using the Flow Monitor Custom threshold report.....	533
Using the Flow Monitor Failed Connections threshold report.....	533
Flow Monitor Interface Traffic threshold report.....	534
Using the Flow Monitor Top Sender/Receiver threshold report	534
Using the Blackout Summary threshold report.....	534
Using the WhatsUp Health threshold report	535
Failover threshold report	535
Using the WhatsConfigured Threshold report.....	535
WhatsVirtual events threshold report.....	536
Using the All Wireless Thresholds report.....	536
Using the Wireless Access Point RSSI report	536
Using the Wireless Banned Client MAC Addresses report.....	537
Using the Wireless CPU report.....	537
Using the Wireless Client Bandwidth report.....	537
Using the Wireless Device Over Subscription report	537
Using the Wireless Excessive Rogue Alert report.....	538
Using the Wireless Memory report.....	538
Using the Wireless Rogue Access Point MAC Address Alert report	538
Using the Wireless Rogue Hidden SSID Alert report	538
Using the Wireless Rogue Specific SSID Alert report.....	538

Using the Performance CPU threshold report

This Alert Center Home report displays the following threshold information for a CPU utilization threshold:

- § **Device.** The network device that has gone out of the parameters of the CPU utilization threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- § **Number of CPUs.** Indicates the number of CPUs used to calculate the overall CPU utilization for the device that has gone out of the parameters of the CPU utilization threshold.

- or -

CPU. Indicates the CPU name that has gone out of the parameters of the CPU utilization threshold.

- § **Average Utilization**

- § **Device.** If the *device* option is selected for the Report Per CPU threshold option, this is the average CPU utilization (all CPUs combined). Therefore, if the average CPU performance of a quad-core CPU (an average of all CPU performance combined) exceeds the threshold, then the average utilization for the combined CPU is displayed and an alert is triggered.

- or -

- § **CPU.** If the *CPU* option is selected for the Report Per CPU threshold, this is the average utilization of a specific CPU. Therefore, if one of the CPUs on a quad-core CPU exceeds the threshold, then the average utilization for the individual CPU is displayed and an alert is triggered.



Tip: Click an average utilization value to view the *CPU Utilization* (on page 692) report for that device.

- § **Time alerted.** The time the Alert Center discovered the CPU out of threshold.

Using the Performance Custom threshold report

This Alert Center Home report displays the following threshold information for a custom performance monitor threshold:

- § **Device.** The network device that has gone out of the parameters of the custom performance monitor threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Custom performance monitor.** The specific custom performance monitor on this device that has gone out of the parameters of this threshold.

- § **Value.** The value of the custom performance monitor.
- § **Time alerted.** The time the Alert Center discovered the monitor out of threshold.

Using the Performance Disk threshold report

This Alert Center Home report displays the following threshold information for a disk utilization or free space threshold:

- § **Device.** The network device that has gone out of the parameters of the disk utilization or free space threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- § **Disk.** The disk that has gone out of the parameters of the disk utilization or free space threshold.
- § **Average utilization.** The average utilization of the disk or free space available during the sample time period.



Tip: Click an average utilization value to view the *Disk Utilization* (on page 694) report for that device.

- § **Time alerted.** The time the Alert Center discovered the disk utilization or free space out of threshold.

Using the Performance Interface threshold report

This Alert Center Home report displays the following threshold information for an interface utilization threshold:

- § **Device.** The network device that has gone out of the parameters of the interface utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Interface.** The specific interface that has gone out of the parameters of the interface utilization threshold.
- § **Average utilization.** The average utilization of the interface during the sample time period.



Tip: Click an average utilization value to view the *Interface Utilization* (on page 700) report for that device.

- § **Time alerted.** The time the Alert Center discovered the interface was out of threshold.

Using the Interface Errors and Discards threshold report

This Alert Center Home report displays the following threshold information for inbound and outbound device interface discards or errors response time thresholds.

§ **Device.** The network device that has gone out of the threshold parameters.



Tip: Click a device to view the Alert Center Item Details for that device.

§ **Interface.** The specific interface on which the inbound and/or outbound interface discards or errors response time is out of threshold.

§ **Discards or Errors.** The number of inbound and/or outbound interface discards or errors per minute during the sample time period.



Tip: Click an average response time to view the *Ping Response Time* (on page 706) report for that device.

§ **Time Alerted.** The time the Alert Center discovered the inbound and outbound interface discards or errors out of threshold.

Using the Performance Memory threshold report

This Alert Center Home report displays the following threshold information for a memory utilization threshold:

§ **Device.** The network device that has gone out of the parameters of the memory utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

§ **Memory.** The specific memory that has gone out of the parameters of the memory utilization threshold.

§ **Average utilization.** The average utilization of the memory during the sample time period.



Tip: Click an average utilization value to view the *Memory Utilization* (on page 696) report for that device.

§ **Time alerted.** The time the Alert Center discovered the memory out of threshold.

Using the Performance Ping Availability threshold report

This Alert Center Home report displays the following threshold information for a ping availability threshold.

§ **Device.** The network device that has gone out of the parameters of the ping availability threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- § **Interface.** The specific interface on which the ping packet loss is occurring.
- § **Percent Packet Loss.** The percentage of packets lost during the sample time period.



Tip: Click a packet loss value to view the *Ping Availability* (on page 704) report for that device.

- § **Time Alerted.** The time the Alert Center discovered the ping availability out of threshold.

Using the Ping Response Time threshold report

This Alert Center Home report displays the following threshold information for a ping response time threshold.

- § **Device.** The network device that has gone out of the parameters of the ping response time threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Interface.** The specific interface on which the ping response time is out of threshold.
- § **Response Time Average.** The average ping response time during the sample time period.



Tip: Click an average response time to view the *Ping Response Time* (on page 706) report for that device.

- § **Time Alerted.** The time the Alert Center discovered the ping response time out of threshold.

Using the SNMP Trap threshold report

This Alert Center Home report displays the following threshold information for an SNMP Trap threshold.

- § **Device.** The network device that has gone out of the parameters of the SNMP trap threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Trap.** The specific trap that has gone out of the parameters of the threshold.
- § **Trap Count.** The number of traps received for this specific trap during the sample time period.



Tip: Click a trap count value to view the *SNMP Trap Log* (on page 731) for that device.

- § **Time Alerted.** The time the Alert Center discovered the number SNMP traps out of threshold.

Using the Syslog threshold report

This Alert Center Home report displays the following threshold information for a Syslog threshold.

- § **Device.** The device that has gone out of the parameters of the Syslog threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Syslog.** The specific Syslog that has gone out of the parameters of the threshold.
- § **Message Count.** The number of Syslog messages received for that specific Syslog.



Tip: Click a message count value to view the *Syslog* (on page 732) report for that device.

- § **Time Alerted.** The time the Alert Center discovered the number of Syslog messages out of threshold.

Using the Windows Event Log threshold report

This Alert Center Home report displays the following threshold information for a Windows Event threshold.

- § **Device.** The network device that has gone out of the parameters of the SNMP trap threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Windows Event.** The specific Windows event that has gone out of the parameters of the threshold.
- § **Windows Event Count.** The number of Windows events received for this specific event type during the sample time period.



Tip: Click an event count value to view the *Windows Event Log* (on page 733) for that device.

- § **Time Alerted.** The time the Alert Center discovered the number of Windows events out of threshold.

Using the Flow Monitor Conversation Partners threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor conversation partners threshold.

- § **Host.** The host that has gone out of the parameters of the conversation partners threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Conversation Partners.** The number of conversation partners sending or receiving data with the host.



Tip: Click a conversation partners value to view the Interface Details report.

- § **Time Alerted.** The time the Alert Center discovered the host's number of conversation partners out of threshold.

Using the Flow Monitor Custom threshold report

This Alert Center Home report displays the following threshold information for a Flow custom threshold.

- § **Host.** The Flow Monitor host that has gone out of the parameters of the custom threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Bytes.** The number of bytes transferred.



Tip: Click a bytes value to view the Interface Details report.

- § **Time Alerted.** The time the Alert Center discovered the number of bytes out of threshold.

Using the Flow Monitor Failed Connections threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor failed connections threshold.

- § **Host.** The host that has gone out of the parameters of the failed connections threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Failed connections.** The number of failed connections the host has sent or received.



Tip: Click a failed connections value to view the Interface Details report.

- § **Time Alerted.** The time the Alert Center discovered the host's number of failed connections out of threshold.

Flow Monitor Interface Traffic threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor interface traffic threshold.

§ **Interface** displays the source interface over which traffic is transmitting.



Tip: Click a host to view the Alert Center Item Details for that interface.

§ **Interface traffic** displays the amount of traffic that has been transmitted over the sample time period.



Tip: Click an interface value to view the Interface Details report.

§ **Time Alerted** displays the time Alert Center discovered the interface's traffic amount out of threshold.

Using the Flow Monitor Top Sender/Receiver threshold report

This Alert Center Home report displays the following threshold information for the Flow Monitor top sender/receiver threshold.

§ **Host.** The host that has gone out of the parameters of the top sender/receiver threshold.



Tip: click a device to view the Alert Center Items Report for that device.

§ **Bytes transferred.** The number of bytes sent or received by a host.



Tip: Click a bytes value to view the Interface Details report.

§ **Time Alerted.** The time the Alert Center discovered the host's total number of bytes sent or received out of threshold.

Using the Blackout Summary threshold report

This Alert Center Home report displays the following threshold information for a blackout summary threshold.

§ **Device.** The device for which the action would have been triggered.

§ **Action.** The action that was not fired due to the blackout.

§ **Occurrences.** The number of times the action would have fired had the action not been in a blackout period.



Tip: Click an entry in the **Occurrences** column to view the *Blackout Summary Log* (on page 736).

- § **Time Alerted.** The time the Alert Center was alerted; Alert Center is notified of action activity when the blackout period ends.

Using the WhatsUp Health threshold report

This Alert Center Home report displays the following threshold information for a WhatsUp Health threshold.

- § **System Aspect.** The aspect of your system that has gone out of threshold. For example, Flow service, Total expired records, or WUG service.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Value.** The length of time in which the service has met the threshold parameters.
- § **Help Link.** Click this link for a list of ways you can resolve problems associated with the out of threshold item.
- § **Time Alerted.** The time the Alert Center discovered the system aspect out of threshold.

Failover threshold report

This Alert Center Home report displays the following threshold information for a Failover threshold.

- § **Source.** The machine on which the failover event took place.



Tip: Click a device to view the Alert Center Item Details for that device.

- § **Category.** The category of activity and message; either information or error.
- § **Message.** The message generated as a result of the failover event.



Tip: Hover over a message with your mouse to view the message in its entirety.



Tip: Click an entry in the Message column to view the *General Error Log* (on page 729).

- § **Time Alerted.** The time the Alert Center discovered the failover event.

Using the WhatsConfigured Threshold report

This Alert Center Home report displays the following threshold information about a WhatsConfigured task.

- § **Description.** Describes the task threshold.
- § **Device.** The device where the WhatsConfigured task ran.
- § **Configuration result.** The WhatsConfigured task result.
- § **Time Alerted.** The time Alert Center received the tasks configuration results.

WhatsVirtual events threshold report

The WhatsVirtual events threshold report displays events collected from the vCenter server that are of the type selected in the threshold definition. The events appear in reverse chronological order, so that the last event received appears at the top of the list.

- § **Target.** Displays the virtual server, host or virtual device that was the target of the event. The display format is either *<Datacenter - VMware Host name - virtual machine name>*, or *<vCenter server name>*.
- § **User.** Displays the user that initiated the event.
- § **Message.** Displays the message received from the vCenter server that describes the event.
- § **Date.** Displays the date and time that the event was received by the Alert Center.



Note: The WhatsVirtual events threshold can be created for any of the event groups that WhatsVirtual can collect from the vCenter server.

Using the All Wireless Thresholds report

The Alert Center Home report displays all active wireless threshold reports in dashboard format when the Wireless filter is applied. The wireless threshold report filter options are:

- § *Wireless Access Point RSSI* (on page 536)
- § *Wireless Banned Client MAC Addresses* (on page 537)
- § *Wireless Client Bandwidth*
- § *Wireless CPU* (on page 537)
- § *Wireless Device Over Subscription* (on page 537)
- § *Wireless Excessive Rogues* (on page 538)
- § *Wireless Memory* (on page 538)
- § *Wireless Rogue Access Point MAC Addresses* (on page 538)
- § *Wireless Rogue Hidden SSID* (on page 538)
- § *Wireless Rogue Specific SSID* (on page 538)
- § *Wireless Rogue Unknown* (on page 539)

Using the Wireless Access Point RSSI report

The Alert Center Home report displays the following threshold information when the Wireless Access Point RSSI filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **RSSI%.** Displays the percentage when the average RSSI exceeds the configured percentage for more than the specified time range. The default threshold percentage is 20%.

- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Banned Client MAC Addresses report

The Alert Center Home report displays the following threshold information when the Wireless Banned Client MAC Address Alert filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the banned MAC address associated with the device that triggered the alert.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless CPU report

The Alert Center Home report displays the following threshold information when the Wireless CPU filter is applied:

- § **Device.** Displays the name of the device.
- § **CPU.** Displays the type of CPU for the selected device.
- § **Average Utilization.** Displays the average wireless CPU utilization percentage for the selected time interval when utilization exceeds the selected utilization threshold.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Client Bandwidth report

The Wireless Client Bandwidth report displays the following threshold information when the Wireless Client Bandwidth filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the banned MAC address associated with the device broadcasting SSIDs in the specified time interval.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Device Over Subscription report

The Alert Center Home report displays the following threshold information when the Wireless Access Point Over Subscription filter is applied:

- § **Device.** Displays the name of the device.
- § **Number of Clients.** Displays the average number of clients over the selected time period that have run on the device since the threshold was initially measured. The client average is rounded to two decimal places.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Excessive Rogue Alert report

The Alert Center Home report displays the following threshold information when the Wireless Excessive Rogue Alert filter is applied:

- § **Device.** Displays the name or IP address of the access point hosting one or more potential rogue devices depending on the threshold configuration.
- § **Number of Clients.** Displays the number of potential rogues seen on the displayed access point.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Memory report

The Alert Center Home report displays the following threshold information when the Wireless CPU filter is applied:

- § **Device.** Displays the name of the device.
- § **Memory.** Displays the available memory for the selected device.
- § **Average Utilization.** Displays the average wireless memory utilization percentage for the selected time interval when utilization exceeds the selected utilization threshold.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Access Point MAC Address Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Access Point MAC Address Alert filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the rogue MAC address associated with the device that triggered the alert.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Hidden SSID Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Hidden SSID filter is applied:

- § **Device.** Displays the name of the device.
- § **MAC Address.** Displays the MAC address associated with the device.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Specific SSID Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Specific SSID filter is applied:

- § **Device.** Displays the name of the device.

- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the MAC address associated with the device.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Unknown SSID Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Unknown SSID filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the MAC address associated with the device.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Configuring notifications

In This Chapter

Alert Center Percent Variables.....	540
Using Alert Center Notification Policy options	542
Configuring a notification policy.....	542
Configuring an Alert Center email notification	544
Configuring an Alert Center SMS Direct notification.....	546
Configuring an Alert Center SMS Action notification.....	548
Configuring email notification message settings.....	550
Stopping a running notification policy.....	551
Using the E-mail Action.....	552
Using the SMS Direct Action.....	552
Using the SMS Action.....	552

Alert Center Percent Variables

The Email, SMS, and SMS Direct Actions can include three categories of percent variables in Alert Center notification message:

- § Threshold
- § Notification Policy
- § System

Use Alert Center percent variables in the Alert Center message body for SMS Direct and SMS action notifications, and in the subject line of Email notifications.

Threshold percent variables

Name	Description
%AlertCenter.Threshold.ID	The threshold ID listed in the ProActiveAlert table.
%AlertCenter.Threshold.Name	The threshold name.
%AlertCenter.Threshold.Description	The threshold description.
%AlertCenter.Threshold.PollingInterval	The threshold polling interval.
%AlertCenter.Threshold.TotalItems	The total new and current items out of threshold.
%AlertCenter.Threshold.TotalNewItem	The total of newly alerted items.

%AlertCenter.Threshold.TotalCurrentItems	The total of existing items out of threshold (not including new items).
%AlertCenter.Threshold.TotalMonitoredItems	The count of items that can be evaluated in the threshold, i.e. there are 22 devices that have a Disk Performance Monitor configured.
%AlertCenter.Threshold.TotalAutoResolvedItems	The number of items automatically resolved.
%AlertCenter.Threshold.NewItemNames	The display name of each new item in an alert.
%AlertCenter.Threshold.CurrentItemNames	The display name of each current item in an alert.

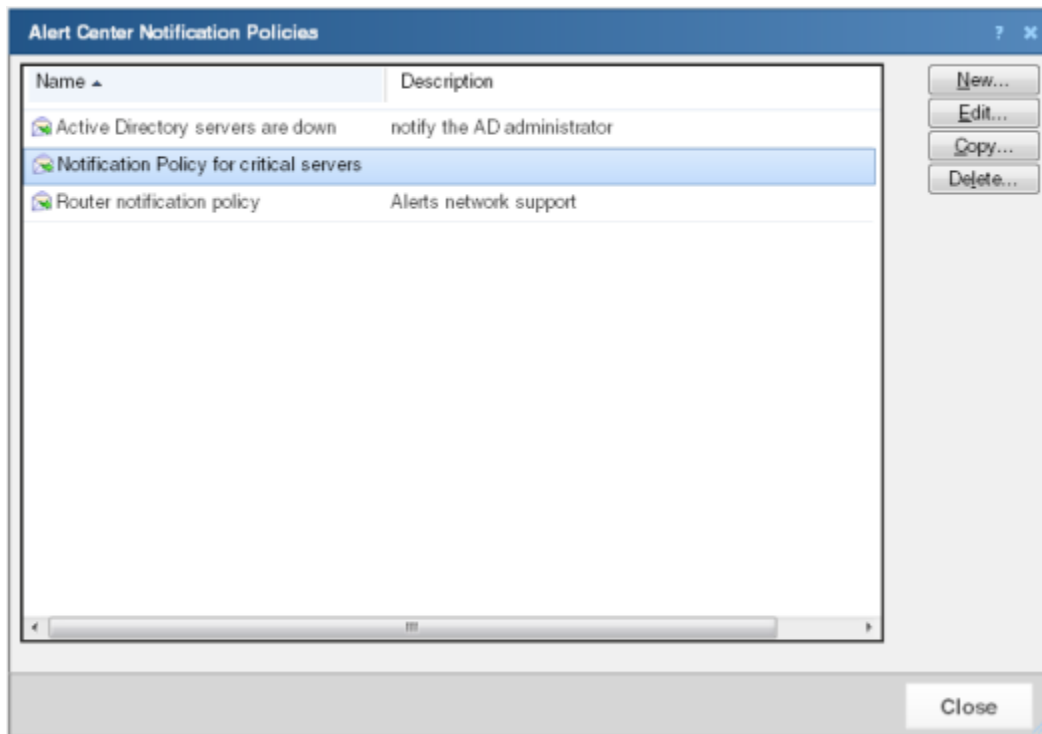
Notification policy percent variables

Name	Description
%AlertCenter.NotificationPolicy.ID	The notification policy ID.
%AlertCenter.NotificationPolicy.Name	The notification policy name.
%AlertCenter.NotificationPolicy.Description	The notification policy description.
%AlertCenter.NotificationPolicy.Recipients	The list of actions included in the policy.
%AlertCenter.NotificationPolicy.NextEscalationTime	When the next step is to be sent.
%AlertCenter.NotificationPolicy.EscalationStep	The current escalation step.

System percent variables

Name	Description
%System.Date	The current system date.
%System.Time	The current system time.

Using Alert Center Notification Policy options



To access notification policy options:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Policies**. The Alert Center Notification Policies dialog appears.
 - § Click **New** to configure a new policy.
 - § Select a policy, then click **Edit** to modify the policy configuration.
 - § Select a policy, then click **Copy** to make a duplicate of the selected policy.
 - § Select a policy, then click **Delete** to remove the policy from the dialog.



Caution: When you delete a policy from the list, it is removed from any threshold to which it is assigned.

Configuring a notification policy



Note: It is not required that you select a notification policy for use with every threshold. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report with the out of threshold items appears on the Alerts Home page.

To create a notification policy:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Policies**. The Alert Center Notification Policies dialog appears.

- 3 Click **New**. The New Alert Center Notification Policy dialog appears.

Edit Alert Center Notification Policy
?
x

Name:

Description:

Select which notifications will be delivered by each step of this policy:

Notification ▲	Type	Step 1	Step 2	Step 3	Blackout Policy
Test Action	SMS Action	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Business Hours (Te: ▼
Test Action 2	SMS Action	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	On Call Work Week ▼
Test Action 3	SMS Action	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	(None) ▼

Escalation Steps

Step 2 begins after the notification starts

Step 3 begins after the notification starts

☐ Repeat step 3 every until the notification is stopped

Show me a graph of this notification policy in action

OK

Cancel

- 4 Complete the identifying information for the policy.
 - § **Name.** Type a name for the notification policy. The name identifies the policy in the Alert Center Notification Policies dialog.
 - § **Description.** Enter a description of the policy. The description appears next to the policy name in the Alert Center Notification Policies dialog.
- 5 Select the notifications you would like delivered for each of the three steps in the policy. You can select multiple notifications for each policy step. To select a notification, click the boxes for the step of the policy that you would like the notification to be sent. For example, if you would like an email sent to Bob for the policy's first step, select the **Step 1** boxes for the Email Bob notification. Continue the same for Step 2 and Step 3. Step 1 of the notification policy begins as soon as an item falls out of threshold. You can specify when steps 2 and 3 begin in the Escalation Steps section of the dialog. If you do not see


an appropriate notification, or if the list is empty, click browse (...) to open the Notification Library and configure a new notification.

- 6 If desired, use the drop-down list to select and apply a configured blackout policy for any individual notification. If an applied blackout policy is in effect:
 - a) Notifications for the threshold will resume after that blackout policy ends.
 - b) The subsequent action in the notification policy will continue to fire.
- 7 Select the how the policy notifications proceed after Step 1 in the **Escalation Steps** section.
 - § Specify a start time for steps 2 and 3 of the policy. By default, step 2 is set to begin 1 hour after the first notification occurs, and step 3 is set to begin 2 hours after the first notification.
 - § You can choose to repeat step 3 of the policy at a regular interval until the notification is stopped. By default, the policy is set to repeat step 3 every hour until the notification is stopped.



Note: In order for this repeat function to work properly, step 3 must be enabled for at least one notification in the policy.



Tip: You can view a graph of the notification policy in action by clicking  **Show me a graph of this notification policy in action.**

- 8 Click **OK** to save changes.

Configuring an Alert Center email notification

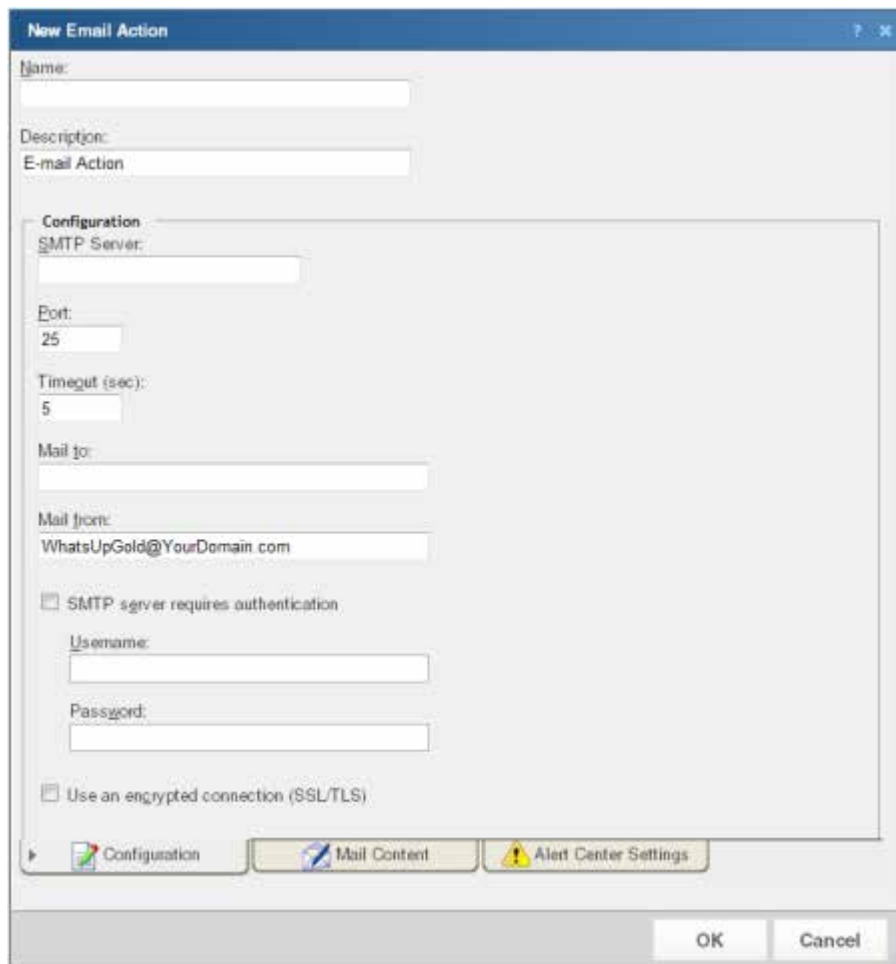
Alert Center email notifications and WhatsUp Gold email actions use the same configuration dialog.

For more information about Email Actions, see *Using the Email Action* (on page 552).

To configure an email notification:

- 1 Click the **Alert Center** tab, then click **Notification Library**. The Alert Center Notification Library dialog appears.
- 2 Click **New**. The Select Notification Type dialog appears.

- 3 Select **E-mail Action**, then click **OK**. The New Email Action dialog appears.



- 4 Complete the appropriate information in the dialog box.
 - § **Name.** Type a name for the action. This name identifies the action in the Notification Library.
 - § **Description.** Enter a few words to describe the action. This description displays beside the action name in the Notification Library.
- 5 Click the **Alert Center** tab to complete the appropriate Alert Center settings for the Email notification.

The **Alert Center Settings** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

- § **Alert Center Message Subject.** Enter a subject for the message. This text appears as the subject in the email that is sent by the Alert Center notification. This subject can include percent variables.



Tip: To include *Alert Center percent variables* (on page 540), right click inside the above boxes.

- § **Alert Center Link.** Select **Include hyperlink to Alert Center in the email content** to include a link to the Alerts Home page in the email message sent by the Alert Center notification.
- § **Use HTTP or Use HTTPS.** Select the appropriate protocol to use in the link address.
- § **Use dynamic address or Use static hostname or IP address.** If you select to use the dynamic address, WhatsUp Gold automatically renders the hostname or IP address at the time the action runs.
- § **Hostname or IP address.** If you selected Use static hostname or IP address, type the server address in the boxes.
- § **Port.** Specify the specific port to include in the link address.



Important: The address you enter here must be the exact address of the Alerts Home page to which you want to connect. Verify the address and enter its exact contents in the above options.



Note: Click the **Configuration** tab to edit the email action settings and specify a destination address for the notification.

- 6 Click **OK** to save changes.

Configuring an Alert Center SMS Direct notification

Alert Center SMS Direct notifications and WhatsUp Gold SMS Direct actions use the same configuration dialog.

For more information about SMS Direct Actions, see Using the SMS Direct Action.

To configure an SMS Direct notification:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Library**.

- 3 Click **New**. The Select Notification Type dialog appears.
- 4 Select **SMS Direct**. The New SMS Direct Action dialog appears.

New SMS Direct Action

Name:

Description:

Phone Number:

COM Port:

Alert Center Message

```
WhatsUp Gold Alert Center: Threshold '%
AlertCenter.Threshold.Name' has %
AlertCenter.Threshold.TotalNewItem new
items. %System.Date - %System.Time
```

Right Click in the message box for percent variable support.

- 5 Specify or select the appropriate information in the dialog boxes.
 - § **Name**. Enter a name for this notification. This name is for your reference only and will never be displayed to the notification recipient.
 - § **Description**. Create or modify the description. This description appears in the Action Library and is for your reference only.
 - § **Phone number**. Type the cell phone number(s) of the intended SMS message recipients.



Note: All non-numeric characters such as "-" and ".", will be ignored.



Note: There is a 2,000 character limit in this boxes, so you can enter many numbers.

- § **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.

- 6 Select the **Alert Center Message** tab to specify the appropriate settings for the SMS notification 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 necessary percent variable codes. Keep in mind that using percent variables can greatly increase the character count.



Tip: To enter *Alert Center percent variables* (on page 540), right-click inside the message boxes.



Note: The size limit for the message is 160 characters (140 bytes).

- 7 Click **OK** to save changes.
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.



Tip: To enter Alert Center percent variables, right click inside the message boxes.



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.).

- 8 Click **OK** to save changes.

Configuring an Alert Center SMS Action notification

Alert Center SMS notifications and WhatsUp Gold SMS actions use the same configuration dialog.

For more information about SMS Actions, see Using the SMS Action.

To configure an SMS notification:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Library**. The Alert Center Notification Library dialog appears.

- 3 Click **New**. The Select Notification Type dialog appears.
- 4 Select **SMS Action** and click **OK**. The New SMS Action dialog appears.



- 5 Specify or select the appropriate information in the dialog boxes.
 - § **Name**. Type a unique display name to identify the SMS notification.
 - § **Description**. Type a short description of the action. This description is displayed in the Action Library along with the action name.
 - § **Country**. Select the country for the SMS provider from the list.
 - § **Provider**. Select the appropriate SMS provider from the list.



Note: If the provider list is incomplete and/or incorrect, you can click browse (...), then click **New** or **Edit** to add or edit an SMS provider.

- § **Mode**. Select either Email or Dialup, depending on the Provider configuration in the system.
- § **Email to**. If Email is selected as the Mode, type the SMS device email address.
- § **Phone Number**. If Dialup is selected as the Mode, type 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 boxes, so you can enter many numbers.



Note: Non-numeric characters such as "-" and "." are ignored.

- 6 In the **Alert Center Message** boxes, specify the options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.
Enter a text message plus any necessary percent variable codes. Keep in mind that using percent variables can greatly increase the character count.



Tip: To add *Alert Center percent variables* (on page 540), right-click inside the message boxes and make selections from the lists.



Note: The size limit for the message is 160 characters (140 bytes).

- 7 Click **OK** to save the changes.

Configuring email notification message settings

To configure email notification message settings:

- 1 Click the **Alert Center** tab.
- 2 Click **Email Notification Message Settings**. The Configure Email Notification Message dialog appears.

- 3 Select or specify the appropriate settings:
 - § **Maximum newly alarmed items.** Enter the maximum number of new, previously unreported alerts to display in notification email messages.
 - § **Show currently alarmed items.** Select to include previously reported items that are still generating alerts in addition to newly alarmed items.
 - § **Maximum currently alarmed items.** Enter the maximum number of previously reported alerts to display in notification email messages.
- 4 Click **OK** to save changes.

Stopping a running notification policy

After resolving a problem, you can stop proceeding steps in a notification policy using the Stop Notification dialog.

To stop a notification policy:

- 1 Click the **Alert Center** tab.
- 2 Click **Running Notification Policies**. The Alert Center Running Notification Policies page appears.
- 3 Next to the notification policy that you want to stop, click **Stop notification**. The Stop Notification dialog appears.



Tip: You can send an optional message to the recipients listed in this dialog to notify them that you have resolved the problem and are stopping the notification policy from this point forward.



If you choose to do so, select **Send a message to the recipients listed above**, and enter a **Subject** and **Body** for the message.

- 4 Click **Stop** to prevent further steps in the notification policy from firing.

The screenshot shows the 'Stop Notification' dialog box. The title bar is blue with a question mark and a close button. The main content area is white. At the top, it says 'Notification triggered by: CPU Utilization exceeds 10%'. Below this is a section titled 'Finished Notifications' with a sub-header 'The following notifications have been sent successfully:' and a list item 'Email support' with a checked checkbox. Another section titled 'Notify Recipients' contains a checkbox 'Send a message to the recipients listed above' which is currently unchecked. Below the checkbox are two text input fields: 'Subject:' with the text 'Stopping further notifications for CPU Utiliza' and 'Body:' with a large empty text area. At the bottom of the dialog are two buttons: 'Stop' and 'Cancel'.



Note: SMS message recipients only receive the message body contents; the message subject is not included.

Using the E-mail Action

The E-mail Action sends an SMTP mail message to a specific email account. An E-mail Action can also be used as an email 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 email notification* (on page 544).

Using the SMS Direct Action

The SMS Direct Action send SMS messages directly through an SMS modem, unlike SMS actions, which use email gateways or dial-up modems. For more information, see *Configuring an Alert Center SMS Direct Notification* (on page 546). If you want to send an SMS message and do not have an SMS modem, see *Configuring an Alert Center SMS Action notification* (on page 548).

Using the 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. 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 SMS Action notification* (on page 548).

Configuring thresholds

In This Chapter

Configuring Alert Center thresholds.....	553
Selecting threshold devices.....	554
Configuring performance thresholds.....	558
Configuring passive thresholds	573
Configuring Flow Monitor thresholds.....	580
Configuring system thresholds	593
Configuring wireless thresholds.....	601

Configuring Alert Center thresholds

To configure any of the five types of Alert Center thresholds:

- 1 From the web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Select the type of threshold you want to configure. You can select from the following thresholds:
 - § Performance
 - § *CPU* (on page 558)
 - § *Custom* (on page 559)
 - § *Disk* (on page 561)
 - § *Interface* (on page 563)
 - § *Interface Errors and Discards* (on page 565)
 - § *Memory* (on page 567)
 - § *Ping Availability* (on page 569)
 - § *Ping Response Time* (on page 570)
 - § Passive
 - § *SNMP trap* (on page 573)
 - § *Syslog* (on page 575)
 - § *Windows Event Log* (on page 577)
 - § Flow Monitor
 - § *Conversation Partners* (on page 583)
 - § *Custom Threshold* (on page 584)

- § *Failed Connections* (on page 586)
 - § *Interface Traffic* (on page 588)
 - § *Top Sender/Receiver* (on page 590)
 - § System
 - § *Blackout Summary* (on page 593)
 - § *VMware* (on page 595) (available if licensed)
 - § *Failover* (available if licensed)
 - § *WhatsUpHealth* (on page 598)
 - § Wireless (available if licensed)
 - § *Wireless Access Point RSSI* (on page 601)
 - § *Wireless Banned Client MAC* (on page 602)
 - § *Wireless CPU* (on page 603)
 - § *Wireless Device Over Subscription* (on page 605)
 - § *Wireless Excessive Rogue* (on page 606)
 - § *Wireless Memory* (on page 606)
 - § *Wireless Rogue Access Point MAC* (on page 607)
 - § *Wireless Rogue Hidden SSID* (on page 608)
 - § *Wireless Rogue Specific SSID* (on page 609)
 - § *Wireless Rogue Unknown SSID* (on page 609)
- 3 Click **OK** to save changes.

Selecting threshold devices

For each performance or passive threshold that you configure you can include a list of devices or device group exceptions to which the threshold will apply. If you choose not to select specific devices to include or to exclude, by default, the threshold monitors all devices on which the applicable monitor is enabled.

To select threshold devices:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.

- 4 Select the desired threshold type, then click **OK**. The dialog where you configure threshold properties appears.

New CPU Utilization Threshold

Name:

Threshold
This threshold will alert when:
CPU utilization **exceeds** %
for more than **minutes**

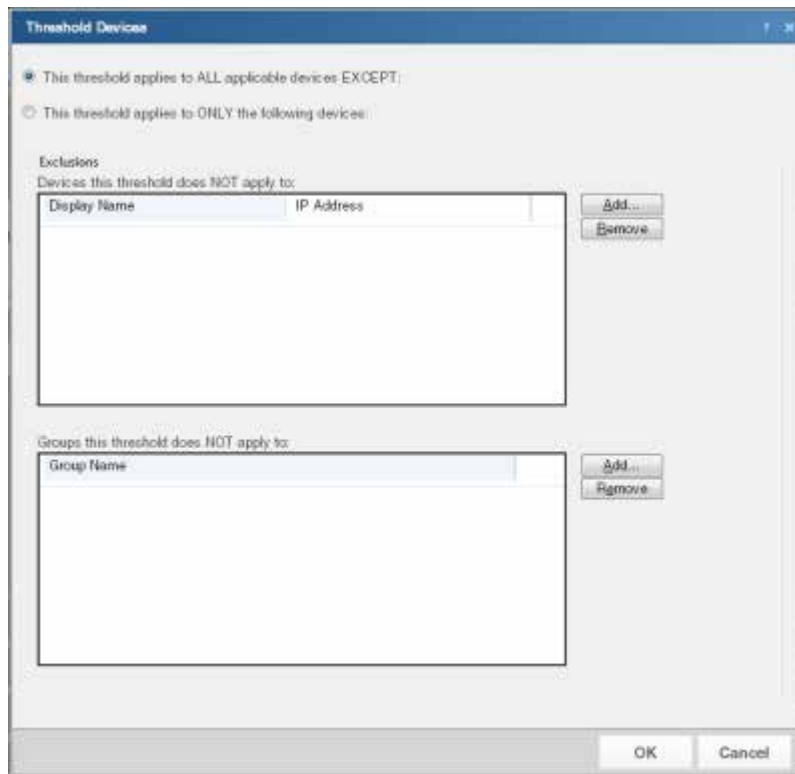
Devices to Monitor
Monitor all devices with CPU performance data by default
Select...

Notification
(No policy)

Threshold Check
Check threshold every minutes.
☐ Automatically resolve items no longer out of threshold

OK **Cancel**

- 5 In the **Devices to Monitor** section, click **Select**. The Threshold Devices dialog appears.



- 6 Select the devices to which the threshold will apply:
- § To apply the threshold to all devices except for the device(s) or group of devices that you specify, select **This threshold applies to ALL applicable devices EXCEPT**. After you select this option, you will choose the devices to exclude from the threshold.
 - § To apply the threshold to only the device(s) or group of devices that you specify, select **This threshold applies to ONLY the following devices**. After you select this option, you will choose the devices to include in the threshold.
- 7 Select the specific devices to include or exclude from the threshold.
- § To specify a device to exclude or include in the threshold, in the upper section of the dialog, click **Add**.
 - § To specify a group of devices to exclude or include in the threshold, in the lower section of the dialog, click **Add**.



Note: You can select Dynamic Groups.



Note: When you add a device group to the list of exceptions, all devices within the device group, as well as any sub-groups contained within the group (and devices in those sub-groups), are excluded from the threshold. Additionally, if you add a device group to the list of exceptions that contains a device shortcut, then that device is excluded from the threshold—even if that device is also a member of another group which is not part of the list of excluded groups.



Tip: To delete a device or device group from the list, select it, then click **Remove**.

- 8 Click **OK** to save changes.

Configuring performance thresholds

In This Chapter

Configuring performance thresholds.....	558
Configuring a CPU utilization threshold	558
Configuring a custom performance monitor threshold.....	559
Configuring a disk utilization threshold.....	561
Configuring an interface utilization threshold.....	563
Configuring an interface errors and discards threshold.....	565
Configuring a memory utilization threshold	567
Configuring a ping availability threshold.....	569
Configuring a ping response time threshold.....	570

Configuring performance thresholds

Alert Center performance thresholds notify you about WhatsUp Gold performance monitors that have exceeded or dropped below threshold limits. You can create the following performance threshold types:

- § *CPU* (on page 558)
- § *Custom Performance Monitor* (on page 559)
- § *Disk* (on page 561)
- § *Interface* (on page 563)
- § *Interface Errors and Discards* (on page 565)
- § *Memory* (on page 567)
- § *Ping Availability* (on page 569)
- § *Ping Response Time* (on page 570)

Configuring a CPU utilization threshold

To configure a CPU utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Performance CPU**, then click **OK**. The New/Edit CPU Utilization Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog box:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.

- § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when CPU utilization exceeds 90% for more than 30 minutes.
- § **Report per.** Select the the CPU utilization threshold monitor method, device or CPU option.
 - § **Device.** Select this option to calculate the threshold based on the average CPU load evaluated as a single device. Therefore, if the average CPU performance of a quad-core CPU (an average of all CPU performance combined) exceeds the threshold, then an alert is triggered.
 - § **CPU.** Select this option to calculate the threshold based on individual CPU load for the selected device. Therefore, if one of the CPUs on a quad-core CPU exceeds the threshold, then an alert is triggered.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a custom performance monitor threshold

To configure a custom performance monitor threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Custom**, then click **OK**. The New Custom Performance Monitor Threshold dialog appears.

New Custom Performance Monitor Threshold

Name:

Show: ☒ Global Monitors ☐ Device Specific Monitors

Custom performance monitor type:

Global Monitor Monitor Name

No global monitors of this type available...

Threshold

This threshold will alert when the custom performance monitor's average value 10 for more than 30 minutes

Devices to Monitor

Monitor all devices with this custom performance data by default

Notification

(No policy)

Threshold Check

Check threshold every 10 minutes

☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Show.** Select either **Global Monitors** or **Device Specific Monitors** for the custom performance monitor type that you choose.
 - § **Custom performance monitor type.** Select the custom performance monitor type from the menu. Select APC UPS, Printer, Active Script, SNMP, or WMI.
 - § **Monitor.** The configured monitors of the selected type. These are the monitors used to determine if the measured parameters have dropped below or exceeded threshold limits.



Note: When you select Global Monitors, this list is populated with custom performance monitors currently configured in the *Performance Monitor Library* (on page 452). When you select Device Specific Monitors, this list is populated with custom performance monitors currently configured for specific devices.

- § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the custom performance monitor average value exceeds 10 for 30 minutes.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a disk utilization threshold

To configure a disk threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Disk**, then click **OK**. The New/Edit Disk Utilization Threshold dialog appears.

Edit Disk Utilization Threshold

Name: PD free space

Threshold

The threshold will alert when:

disk free space falls below 40 GB

for more than 1 days

Devices to Monitor

Monitor all devices with disk performance data by default

Select...

Notification

(No policy)

Threshold Check

Check threshold every 5 minutes.

☐ Automatically resolve items no longer out of threshold

OK Cancel

- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold triggers an alert when disk utilization exceeds 95% for more than 1 day. In addition to disk utilization, this threshold can also be configured to alert when free space exceeds or falls below a specific value.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database for items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold.

Configuring an interface utilization threshold

To configure an interface utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Interface**, then click **OK**. The New Interface Utilization Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the threshold criteria variables and values. The default threshold is configured to alert when inbound or outbound utilization exceeds 90% for more than 60 minutes.
 - § **Devices to Monitor.** Click Select to choose the devices to which the threshold applies. By default, the threshold monitors all devices where the applicable monitor is enabled.
 - § **Notification.** Select the notification policy you would like to apply to this threshold. This policy kicks off when an item falls out of the threshold you configure above. If you do not see an appropriate threshold policy, or if the list is empty, browse (...) to the Notification Policy dialog to configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring an interface errors and discards threshold

To configure an interface utilization discard and error threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Interface Errors and Discards**, then click **OK**. The New/Edit Interface Error and Discard Threshold dialog appears.

New Interface Error and Discard Threshold

Name:

Threshold
The threshold will alert when either:

☐ Discards for interface traffic
exceed discards per minute
for more than minutes

☐ Errors for interface traffic
exceed errors per minute
for more than minutes

Devices to Monitor
Monitor all devices with interface error and discard data by default

Notification
(No policy)

Threshold Check
Check threshold every minutes.
☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the threshold criteria variables and values. You can choose to create a threshold based on discards, errors, or a combination of the two. The default threshold is configured to alert when inbound or outbound interface utilization exceeds 100 discards per minute for more than 20 minutes.
- and / or -
when errors for inbound or outbound interface utilization exceeds 100 errors per minute for more than 20 minutes.



Note: If you select both error and discard thresholds, each error and discard are reported as separate items (rows) in the dashboard report.

- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices where the applicable monitor is enabled.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters. The default threshold check is 10 minutes.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a memory utilization threshold

To configure a memory utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Memory**, then click **OK**. The New/Edit Memory Utilization Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when disk utilization exceeds 95% for more than 1 hour.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a ping availability threshold

To configure a ping availability threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Ping Availability**, then click **OK**. The New/Edit Ping Availability Threshold dialog appears.

New Ping Availability Threshold

Name:

Threshold
This threshold will alert when:
Ping availability average falls below %
for more than

Devices to Monitor
Monitor all devices with ping availability performance data by default

Notification
(No policy)

Threshold Check
Check threshold every minutes
☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when ping availability average falls below 95% for more than 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a ping response time threshold

To configure a ping response time threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Ping Response Time**, then click **OK**. The New Ping Response Time Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when ping response time average exceeds 2 ms for more than 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring passive thresholds

In This Chapter

Configuring passive thresholds	573
Configuring an SNMP trap threshold.....	573
Configuring a Syslog threshold.....	575
Configuring a Windows Event Log threshold.....	577

Configuring passive thresholds

Alert Center passive thresholds notify you when WhatsUp Gold passive monitors fall out of the parameters of the thresholds you configure. You can create three passive threshold types:

- § *SNMP trap* (on page 573)
- § *Syslog* (on page 575)
- § *Windows Event Log* (on page 577)

Several things to keep in mind when configuring thresholds for passive monitors:

- § Each Alert Center threshold is associated with a specific passive monitor. The passive monitor associated with the threshold you are creating must be assigned to at least one device. Otherwise, the threshold will not work.
- § When creating a passive threshold, you must select a passive monitor from a list to associate with the threshold. This list contains the passive monitors already configured in the Passive Monitor Library. These monitors are not necessarily assigned to devices, however. To determine which devices have passive monitors assigned to them, you can create a dynamic group. For more information, see *Configuring Dynamic Groups*.
- § It is not possible to monitor unsolicited traps using Alert Center.

Configuring an SNMP trap threshold

To configure an SNMP trap threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **SNMP Trap**, then click **OK**. The New SNMP Trap Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **SNMP Trap type.** Select the SNMP trap type from the list that you want to associate with this threshold. The list is populated with SNMP traps currently configured in the Passive Monitor Library.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of traps exceeds 500 in the past 60 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters. By default, the threshold check is set to every five minutes.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a Syslog threshold

To configure a Syslog threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Syslog**, then click **OK**. The New Syslog Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Syslog type.** Select the Syslog monitor to use with the threshold. This list is populated with Syslog monitors currently configured in the Passive Monitor Library.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of messages exceeds 500 in the past 60 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a Windows Event Log threshold

To configure a Windows Event Log threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Windows Event Log**, then click **OK**. The Windows Event Log Threshold dialog appears.

New Windows Event Log Threshold

Name:

Windows Event Log type:

Threshold
The threshold will alert when:
Number of events
in the past

Devices to Monitor
Monitor all devices sending Windows events by default

Notification

Threshold Check
Check threshold every
☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Windows event type.** Select the Windows Event Log monitor to use with this threshold. The list is populated with Windows Event Log monitors currently configured in the Passive Monitor Library.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of events exceeds 500 in the past 60 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK** to save the threshold settings.

Configuring Flow Monitor thresholds

In This Chapter

Configuring Flow Monitor thresholds.....	580
Selecting Flow Monitor threshold hosts.....	580
Configuring a conversation partners threshold	583
Configuring a Flow Monitor custom threshold	584
Configuring a failed connections threshold.....	586
Configuring a Flow Monitor Interface Traffic threshold	588
Configuring a top sender/receiver threshold.....	590

Configuring Flow Monitor thresholds

Alert Center Flow Monitor thresholds notify you on WhatsUp Gold Flow Monitor plug-in aspects that fall out of the parameters of the thresholds you create.

You can create five Flow Monitor threshold types:

- § *Flow Monitor Conversation Partners* (on page 583)
- § *Flow Monitor Custom Threshold* (on page 584)
- § *Flow Monitor Failed Connections* (on page 586)
- § *Flow Monitor Interface Traffic* (on page 588)
- § *Flow Monitor Top Sender/Receiver* (on page 590)

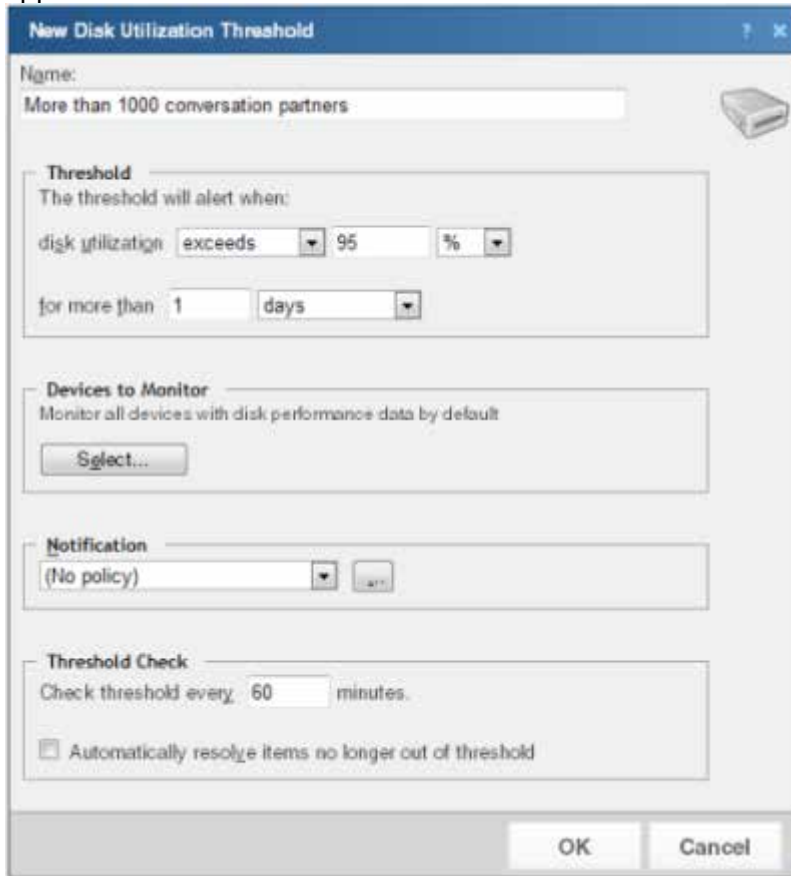
Selecting Flow Monitor threshold hosts

For each Flow threshold that you configure you can include a list of Flow Monitor groups, hosts, or a range of IP addresses to which the threshold will not apply.

To configure a list of Flow threshold exceptions:

- 1** Click the **Alert Center** tab.
- 2** Click **Threshold Library**. The Alert Center Threshold Library dialog appears.

- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select the desired Flow threshold type, then click **OK**. The threshold properties dialog appears.



The screenshot shows a Windows-style dialog box titled "New Disk Utilization Threshold". It contains several sections for configuring a threshold:

- Name:** A text field containing "More than 1000 conversation partners".
- Threshold:** A section with the text "The threshold will alert when:". It includes a dropdown menu set to "disk utilization", a value of "95", a unit dropdown set to "%", and a section for "for more than" with a value of "1" and a unit dropdown set to "days".
- Devices to Monitor:** A section with the text "Monitor all devices with disk performance data by default" and a "Select..." button.
- Notification:** A section with a dropdown menu set to "(No policy)" and a small "OK" button.
- Threshold Check:** A section with the text "Check threshold every" followed by a value of "60" and the word "minutes". Below this is a checkbox labeled "Automatically resolve items no longer out of threshold".

At the bottom right of the dialog are "OK" and "Cancel" buttons.

- 5 In the **Devices to monitor** section, click **Select**. The Threshold Hosts dialog appears.

- 6 Select the hosts to which the threshold applies.
- § To apply the threshold to all hosts except the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ALL hosts EXCEPT**. After you select this option, you will choose the hosts to exclude from the threshold.
 - § To apply the threshold to only the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ONLY the following hosts**. After you select this option, you will choose the hosts to include in the threshold.
- 7 Select the specific hosts to include or exclude from the threshold.
- § To specify a Flow Group to include or exclude from this threshold, in the upper section of the dialog, click **Add**.



Tip: To delete a Flow group, host, or IP range from the list, select it, and then click **Remove**.

- § To specify a single host or IP address to include or exclude from this threshold, enter a **Hostname or IP Address**, and then click **Add**.
 - § To specify an IP address range to include or exclude from this threshold, enter a **Start IP Address** and an **End IP Address**, and then click **Add**.
- 8 Click **OK** to save changes.

Configuring a conversation partners threshold

To configure a Flow Monitor conversation partners threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Click the menu, select **Flow Conversation Partners**, and then click **OK**. The New Flow Conversation Partners Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when a host has sent to or received from more than 1000 conversation partners in the past 15 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a time interval for Alert Center to check the WhatsUp Gold database for items that are out of the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they return to the parameters inside the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a Flow Monitor custom threshold

To configure a Flow Monitor custom threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Flow Monitor Custom Threshold**, then click **OK**. The New Flow Monitor Custom Threshold dialog appears.

The screenshot shows the 'New Flow Monitor Custom Threshold' dialog box. It contains the following fields and sections:

- Name:** A text input field.
- Description:** A text input field with a preview text: "Any host with ... that sent or received more than ... MB of traffic in the past 15 minutes".
- Threshold:** A section titled "This threshold will alert when:" containing three filter rows:
 - Select filter... matching [] and
 - Select filter... matching [] and
 - Select filter... matching []
 Below these is a condition: "sent or received" more than [] MB of data in the past: 15 minutes.
- Traffic to monitor:** A dropdown menu currently showing "All Flow Monitor Sources".
- Hosts to monitor:** A "Select..." button.
- Notification:** A dropdown menu currently showing "(No policy)".
- Threshold Check:** A section with "Check threshold every: 10 minutes" and a checkbox for "Automatically resolve items no longer out of threshold".
- Buttons:** "OK" and "Cancel" at the bottom right.

- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Description.** As you configure threshold criteria settings, the description automatically updates to include your selections.
 - § **Threshold.** Select the threshold filters and limits, and enter the values to use for each. You can define up to three filters for each Flow Monitor custom threshold.

 An example threshold involving multiple filters could state, "This threshold will alert when any host with Protocol matching TCP and Application matching pop3 sent or received more than 100 MB of data in the past 15 minutes."

 The default threshold time value is data in the past 15 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
 When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
 By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a failed connections threshold

To configure a Flow failed connections threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Flow Monitor Failed Connections**, then click **OK**. The New Flow Monitor Failed Connections Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is exceeded when when a host has sent or received more than 1000 failed connections in the past 15 minutes.



Note: WhatsUp Gold Flow Monitor can only find failed connections on sources that are not sending sampled data.

- § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold.

Configuring a Flow Monitor Interface Traffic threshold

To configure a Flow Monitor interface traffic threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Flow Monitor Interface Traffic**, then click **OK**. The New Flow Monitor Interface Traffic Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when incoming or outgoing interface traffic exceeds 90% for more than 60 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor sources from which to monitor traffic; all interfaces on a Flow source are monitored. By default, the threshold is set to monitor traffic from all Flow sources.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a top sender/receiver threshold

To configure a Flow Monitor top sender/receiver threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Flow Monitor Top Sender/Receiver**, then click **OK**. The New Flow Monitor Top Sender/Receiver Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variable and values. The default threshold is configured to alert when a host has sent or received more than 500 MB in the past 15 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.
 - § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default polling interval is 5 minutes.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring system thresholds

In This Chapter

Configuring system thresholds.....	593
Configuring a Blackout Summary threshold.....	593
Configuring a VMware threshold.....	595
Configuring a Failover threshold.....	596
Configuring a WhatsUp Health threshold.....	598

Configuring system thresholds

Alert Center system thresholds alert you on aspects of your WhatsUp Gold system according to the threshold parameters you configure. You can create five system threshold types:

- § *Blackout Summary* (on page 593)
- § *VMWare* (on page 595)
- § *Failover* (on page 596)
- § *WhatsConfigured Threshold*
- § *WhatsUp Health* (on page 598)



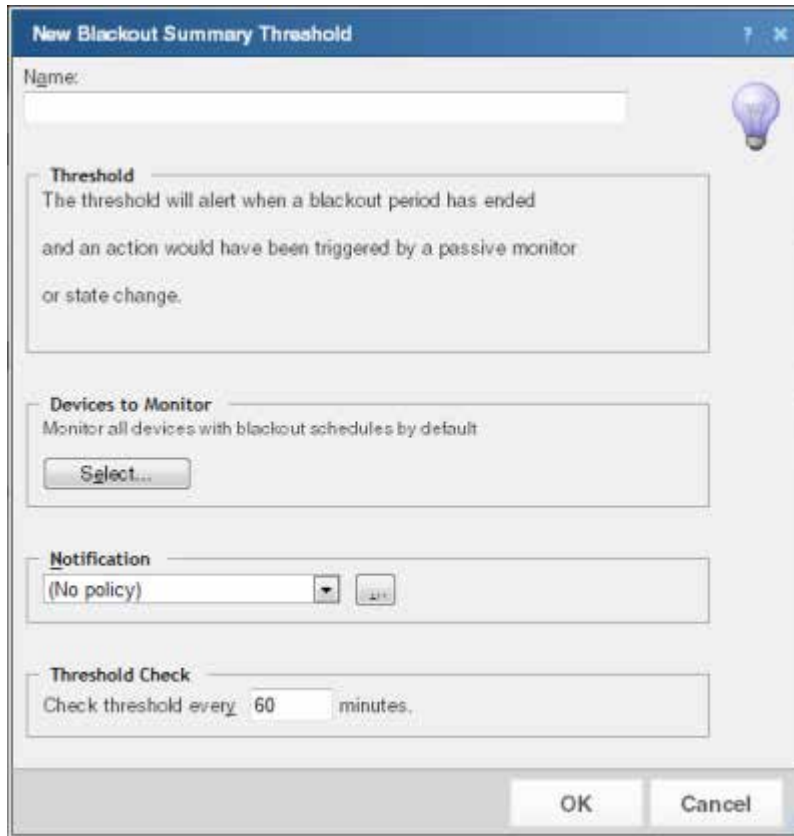
Note: The thresholds listed in the Threshold Library may vary, depending on your WhatsUp Gold license.

Configuring a Blackout Summary threshold

To configure a **Blackout Summary** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Blackout Summary** from the menu, then click **OK**. The New/Edit Blackout Summary Threshold dialog appears.



The dialog box is titled "New Blackout Summary Threshold". It contains the following fields and controls:

- Name:** A text input field.
- Threshold:** A text area containing the text: "The threshold will alert when a blackout period has ended and an action would have been triggered by a passive monitor or state change."
- Devices to Monitor:** A text area containing the text: "Monitor all devices with blackout schedules by default". Below it is a "Select..." button.
- Notification:** A dropdown menu showing "(No policy)" and a browse button (...).
- Threshold Check:** A text area containing the text: "Check threshold every 60 minutes".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** The threshold alerts you when a blackout period has ended and an action would have been triggered by a passive monitor or state change.



Note: You cannot configure threshold criteria for the Blackout Summary threshold.

- § **Devices to Monitor.** Click Select to select the devices to which the threshold applies. By default, the threshold applies to all devices. Use this dialog to select groups to which this threshold does not apply.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.
- § **Threshold check.** Enter a time interval for Alert Center to check the WhatsUp Gold database for actions that were not triggered because of a scheduled blackout period that has finished.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a VMware threshold

To configure a VMware threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **VMware** from the menu, then click **OK**. The New/Edit Blackout Summary Threshold dialog appears.

- 4 Complete the box with the appropriate information:
 - § **Name.** Enter a name for the VMware threshold. The name entered here is displayed as the threshold's dashboard report title on the Alert Center Home page.
 - § **Virtualization Events type.** Select the event type for which you want to create a threshold. The following options are available:

- § **All HA (High Availability) error events**
- § **All Virtual machine migration events**
- § **All security related events**
- § **Other events**



Note: When **Other events** are collected from the vCenter server, and you select **Other events** in the threshold configuration, you only see those events that were selected when event collection was configured in the Device Properties - Virtualization menu.



Note: For more information about event types and event type selection, see the Configure VMware event listener dialog help.

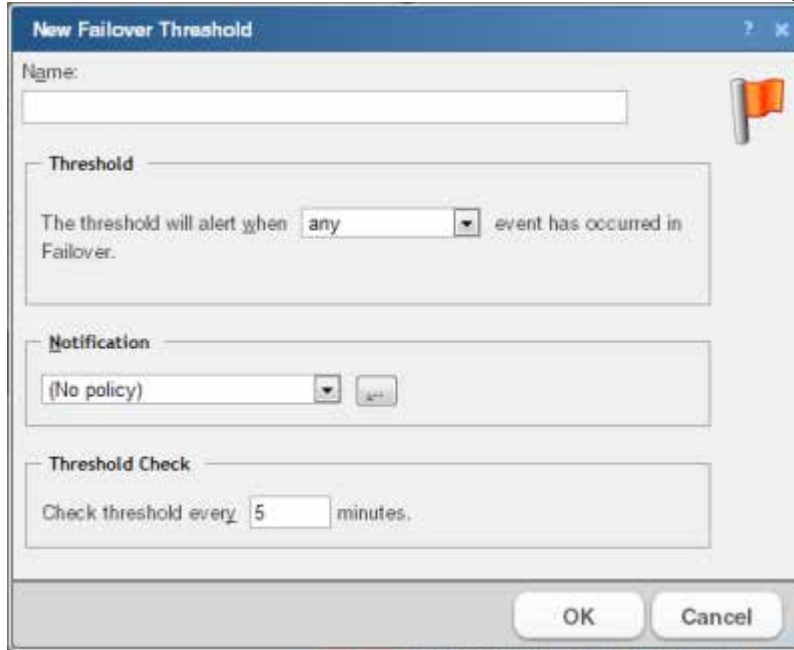
- 5 Select one of the following alert criteria:
 - § **The threshold will alert immediately if an event occurred within the last Threshold Check of *<Threshold_Check_Period>* minutes.** Select this option if you want alerts to occur immediately when an event has occurred within the threshold check period, where *<Threshold_Check_Period>* is the value defined in the Threshold Check area of this dialog.
 - § **The threshold will alert when:** Select this option if you want to define a number of events and time range for the threshold alert.
 - § **Number of events *<exceeds_or_falls_below>* *<number>*.** Use this setting to configure the number of events of the selected event type that must be received before firing the alert, where *<exceeds_or_falls_below>* determines if the number should **Exceed** or **Fall Below** the threshold value, and *<number>* is the threshold value.
 - § **in the past *<number>* *<unit_of_time>*.** Use this setting to configure the number and units of time that the threshold check should check for events, where *<number>* is the number of units of time, and *<unit_of_time>* is the unit of time.
- 6 Select the policy you want to apply to the threshold from the **Notification** boxes. Use the browse (...) button to access the Alert Center Notification Policies dialog. You can create new policies or edit existing policies from the Alert Center Notification Policies dialog.
- 7 Enter the number of minutes to wait between threshold checks in the **Threshold Check** area of the dialog.
- 8 Click **OK** when you have completed your configuration.

Configuring a Failover threshold

To configure a failover threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.

- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Failover**, then click **OK**. The New Failover Threshold dialog appears.



- 4 Specify or select the appropriate information in the dialog box.
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select the desired threshold criteria variables and values. You can configure the threshold to alert you when any event occurs, when an error occurs, or when an informational event occurs. By default, the threshold is configured to alert you when any event has occurred in Failover.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold.

Configuring a WhatsUp Health threshold

To configure a WhatsUp Health threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **WhatsUp Health**, then click **OK**. The New WhatsUp Health Threshold dialog appears.
- 4 Enter a **Name** for the threshold. This name is displayed as the threshold dashboard report title on the Alerts Home page.
- 5 Click the **Database** tab. Enter the appropriate threshold information:
 - § **Database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the database size exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- § **Total performance monitors exceed ____.** Select this option to have the threshold alert when the total number of performance monitors exceeds the number you specify. The default number of total performance monitors is 3,000.
- § **Total performance monitor records exceed ____.** Select this option to have the threshold alert when the total number of performance monitor records exceeds the number you specify. The default number of total performance monitor records is 2,000,000.
- § **Total passive monitor records exceed ____.** Select this option to have the threshold alert when the total number of passive monitor records exceeds the number you specify. The default number of total passive monitor records is 1,000,000.
- § **Total expired records exceed ____.** Select this option to have the threshold alert when the total number of expired records exceeds the number you specify. The default number of total expired records is 500,000.
- § **Total devices being monitored exceeds ____ % of license limit.** Select this option to have the threshold alert when the total number of devices being monitored exceeds the percentage of the license limit you specify. The default percentage of the license limit is 90%.



Tip: Click **View WhatsUp database** to view a graph of the current WhatsUp database usage.

- 6 Click the **Services** tab. Enter the appropriate threshold information:
 - § **WhatsUp polling service is down ____ minutes.** Select this option to have the threshold alert when the WhatsUp service has been down for the number of minutes you specify. The default threshold value is 5 minutes.
 - § **WhatsUp discovery service is down ____ minutes.** Select this option to have the threshold alert when the WhatsUp discovery service is down the number of minutes that you specify. The default number is 5 minutes.



Note: Web service threshold checks do not apply to users running IIS.



Note: If you are experiencing a high volume of errors from your WhatsUp Health threshold service checks, please see Troubleshooting the WhatsUp Health Threshold.

- 7 Click the **Flow Monitor** tab. Enter the appropriate threshold information pertaining to the WhatsUp Gold Flow Monitor.
 - § **Netflow database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the Netflow database exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- § **NfArchive database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the NfArchive database size exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- § **Flow collector service is down ____ minutes.** Select this option to have the threshold alert when the Flow collector service is down for the number of minutes you specify. The default threshold value is 5 minutes.
- § **Any bounce traffic occurs.** Select this option to have the threshold alert when bounce traffic occurs on a Flow Monitor source.
- § **Host records exceed ____.** Select this option to have the threshold alert when the number of host records exceeds the amount you specify. The default threshold value is 2,000,000 records.
- § **Raw, hourly, or daily records exceed ____.** Select this option to have the threshold alert when the number of raw data records exceeds the amount you specify. The default threshold value is 10,000,000 records.

- § **Total sources sending data exceeds ____ % of license limit.** Select this option to have the threshold alert when the total sources sending data exceeds the percentage of license limit that you specify. The default threshold value is 90% of license limit.



Tip: Click View Netflow database usage to view a graph of the current Netflow database usage. Click View NfArchive database usage to view a graph of the current NfArchive database usage.

- 8 After selecting the desired options for each tab and entering the appropriate threshold variables and values, specify your choices for the Notification and Polling sections of the dialog.

- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alerts Home page.

- § **Threshold check.** Enter a value for the polling interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items out of the threshold's parameters. The default polling interval is 5 minutes.
Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 9 Click **OK** to save the threshold settings.

Configuring wireless thresholds

In This Chapter

Configuring wireless thresholds	601
Configuring a Wireless Access Point RSSI threshold	601
Configuring a Wireless Banned Client MAC Addresses threshold ..	602
Configuring a Wireless CPU Utilization threshold	603
Configuring a Wireless Client Bandwidth threshold	604
Configuring a Wireless Device Over Subscription threshold	605
Configuring a Wireless Excessive Rogues threshold	606
Configuring a Wireless Memory Utilization threshold	606
Configuring a Wireless Rogue Access Point MAC Addresses threshold	607
Configuring a Wireless Rogue Hidden SSID threshold	608
Configuring a Wireless Rogue Specific SSID threshold	609
Configuring a Wireless Rogue Unknown SSID threshold	609

Configuring wireless thresholds

You can use WhatsUp Gold Alert Center to configure wireless thresholds to alert you about the health of your Wireless infrastructure devices according to the threshold parameters you configure. There are multiple wireless threshold types:

- § *Wireless Access Point RSSI* (on page 601)
- § *Wireless Banned Client MAC Address* (on page 602)
- § *Wireless Client Bandwidth* (on page 604)
- § *Wireless CPU* (on page 603)
- § *Wireless Device Over Subscription* (on page 605)
- § *Wireless Excessive Rogues* (on page 606)
- § *Wireless Memory* (on page 606)
- § *Wireless Rogue Access Point MAC Addresses* (on page 607)
- § *Wireless Rogue Hidden SSID* (on page 608)
- § *Wireless Rogue Specific SSID* (on page 609)
- § *Wireless Rogue Unknown* (on page 609)

Configuring a Wireless Access Point RSSI threshold

To configure a new Wireless Access Point RSSI (Received Signal Strength Indication) threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.

- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Access Point RSSI** from the list, then click **OK**. The New Wireless Access RSSI Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when RSSI falls below 20% for more than 30 minutes. Additionally, specify the minimum number of clients to user in the averaging. The default minimum is 3.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Banned Client MAC Addresses threshold

To configure a new Wireless Banned Client MAC Address threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Banned Client MAC Addresses** from the list, then click **OK**. The New Wireless Banned Client MAC Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.

- § **Threshold.** Enter any banned MAC addresses separated by commas and select an interval time range. The default range is 30 minutes. The threshold will alert when any MAC addresses listed are connected to the network in the given time interval.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless CPU Utilization threshold

To configure a new Wireless CPU Utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless CPU** from the list, then click **OK**. The New Wireless CPU Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when CPU utilization exceeds 90% for more than 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. The user has the option to specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Client Bandwidth threshold

To configure a new Wireless Client Bandwidth threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Client Bandwidth** from the list, then click **OK**. The New Wireless Client Bandwidth Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The threshold will alert when clients that are connected to the specified SSID(s) exceed their bandwidth quota for the specified traffic direction, in the given time range. The default criteria is 20 MB transmitted and received in a time range of 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. The user has the option to specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items

that are out of the threshold's parameters. The default check interval is every 5 minutes.

- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.

5 Click **OK**.

Configuring a Wireless Device Over Subscription threshold

To configure a new **Wireless Access Point Oversubscription** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Access Point Over Subscription** from the list, then click **OK**. The New Wireless Access Point Over Subscription Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the average number of clients attached exceeds the 'Client Count' for more than the specified 'Time Range'.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 10 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Excessive Rogues threshold

To configure a new **Wireless Excessive Rogues** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Excessive Rogues Alert** from the list, then click **OK**. The New Wireless Excessive Rogues Alert Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired rogue alert threshold criteria. The default time range interval is 30 minutes.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Memory Utilization threshold

To configure a new **Wireless Memory Utilization** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Memory** from the list, then click **OK**. The New Wireless Memory Utilization Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.

- § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when memory utilization exceeds 90% for more than 30 minutes.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Access Point MAC Addresses threshold

To configure a new **Wireless Rogue Access Point MAC Addresses** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Access Point MAC Addresses** from the list, then click **OK**. The New Wireless Access Point MAC Addresses dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Enter any rogue MAC addresses separated by commas and select an interval time range. The default range is 30 minutes. The threshold will alert when any MAC addresses listed here broadcast SSID's in the given time interval.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Hidden SSID threshold

To configure a new Wireless Rogue Hidden SSID threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Hidden SSID** from the list, then click **OK**. The New Wireless Rogue Hidden SSID Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Click the hyperlink to edit the list of acceptable rogues and select an interval time range. The default range is 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.

- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Specific SSID threshold

To configure a new Wireless Rogue Specific SSID threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Specific SSID** from the list, then click **OK**. The New Wireless Rogue Specific SSID Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Enter one or more SSIDs and select an interval time range. The threshold is configured to alert when any of the listed SSIDs are detected in the specified time range. The default range is 30 minutes.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Unknown SSID threshold

To configure a new Wireless Rogue Unknown SSID threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.

- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Unknown SSID** from the list, then click **OK**. The New Wireless Rogue Unknown SSID Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. The threshold is configured to alert when any new or previously unseen SSIDs are detected in the specified time range. The default range is 30 minutes.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Using Actions

In This Chapter

Actions overview.....	611
Managing Action Strategies	611
About the Action Library.....	612
Selecting an action type	613
Configuring an action.....	613
About Percent Variables.....	649
Testing an action.....	652
Assigning an action.....	652
Removing an action.....	654
Creating a Blackout Period.....	655
Action Policies	656

Actions overview

WhatsUp Gold actions are designed to perform a task as a device or monitor state change occurs. Alerting action tasks send various types of alerts to notify you of state changes. Functional action tasks can log the problem, launch an external application, perform a custom script, and other functions after device or monitor state changes.

As you configure an action, you choose the task it is to perform. Also, when you configure an action, you choose whether to assign it to a device, or to an active or passive monitor. For more information, see *Configuring an action* (on page 613).

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. When assigned to a device, actions fire according to the device's state. For more information, see *Assigning an action* (on page 652).

You can configure actions on a single device or monitor, or define an *Action Policy* (on page 656) 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 295).

§ 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* (on page 656) 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 653)
- § *Assigning an action to an active monitor* (on page 653)
- § *Creating a custom action policy* (on page 656)

After the actions have been completely configured, WhatsUp Gold launches the action as soon as the proper state change is reached.

Alerting actions

The following actions perform an alerting task to notify you when a device or monitor state changes.

- § *Beeper action* (on page 614)
- § *E-mail action* (on page 616)
- § *Pager action* (on page 620)
- § *SMS action* (on page 621)
- § *SMS Direct action* (on page 623)
- § *Web Alarm action* (on page 625)
- § *Sound action* (on page 628)
- § *Text To Speech action* (on page 629)

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* (on page 544).

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 listening.
 - § **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 SMTP server. This is considered a failed connection.
 - § **Mail To.** Enter the email addresses to which you want to send the alert. Email addresses must be fully qualified. You can enter multiple addresses, separated by a semi-colon (;), comma (,), or the [SPACE] character. The address should not contain brackets, braces, quotes, or parentheses.
 - § **Mail From.** Enter the email address you want to appear in the From field of the e-mail that is sent by the Email 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).
- 6 Complete the information on the **Mail Content** tab. This tab contains options pertaining to the action email message content.
 - § **Subject.** Enter a text message or edit the default message. You can use *percent variables* (on page 649) to display specific information in the subject.
 - § **Message body.** Enter a text message or edit the default message. You can use *percent variables* (on page 649) to display specific information in the message body.
- 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 SMTP server. 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 variables* (on page 649) to display specific information in the subject.

§ **Message body.** Enter a text message or edit the default message. You can use *percent variables* (on page 649) 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 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 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 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:

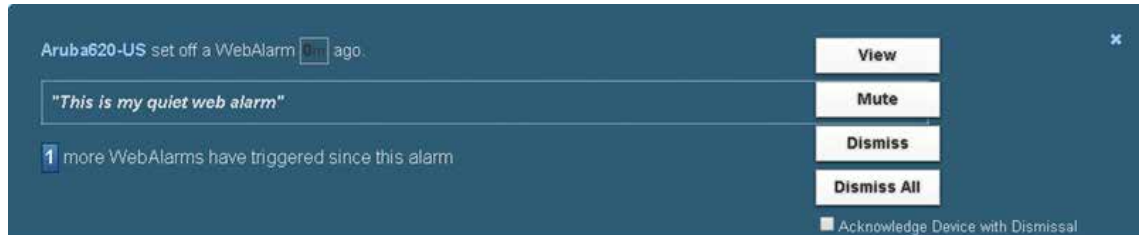
- 1 From the WhatsUp Gold web interface, go to **Admin > Actions**. The Action Library dialog appears.
- 2 Select the action you would like to edit, then click **Edit**.
- 3 Enter or select the appropriate information:
 - § **Name**. Enter a unique name for the action. This name displays in the Action 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.

Web Alarm popup actions

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:

- § Click **View** to access the *Web Alarms* (on page 627) interface.
- § Click **Mute** to stop the alarm from sounding.
- § Click **Dismiss** or **Dismiss All** to temporarily ignore one or all of the alarms sounding.



Tip: Select **Acknowledge Device with Dismissal** to automatically acknowledge the device(s) sounding an alarm when clicking the **Dismiss** or **Dismiss All** buttons.

Additionally, you can access detailed information by clicking the device name/IP address shown to launch the Device Status Dashboard.



Note: The Manage Devices right must be enabled for the user to view the web alarm pop-up and hear the alarm sound, if applicable. For more information, see About user rights. If multiple alarms are triggered with different sounds configured for each, the sound associated with the web alarm configured first takes priority. When dismissed or acknowledged, the sound for the next oldest alarm is heard.

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 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 20).



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 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**.

Functional actions

The following actions perform a functional task when a device or monitor state changes.

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 952).

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 SMTP server. This is considered a failed connection.



Note: Though the maximum timeout is 60 seconds, you are 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 SMTP server. 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 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 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
```

- 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 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 635).



Important: WhatsUp Gold uses a 32-bit (i.e. x86) PowerShell engine. Therefore, only 32-bit PowerShell snap-ins are supported and 64-bit only snap-ins will not function properly. Snap-ins usable in both 32-bit and 64-bit operating systems are configured for 64-bit systems by default and must be manually configured for 32-bit PowerShell engine to function properly with WhatsUp Gold.



If you are using *additional pollers* (on page 35) with WhatsUp Gold, PowerShell must be installed and any desired snap-ins must be registered identically on all poller machines for any PowerShell performance monitors, active monitors, and actions to function properly. Associated errors resulting from failed monitors will appear in the *WhatsUp Gold Status Center* (on page 20). Errors resulting from failed actions will appear in the WhatsUp Gold Event Viewer.

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.

- § **Run under device credentials**. Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see Using the Credentials Library.
- § **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 SMTP server. 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.

- § **Run under device credentials.** Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see Using the Credentials Library.
 - § **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

To set up the service restart action:

- 1 Go to **Windows Control Panel > Administrative Tools > Services**.
- 2 Right click **Ipswitch Service Control Manager**, 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.

- 4 **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**.
- 5 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 Service Restart 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.
 - § **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.
- 6 Click **OK** to save changes.

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 Service Restart 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.
 - § **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 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 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.

- § **Line end character.** Select the appropriate character type; either *None*, *Linefeed*, *Carriage return*, or *Carriage return linefeed*.
- § **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** 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.

- § **Line end character**. Select the appropriate character type; either *None*, *Linefeed*, *Carriage return*, or *Carriage return linefeed*.
 - § **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 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 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 649) 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 649) 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
<code>%ActiveMonitor.Argument</code>	SNMP instance number. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
<code>%ActiveMonitor.Comment</code>	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.
<code>%ActiveMonitor.Name</code>	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.
<code>%ActiveMonitor.NetworkInterfaceAddress</code>	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.
<code>%ActiveMonitor.Payload</code>	<p>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.</p> <p>For Active Script Active Monitors, the payload is the text that is passed to the <code>SetResult()</code> method in the script.</p>
<code>%ActiveMonitor.State</code>	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
<code>%Device.ActiveMonitorDownNames</code>	List of down services using the abbreviated name if available.
<code>%Device.ActiveMonitorUpNames</code>	Full service names of all UP monitored services on a device.
<code>%Device.Address</code>	IP address (from device properties).
<code>%Device.Attribute.[Attribute Name]</code>	<p>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: <code>%Device.Attribute.Contact</code>, returns the contact name.</p> <p>Default categories:</p> <ul style="list-style-type: none"> · *. 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

	<p>• Custom. If you have created a custom attribute you can use the name of that custom attribute in the percent variable.</p> <p>Example:</p> <p>%Device.Attribute.Phone %Device.Attribute.RackPosition</p> <p>To avoid an error, always place a space or line break after the attribute name.</p>
%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	<p>This shows the name of the active monitor, preceded by the device state id. For example, 10 DNS.</p> <p>Device State ID values:</p> <p>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</p>
%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

When actions are assigned to devices, the action fires when an assigned device enters the state specified in the action. For example, if you assign an E-mail action to a device that is to fire when the device goes into a down state, an e-mail is sent to the email address specified in the E-mail action when the devices goes into a down state.

To assign an action to a device:

- 1 In the Details or Map View, right-click a device, then click **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

When actions are assigned to active monitors, the action fires when the monitor issues the state specified in the action configuration. For example, if you assign a Web Alarm action to a Ping active monitor, every time the monitor cannot reach a device to which it is associated, it issues a down state for the unreachable device. After the monitor issues the down state for an unreachable device, a web alarm fires notifying you that the device is unreachable by ping.

As you configure active monitors, you have the opportunity to assign actions; however, it is not required that you assign them at the time of configuration. If you decide to assign an action to the monitor at a later time, you can do so through device Properties.

To assign an action to an active monitor:

- 1 In the Details or Map View, right-click a device, then click **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

When actions are assigned to passive monitors, actions fire when the passive monitor listener for a monitor observes a specific message. For example, if you assign an SMS Direct action to a Windows Event Log passive monitor, the action fires if the Windows Event Log Listener observes a specified condition on the associated device and an SMS text message is sent to the phone number specified in the action.

As you configure passive monitors, you have the opportunity to assign actions; however, it is not required that you assign them at the time of configuration. If you decide to assign an action to the monitor at a later time, you can do so through device Properties.

To assign an action to a passive monitor:

- 1 In 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 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

Similar to Alert Center notification policies, action policies allow you to group or sequence multiple actions together for use on any device, active, or passive 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* (on page 657)
- § *Configuring an implicit Action Policy* (on page 657)

Creating an action policy

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**. The New Action Policy dialog appears.
- 3 Enter a name in **Policy name**. This name is used to identify the policy later, so you should make sure the name is something that helps you remember what is contained in this policy.
- 4 Click **Add**. The Action Builder wizard appears.
- 5 Follow the directions in the wizard.
- 6 Click **Finish** at the end of the wizard to add the action to the policy.
- 7 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.

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.
- 8 After you have added all of the you would like 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.

Assigning an action policy to a device

To assign an action policy to a device:

- 1 In Device or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Actions dialog appears.
- 3 Select **Apply this Action Policy**.

- 4 Click the list and select the action policy to apply.



Note: If the list is empty, click browse (...) and create a new action policy. Click **Add** to access the Action Builder dialog.

- 5 Click **OK** to save changes.

After an action has been added to the device, the action fires when that device reaches the specified state.

Adding and editing an action policy

To add or edit an action policy:

- 1 From the WhatsUp Gold web interface, go to **Admin > Action Policies**. The Action Policies dialog appears.
- 2 Click **New** to create a new action policy.
- or -
Select the policy you want to change from the list of current action policies, and then click **Edit**.
- 3 Enter or select the appropriate information:
 - § **Policy Name.** Enter a unique name for the policy. The name should be something you can easily associate with the actions performed in the policy.
 - § **Actions in the policy.** This list shows all of the actions configured for this policy. The list displays which state change triggers what action.
 - § Click **Add** to configure an action to add to the policy.
 - § Select an action on the list and click **Edit** to change how the action is configured.
 - § Select an action on the list and click **Delete** to remove the action from the list.
 - § Select **Only execute first action (for each state)** to keep from firing multiple actions assigned to the current policy.
 - § Use the **Up** and **Down** arrows to change the order of the actions.
- 4 Click **OK** to save changes.

Configuring an implicit action policy

The Implicit Action policy automatically assigns actions to all devices in your database. You cannot opt out of the Implicit Action policy.



Note: The Implicit Action Policy only assigns actions to devices. You must create separate action policies for device monitors.

If at any time during the normal operation of WhatsUp Gold you notice that actions are firing and you cannot find the action associated to the down device or monitor, remember to check the Implicit Action Policy.



Note: In previous versions of WhatsUp Gold, the Web Alarm action was included in the Implicit Action Policy. This is no longer true in Ipswitch WhatsUp Gold. For more information on the Web Alarm action, see *About Web Alarms* (on page 303).

To configure the Implicit Action Policy

- 1 From the WhatsUp Gold web interface, go to **Admin > Action Policies**. The Action Policies dialog appears.
- 2 Select the Implicit Action Policy, then click **Edit**. The Edit Action Policy dialog appears.
 - § To add an action to the policy, click **Add**.
 - § To modify an action in the policy, select it, then click **Edit**.
 - § To delete an action from the policy, select it, then click **Remove**.
 - § To have WhatsUp Gold execute only the first action in the list for each state, and stop when that action fires successfully, select **Only execute first action**.



Tip: Use **Up** and **Down** to modify an action's placement in the list.

- 3 Click **OK** to save changes.

Example: getting an Email alert when the Web server fails

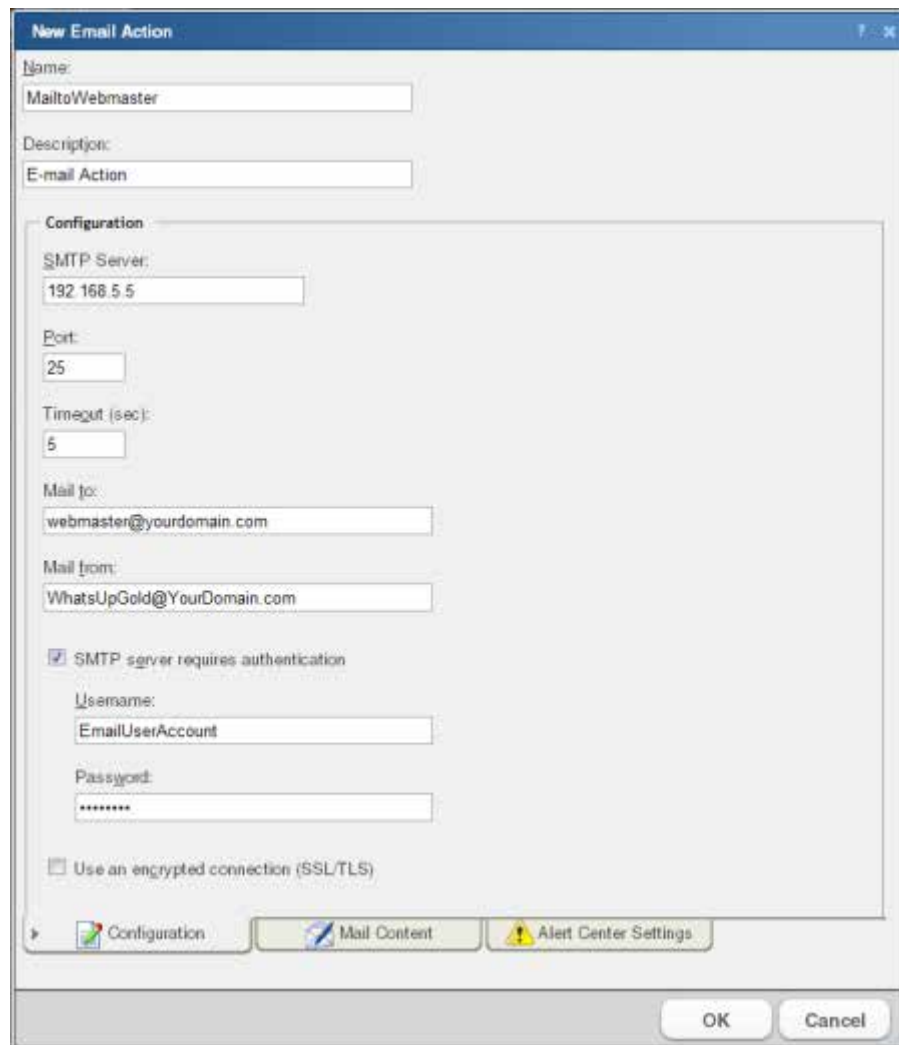
This example shows how to set up monitoring for your Web server so that an email alert is sent when the Web server fails, or when web content is not available.

First, you need to set up the monitors for your web server. Then, create an Email Action and assign it to the monitors.

Setting up monitors for a Web server and creating an Email Action that is assigned to monitors:

- 1 In either Details or Map View, right-click on the web server device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.
- 4 Use the following dialogs to add the HTTP active monitor to your web server device; this monitor checks that HTTP (port 80) is active.
 - a) On the Select Active Monitor Type dialog, select **HTTP**, then click **Next**. The Set Polling Properties dialog appears.
 - b) Ensure that the default settings are selected (**Enable polling for this Active Monitor** and **Use default network interface**), then click **Next**. The Setup Actions for Monitor State Changes dialog appears.
 - c) Select **Apply individual actions**, then click **Add**. The Select or Create Action dialog appears.
 - d) Select **Create a new action**, then click **Next**. The Select Action Type dialog appears.
 - e) In the **Select the actions type to create** list, select **E-Mail Action**, then click **Next**. The Select State Change dialog appears.

- f) Select **Down** from the **Execute the action on the following state change** list, then click **Finish**. The New Email Action dialog appears.
- g) Enter the information using your mail and SMTP server settings:



The image shows a 'New Email Action' dialog box with the following fields and options:

- Name:** MailtoWebmaster
- Description:** E-mail Action
- Configuration** section:
 - SMTP Server:** 192.168.5.5
 - Port:** 25
 - Timeout (sec):** 5
 - Mail to:** webmaster@yourdomain.com
 - Mail from:** WhatsUpGold@YourDomain.com
 - ☒ SMTP server requires authentication
 - Username:** EmailUserAccount
 - Password:** *****
 - ☐ Use an encrypted connection (SSL/TLS)

At the bottom, there are three tabs: Configuration (selected), Mail Content, and Alert Center Settings. The dialog ends with OK and Cancel buttons.

- h) Click **Mail Content**. The following information is included in the Edit Mail Content tab and can be customized:

New Email Action

Name:

Description:

Mail Content

Subject:

Message body:

```
%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 mail was sent on %System.Date at %System.Time
Ipswitch WhatsUp Gold
```

Right Click in the Subject or Message body field for percent variable support.

Insert link to device status

Configuration Mail Content Alert Center Settings

OK Cancel

- i) Click **OK** to save changes and to return to the previous dialog. Click **OK** again to return to the Setup Actions for Monitor State Changes dialog, then click **Finish**.

Setting up an HTTP Content active monitor with an email alert:

- 1 In either Details or Map View, right-click on the web server device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.
- 4 Use the same process to add the HTTP active monitor; this monitor checks that the Web server returns valid content in response to an HTTP request.
 - a) On the Select Active Monitor Type dialog, select **HTTP**, then click **Next**. The Set Polling Properties dialog appears.
 - b) Ensure that the default settings are selected (**Enable polling for this Active Monitor** and **Use default network interface**), then click **Next**. The Setup Actions for Monitor State Changes dialog appears.
 - c) Select **Apply individual actions**, then click **Add**. The Select or Create Action dialog appears.

- d) Select **Select an action from the Action Library**, then click **Next**. The Select Action and State dialog appears.
- e) Under **Select an action from the Action Library**, select **MailtoWebmaster**. This is the action that you created in the previous steps.
- f) Under **Execute the actions on the following state change**, select **Down**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.
- g) On the Select Action and State dialog, select **MailtoWebmaster**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.
- h) Click **Finish**.

The two active monitors and resulting email actions are now enabled.

When the Web server is down, the HTTP Active Monitor fails and triggers the Email Action, which sends an email message similar to the following:

```
Web1 is down on server: web1.YourDomain.com (192.168.5.5)
```

```
Details:
```

```
Monitors that are down include:
```

```
Monitors that are up include:
```

```
HTTP Content
```

```
Notes on this device (from device property page):
```

```
Lamar Bldg; 2nd floor
```

```
-----
```

```
This mail was sent on 11/28/2007 at 15:34:01
```

```
Ipswitch WhatsUp Gold
```

If the Web server cannot return web content, the Email Action report reads:

```
HTTP Content is down on server: web1.YourDomain.com (192.168.5.5)
```

Any details or notes specified in the action are also reported.

Using 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.



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 920).

Reports

In This Chapter

Working with monitor reports.....	663
Using Favorites.....	677
Using WhatsUp Gold monitor reports	680
Performance monitor reports	692
Network monitor reports	700
Using Device monitor reports.....	712

Working with monitor reports

In This Chapter

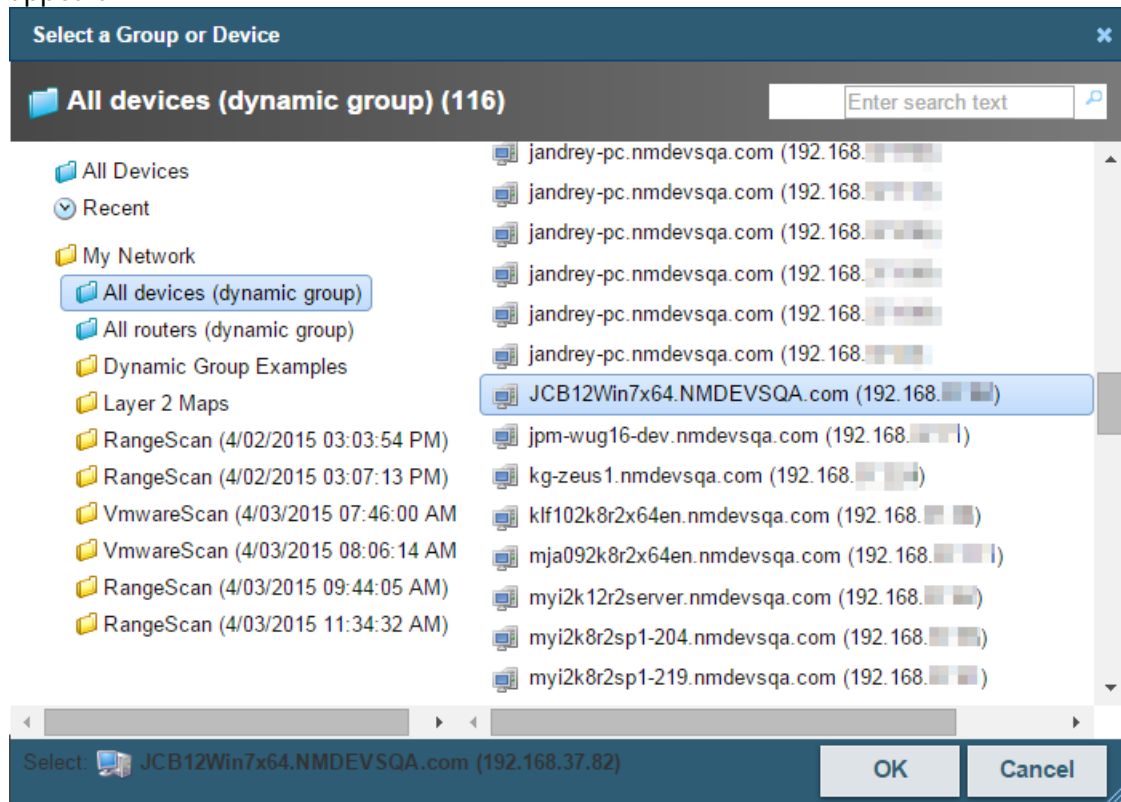
Viewing device reports.....	663
Viewing group reports	665
Using Business Hours settings in monitor reports	667
Viewing real-time data in monitor reports.....	668
About report refresh intervals	668
Changing the date range	669
Using the Zoom tool	670
Using paging options	670
Changing preferences	671
Using the WhatsUp Gold toolbar buttons.....	672
Configuring monitor report charts.....	672
Resizing and sorting report columns.....	673
Disabling Instant Info popups	674
Understanding graph types.....	675

Viewing device reports

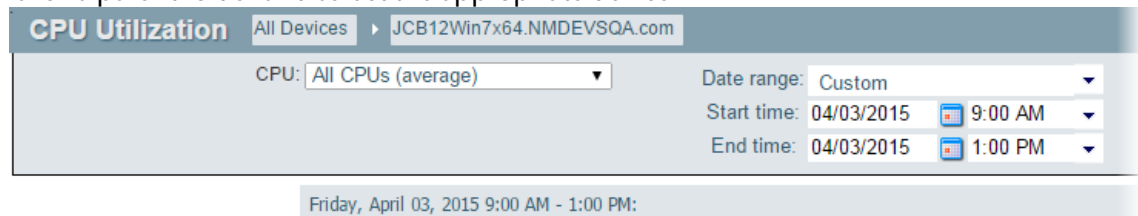
Device monitor reports display information related to specific devices. For example, you can view reports for a specific Cisco router with Interface Utilization performance monitors.

To view a report for a specific device:

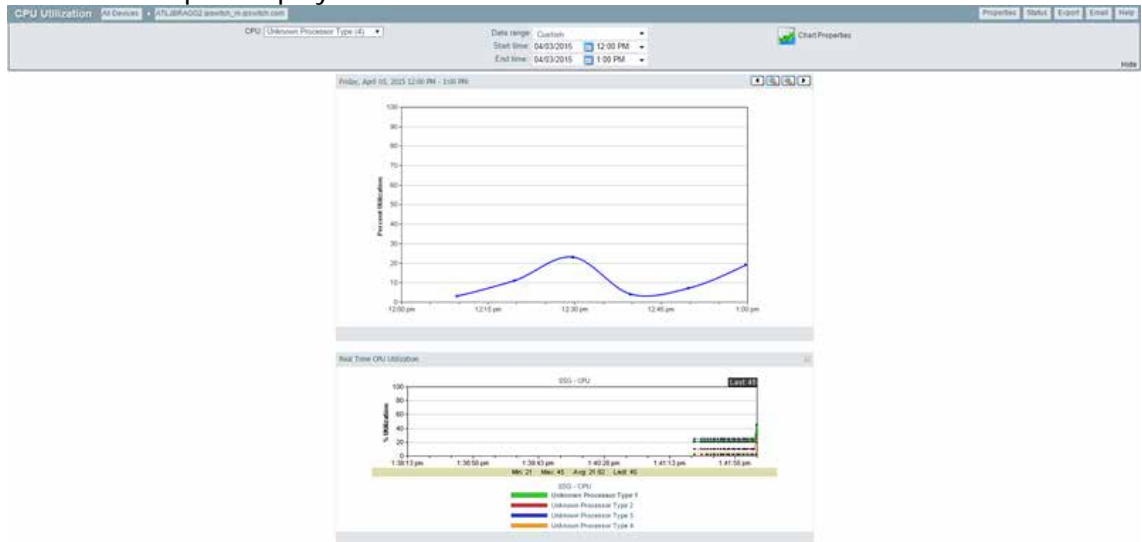
- 1 Click the **Reports** tab, then select the report you want to view.
- 2 In the page title bar, click the device context. The Select a Group or Device dialog appears.



- 3 Click a parent folder and select the appropriate device.



- 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.



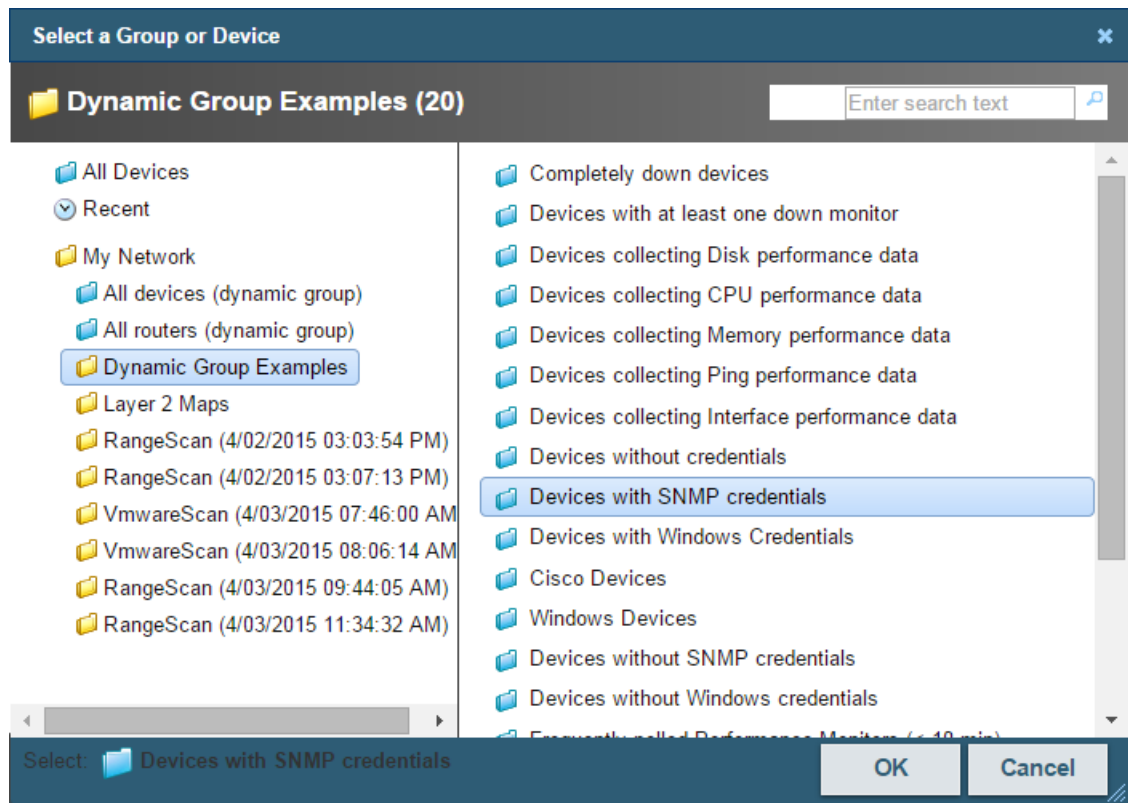
- § Click the current device context to open the device picker and select a device or group from a list of devices and groups on your network.
- § Click other reports on the navigation bar to view other reports for the same device.
- § Use the report **Date/Time Picker**, located in the middle of the 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 688).

Viewing group reports

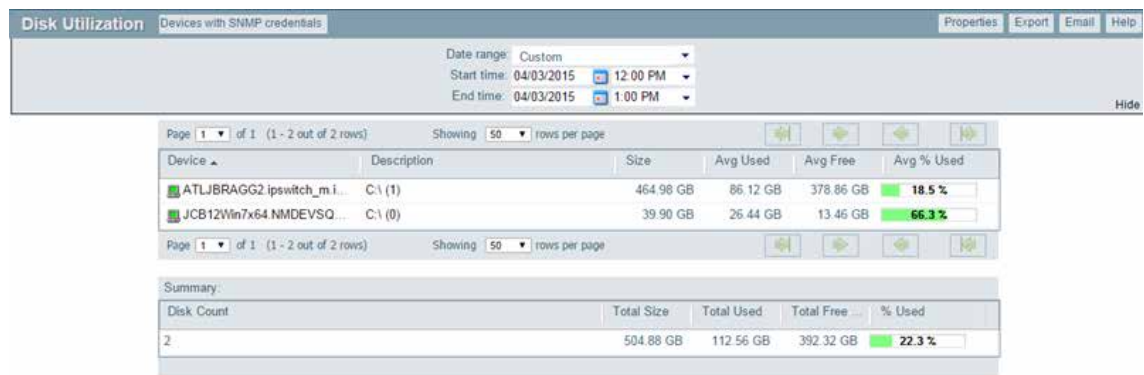
Group monitor reports display information related to specific groups. For example, you can view reports for Cisco devices with Interface Utilization performance monitors.

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.
Click a parent folder and select the appropriate group.



- 3 Click **OK** to make your selection. The selected group displays as the new context and the monitor report displays information for the selected group.



- § 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** 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 688).

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.
- 2 Select **Edit Business Hours**. The Business Hours dialog appears.

- 3 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**.

- 4 Select the **Link days** option if you want to use the same start and end time for each scheduled day.
- 5 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.
- 6 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

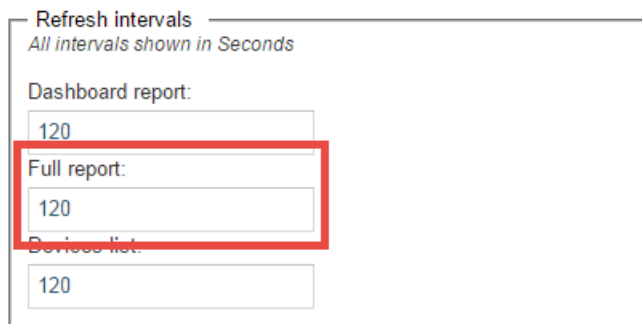
Reports are refreshed at an interval specified in the User Preferences dialog called the report refresh interval. The default report refresh interval is 120 seconds.



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 670) 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* (on page 47) should refresh.
- § **Full report.** Enter a time (in seconds) for how often *monitor reports* (on page 682) 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 303).



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.

WUGSpace Community

If you enter your community credentials in this dialog, they will be saved and used to automatically log into the community each time you download, import, or publish application profiles in WhatsUp Gold APM.

Using the WhatsUp Gold toolbar buttons

The following toolbar buttons are available:

- § **Add Content.** Add additional dashboard reports to the current dashboard view
- § **Edit View.** Edit settings for the currently displayed dashboard view.
- § **Export.** Export a log from WhatsUp Gold to a PDF file.
- § **Email.** Email a report/log as a PDF attachment or schedule the report/log to be emailed at regular intervals.
- § **Help.** View help content for the current page.

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 675).



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

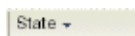
Both column sizing and sorting are maintained on a per user basis, and only for the report where the column changes are made.

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.

The screenshot shows the 'Preferences' dialog box with the 'Instant Info' section highlighted by a red rectangle. The 'Instant Info' section contains the following options:

- Show popups on...**
 - ☒ Dashboard reports
 - ☒ Device list
 - ☒ Full reports

The other sections visible in the dialog are:

- General**: Includes a 'Change your password...' button and a 'Show Getting Started Pane' checkbox.
- Refresh intervals**: Includes input fields for 'Dashboard report:', 'Full report:', and 'Devices list:', all set to '120'.
- Reports**: Includes a dropdown for 'records per page for long reports by default' set to '50' and a 'Collapse legends on split second graph dashboard reports' checkbox.
- Web Alarms**: Includes an 'Enable web alarms' checkbox (checked) and a 'Check every: (seconds)' input field set to '120'.

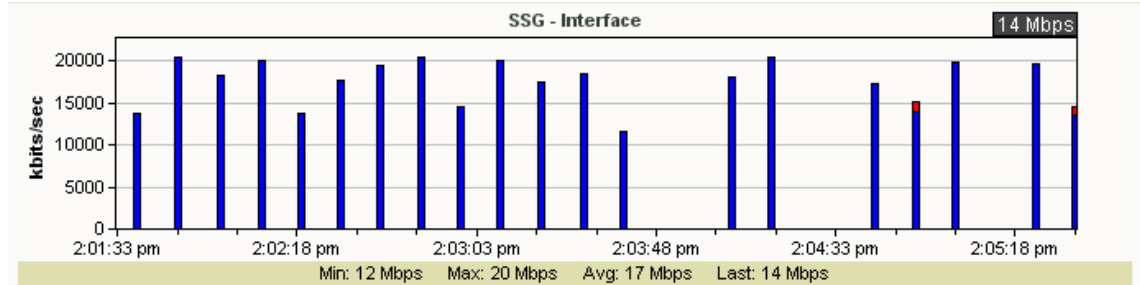
At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- 3 Click **OK** to save changes.

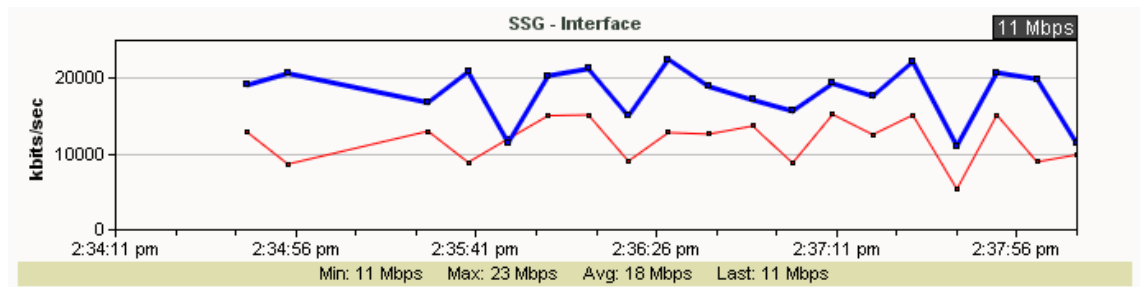
Understanding graph types

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.

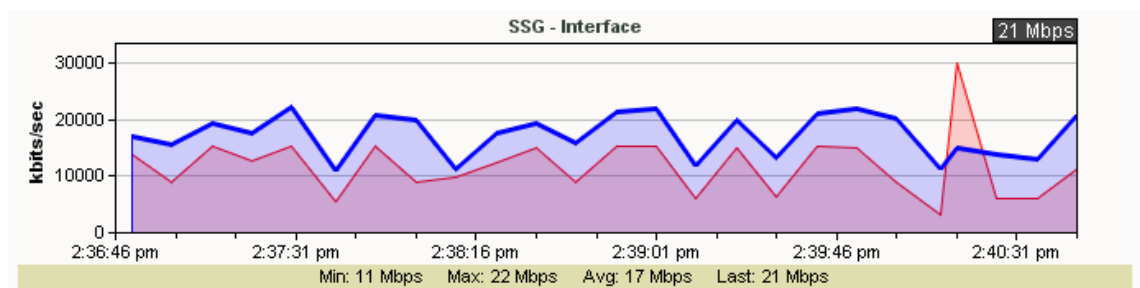
§ **Bar.** A vertical bar is displayed for each data point.



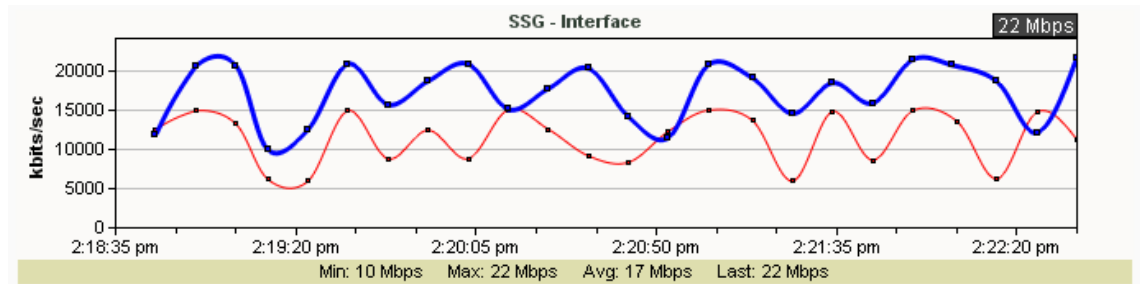
§ **Line.** A segmented line connects each of the data points. These data points are represented as small squares. Line graphs are useful for viewing each individual data point or for viewing several counters on the same graph (when used with Split Second Graphs).



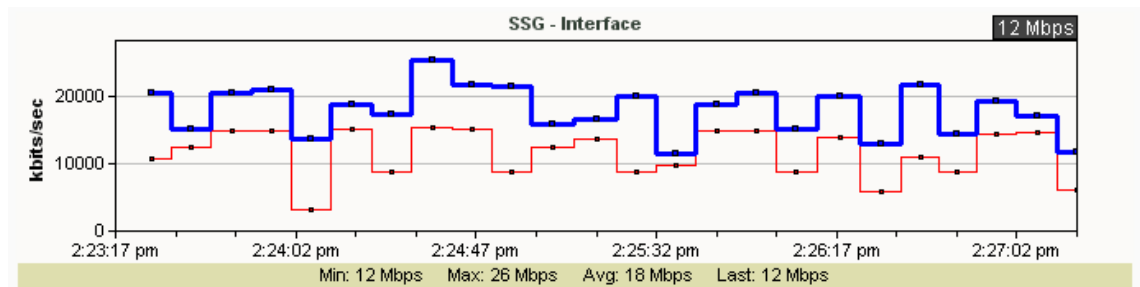
§ **Area.** A solid line connects each data point. The area between the data point and the X-axis is filled with a semi-transparent background color. This graph type has the greatest visibility at a glance, but when used with Split Second Graphs, is only useful for viewing one to two performance counters 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

Understanding favorites

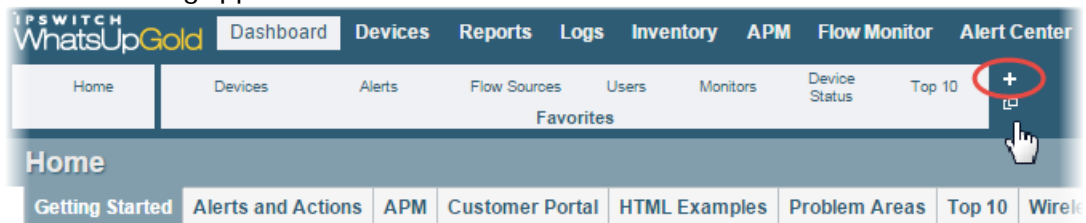
WhatsUp Gold favorites let you create your own customized toolbar by adding the WhatsUp Gold options you use most often to a single tab. You can edit and organize your favorites the way that best fits your needs. For more information, see *Adding favorites* (on page 55).

To access WhatsUp Gold Favorites, go to the **Dashboard > Favorites**.

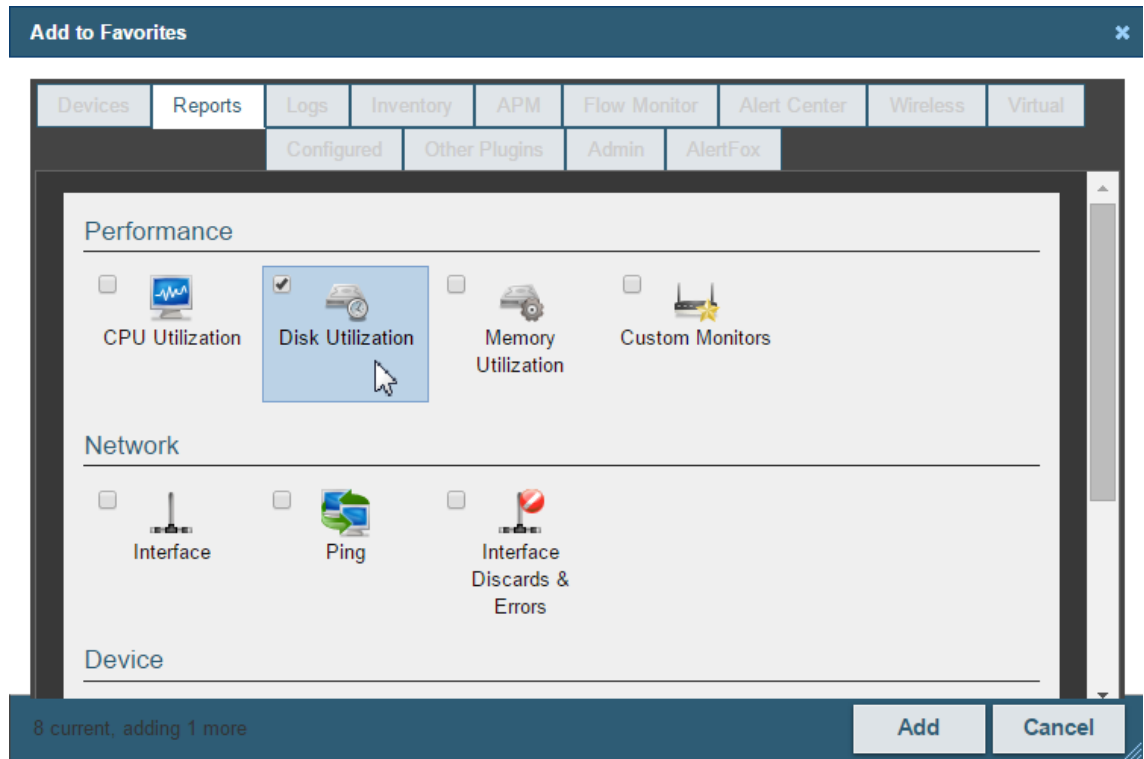
Adding favorites

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.

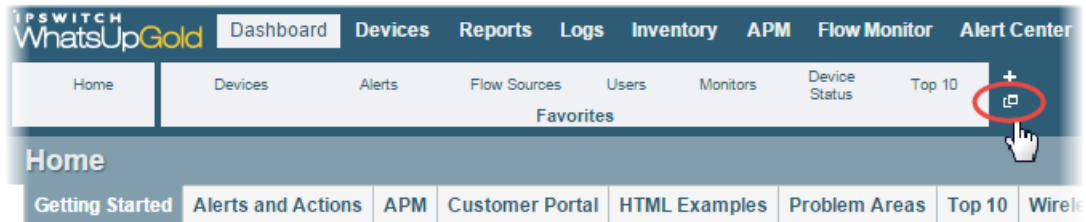


- 5 Continue clicking tabs and selecting buttons until you have added as many as you want to add.
- 6 Click **Add** to save your changes and add the selected buttons to your Favorites. The selected buttons appear in your Favorites group.

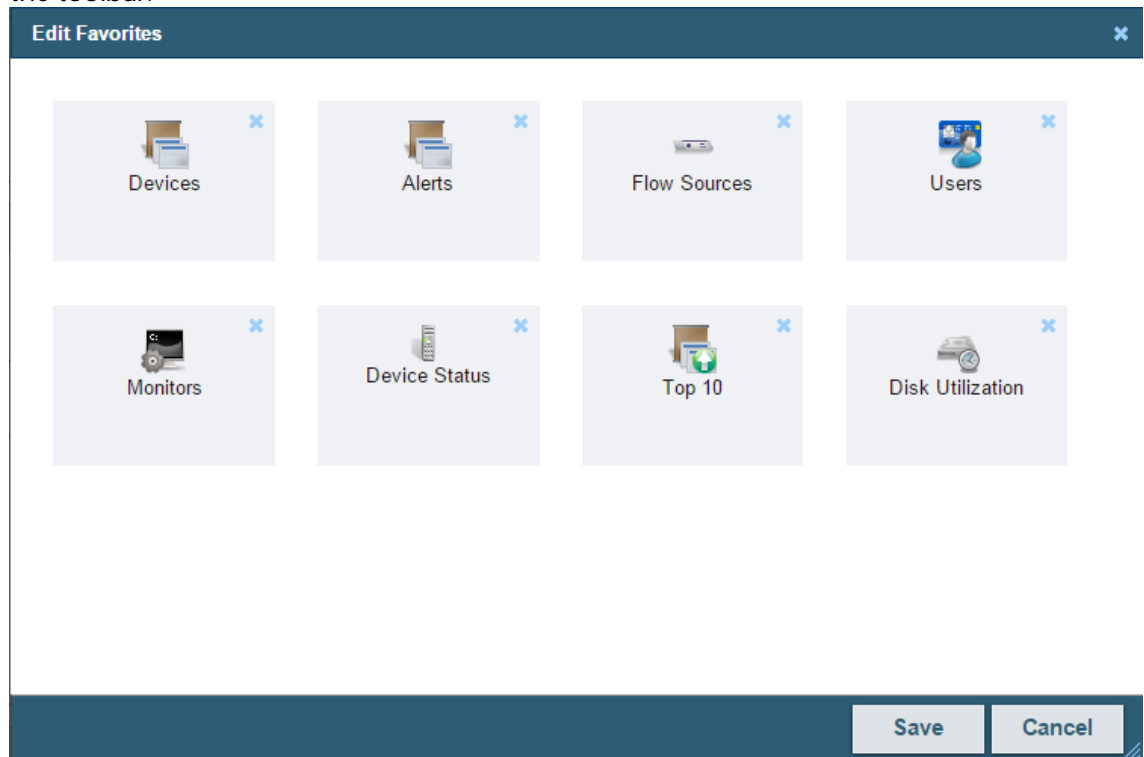
Editing favorites

To remove buttons from your Favorites group:

- 1 Click **Dashboard**.
- 2 Click the **Edit Favorites** icon.



- 3 From the dialog, click the **X** at the upper right of each button you want to remove from the toolbar.



- 4 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 Click and drag the buttons within the Edit Favorites dialog to the order you prefer.
- 2 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.....	680
Learning about monitor reports.....	682
Device Properties - Performance Monitors.....	685
Using the Performance Monitor Library.....	686
Scheduling reports.....	688
Exporting reports and logs.....	689
Emailing reports and logs.....	690
Printing reports and logs.....	691
Viewing scheduled reports	691

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 727)	A record of all actions that WhatsUp Gold attempts to fire.
Activity Log (on page 734)	A history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the selected time period.
General Error Log (on page 729)	A record of error messages generated by WhatsUp Gold.
Home Dashboard (on page 44)	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 730)	A record of Passive Monitor errors reported by WhatsUp Gold.
Performance Monitor Error Log (on page 730)	A record of Performance Monitor errors reported by WhatsUp Gold for all devices or for a selected device.
Recurring Action Log (on page 735)	Results of Recurring Action executions.
Recurring / Scheduled Report Log (on page 734)	Results of Recurring and Scheduled Report executions.

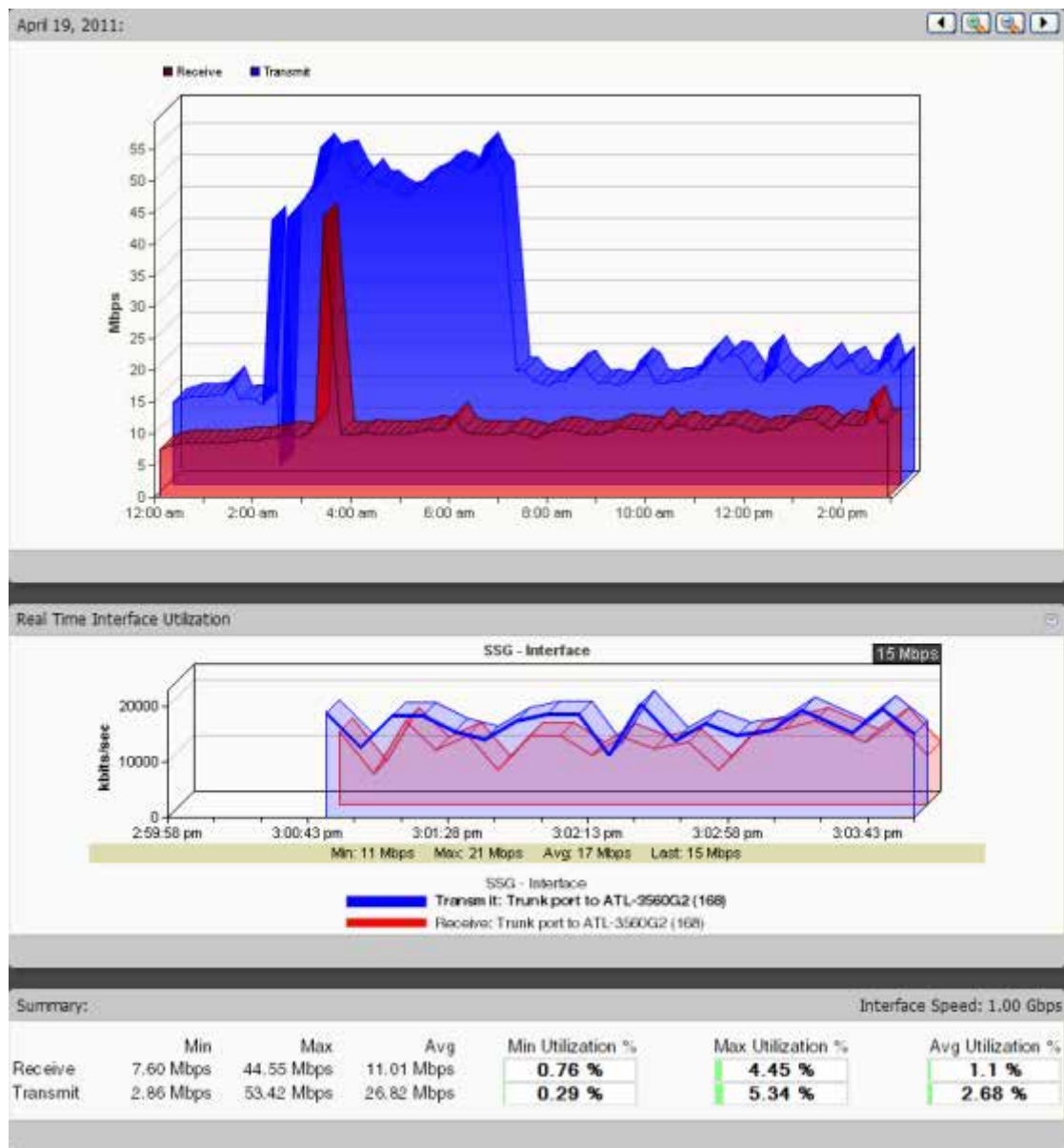
Remote Site Log	A record of messages generated by Remote Server connection attempts. Available in WhatsUp Gold MSP and WhatsUp Gold Distributed editions.
Remote Site Status	View the Remote Location State of devices and Active Monitors. Available only in the central installation of WhatsUp Gold MSP and WhatsUp Gold Distributed editions.
SNMP Trap Log (on page 731)	A history of SNMP traps occurring 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 732)	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 735)	Shows the history of user activity on the system.
Windows Event Log (on page 733)	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 736)	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 714)	Compare the amount of time the active monitors on your devices have been down.
Blackout Summary Log (on page 736)	A detailed view of actions that were not fired during a blackout period.
CPU Utilization (on page 692)	CPU utilization statistics for devices by group or device.
Device Uptime (on page 714)	Shows the percentage of uptime, maintenance, unknown, down, and availability for devices by group.
Disk Utilization (on page 694)	Disk space utilization statistics for devices and by group.
Device Health (on page 715)	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 700)	Interface utilization for devices by group or for a selected device (by percentage).
Interface Traffic (on page 702)	Interface traffic for devices by group or for a selected device (in bps).
Memory Utilization (on page 696)	Memory utilization statistics for devices by group or for a selected device.
Monitors Applied (on page 737)	A list of monitors applied to devices in the group currently in context.
Ping Availability (on page 704)	Ping availability statistics for devices by group or device.
Ping Response Time (on page 706)	Ping response times for devices by group or for an individual device.
Quarterly Availability Summary (on page 738)	Shows the availability summary for a group.
State Change Acknowledgement (on page 716)	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 716)	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 740)	A summary of device states organized by device group.
Top 10 (on page 46)	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 698)	View information on groups and devices collected by custom monitors.
Device Status (on page 45)	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:



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 Transm	Bytes Received
QA-2821.ipswit...	199.x Network (1)	0.79 %	0.09 %	7.94 Mbps	828.41 Kbps	77.20 GB	9.00 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	1.16 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	406.86 MB
QA-2901.yourd...	Connection to QA-3750 (1)	0.05 %	0.05 %	48.49 Kbps	49.13 Kbps	482.66 MB	488.12 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	234.13 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 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.

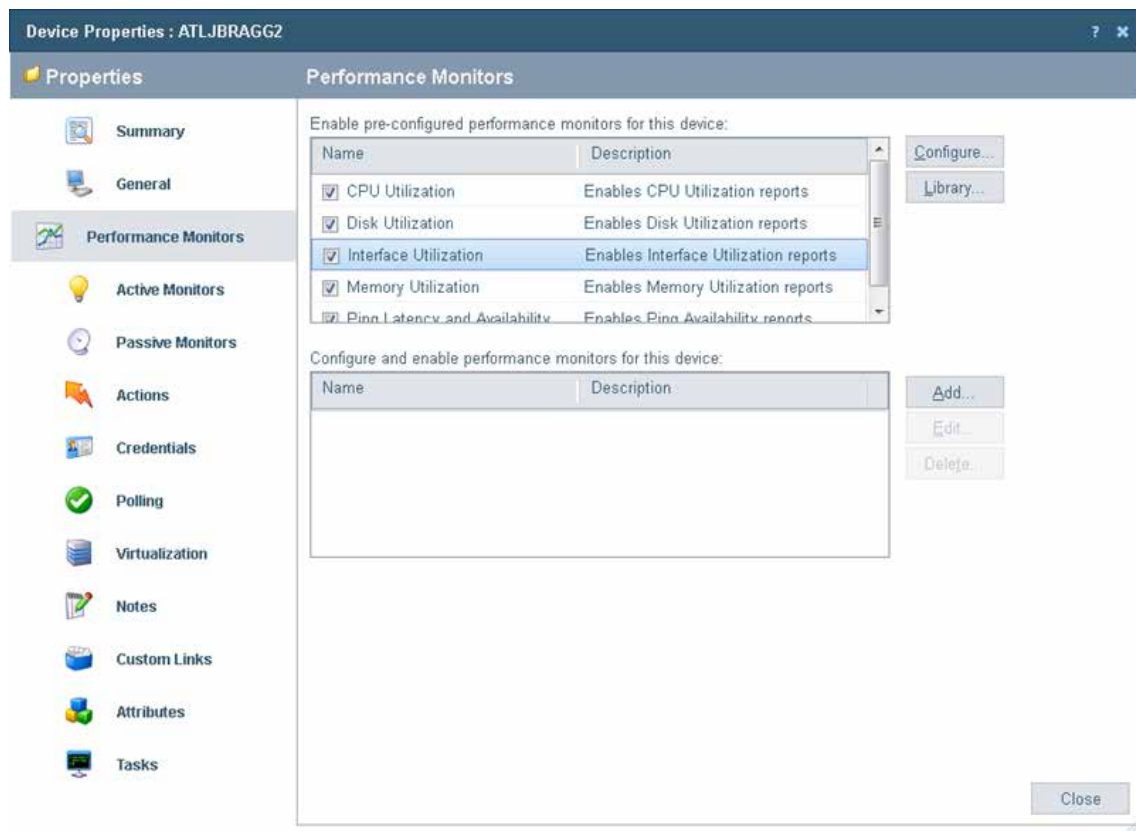
- § Click the options within the same tab in the navigation bar to quickly access other monitor reports. The currently selected group or device and date range is applied to the next monitor report you access.
- § The data in monitor reports can be exported to a formatted text file, Microsoft Excel, or 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 307).



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.** Select options in this list to enable monitors. The following monitors are populated by entries in the *Performance Monitor Library* (on page 452), 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 455).



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.

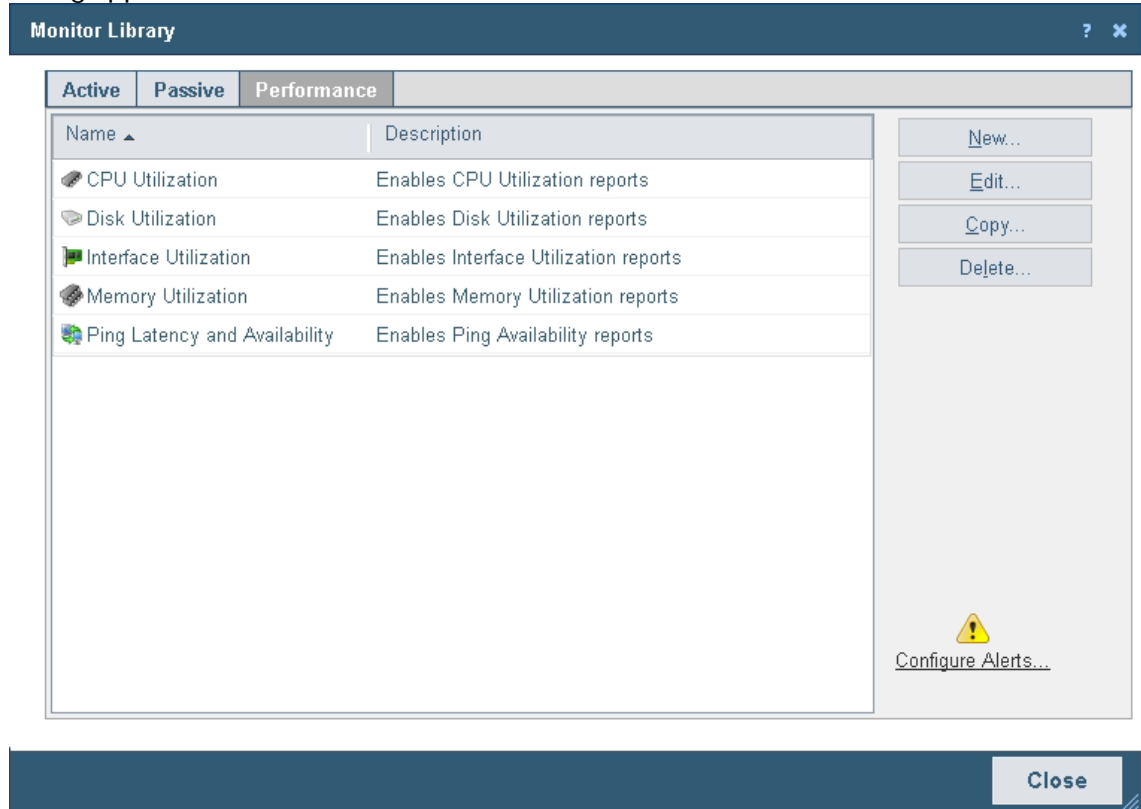
Using the Performance Monitor Library

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.



- 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 685).

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 689) 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 689) 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 688) 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	692
CPU Utilization	692
About the Disk Utilization report	694
About the Memory Utilization report.....	696
About the Custom performance monitor report.....	698

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 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 480).

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.

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.



Note: The Disk Utilization performance monitor data collection is limited to drives that are 16 TB or less.

- § 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.



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 space 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.



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.

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.

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.

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.

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* (on page 45), 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.

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 Time.** 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* (on page 45), 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.

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 description.
- § **Avg Transmit.** The average 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.

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.

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.

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.

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.

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 Acknowledgment 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 Acknowledgment mode, it remains so until you actively acknowledge the state change.



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

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.

- § **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.

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* (on page 45) for that device.

Click the current state to access the State Change Timeline for that device.

Navigation

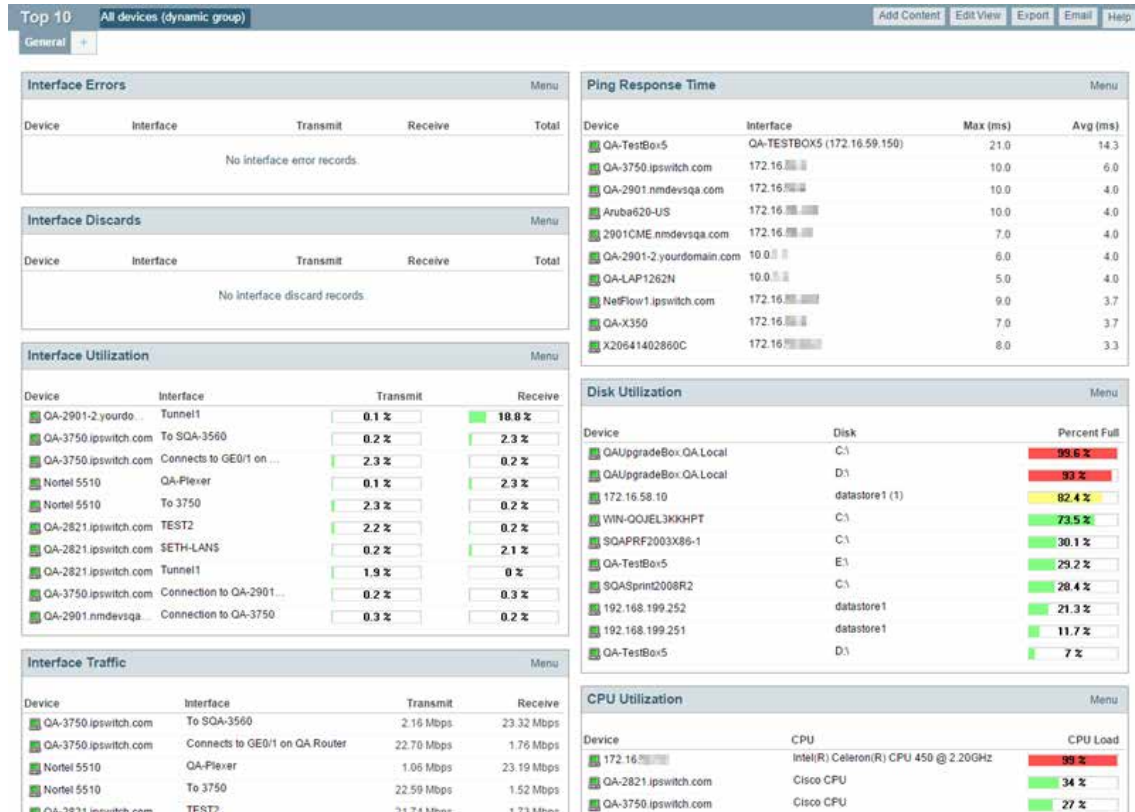
- § Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- § Change to another device monitor report by selecting a different report button.

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.



You can add any of the *Top 10 reports* (on page 229) 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* (on page 48).
- § 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* (on page 50).

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 Chapter

Working with logs.....	721
Using WhatsUp Gold System Logs	727
Using WhatsUp Gold Group / Device Logs.....	736

Working with logs

In This Chapter

Learning about Logs	721
Selecting a device to view logs	722
Changing the report or log date range	722
Changing the date range	722
Using paging options	723
Navigating between logs.....	723
Printing reports and logs.....	723
Using the WhatsUp Gold toolbar buttons.....	723
Managing server options.....	724
Managing Action Policies.....	725
Viewing payload details.....	726

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 669) at the top of a report or log to select a date range and time frame.

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.

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 670) 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

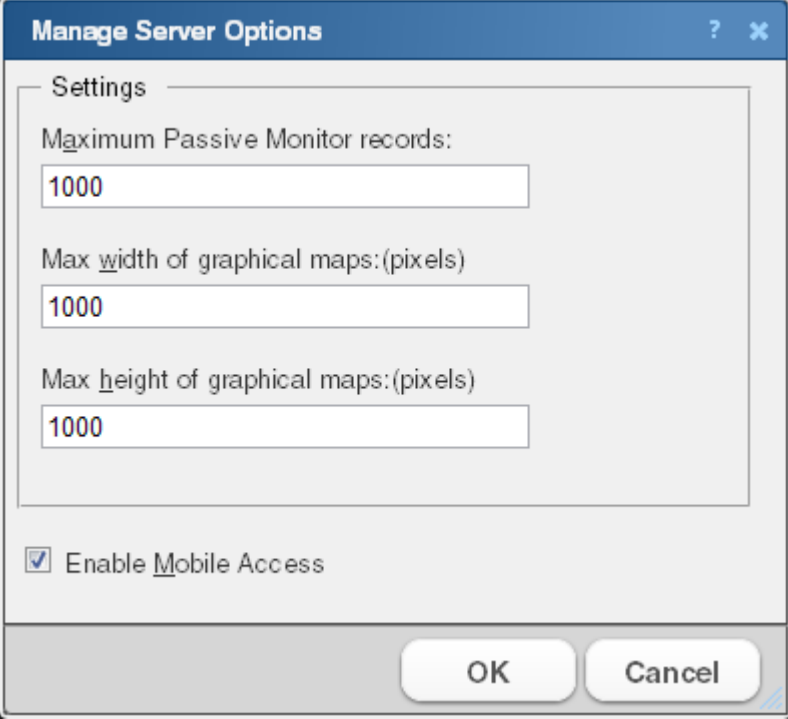
The following toolbar buttons are available:

- § **Add Content.** Add additional dashboard reports to the current dashboard view
- § **Edit View.** Edit settings for the currently displayed dashboard view.
- § **Export.** Export a log from WhatsUp Gold to a PDF file.

- § **Email.** Email a report/log as a PDF attachment or schedule the report/log to be emailed at regular intervals.
- § **Help.** View help content for the current page.

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.

The image shows a 'Manage Server Options' dialog box with a blue title bar. Inside, there is a 'Settings' section with three input fields: 'Maximum Passive Monitor records:' with the value '1000', 'Max width of graphical maps:(pixels)' with the value '1000', and 'Max height of graphical maps:(pixels)' with the value '1000'. Below these fields is a checkbox labeled 'Enable Mobile Access' which is checked. At the bottom right are 'OK' and 'Cancel' buttons.

- 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.

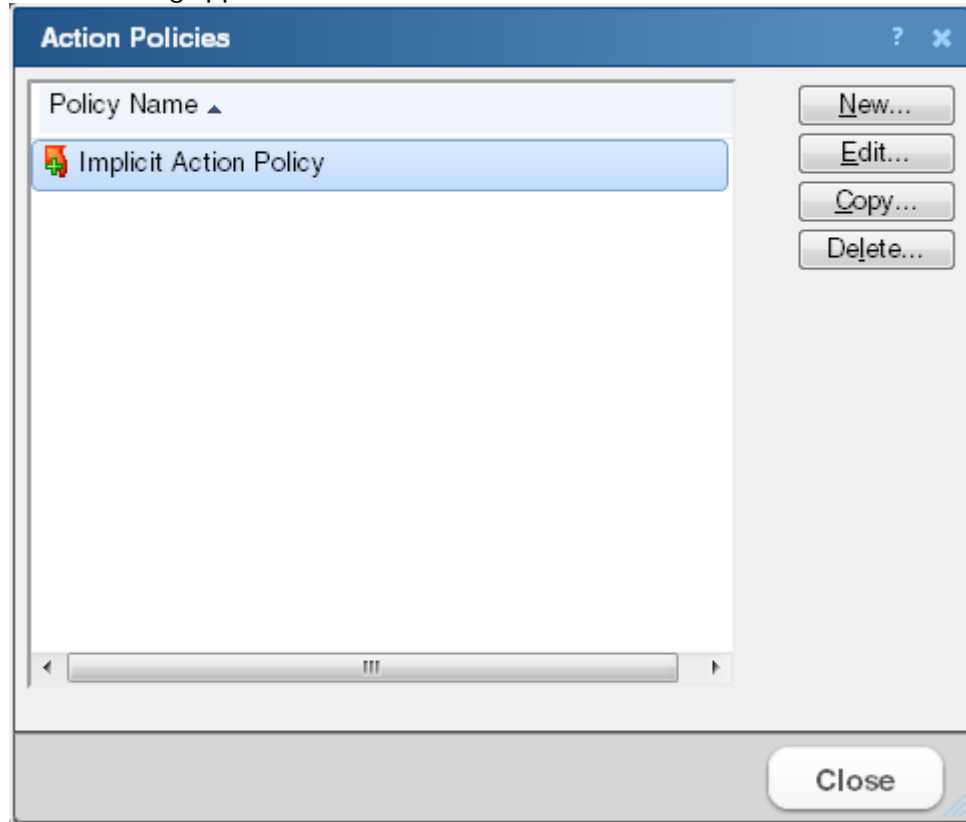
Managing Action Policies

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 656).

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.



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

About the Action Log.....	727
Error Logs.....	729
About the SNMP Trap Log.....	731
About the Syslog Events Log.....	732
About the Windows Event Log.....	733
About the Activity Log	734
About the Scheduled Report Log.....	734
About the Recurring Action Log.....	735
About the Web User Activity Log.....	735

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.

Action Log							
Date range: Today							
Start time: 04/03/2015 12:00 AM							
End time: 04/03/2015 3:33 PM							
Page 1 of 1 (1 - 1 out of 1 rows) Showing 50 rows per page							
Date	Action	Category	Device	Active Monitor	Passive Monitor	Trigger State	Details
Friday, April 03, 2015 03:14:21 PM	Default Web Alarm	cancelled	ATLJBAG...			Maintenance	Cancelled before it could start
Page 1 of 1 (1 - 1 out of 1 rows) Showing 50 rows per page							

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 725).

Error Logs

In This Chapter

About the General Error Log.....	729
About the Passive Monitor Error Log.....	730
About the Performance Monitor Error Log.....	730
About the Logger Error Log.....	730

About the General Error Log

The General Error Log shows a list of error messages generated by WhatsUp Gold for the selected time period.

Error Logs			
General Passive Monitor Performance Monitor Logger			
Date range: Today			
Start time: 04/03/2015 12:00 AM			
End time: 04/03/2015 3:28 PM			
Hide			
Page 1 of 1 (1 - 22 out of 22 rows) Showing 50 rows per page			
Date	Category	Source	Details
Friday, April 03, 2015 12:32:08 PM	failure	NmEngine	Sending an event to the Alert Center threw exception when firing an event through the notification bridge.
Friday, April 03, 2015 12:32:08 PM	failure	NmEngine	Sending an event to the Alert Center threw exception when firing an event through the notification bridge.
Friday, April 03, 2015 12:32:08 PM	failure	NmEngine	Sending an event to the Alert Center threw exception when firing an event through the notification bridge.
Friday, April 03, 2015 12:32:08 PM	failure	NmEngine	Sending an event to the Alert Center threw exception when firing an event through the notification bridge.
Friday, April 03, 2015 08:21:06 AM	Error	NmCollectors	Translation Rate on 192.168.37.82 (device - 2) caused an exception: Invalid class
Friday, April 03, 2015 08:21:06 AM	Error	NmCollectors	Pending Replication Synchronizations on 192.168.37.82 (device - 2) caused an exception: Invalid class
Friday, April 03, 2015 08:21:06 AM	Error	NmCollectors	Pending Inbound Sync Objects on 192.168.37.82 (device - 2) caused an exception: Invalid class
Friday, April 03, 2015 08:21:06 AM	Error	NmCollectors	Pending Replication Operations on 192.168.37.82 (device - 2) caused an exception: Invalid class

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.

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.

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 poller and some WhatsUp Gold services 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.

- § 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* (on page 903). 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 724).

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 726).



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 670) to view more records for the log. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) 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.

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* (on page 904). 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 724).

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 726).



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 670) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) 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.

- § 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* (on page 904).



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 724).

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 726).



Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 670) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) 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.

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 670) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) 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.

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 it 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 670) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) dialog.

About the Recurring Action Log

This log shows a log of recurring actions that were scheduled to fire.

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 670) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) 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.

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 670) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 671) dialog.

Using WhatsUp Gold Group / Device Logs

In This Chapter

About the Actions Applied Log.....	736
About the Blackout Summary Log.....	736
About the Monitors Applied Log.....	737
About the Quarterly Availability Summary.....	738
About the State Summary	740

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.

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.

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 device group, click the Device Group icon located to the right of the web interface tabs.

Log Body

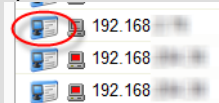
A table displays below the Monitor and Device lists containing data specific to your log selections. For example, if you have selected to view all devices in the group for which a Ping monitor has been configured and assigned, you will see a list of devices on the left-hand side of the log, and a series 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.



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.

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.

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 305) dialog for that device.

Inventory

In This Chapter

Viewing Inventory Reports.....742

Viewing Inventory Reports

In This Chapter

About the Device Info report	742
About the Asset Inventory report	752
About the Device Connectivity report.....	754
About the Installed Software report	755
About the Switch Port Utilization report	756
About the VLAN View	758
About the Subnet View.....	759
About the Computer System report.....	760
About the BIOS report	761
Windows Software Update Report.....	762
About the Windows Services report	764
About the Warranty Information report.....	765

About the Device Info report

The Device Viewer/Device Info report provides detailed information of the layer 2 and inventory details that have been collected for a network device.

Device information is displayed in a series of pages viewable from the **Device Information Type** list. The number of pages displayed in the report list are dependent on the information that was collected from the device during discovery.

The following Device Information Type pages are available:

- § *System* (on page 743)
- § *IP Addresses* (on page 744)
- § *Interfaces* (on page 744)
- § *BridgePorts* (on page 744)
- § *VLANs* (on page 745)
- § *Assets 1* (on page 745)
- § *Assets 2* (on page 746)
- § *Links* (on page 746)
- § *IP Routes* (on page 747)
- § *Spanning Tree Protocol (STP)* (on page 749)
- § *ARP Cache* (on page 749)

- § *Forwarding* (on page 749)
- § *LAG Trunks* (on page 745)
- § *Installed Software* (on page 746)
- § *HSRP 1* (on page 747)
- § *HSRP 2* (on page 747)
- § *VRRP 1* (on page 748)
- § *VRRP 2* (on page 748)
- § *Virtual Machine Host* (on page 750)
- § *Hosted Virtual Machines* (on page 750)
- § *Virtual Machine* (on page 750)
- § *IP Phone Manager* (on page 750)
- § *Windows Computer System* (on page 751)
- § *Windows Operating System* (on page 751)
- § *Windows Logical Disks* (on page 752)
- § *Windows Physical Memory* (on page 752)
- § *Windows Processor* (on page 752)
- § *Windows Services*
- § *Windows Software Updates*
- § *Windows BIOS* (on page 751)
- § *Windows Warranty*

To use the Device Viewer:

- 1 From the WhatsUp Gold web interface, right-click a device in a Device View or Map View tab. The right-click menu appears.
- 2 Click **Device Viewer**. The Device Viewer dialog appears.

- or -

From the WhatsUp Gold web interface, click **Inventory > Device Inventory**. The Device Viewer dialog appears.

- 3 Use the **Device Information Type** list at the top of the report to choose and view report specific report data for the device.

Device Info Report - System information

System Information displays a combination of basic device information from the various ICMP, SNMP, DNS, and NetBIOS protocols.

The page displays the following system information.

- § **IP Address**. The main IP address used to discover the device.
- § **MAC Address**. The MAC address associated with the main IP address.
- § **Host Name**. The DNS host name for the device.
- § **NetBIOS Name**. The NetBIOS name of the machine (if supported).
- § **NetBIOS Domain**. The NetBIOS domain that the machine belongs to (if supported).

- § **System Name.** The SNMP MIB II System Name.
- § **System Location.** The SNMP MIB II System Location.
- § **System Description.** The SNMP MIB II System Description.
- § **System OID.** The SNMP MIB II System Object ID.
- § **System Contact.** The SNMP MIB II System Contact
- § **System Up-Time.** The SNMP MIB II System Up-Time (since last restart)
- § **Category.** The device category that has been assigned to the system based on its functional characteristics.
- § **Network Device.** Flag that indicates whether the device is performing a network device function. (i.e. Router, Switch, Hub, etc.)
- § **Vendor.** Manufacturer of the device
- § **Model.** Model number of the device.
- § **Virtualization Type.** If the device represents a virtual device, this field indicates the type of virtual device (VMware or VirtualPC).

Device Info Report - IP Addresses information

IP Address Information displays the following IP address information.

- § **IP Address.** The device's IP address.
- § **Interface Index.** The IF Index that this IP address is bound to.
- § **Net Mask.** The Net Mask used in association with the IP address.
- § **MAC Address.** The MAC address associated with the IP address.
- § **Hostname.** The hostname of the device associated with the IP address.

Device Info Report - Interfaces information

The Interfaces page displays the following index information.

- § **Index.** The interface index normally associated with the ifIndex of the RFC 1213 ifTable.
- § **Name.** The interface name.
- § **Description.** The interface description.
- § **Alias.** The interface alias name.
- § **Type.** The interface type. This field is defined by the ifType enumeration from the RFC 1213 MIB.
- § **Speed.** The configured data speed of the interface.
- § **Admin Status.** The administration state of the interface (i.e. up, down, unknown).
- § **Oper Status.** The operational state of the interface (i.e. up, down, unknown, testing).
- § **MAC Address.** The MAC address of the interface.

Device Info Report - BridgePorts information

The BridgePort page displays the following bridgeport information.

- § **Index.** The bridge port index.

- § **Interface Index.** The interface index associated with this bridgeport.
- § **IF Name/Descr.** The IF Name + IF Description associated with this bridgeport.
- § **Name.** The name of the bridgeport.
- § **VLAN Name.** The name of the VLAN assigned to this bridgeport.
- § **VLAN Index.** The VLAN index that is assigned to this bridgeport.
- § **VLAN Trunk.** A flag that indicates whether the bridgeport is a VLAN truck (forwarding traffic for more than one VLAN).
- § **LAG Port.** A flag that indicates whether the bridgeport is a member of a Link Aggregation Group (LAG).
- § **Inter-Switch Link.** A flag that indicates whether the bridgeport is used in a connection between two switches (or similar devices).

Device Info Report - VLANs information

The VLANs page displays the following information.

- § **Index.** The VLAN index.
- § **Name.** The VLAN name.
- § **Dot1q Index.** This field indicates if the Dot1q VLAN index differs from the base VLAN Index.
- § **Egress Ports.** The bridge ports that are forwarding traffic for this VLAN. The VLAN traffic is transmitted as TAGGED or ENCAPSULATED unless indicated in **Untagged Ports**.
- § **Untagged Ports.** The bridge ports that are forwarding traffic from this VLAN. The VLAN traffic will be transmitted "in the clear" or UNTAGGED on these bridge ports.
- § **Forbidden Ports.** The bridge ports that are not allowed to forward this VLAN.

Device Info Report - LAG Trunks information

The Link Aggregation Group (LAG) trunk page displays the LAG trunk configuration discovered on the device.

The tab displays the following LAG trunk information.

- § **Index.** Lists the unique index of this LAG trunk.
- § **Name.** Lists the name associated with this LAG trunk.
- § **Base BP Index.** Lists the base Bridgeport index for this LAG trunk.
- § **Member Ports.** A list of Bridgeports that are members of this LAG trunk.

Device Info Report - Assets 1 information

The Assets 1 page displays the following information.

- § **Index.** A unique index for this asset entry.
- § **Class.** The physical class that describes this component (i.e. chassis, module, port, fan).
- § **Name.** The name of the physical component.
- § **Description.** The manufacturer's description of the physical component.

- § **Manufacturer.** The name of the manufacturer.
- § **Model.** The model name for the physical component.
- § **Serial Number.** The serial number for the physical component.
- § **Hardware Version.** The hardware revision for the physical component.
- § **Firmware Version.** The firmware revision for the physical component.
- § **Software Version.** The software version the physical component.

Device Info Report - Assets 2 information

Assets 2 Information displays the following information.

- § **Index.** A unique index for this asset entry.
- § **Port Count.** The port count of the component (if it is a switch/switch module).
- § **Physical Index.** The Entity MIB index.
- § **Switch Index.** In the case of a stacked switch, the switch index in the stack.
- § **Module Index.** In the case of an enclosed chassis/module configuration, the module index of the physical component.
- § **Card Index.** In the case of an enclosed chassis/module configuration, the card index of the physical component.
- § **Alias.** An alias name for the physical component.
- § **Vendor Type.** A vendor index number that is specific to the hardware vendor.
- § **Status.** The current status of the physical component.
- § **Asset ID.** The proprietary asset ID that is assigned to the physical component.
- § **Contained In.** Indicates the index of the physical component that this component is contained in.
- § **Parent Relative Position.** Indicates the relative position when the component is contained in another component (for example, a module index in a chassis configuration)
- § **Field Replaceable Unit.** Indicates whether the item can be replaced in the field.

Device Info Report - Installed Software information

The Software information page shows the installed software that was discovered on the device.

The tab displays the following software information.

- § **Index.** Lists the unique index for the software entry.
- § **Name.** Lists the name of the software package or installation.
- § **Version.** Lists the version of the software element.
- § **Vendor.** Lists the software element's vendor.
- § **Identifying Number.** Lists the manufacturer's identifier for this software element.

Device Info Report - Links information

The Links page displays the following information.

- § **Local Link.** The local physical link, or interface. If no interface information is shown, the connection was made to the device.
- § **Remote Link.** The remote physical link

Device Info Report - IP Routes information

The IP Routes page displays the following information.

- § **Destination.** The destination IP address of this route. Entries of 0.0.0.0 are considered to be a default route.
- § **Net Mask.** The mask used in conjunction with the destination address.
- § **Next Hop.** The IP address of the next hop of this route.
- § **Interface Index.** The index of the local interface through which the next hop of this route should be reached.
- § **Type.** The type of route (i.e. local, direct, indirect)
- § **Protocol.** Routing mechanism by which this route was learned.

Device Info Report - HSRP 1 information

Hot Standby Router Protocol (HSRP) information discovered on this device is displayed on this page. HSRP is the Cisco implementation of VRRP. The information relates to the standby nature of routers.

- § **IF Index.** Lists the interface index on which HSRP is configured.
- § **Group Number.** Lists the HSRP group number. This number in conjunction with the IF Index uniquely identify a HSRP group.
- § **Virtual IP.** Lists the virtual IP address assigned to this interface.
- § **Secondary IPs.** Lists any secondary IP addresses assigned to this HSRP group.
- § **Virtual MAC.** Lists the virtual MAC address assigned to the virtual IP address.
- § **Active Router.** Lists the IP address of the current active router.
- § **Standby Router.** Lists the IP address of the router in standby or backup mode.
- § **Standby State.** Lists the standby state of this HSRP group (initial, learn, listen, speak, standby, active).
- § **Priority.** Lists the priority setting. This setting is used to determine the selection of the active router.
- § **Authentication.** Lists the unencrypted authentication string used in the HSRP configuration.

Device Info Report - HSRP 2 information

Hot Standby Router Protocol (HSRP) information discovered on this device is displayed on this page. HSRP is the Cisco implementation of VRRP. The information relates to the standby nature of routers.

- § **IF Index.** Lists the interface index on which HSRP is configured.
- § **Use Configured Virtual IP.** Lists the setting used to determine if a configured Virtual IP address is used. (TRUE - Virtual IP address is configured, FALSE - Virtual IP address was learned)

- § **Preempt.** Lists the setting used to determine if a router should attempt to overthrow a lower priority active router and attempt to become the active router. (TRUE - the router should attempt to overthrow lower priority active routers, FALSE - the router should not attempt to overthrow lower priority routers; this router will become active only if there are no active routers.)
- § **Preempt Delay.** Lists the time difference between power up and the time the router can start preempting the currently active router.
- § **Use Configured Timers.** Lists setting that determines whether the router should use configured hellotime and holdtime. (TRUE - use configured hellotime and holdtime; FALSE - use learned hellotime and holdtime.)
- § **Configured Hello Time.** Lists the configured hellotime, which is used to determine the frequency of generating hello messages; all routers in a LAN must use the same hellotime. The configured hellotime is used when a router is the active router, otherwise it uses the learned hellotime which is propagated by the active router.
- § **Configured Hold Time.** Lists the configured holdtime; all routers in a LAN should use the same holdtime. The configured holdtime is used when a router is the active router, otherwise it uses the learned holdtime which is propagated by the active router.
- § **Learned Hello Time.** Lists the current learned hellotime.
- § **Learned Hold Time.** Lists the current learned holdtime.

Device Info Report - VRRP 1 information

The Virtual Router Redundancy Protocol (VRRP) information on the device is displayed on this page. The information relates to the standby nature of routers.

- § **IF Index.** Displays the interface used in the virtual routing configuration.
- § **Virtual Router ID.** Displays the virtual router ID (VRID).
- § **Virtual MAC Address.** Displays the virtual MAC address for the virtual routing group.
- § **State.** Displays the operational state of the virtual routing group; either *1 - initialize*, *2 - backup*, or *3 - master*.
- § **Master IP Address.** Displays the primary (primary) IP address. This is the IP address listed as the source in the last VRRP advertisement sent to this router.
- § **Primary IP Address.** Displays the primary or default virtual IP.
- § **Associated IP Addresses.** Displays any secondary virtual IP addresses for the virtual routing group.

Device Info Report - VRRP 2 information

The Virtual Router Redundancy Protocol (VRRP) information on the device is displayed on this page. The information relates to the standby nature of routers.

- § **IF Index.** Displays the interface used in the virtual routing configuration.
- § **Priority.** Displays the priority to be used for the virtual router master election process. A higher value implies a higher priority.
- § **Auth Type.** Displays the authentication type used for VRRP protocol exchanges between virtual routers.

- § **Advertisement Interval.** Displays the time interval in seconds between sending advertisement messages. Only the master router sends VRRP advertisements.
- § **Preempt Mode.** Displays the preempt mode. This mode controls whether a higher priority virtual router will preempt a lower priority master.
- § **Virtual Router Up Time.** Displays the up time, measured since the virtual router transitioned out of the initialized state.
- § **Protocol.** Displays the particular protocol that is controlled by the VRRP; either *1 - ip*, *2 - bridge*, *3 - decnet*, or *4 - other*.

Device Info Report - STP information

The Spanning Tree Protocol (STP) page displays the following information.

- § **Index.** The BridgePort index to which this entry applies.
- § **Designated Root.** The MAC address of the designated spanning-tree root for this bridge port.
- § **Designated Root Device.** The Display Name of the designated root.
- § **Designated Bridge.** The MAC address of the designated bridge for this bridge port.
- § **Designated Bridge Device.** The Display Name of the designated bridge device.
- § **Designated Port.** The designated remote port on the designated bridge device.
- § **State.** The current state of the spanning-tree protocol for this bridge port.

Device Info Report - ARP Cache

The Address Resolution Protocol (ARP) page displays the following information.

- § **IP Address.** The IP address of the ARP entry.
- § **MAC Address.** The MAC address that is associated with the IP address.
- § **IF Index.** The IF index of the interface that this entry was associated with.
- § **Type.** The type of cache element. Each cache element is assigned one of the following values: *1 - other*, *2 - invalid*, *3 - dynamic*, *4 - static*

Device Info Report - Forwarding information

The Forwarding page displays the following information.

- § **BP Index.** The bridge port index associated with this forwarding entry.
- § **IF Name.** The display name of the interface associated with the bridge port.
- § **Remote MAC Address.** The MAC address that is forwarded on the identified bridge port.
- § **Remote Device Name.** The display name of the remote device.
- § **Remote IF Name.** The display name of the interface associated with the bridge port.



Note: A name is only shown when a remote device can be associated with the given MAC address.

- § **Remote MAC Vendor.** The vendor name of the remote device.

Device Info Report - Virtual Machine Host information

The Virtual Machine Host page displays information about the Virtual Machine Host.

- § **Name.** The user-given name for the Virtual Server.
- § **Description.** The user-given description for the Virtual Server.
- § **Host OS.** The operating system of the host machine.
- § **Model.** The vendor model name.
- § **Vendor.** The virtual server's vendor.
- § **Version.** The virtual server's operating system version.
- § **Build.** The vendor's specific build number.

Device Info Report - Hosted Virtual Machines information

The Hosted Virtual Machine page shows all of the defined virtual machines that are hosted by the virtual server.

- § **ID.** The ID assigned to the virtual machine by the host.
- § **Name.** The user-given name for the virtual machine.
- § **Guest OS.** The operating system used in the virtual machine.
- § **State.** Power state of the virtual machine. The available options are: Powered On, Powered Off, or Suspended.
- § **IP Address.** The IP address of the virtual machine (if one can be determined).
- § **MAC Address.** The MAC address assigned to the virtual machine.

Device Info Report - Virtual Machine information

This tab displays information on a single virtual machine.

- § **VMID.** The ID assigned to the virtual machine by the VM host.
- § **Name.** The VM name.
- § **Guest OS.** The operating system type used in the virtual machine.
- § **State.** Power state of the virtual machine; either *Powered On*, *Powered Off*, or *Suspended*.
- § **IP Address.** The IP address of the virtual machine.
- § **MAC Address.** The MAC address of the virtual machine.

Device Info Report - IP Phone Manager information

The IP Phone Manager page details the IP phones that have registered or are communicating with the call manager.

The tab displays the following IP phone information.

- § **IP Address.** Lists the current IP address of the registered IP Phone.
- § **MAC Address.** Lists the MAC address of the registered IP Phone.
- § **Name.** Lists the name of the IP phone.
- § **Description.** Lists the vendor description of the IP phone.

- § **Model.** Lists the model of the IP phone.
- § **Hw Revision.** Lists the hardware revision of the IP phone.
- § **Fw Revision.** Lists the firmware revision of the IP phone.
- § **Sw Revision.** Lists the software revision of the IP phone.
- § **Vendor.** Lists the vendor/manufacturer of the IP phone.
- § **User Name.** Lists the user name registered for this IP phone.
- § **Extension.** Lists the phone extension associated with this IP phone.
- § **E911 Location.** Lists the emergency 911 location of the IP phone.
- § **Status.** Lists the current status of the IP phone.

Device Info Report - Windows Computer System information

The Windows Computer System page displays the following information.

This page displays the following information about the Windows system.

- § **Name.** The type of system, such as a *Virtual Machine*.
- § **Vendor.** The name of the computer system, such as *Microsoft Corporation*.
- § **Identification Number.** The system's unique identification number.
- § **Product Number.** Product identification, such as a serial number on software or a die number on a hardware chip.

Device Info Report - Windows Operating System information

This page displays the following information about the operating system installed on the Windows machine.

- § **Name.** The operating system instance within a computer system, such as *Microsoft Windows Server 2008/C:/Windows/Devices/Harddisk0/Partition3*.
- § **Description.** A description of the Windows operating system.
- § **Caption.** A short description of the operating system and version. Such as, *Microsoft Windows XP Professional Version = 5.1.2500*.
- § **Version.** The operating system version.
- § **OS Architecture.** Architecture of the operating system, as opposed to the processor, such as *32-bit*.
- § **CSD Version.** Indicates the latest service pack installed on the Windows computer.
- § **Serial Number.** The operating system product serial identification number.
- § **Manufacturer.** The name of the operating system manufacturer. For Windows-based systems, this value is *Microsoft Corporation*.
- § **Registered User.** Name of the registered user of the operating system.

Device Info Report - Windows BIOS information

This page displays the following information about the Windows system BIOS.

- § **Name.** The name used to identify the Window BIOS.
- § **Caption.** A short description of the Windows BIOS.

- § **Description.** A description of the Windows BIOS.
- § **Manufacturer.** The BIOS manufacturer.
- § **Release Date.** The release date of the Windows BIOS
- § **Serial Number.** The assigned serial number of the Windows BIOS.

Device Info Report - Windows Processor information

This page displays the following information about the Windows system processor.

- § **Name.** The processor name.
- § **Description.** The processor description.
- § **Address Width.** The address bus width in bits.
- § **Data Width.** The data bus width in bits.
- § **Manufacturer.** The processor manufacturer.

Device Info Report - Windows Physical Memory information

This page displays the following information about the Windows system physical memory.

- § **Tag.** The unique identifier for the physical memory device.
- § **Device Locator.** The socket or circuit board that holds the memory.
- § **Capacity.** The total capacity of the physical memory—in bytes
- § **Speed.** The physical memory speed—in nanoseconds.
- § **Serial Number.** The manufacturer-allocated number to identify the physical element.
- § **Part Number.** The part number assigned by the organization responsible for producing or manufacturing the physical element.

Device Info Report - Windows Logical Disks information

This page displays the following information about the Windows system logical disks.

- § **Name.** Label by which the logical disk is known.
- § **Description.** The description of the logical disk.
- § **File System.** The file system on the logical disk, such as *NTFS*.
- § **Size.** The size of the disk drive.
- § **Free Space.** The space, in bytes, available on the logical disk.

About the Asset Inventory report

The Asset Inventory Report provides a view of the network assets discovered by WhatsUp Gold in the selected device group.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Asset Inventory**.

Log body

The following information is listed in the report:

- § **Device.** Displays the device name.
- § **Description.** Displays the manufacturer's description of the physical component. This column is displayed in the report summary.
- § **Category.** Displays the category in which the device was placed during discovery.
- § **Location.** Displays the physical location of the device.
- § **Contact.** Displays the name of the contact person associated with the device.
- § **SNMP OID.** Displays the SNMP OID associated with the device.
- § **IP Address.** Displays the IP address assigned to the device. This column is displayed in the report summary.
- § **MAC Address.** Displays the MAC address assigned to the device.
- § **Model.** Displays the device model.
- § **Vendor.** Displays the device vendor.
- § **Serial Number.** Displays the serial number of the device. This column is displayed in the report summary.
- § **Service Tag.** Displays the service tag associated with the device.
- § **HW Rev.** Displays the device hardware revision. This column is displayed in the report summary.
- § **Software Rev.** Displays the software revision of the operating system used by the device.
- § **Firmware Rev.** Displays the device firmware revision.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Device Connectivity report

The Device Connectivity Report provides a list of the devices connected to a network device in the selected device group.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Device Connectivity**.

Log body

The following information is listed in the report:

- § **Device.** Displays the name of the device. This column is displayed in the report summary.
- § **Description.** Displays the manufacturer's description of the device.
- § **Category.** Displays the assigned category based on functional characteristics.
- § **Location.** Displays the physical location of the device.
- § **Contact.** Displays the name of the contact associated with the device.
- § **SNMP OID.** Displays the SNMP Object ID assigned to the device.
- § **IP Address.** Displays the IP address of the connected device. This column is displayed in the report summary.
- § **IF Name/Port.** Displays the interface name and associated port. This column is displayed in the report summary.
- § **IF Index.** Displays the interface index.
- § **Connected Device.** Displays the hostname of the connected device. This column is displayed in the report summary.
- § **Connected IP Address.** Displays the IP address of the connected device.

Filtering the report

Use the various lists at the top of the page to filter report data.

- § **Device Filter list.** Select a specific type of device for which to view report data. You can select to view data for *All Network Devices*, *All SNMP Devices*, *All Servers*, or *All Workstations*. Alternatively, keep the default selection of *All Devices* to view report data for all devices in the selected group.
- § **Connected Device Filter list.** Select a specific type of device for which to view report data. You can select to view data for *All Network Devices*, *All SNMP Devices*, *All Servers*, or *All Workstations*. Alternatively, keep the default selection of *All Devices* to view report data for all devices in the selected group.

After you make report filter selections using the lists above, click **Apply** to reload the report with the filtered report information.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Installed Software report

The Software Inventory Report provides a view of software installed on device systems that WhatsUp Gold discovers on the network through SNMP or/and WMI for the selected device group.



Important: Each host device for which you want to collect software inventory information must have SNMP or/and WMI enabled. For more information about enabling SNMP, see the operating system help. Additionally, make sure that SNMP/WMI credentials are configured in WhatsUp Gold. For more information, see *Using the Credentials Library*.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Installed Software**.

Log body

The following information is listed in the report:

- § **Device.** Displays the device name.

- § **Category.** Displays the category in which the device was placed during discovery.
- § **IP Address.** Displays the IP address of the device.
- § **Software Name.** Displays the name of the software found on the device.
- § **Product ID.** Displays the software product ID information.

Filtering the report

To view information for a specific aspect, enter an alphanumeric filter in the **View Filter** box at the top of the report, then click **Apply**. To view information that does not include the filter you specify, select **NOT**.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Switch Port Utilization report

The Switch Port Utilization report provides a list of the bridge ports available on network devices in the selected device group.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Switch Port Utilization**.

Log body

The following information is listed in the report:

- § **Port Total.** Displays the total number of bridge ports provided by all of the discovered network devices. This number is displayed in the report summary.
- § **Ports Used.** Displays the total number of bridge ports being used on all of the discovered network devices. This number is displayed in the report summary.
- § **Device.** Displays the device name. This column is displayed in the report summary.
- § **Description.** Displays the manufacturer's description of the physical component.
- § **Location.** Displays the physical location of the device.
- § **Contact.** Displays the name of the contact person associated with the device.
- § **SNMP OID.** Displays the SNMP Object ID of the network device.
- § **IP Address.** Displays the IP Address of the network device. This column is displayed in the report summary.
- § **Port Count.** Displays the total number of bridge ports provided by the network device. This column is displayed in the report summary.
- § **Ports Used.** Displays the number of bridge ports that are being used on the network device. This column is displayed in the report summary.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the VLAN View

The VLAN Report displays devices in the selected device group that belong to network VLANs.

To view the report:

On the WhatsUp Gold web interface, click Inventory > VLAN View.

Log body

The following information is listed in the report:

- § **VLAN.** The network VLAN name.
- § **Device.** The network device name.
- § **IP Address.** The network device IP address.
- § **Description.** The network device description.

Filtering the report

Use the VLAN list at the top center of the report to select a specific VLAN for which to view report data.

Report customization

Selecting columns

Use the Columns list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the X to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click Filter to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Subnet View

The Subnet Report displays devices in the selected subnets that also exist in the selected device group.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Subnet View**.

Log body

The following information is listed in the report:

- § **Subnet.** The network subnet name.
- § **Device.** The network device name.
- § **IP Address.** The network device IP address.
- § **Description.** The network device description.

Filtering the report

Use the **Subnet** list at the top center of the report to select a specific subnet for which to view report data.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Computer System report

The Windows Computer System Report provides a view of operating system installed on Windows systems that WhatsUp Gold discovers on the network.



Important: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help. Additionally, make sure that WMI credentials are configured in WhatsUp Gold. For more information, see Using the Credentials Library.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Computer System**.

Log body

The following information is listed in the report:

- § **Device.** Displays the device name. This column is displayed in the report summary.
- § **Category.** Displays the category in which the device was placed during discovery.
- § **System Description.** This column is displayed in the report summary.
- § **System Vendor.** Displays the device vendor.
- § **System ID Number.** Displays the device serial number.
- § **Operating System.** Displays the operating system running on the device. This column is displayed in the report summary.
- § **OS Service Pack.** Displays information about the operating system service packs installed on the computer. This column is displayed in the report summary.
- § **OS Manufacturer.** Displays the operating system's manufacturer.
- § **OS Serial Number.** Displays the serial number that was used to register the operating system.
- § **OS Version.** Displays operating system version information. This column is displayed in the report summary.
- § **Memory Capacity.** Displays the amount of the device's RAM that is currently in use. This column is displayed in the report summary.
- § **Total Disk Space.** Displays the total amount of the device's disk space. This column is displayed in the report summary.
- § **Free Disk Space.** Displays the amount of device disk space that is currently free for use.
- § **Processors.** Displays the device processor(s). This column is displayed in the report summary.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the BIOS report

The Basic Input Output System (BIOS) report provides a view of the hardware operating system information for the Windows systems that WhatsUp Gold discovers on the network.



Important: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help. Additionally, make sure that WMI credentials are configured in WhatsUp Gold. For more information, see Using the Credentials Library.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > BIOS**.

Log body

The Device, BIOS Name, and BIOS Description columns display by default. The following is a list of the information available for the report:

- § **Device.** Displays the device name. This column is displayed in the report summary.
- § **Category.** Displays the category in which the device was placed during discovery.
- § **IP Address.** Displays the computer IP address.
- § **BIOS Name.** Displays the name of the BIOS manufacturer. This column is displayed in the report summary.
- § **BIOS Description.** Displays additional BIOS manufacturer description information. This column is displayed in the report summary.
- § **Caption.** Short description of the BIOS.
- § **Release Date.** Displays the BIOS release date information.
- § **Manufacturer.** The manufacturer of this software element.
- § **Serial Number.** Displays the device serial number. This column is displayed in the report summary.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

Windows Software Update Report

The Software Update Report provides a view of software updates on Windows systems that WhatsUp Gold discovers on the network.



Important: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help. Additionally, make sure that WMI credentials are configured in WhatsUp Gold. For more information, see Using the Credentials Library.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Software Updates**.

Log body

The following information is listed in the report:

- § **Device.** Displays the device name. This column is displayed in the report summary.
- § **Category.** Displays the category in which the device was placed during discovery.
- § **IP Address.** Displays the IP address of the device.
- § **Hot Fix.** Displays the KB article associated with the software update fix. This column is displayed in the report summary.
- § **Caption.** Displays the KB article url associated with the hot fix update. This column is displayed in the report summary.
- § **Fix Description.** Displays information about the type of software update that was installed. For example, a security fix or a hot fix. This column is displayed in the report summary.
- § **Comments.** Displays any comments provided about the software update.
- § **Installed By.** Displays username of the person that installed the software.
- § **Installed On.** Displays the date that the software update was installed.
- § **Status.** Displays status information about the software update

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.

- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Windows Services report

The Windows Services Report provides a view of Windows services that WhatsUp Gold discovers running on each network device.



Important: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help. Additionally, make sure that WMI credentials are configured in WhatsUp Gold. For more information, see Using the Credentials Library.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Windows Services**.

Log body

The following information is listed in the report:

- § **Device.** Displays the device name. This column is displayed in the report summary.
- § **Category.** Displays the category in which the device was placed during discovery.
- § **IP Address.** Displays the device IP address.
- § **Name.** Displays the device name.
- § **Caption.** Displays a short description of the service.
- § **Display Name.** Displays the display name of the application service. This column is displayed in the report summary.
- § **Description.** Displays a description for the application service. This column is displayed in the report summary.
- § **Install Date.** Displays the date on which the service was installed.
- § **PathName.** Displays the application service directory path for the executable (.exe) file.
- § **ProcessId.** Displays the service's process ID.
- § **Service Type.** Displays information about whether the application service is a unique or shared service.
- § **Started.** Displays whether the service has started; *True* or *False*.

- § **Start Mode.** Displays the start mode of the Windows base service; either *Boot*, *System*, *Auto*, *Manual*, or *Disabled*.
- § **Start Name.** Displays the account name under which a service runs.
- § **State.** Displays whether the status of the application service (Running or Stopped). This column is displayed in the report summary.
- § **Status.** Displays status information about the software update.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

About the Warranty Information report

The Warranty Information Report provides a view of the hardware warranty information for the Windows systems that WhatsUp Gold discovers on the network.



Important: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help. Additionally, make sure that WMI credentials are configured in WhatsUp Gold. For more information, see Using the Credentials Library.

To view the report:

On the WhatsUp Gold web interface, click **Inventory > Warranty Information**.

Log body

The following information is listed in the report:

- § **Device**. Displays the device name. This column is displayed in the report summary.
- § **Category**. Displays the category in which the device was placed during discovery.
- § **IP Address**. Displays the device IP address.
- § **Warranty**. Displays a information about the software support agreement. This column is displayed in the report summary.
- § **Start Date**. Displays the software support agreement beginning date. This column is displayed in the report summary.
- § **End Date**. Displays the software support agreement ending date. This column is displayed in the report summary.

Report customization

Selecting columns

Use the **Columns** list to select the columns you want displayed in the report. Click to select the check box to the left of a column name to have it display in the report. Clear the check box to remove a column from the report.


Grouping columns

You can click and drag column headers to group report data by one or more columns. Click the **X** to the right of a column name to remove grouping for that column.

Filtering columns

You can view report column data according to user-defined filters.

To create a custom filter for a column:

- 1 Click the  icon for the column you want to filter.
- 2 Use the dialog that appears to define the filter.
- 3 Click **Filter** to apply the filter to the column.



Note: Multiple columns can have filters applied simultaneously.

For information on exporting or emailing the information provided in this report, see *Working with logs* (on page 721).

Alert Center

In This Chapter

Working with Alert Center reports.....768

Using the Alerts Home reports.....774

Configuring notifications.....786

Configuring thresholds.....799

Working with Alert Center reports

Using Alert Center reports

Alert Center reports are used to troubleshoot and monitor Alert Center data.

There are three Alert Center reports:

- § Running Notifications Policies
- § Log Report
- § Items Report

Filtering the Items report

Filter the Items Report by threshold and/or state.

To filter by threshold:

Using the **Filter by threshold** list, select the desired threshold(s).



Note: This list is populated with thresholds currently configured in the Threshold Library.

- § To view items for all thresholds, select **No Filter**.
- § To view items for a specific threshold, select that threshold.
- § To view items for specific threshold type, such as Flow, select that threshold type.

To filter by state:

Using the Filter by state list, select the desired item state(s).

- § To view items in all states, select **No Filter**.

To view items that have been updated to a specific state, select that state. You can select Acknowledged, Resolved, or Acknowledged and Resolved.

To filter by date:

Use the *date/time picker* (on page 669) at the top of the report to select a date range and time frame.

In the **Date range** list, many reports also allow you to specify and customize the business hour report times for reports to display. This allows you to view the network activity only for specified business hours. The date and time format for the date on this report matches the format specified in **Program Options > Regional** set in the WhatsUp Gold console.



Note: The Business Hours setting is available for group reports only.

Using the Item History report

To access the Item History report, click an item in the first column in the Items Report. The history of the selected item displays.

The Items report tracks an item through the system from creation to completion.

The report heading displays the item name, the threshold that triggered the item, the monitored device activity, and the threshold description.

Report body

Below the heading, the report displays the following information for the selected item:

- § **State.** Displays the current state of the item. Possible states include *Out of threshold*, *In threshold*, or *Disabled*.
- § **Notification progress.** Displays the progress status of an assigned notification policy. Possible progress statuses include *Pending*, *Step 1*, *Step 2*, *Step 3*, *Done*, *Acknowledged*, *Resolved*, or *Repeating Step 3*.
- § **Value.** Displays the logged value that caused the item to go out of threshold.
- § **Comment.** Displays any comments entered by the user or the system at the time the item was updated.
- § **Entry time.** Displays the time the item was updated.
- § **Duration.** Displays how long the item spent in the displayed state after it went out of threshold.

Updating Alert Center items

When a monitored device property begins to operate outside of the defined threshold, it appears as an item in a threshold dashboard report on the Alerts Home page. You can update items to either indicate that the issue is known, or remove them from the dashboard report.

To update an item:

- 1 In a threshold dashboard report, click a device name. The Alert Center Item Details dialog appears.

The dialog box is titled "Alert Center Item Details" and contains two main sections: "Item details" and "Update item(s)".

Item details:

- Item icon: A small icon representing a device or server.
- Item name: [Redacted]
- Created by: Performance Disk Utilization Exceeds
- Value: 95%
- Aspect: C:\
- Value: 99.6 %
- Current state: Out of threshold
- Notification progress: Pending
- Created on: April 02, 2015 11:08 PM

Update item(s):

At the top of this section is a dropdown menu set to "Acknowledge". To its right, a note states: "Acknowledged items are being dealt with. Notifications will continue to be sent. The items still appear in the report."

Below the dropdown are four radio button options:

- ☒ Apply to this item.
- ☐ Apply to any items created at the same time as this item
- ☐ Apply to any items older than [] hours
- ☐ Apply to all items in this threshold

At the bottom of the "Update item(s)" section is a text area labeled "Update comments:".

The dialog box has "OK" and "Cancel" buttons at the bottom right.

- 2 In the Update Items area, select how you would like to update the item(s).
 - § **Acknowledge.** Select to indicate that the issue with the item is known. Alert Center continues to send any related notifications regarding the item. The item continues to appear in the dashboard report.
 - § **Resolve.** Select to indicate that any actions required to address the item are complete. Notifications regarding the item stop. The item is removed from the dashboard report.
- 3 Select the item(s) to which you would like to apply the update. Options include:
 - § **Apply to this item.** Select this option to update only the currently viewed item.
 - § **Apply to any items created at the same time as this item.** Select this option to apply the update to any matching items that were created during the same poll.
 - § **Apply to any items older than ____ hours/minutes/days.** Select this option to apply the update to all alerts older than the time you select. This option is useful when one device fails and impacts numerous other devices, such as when attempting to ping devices on the other side of a failed router. Selecting to resolve all items that were

added at the same time as the router failure saves the time it would otherwise take to acknowledge each item individually.

§ **Apply to all items in this threshold.** Select this option to update any items that currently exist for this threshold.


- 4 After selecting the appropriate update, enter a brief comment in the **Update comment** boxes explaining the actions taken to address the issue.



Note: Comments are optional but recommended for your records.

- 5 Click **OK** to save changes.



Note: Items that have been acknowledged display a green check mark  next to their name on Alert Center Home threshold dashboard reports.

A note about notifications

Notifications are affected depending upon how you choose to acknowledge items. There are two basic scenarios when resolving items:

Single-item threshold

One item exists in a threshold and you acknowledge or resolve that item. The corresponding notification is also deleted and no more notifications for the item are sent.

Multiple-item threshold

Several items fall out of threshold at the same time and one notification is sent for the group of items. If you acknowledge or resolve only one item, a corresponding notification persists for all other unacknowledged and unresolved items.

However, if you select one item from the group, acknowledge or resolve it, and then select **Apply to any items created at the same time as this item**, the corresponding notification stops for all items that were created at the same time as the selected item.

Understanding resolving items - examples

When you mark an out-of-threshold item as resolved, the Alert Center ignores the item until the sample period does not include the time the item was resolved. This gives you one full sample period to fix the problem.

Example #1 - Marking an item as resolved without fixing the underlying problem will cause the item to appear again during the next sampling interval

Threshold: Disk Utilization exceeds 90%

Sample period: 1 day

Polling interval: 1 hour

Scenario:

Tuesday, 1:00 pm - Device exceeds disk utilization threshold and appears in the Items Report.

Tuesday, 1:05 pm - Item is marked as resolved, but no additional resources are provided to the device to solve the disk utilization issue.

Wednesday, 2:00 - During the next sample period, WhatsUp Gold checks the database and finds the device is out-of-threshold again. The device appears in the Items Report a second time.

Example #2 - Marking an item as resolved and fixing the issue before the next poll causes Alert Center to ignore the device during the next poll

Threshold: SNMP Trap exceeds 500 traps per hour

Sample period: 1 day

Polling interval: 30 minutes

Scenario:

Tuesday, 1:00 pm - Alert Center checks the WhatsUp Gold database for the previous 30 minutes and finds a device exceeding the threshold for SNMP traps.

Tuesday, 1:10 pm - You see the device listed as out-of-threshold, and you mark it resolved.

Tuesday, 1:30 pm - Alert Center checks the WhatsUp Gold database. The device is marked "resolved," so Alert Center ignores the device.

Tuesday, 1:35 pm - You turn off the SNMP trap agent on the device that is sending so many messages to the receiving device.

Tuesday, 2:00 pm - The device does not appear in the out of threshold items list.



Note: If you did not address the SNMP agent before the next poll, the device would again appear in the list of out of threshold devices.



Note: This method of resolving items does not apply to the WhatsUp Health threshold.

Filtering the Log report

You can filter the log report using the following methods:

Filter by date:

Use the **Date range** list at the top of the report to select a time frame for the report. By default, the report displays log entries for the previous hour.

Filter by severity level:

Use the **Filter by severity level** list to select a logging level for the report.

- § **No Filter** displays messages for every entry level.
- § **Critical** displays only critical messages.
- § **Error** displays only error messages.
- § **Warning** displays only warning messages.
- § **Information** displays only information messages.

Configuring Alert Center records to expire

You can configure the length of time to keep Alert Center data in your database on the Configure Database Record Expiration dialog.

To configure Alert Center data expiration settings:

- 1 From the Alert Center tab, click **Record Maintenance**. The **Configure Database Record Expiration** dialog appears.
- 2 Specify expiration settings:
 - § **Alert Center Log**. Enter a number of days and/or hours after which you would like to expire data for this report. Data that is expired is deleted from the database.
 - § **Alert Center Items**. Enter a number of days and/or hours after which you would like to expire data for this report.
- 3 Click **OK** to save changes.

Using the Alerts Home reports

Using the Performance CPU threshold report

This Alert Center Home report displays the following threshold information for a CPU utilization threshold:

- § **Device.** The network device that has gone out of the parameters of the CPU utilization threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- § **Number of CPUs.** Indicates the number of CPUs used to calculate the overall CPU utilization for the device that has gone out of the parameters of the CPU utilization threshold.
- or -
CPU. Indicates the CPU name that has gone out of the parameters of the CPU utilization threshold.
- § **Average Utilization**
- § **Device.** If the *device* option is selected for the Report Per CPU threshold option, this is the average CPU utilization (all CPUs combined). Therefore, if the average CPU performance of a quad-core CPU (an average of all CPU performance combined) exceeds the threshold, then the average utilization for the combined CPU is displayed and an alert is triggered.
- or -
- § **CPU.** If the *CPU* option is selected for the Report Per CPU threshold, this is the average utilization of a specific CPU. Therefore, if one of the CPUs on a quad-core CPU exceeds the threshold, then the average utilization for the individual CPU is displayed and an alert is triggered.



Tip: Click an average utilization value to view the *CPU Utilization* (on page 692) report for that device.

- § **Time alerted.** The time the Alert Center discovered the CPU out of threshold.

Using the Performance Custom threshold report

This Alert Center Home report displays the following threshold information for a custom performance monitor threshold:

- § **Device.** The network device that has gone out of the parameters of the custom performance monitor threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Custom performance monitor.** The specific custom performance monitor on this device that has gone out of the parameters of this threshold.
- § **Value.** The value of the custom performance monitor.
- § **Time alerted.** The time the Alert Center discovered the monitor out of threshold.

Using the Performance Disk threshold report

This Alert Center Home report displays the following threshold information for a disk utilization or free space threshold:

- § **Device.** The network device that has gone out of the parameters of the disk utilization or free space threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- § **Disk.** The disk that has gone out of the parameters of the disk utilization or free space threshold.
- § **Average utilization.** The average utilization of the disk or free space available during the sample time period.



Tip: Click an average utilization value to view the *Disk Utilization* (on page 694) report for that device.

- § **Time alerted.** The time the Alert Center discovered the disk utilization or free space out of threshold.

Using the Performance Interface threshold report

This Alert Center Home report displays the following threshold information for an interface utilization threshold:

- § **Device.** The network device that has gone out of the parameters of the interface utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Interface.** The specific interface that has gone out of the parameters of the interface utilization threshold.
- § **Average utilization.** The average utilization of the interface during the sample time period.



Tip: Click an average utilization value to view the *Interface Utilization* (on page 700) report for that device.

- § **Time alerted.** The time the Alert Center discovered the interface was out of threshold.

Using the Interface Errors and Discards threshold report

This Alert Center Home report displays the following threshold information for inbound and outbound device interface discards or errors response time thresholds.

§ **Device.** The network device that has gone out of the threshold parameters.



Tip: Click a device to view the Alert Center Item Details for that device.

§ **Interface.** The specific interface on which the inbound and/or outbound interface discards or errors response time is out of threshold.

§ **Discards or Errors.** The number of inbound and/or outbound interface discards or errors per minute during the sample time period.



Tip: Click an average response time to view the *Ping Response Time* (on page 706) report for that device.

§ **Time Alerted.** The time the Alert Center discovered the inbound and outbound interface discards or errors out of threshold.

Using the Performance Memory threshold report

This Alert Center Home report displays the following threshold information for a memory utilization threshold:

§ **Device.** The network device that has gone out of the parameters of the memory utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

§ **Memory.** The specific memory that has gone out of the parameters of the memory utilization threshold.

§ **Average utilization.** The average utilization of the memory during the sample time period.



Tip: Click an average utilization value to view the *Memory Utilization* (on page 696) report for that device.

§ **Time alerted.** The time the Alert Center discovered the memory out of threshold.

Using the Performance Ping Availability threshold report

This Alert Center Home report displays the following threshold information for a ping availability threshold.

§ **Device.** The network device that has gone out of the parameters of the ping availability threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- § **Interface.** The specific interface on which the ping packet loss is occurring.
- § **Percent Packet Loss.** The percentage of packets lost during the sample time period.



Tip: Click a packet loss value to view the *Ping Availability* (on page 704) report for that device.

- § **Time Alerted.** The time the Alert Center discovered the ping availability out of threshold.

Using the Ping Response Time threshold report

This Alert Center Home report displays the following threshold information for a ping response time threshold.

- § **Device.** The network device that has gone out of the parameters of the ping response time threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Interface.** The specific interface on which the ping response time is out of threshold.
- § **Response Time Average.** The average ping response time during the sample time period.



Tip: Click an average response time to view the *Ping Response Time* (on page 706) report for that device.

- § **Time Alerted.** The time the Alert Center discovered the ping response time out of threshold.

Using the SNMP Trap threshold report

This Alert Center Home report displays the following threshold information for an SNMP Trap threshold.

- § **Device.** The network device that has gone out of the parameters of the SNMP trap threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Trap.** The specific trap that has gone out of the parameters of the threshold.
- § **Trap Count.** The number of traps received for this specific trap during the sample time period.



Tip: Click a trap count value to view the *SNMP Trap Log* (on page 731) for that device.

- § **Time Alerted.** The time the Alert Center discovered the number SNMP traps out of threshold.

Using the Syslog threshold report

This Alert Center Home report displays the following threshold information for a Syslog threshold.

- § **Device.** The device that has gone out of the parameters of the Syslog threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Syslog.** The specific Syslog that has gone out of the parameters of the threshold.
- § **Message Count.** The number of Syslog messages received for that specific Syslog.



Tip: Click a message count value to view the *Syslog* (on page 732) report for that device.

- § **Time Alerted.** The time the Alert Center discovered the number of Syslog messages out of threshold.

Using the Windows Event Log threshold report

This Alert Center Home report displays the following threshold information for a Windows Event threshold.

- § **Device.** The network device that has gone out of the parameters of the SNMP trap threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Windows Event.** The specific Windows event that has gone out of the parameters of the threshold.
- § **Windows Event Count.** The number of Windows events received for this specific event type during the sample time period.



Tip: Click an event count value to view the *Windows Event Log* (on page 733) for that device.

- § **Time Alerted.** The time the Alert Center discovered the number of Windows events out of threshold.

Using the Flow Monitor Conversation Partners threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor conversation partners threshold.

- § **Host.** The host that has gone out of the parameters of the conversation partners threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Conversation Partners.** The number of conversation partners sending or receiving data with the host.



Tip: Click a conversation partners value to view the Interface Details report.

- § **Time Alerted.** The time the Alert Center discovered the host's number of conversation partners out of threshold.

Using the Flow Monitor Custom threshold report

This Alert Center Home report displays the following threshold information for a Flow custom threshold.

- § **Host.** The Flow Monitor host that has gone out of the parameters of the custom threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Bytes.** The number of bytes transferred.



Tip: Click a bytes value to view the Interface Details report.

- § **Time Alerted.** The time the Alert Center discovered the number of bytes out of threshold.

Using the Flow Monitor Failed Connections threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor failed connections threshold.

- § **Host.** The host that has gone out of the parameters of the failed connections threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Failed connections.** The number of failed connections the host has sent or received.



Tip: Click a failed connections value to view the Interface Details report.

- § **Time Alerted.** The time the Alert Center discovered the host's number of failed connections out of threshold.

Flow Monitor Interface Traffic threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor interface traffic threshold.

§ **Interface** displays the source interface over which traffic is transmitting.



Tip: Click a host to view the Alert Center Item Details for that interface.

§ **Interface traffic** displays the amount of traffic that has been transmitted over the sample time period.



Tip: Click an interface value to view the Interface Details report.

§ **Time Alerted** displays the time Alert Center discovered the interface's traffic amount out of threshold.

Using the Flow Monitor Top Sender/Receiver threshold report

This Alert Center Home report displays the following threshold information for the Flow Monitor top sender/receiver threshold.

§ **Host.** The host that has gone out of the parameters of the top sender/receiver threshold.



Tip: click a device to view the Alert Center Items Report for that device.

§ **Bytes transferred.** The number of bytes sent or received by a host.



Tip: Click a bytes value to view the Interface Details report.

§ **Time Alerted.** The time the Alert Center discovered the host's total number of bytes sent or received out of threshold.

Using the Blackout Summary threshold report

This Alert Center Home report displays the following threshold information for a blackout summary threshold.

§ **Device.** The device for which the action would have been triggered.

§ **Action.** The action that was not fired due to the blackout.

§ **Occurrences.** The number of times the action would have fired had the action not been in a blackout period.



Tip: Click an entry in the **Occurrences** column to view the *Blackout Summary Log* (on page 736).

- § **Time Alerted.** The time the Alert Center was alerted; Alert Center is notified of action activity when the blackout period ends.

Using the WhatsUp Health threshold report

This Alert Center Home report displays the following threshold information for a WhatsUp Health threshold.

- § **System Aspect.** The aspect of your system that has gone out of threshold. For example, Flow service, Total expired records, or WUG service.



Tip: click a device to view the Alert Center Items Report for that device.

- § **Value.** The length of time in which the service has met the threshold parameters.
- § **Help Link.** Click this link for a list of ways you can resolve problems associated with the out of threshold item.
- § **Time Alerted.** The time the Alert Center discovered the system aspect out of threshold.

Failover threshold report

This Alert Center Home report displays the following threshold information for a Failover threshold.

- § **Source.** The machine on which the failover event took place.



Tip: Click a device to view the Alert Center Item Details for that device.

- § **Category.** The category of activity and message; either information or error.
- § **Message.** The message generated as a result of the failover event.



Tip: Hover over a message with your mouse to view the message in its entirety.



Tip: Click an entry in the Message column to view the *General Error Log* (on page 729).

- § **Time Alerted.** The time the Alert Center discovered the failover event.

Using the WhatsConfigured Threshold report

This Alert Center Home report displays the following threshold information about a WhatsConfigured task.

- § **Description.** Describes the task threshold.
- § **Device.** The device where the WhatsConfigured task ran.
- § **Configuration result.** The WhatsConfigured task result.
- § **Time Alerted.** The time Alert Center received the tasks configuration results.

WhatsVirtual events threshold report

The WhatsVirtual events threshold report displays events collected from the vCenter server that are of the type selected in the threshold definition. The events appear in reverse chronological order, so that the last event received appears at the top of the list.

- § **Target.** Displays the virtual server, host or virtual device that was the target of the event. The display format is either *<Datacenter - VMware Host name - virtual machine name>*, or *<vCenter server name>*.
- § **User.** Displays the user that initiated the event.
- § **Message.** Displays the message received from the vCenter server that describes the event.
- § **Date.** Displays the date and time that the event was received by the Alert Center.



Note: The WhatsVirtual events threshold can be created for any of the event groups that WhatsVirtual can collect from the vCenter server.

Using the All Wireless Thresholds report

The Alert Center Home report displays all active wireless threshold reports in dashboard format when the Wireless filter is applied. The wireless threshold report filter options are:

- § *Wireless Access Point RSSI* (on page 536)
- § *Wireless Banned Client MAC Addresses* (on page 537)
- § *Wireless Client Bandwidth*
- § *Wireless CPU* (on page 537)
- § *Wireless Device Over Subscription* (on page 537)
- § *Wireless Excessive Rogues* (on page 538)
- § *Wireless Memory* (on page 538)
- § *Wireless Rogue Access Point MAC Addresses* (on page 538)
- § *Wireless Rogue Hidden SSID* (on page 538)
- § *Wireless Rogue Specific SSID* (on page 538)
- § *Wireless Rogue Unknown* (on page 539)

Using the Wireless Access Point RSSI report

The Alert Center Home report displays the following threshold information when the Wireless Access Point RSSI filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **RSSI%.** Displays the percentage when the average RSSI exceeds the configured percentage for more than the specified time range. The default threshold percentage is 20%.

- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Banned Client MAC Addresses report

The Alert Center Home report displays the following threshold information when the Wireless Banned Client MAC Address Alert filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the banned MAC address associated with the device that triggered the alert.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless CPU report

The Alert Center Home report displays the following threshold information when the Wireless CPU filter is applied:

- § **Device.** Displays the name of the device.
- § **CPU.** Displays the type of CPU for the selected device.
- § **Average Utilization.** Displays the average wireless CPU utilization percentage for the selected time interval when utilization exceeds the selected utilization threshold.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Client Bandwidth report

The Wireless Client Bandwidth report displays the following threshold information when the Wireless Client Bandwidth filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the banned MAC address associated with the device broadcasting SSIDs in the specified time interval.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Device Over Subscription report

The Alert Center Home report displays the following threshold information when the Wireless Access Point Over Subscription filter is applied:

- § **Device.** Displays the name of the device.
- § **Number of Clients.** Displays the average number of clients over the selected time period that have run on the device since the threshold was initially measured. The client average is rounded to two decimal places.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Excessive Rogue Alert report

The Alert Center Home report displays the following threshold information when the Wireless Excessive Rogue Alert filter is applied:

- § **Device.** Displays the name or IP address of the access point hosting one or more potential rogue devices depending on the threshold configuration.
- § **Number of Clients.** Displays the number of potential rogues seen on the displayed access point.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Memory report

The Alert Center Home report displays the following threshold information when the Wireless CPU filter is applied:

- § **Device.** Displays the name of the device.
- § **Memory.** Displays the available memory for the selected device.
- § **Average Utilization.** Displays the average wireless memory utilization percentage for the selected time interval when utilization exceeds the selected utilization threshold.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Access Point MAC Address Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Access Point MAC Address Alert filter is applied:

- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the rogue MAC address associated with the device that triggered the alert.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Hidden SSID Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Hidden SSID filter is applied:

- § **Device.** Displays the name of the device.
- § **MAC Address.** Displays the MAC address associated with the device.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Specific SSID Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Specific SSID filter is applied:

- § **Device.** Displays the name of the device.

- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the MAC address associated with the device.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Using the Wireless Rogue Unknown SSID Alert report

The Alert Center Home report displays the following threshold information when the Wireless Rogue Unknown SSID filter is applied:








- § **Device.** Displays the name of the device.
- § **SSID.** Displays the Service Set Identifier for the device.
- § **MAC Address.** Displays the MAC address associated with the device.
- § **Time Alerted.** Displays the time the threshold was reached or passed.

Configuring notifications

Using Alert Center and actions

Alert Center lets you receive alerts for performance monitors, the WhatsUp Gold system, and WhatsUp Gold Flow Monitor plug-in addition to alerts you can receive for active and passive monitors through actions.

The table below shows the system you use to receive alerts of a particular type.

	Actions	Alert Center
Alerts on active monitors		
Alerts on passive monitors		
Alerts on performance monitors		
Alerts on the WhatsUp Gold database		
Alerts on WhatsUp Gold services		
Alerts on WhatsUp Gold Flow Monitor		

Alert Center and actions are different systems and have different functions.

While Alert Center displays alerts on the Alerts Home page and in email notifications, there are many different types of tasks you can perform using actions. Actions allow you to restart services, reboot systems, send text messages, and perform many other tasks. Used together, Alert Center and actions help you more thoroughly support and manage your network.

For more information on alerting through actions, see *Using Actions* (on page 611).

For more information on alerting through Alert Center, see Using Notification Policies.

Alert Center Percent Variables

The Email, SMS, and SMS Direct Actions can include three categories of percent variables in Alert Center notification message:

- § Threshold
- § Notification Policy
- § System

Use Alert Center percent variables in the Alert Center message body for SMS Direct and SMS action notifications, and in the subject line of Email notifications.

Threshold percent variables

Name	Description
%AlertCenter.Threshold.ID	The threshold ID listed in the ProActiveAlert table.
%AlertCenter.Threshold.Name	The threshold name.
%AlertCenter.Threshold.Description	The threshold description.
%AlertCenter.Threshold.PollingInterval	The threshold polling interval.
%AlertCenter.Threshold.TotalItems	The total new new and current items out of threshold.
%AlertCenter.Threshold.TotalNewItem	The total of newly alerted items.
%AlertCenter.Threshold.TotalCurrentItems	The total of existing items out of threshold (not including new items).
%AlertCenter.Threshold.TotalMonitoredItems	The count of items that can be evaluated in the threshold, i.e. there are 22 devices that have a Disk Performance Monitor configured.
%AlertCenter.Threshold.TotalAutoResolvedItems	The number of items automatically resolved.
%AlertCenter.Threshold.NewItemNames	The display name of each new item in an alert.
%AlertCenter.Threshold.CurrentItemNames	The display name of each current item in an alert.

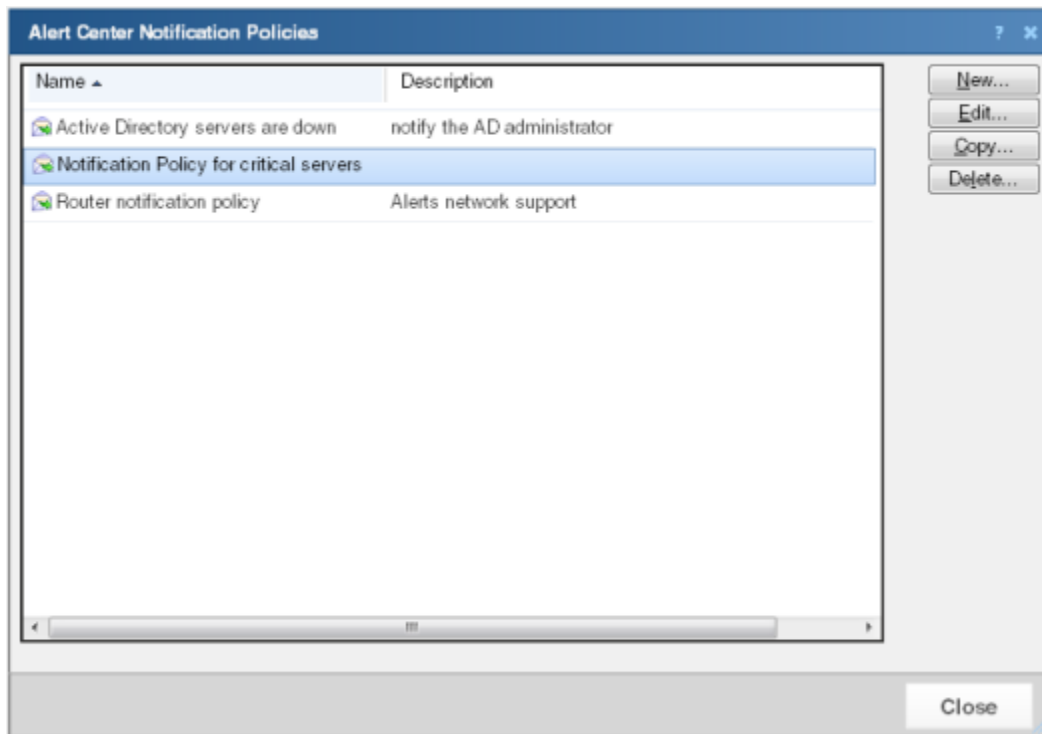
Notification policy percent variables

Name	Description
%AlertCenter.NotificationPolicy.ID	The notification policy ID.
%AlertCenter.NotificationPolicy.Name	The notification policy name.
%AlertCenter.NotificationPolicy.Description	The notification policy description.
%AlertCenter.NotificationPolicy.Recipients	The list of actions included in the policy.
%AlertCenter.NotificationPolicy.NextEscalationTime	When the next step is to be sent.
%AlertCenter.NotificationPolicy.EscalationStep	The current escalation step.

System percent variables

Name	Description
%System.Date	The current system date.
%System.Time	The current system time.

Using Alert Center Notification Policy options



To access notification policy options:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Policies**. The Alert Center Notification Policies dialog appears.
 - § Click **New** to configure a new policy.
 - § Select a policy, then click **Edit** to modify the policy configuration.
 - § Select a policy, then click **Copy** to make a duplicate of the selected policy.
 - § Select a policy, then click **Delete** to remove the policy from the dialog.



Caution: When you delete a policy from the list, it is removed from any threshold to which it is assigned.

Configuring a notification policy



Note: It is not required that you select a notification policy for use with every threshold. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report with the out of threshold items appears on the Alerts Home page.

To create a notification policy:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Policies**. The Alert Center Notification Policies dialog appears.

- 3 Click **New**. The New Alert Center Notification Policy dialog appears.

Edit Alert Center Notification Policy
?
✕

Name:

Test Policy

Description:

Test Policy

Select which notifications will be delivered by each step of this policy:

Notification ▲	Type	Step 1	Step 2	Step 3	Blackout Policy
Test Action	SMS Action	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Business Hours (Te: ▼
Test Action 2	SMS Action	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	On Call Work Week ▼
Test Action 3	SMS Action	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	(None) ▼

Escalation Steps

Step 2 begins

1.00

hours ▼

after the notification starts

Step 3 begins

2.00

hours ▼

after the notification starts

☐ Repeat step 3 every

1

minutes ▼

until the notification is stopped

Show me a graph of this notification policy in action

OK

Cancel

- 4 Complete the identifying information for the policy.
 - § **Name.** Type a name for the notification policy. The name identifies the policy in the Alert Center Notification Policies dialog.
 - § **Description.** Enter a description of the policy. The description appears next to the policy name in the Alert Center Notification Policies dialog.
- 5 Select the notifications you would like delivered for each of the three steps in the policy. You can select multiple notifications for each policy step. To select a notification, click the boxes for the step of the policy that you would like the notification to be sent. For example, if you would like an email sent to Bob for the policy's first step, select the **Step 1** boxes for the Email Bob notification. Continue the same for Step 2 and Step 3. Step 1 of the notification policy begins as soon as an item falls out of threshold. You can specify when steps 2 and 3 begin in the Escalation Steps section of the dialog. If you do not see


an appropriate notification, or if the list is empty, click browse (...) to open the Notification Library and configure a new notification.

- 6 If desired, use the drop-down list to select and apply a configured blackout policy for any individual notification. If an applied blackout policy is in effect:
 - a) Notifications for the threshold will resume after that blackout policy ends.
 - b) The subsequent action in the notification policy will continue to fire.
- 7 Select the how the policy notifications proceed after Step 1 in the **Escalation Steps** section.
 - § Specify a start time for steps 2 and 3 of the policy. By default, step 2 is set to begin 1 hour after the first notification occurs, and step 3 is set to begin 2 hours after the first notification.
 - § You can choose to repeat step 3 of the policy at a regular interval until the notification is stopped. By default, the policy is set to repeat step 3 every hour until the notification is stopped.



Note: In order for this repeat function to work properly, step 3 must be enabled for at least one notification in the policy.



Tip: You can view a graph of the notification policy in action by clicking  **Show me a graph of this notification policy in action.**

- 8 Click **OK** to save changes.

Configuring an Alert Center email notification

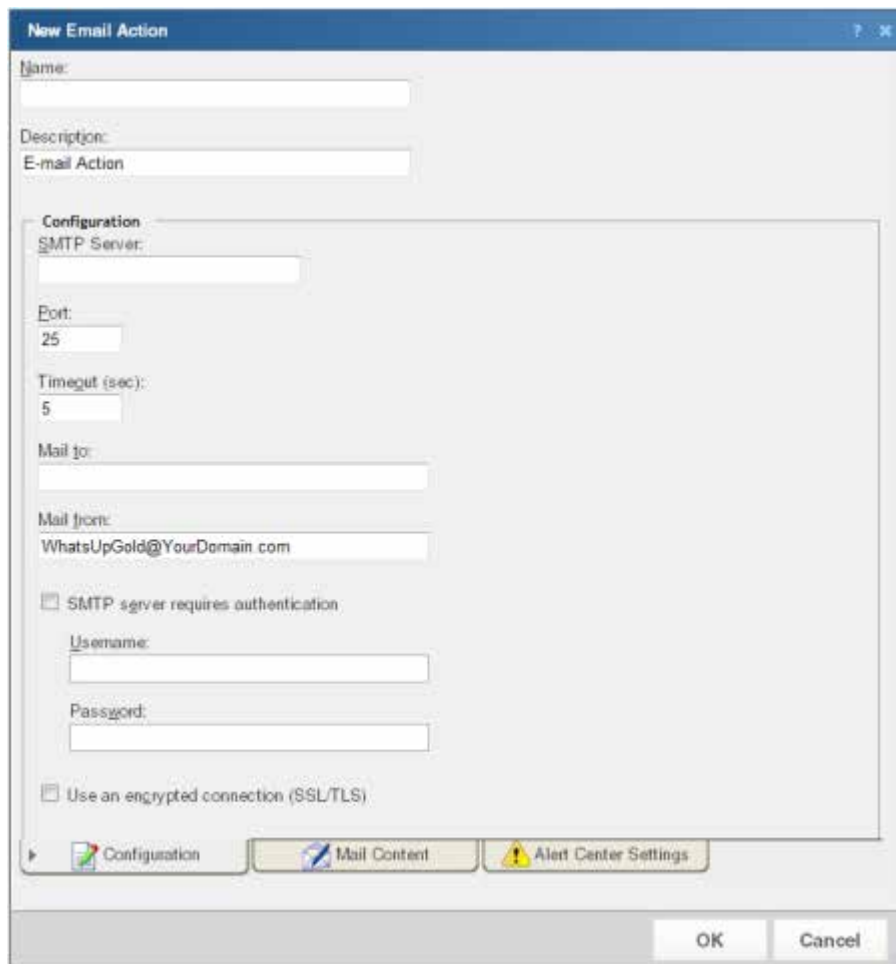
Alert Center email notifications and WhatsUp Gold email actions use the same configuration dialog.

For more information about Email Actions, see *Using the Email Action* (on page 552).

To configure an email notification:

- 1 Click the **Alert Center** tab, then click **Notification Library**. The Alert Center Notification Library dialog appears.
- 2 Click **New**. The Select Notification Type dialog appears.

- 3 Select **E-mail Action**, then click **OK**. The New Email Action dialog appears.



- 4 Complete the appropriate information in the dialog box.
 - § **Name.** Type a name for the action. This name identifies the action in the Notification Library.
 - § **Description.** Enter a few words to describe the action. This description displays beside the action name in the Notification Library.
- 5 Click the **Alert Center** tab to complete the appropriate Alert Center settings for the Email notification.

The **Alert Center Settings** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

- § **Alert Center Message Subject.** Enter a subject for the message. This text appears as the subject in the email that is sent by the Alert Center notification. This subject can include percent variables.



Tip: To include *Alert Center percent variables* (on page 540), right click inside the above boxes.

- § **Alert Center Link.** Select **Include hyperlink to Alert Center in the email content** to include a link to the Alerts Home page in the email message sent by the Alert Center notification.
- § **Use HTTP or Use HTTPS.** Select the appropriate protocol to use in the link address.
- § **Use dynamic address or Use static hostname or IP address.** If you select to use the dynamic address, WhatsUp Gold automatically renders the hostname or IP address at the time the action runs.
- § **Hostname or IP address.** If you selected Use static hostname or IP address, type the server address in the boxes.
- § **Port.** Specify the specific port to include in the link address.



Important: The address you enter here must be the exact address of the Alerts Home page to which you want to connect. Verify the address and enter its exact contents in the above options.



Note: Click the **Configuration** tab to edit the email action settings and specify a destination address for the notification.

- 6 Click **OK** to save changes.

Configuring an Alert Center SMS Direct notification

Alert Center SMS Direct notifications and WhatsUp Gold SMS Direct actions use the same configuration dialog.

For more information about SMS Direct Actions, see Using the SMS Direct Action.

To configure an SMS Direct notification:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Library**.

- 3 Click **New**. The Select Notification Type dialog appears.
- 4 Select **SMS Direct**. The New SMS Direct Action dialog appears.

New SMS Direct Action

Name:

Description:

Phone Number:

COM Port:

Alert Center Message

```
WhatsUp Gold Alert Center: Threshold '%  
AlertCenter.Threshold.Name' has %  
AlertCenter.Threshold.TotalNewItem new  
items. %System.Date - %System.Time
```

Right Click in the message box for percent variable support.

- 5 Specify or select the appropriate information in the dialog boxes.
 - § **Name**. Enter a name for this notification. This name is for your reference only and will never be displayed to the notification recipient.
 - § **Description**. Create or modify the description. This description appears in the Action Library and is for your reference only.
 - § **Phone number**. Type the cell phone number(s) of the intended SMS message recipients.



Note: All non-numeric characters such as "-" and ".", will be ignored.



Note: There is a 2,000 character limit in this boxes, so you can enter many numbers.

- § **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.

- 6 Select the **Alert Center Message** tab to specify the appropriate settings for the SMS notification 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 necessary percent variable codes. Keep in mind that using percent variables can greatly increase the character count.



Tip: To enter *Alert Center percent variables* (on page 540), right-click inside the message boxes.



Note: The size limit for the message is 160 characters (140 bytes).

- 7 Click **OK** to save changes.
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.



Tip: To enter Alert Center percent variables, right click inside the message boxes.



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.).

- 8 Click **OK** to save changes.

Configuring an Alert Center SMS Action notification

Alert Center SMS notifications and WhatsUp Gold SMS actions use the same configuration dialog.

For more information about SMS Actions, see Using the SMS Action.

To configure an SMS notification:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Library**. The Alert Center Notification Library dialog appears.

- 3 Click **New**. The Select Notification Type dialog appears.
- 4 Select **SMS Action** and click **OK**. The New SMS Action dialog appears.

New SMS Action

Name:

Description:

Country:

Provider:

Mode:
☐ Email ☐ Dialup

Phone number:

Alert Center Message

WhatsUp Gold Alert Center: Threshold "% AlertCenter.Threshold.Name" has % AlertCenter.Threshold.TotalNewItems new items. %System.Date - %System.Time

Message characters remaining 14

Right Click in the message box for percent variable support.

- 5 Specify or select the appropriate information in the dialog boxes.
 - § **Name**. Type a unique display name to identify the SMS notification.
 - § **Description**. Type a short description of the action. This description is displayed in the Action Library along with the action name.
 - § **Country**. Select the country for the SMS provider from the list.
 - § **Provider**. Select the appropriate SMS provider from the list.



Note: If the provider list is incomplete and/or incorrect, you can click browse (...), then click **New** or **Edit** to add or edit an SMS provider.

- § **Mode**. Select either Email or Dialup, depending on the Provider configuration in the system.
- § **Email to**. If Email is selected as the Mode, type the SMS device email address.
- § **Phone Number**. If Dialup is selected as the Mode, type 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 boxes, so you can enter many numbers.



Note: Non-numeric characters such as "-" and "." are ignored.

- 6 In the **Alert Center Message** boxes, specify the options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.
Enter a text message plus any necessary percent variable codes. Keep in mind that using percent variables can greatly increase the character count.



Tip: To add *Alert Center percent variables* (on page 540), right-click inside the message boxes and make selections from the lists.



Note: The size limit for the message is 160 characters (140 bytes).

- 7 Click **OK** to save the changes.

Configuring email notification message settings

To configure email notification message settings:

- 1 Click the **Alert Center** tab.
- 2 Click **Email Notification Message Settings**. The Configure Email Notification Message dialog appears.

Configure Email Notification Message

Max email items

Maximum newly alarmed items:
1000

☐ Show currently alarmed items

Maximum currently alarmed items:
1000

OK Cancel

- 3 Select or specify the appropriate settings:
 - § **Maximum newly alarmed items.** Enter the maximum number of new, previously unreported alerts to display in notification email messages.
 - § **Show currently alarmed items.** Select to include previously reported items that are still generating alerts in addition to newly alarmed items.
 - § **Maximum currently alarmed items.** Enter the maximum number of previously reported alerts to display in notification email messages.

- 4 Click **OK** to save changes.

Stopping a running notification policy

After resolving a problem, you can stop proceeding steps in a notification policy using the Stop Notification dialog.

To stop a notification policy:

- 1 Click the **Alert Center** tab.
- 2 Click **Running Notification Policies**. The Alert Center Running Notification Policies page appears.
- 3 Next to the notification policy that you want to stop, click **Stop notification**. The Stop Notification dialog appears.



Tip: You can send an optional message to the recipients listed in this dialog to notify them that you have resolved the problem and are stopping the notification policy from this point forward.



If you choose to do so, select **Send a message to the recipients listed above**, and enter a **Subject** and **Body** for the message.

- 4 Click **Stop** to prevent further steps in the notification policy from firing.

The screenshot shows the 'Stop Notification' dialog box. At the top, it states 'Notification triggered by: CPU Utilization exceeds 10%'. Below this, there is a section titled 'Finished Notifications' which says 'The following notifications have been sent successfully:' followed by a list containing 'Email support' with a checked checkbox. Another section titled 'Notify Recipients' contains a checkbox labeled 'Send a message to the recipients listed above'. This checkbox is currently unchecked. Below the checkbox, there are text input fields for 'Subject:' and 'Body:'. The 'Subject' field contains the text 'Stopping further notifications for CPU Utilize'. The 'Body' field is an empty text area. At the bottom right of the dialog, there are two buttons: 'Stop' and 'Cancel'.



Note: SMS message recipients only receive the message body contents; the message subject is not included.

Using the E-mail Action

The E-mail Action sends an SMTP mail message to a specific email account. An E-mail Action can also be used as an email 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 email notification* (on page 544).

Using the SMS Direct Action

The SMS Direct Action send SMS messages directly through an SMS modem, unlike SMS actions, which use email gateways or dial-up modems. For more information, see *Configuring an Alert Center SMS Direct Notification* (on page 546). If you want to send an SMS message and do not have an SMS modem, see *Configuring an Alert Center SMS Action notification* (on page 548).

Using the 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. 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 SMS Action notification* (on page 548).

Configuring thresholds

Configuring Alert Center thresholds

To configure any of the five types of Alert Center thresholds:

- 1 From the web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Select the type of threshold you want to configure. You can select from the following thresholds:
 - § Performance
 - § *CPU* (on page 558)
 - § *Custom* (on page 559)
 - § *Disk* (on page 561)
 - § *Interface* (on page 563)
 - § *Interface Errors and Discards* (on page 565)
 - § *Memory* (on page 567)
 - § *Ping Availability* (on page 569)
 - § *Ping Response Time* (on page 570)
 - § Passive
 - § *SNMP trap* (on page 573)
 - § *Syslog* (on page 575)
 - § *Windows Event Log* (on page 577)
 - § Flow Monitor
 - § *Conversation Partners* (on page 583)
 - § *Custom Threshold* (on page 584)
 - § *Failed Connections* (on page 586)
 - § *Interface Traffic* (on page 588)
 - § *Top Sender/Receiver* (on page 590)
 - § System
 - § *Blackout Summary* (on page 593)
 - § *VMware* (on page 595) (available if licensed)
 - § *Failover* (available if licensed)
 - § *WhatsUpHealth* (on page 598)
 - § Wireless (available if licensed)
 - § *Wireless Access Point RSSI* (on page 601)

- § *Wireless Banned Client MAC* (on page 602)
 - § *Wireless CPU* (on page 603)
 - § *Wireless Device Over Subscription* (on page 605)
 - § *Wireless Excessive Rogue* (on page 606)
 - § *Wireless Memory* (on page 606)
 - § *Wireless Rogue Access Point MAC* (on page 607)
 - § *Wireless Rogue Hidden SSID* (on page 608)
 - § *Wireless Rogue Specific SSID* (on page 609)
 - § *Wireless Rogue Unknown SSID* (on page 609)
- 3 Click **OK** to save changes.

Selecting threshold devices

For each performance or passive threshold that you configure you can include a list of devices or device group exceptions to which the threshold will apply. If you choose not to select specific devices to include or to exclude, by default, the threshold monitors all devices on which the applicable monitor is enabled.

To select threshold devices:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.

- 4 Select the desired threshold type, then click **OK**. The dialog where you configure threshold properties appears.

New CPU Utilization Threshold

Name:

Threshold
This threshold will alert when:
CPU utilization exceeds 90 %
for more than 30 minutes

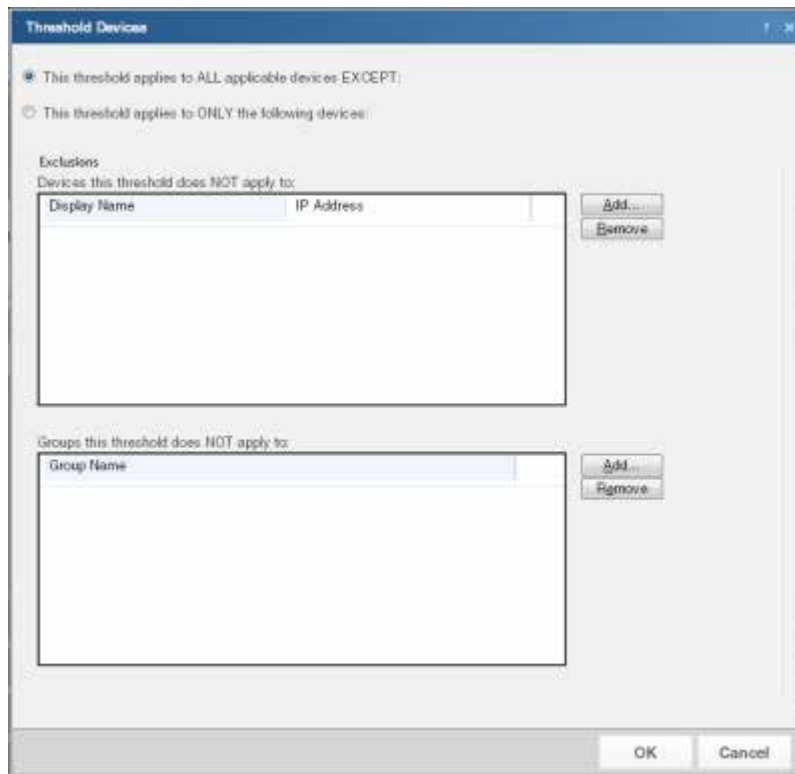
Devices to Monitor
Monitor all devices with CPU performance data by default
Select...

Notification
(No policy)

Threshold Check
Check threshold every 10 minutes.
☐ Automatically resolve items no longer out of threshold

OK Cancel

- 5 In the **Devices to Monitor** section, click **Select**. The Threshold Devices dialog appears.



- 6 Select the devices to which the threshold will apply:
- § To apply the threshold to all devices except for the device(s) or group of devices that you specify, select **This threshold applies to ALL applicable devices EXCEPT**. After you select this option, you will choose the devices to exclude from the threshold.
 - § To apply the threshold to only the device(s) or group of devices that you specify, select **This threshold applies to ONLY the following devices**. After you select this option, you will choose the devices to include in the threshold.
- 7 Select the specific devices to include or exclude from the threshold.
- § To specify a device to exclude or include in the threshold, in the upper section of the dialog, click **Add**.
 - § To specify a group of devices to exclude or include in the threshold, in the lower section of the dialog, click **Add**.



Note: You can select Dynamic Groups.



Note: When you add a device group to the list of exceptions, all devices within the device group, as well as any sub-groups contained within the group (and devices in those sub-groups), are excluded from the threshold. Additionally, if you add a device group to the list of exceptions that contains a device shortcut, then that device is excluded from the threshold—even if that device is also a member of another group which is not part of the list of excluded groups.



Tip: To delete a device or device group from the list, select it, then click **Remove**.

- 8 Click **OK** to save changes.

Configuring performance thresholds

Configuring performance thresholds

Alert Center performance thresholds notify you about WhatsUp Gold performance monitors that have exceeded or dropped below threshold limits. You can create the following performance threshold types:

- § *CPU* (on page 558)
- § *Custom Performance Monitor* (on page 559)
- § *Disk* (on page 561)
- § *Interface* (on page 563)
- § *Interface Errors and Discards* (on page 565)
- § *Memory* (on page 567)
- § *Ping Availability* (on page 569)
- § *Ping Response Time* (on page 570)

Configuring a CPU utilization threshold

To configure a CPU utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Performance CPU**, then click **OK**. The New/Edit CPU Utilization Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog box:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when CPU utilization exceeds 90% for more than 30 minutes.
 - § **Report per**. Select the the CPU utilization threshold monitor method, device or CPU option.
 - § **Device**. Select this option to calculate the threshold based on the average CPU load evaluated as a single device. Therefore, if the average CPU performance of a quad-core CPU (an average of all CPU performance combined) exceeds the threshold, then an alert is triggered.
 - § **CPU**. Select this option to calculate the threshold based on individual CPU load for the selected device. Therefore, if one of the CPUs on a quad-core CPU exceeds the threshold, then an alert is triggered.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a custom performance monitor threshold

To configure a custom performance monitor threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Custom**, then click **OK**. The New Custom Performance Monitor Threshold dialog appears.

New Custom Performance Monitor Threshold

Name:

Show: ☒ Global Monitors ☐ Device Specific Monitors

Custom performance monitor type:

Global Monitor Monitor Name

No global monitors of this type available...

Threshold

This threshold will alert when the custom performance monitor's average value 10 for more than 30 minutes

Devices to Monitor

Monitor all devices with this custom performance data by default

Notification

(No policy)

Threshold Check

Check threshold every 10 minutes

☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Show.** Select either **Global Monitors** or **Device Specific Monitors** for the custom performance monitor type that you choose.
 - § **Custom performance monitor type.** Select the custom performance monitor type from the menu. Select APC UPS, Printer, Active Script, SNMP, or WMI.
 - § **Monitor.** The configured monitors of the selected type. These are the monitors used to determine if the measured parameters have dropped below or exceeded threshold limits.



Note: When you select Global Monitors, this list is populated with custom performance monitors currently configured in the *Performance Monitor Library* (on page 452). When you select Device Specific Monitors, this list is populated with custom performance monitors currently configured for specific devices.

- § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the custom performance monitor average value exceeds 10 for 30 minutes.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a disk utilization threshold

To configure a disk threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Disk**, then click **OK**. The New/Edit Disk Utilization Threshold dialog appears.

Edit Disk Utilization Threshold

Name: PD free space

Threshold

The threshold will alert when:

disk free space falls below 40 GB

for more than days

Devices to Monitor

Monitor all devices with disk performance data by default

Select...

Notification

(No policy)

Threshold Check

Check threshold every 5 minutes.

☐ Automatically resolve items no longer out of threshold

OK Cancel

- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold triggers an alert when disk utilization exceeds 95% for more than 1 day. In addition to disk utilization, this threshold can also be configured to alert when free space exceeds or falls below a specific value.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database for items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold.

Configuring an interface utilization threshold

To configure an interface utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Interface**, then click **OK**. The New Interface Utilization Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the threshold criteria variables and values. The default threshold is configured to alert when inbound or outbound utilization exceeds 90% for more than 60 minutes.
 - § **Devices to Monitor.** Click Select to choose the devices to which the threshold applies. By default, the threshold monitors all devices where the applicable monitor is enabled.
 - § **Notification.** Select the notification policy you would like to apply to this threshold. This policy kicks off when an item falls out of the threshold you configure above. If you do not see an appropriate threshold policy, or if the list is empty, browse (...) to the Notification Policy dialog to configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring an interface errors and discards threshold

To configure an interface utilization discard and error threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Interface Errors and Discards**, then click **OK**. The New/Edit Interface Error and Discard Threshold dialog appears.

New Interface Error and Discard Threshold

Name:

Threshold
The threshold will alert when either:

☐ Discards for interface traffic

exceed discards per minute

for more than minutes

☐ Errors for interface traffic

exceed errors per minute

for more than minutes

Devices to Monitor
Monitor all devices with interface error and discard data by default

Notification
(No policy)

Threshold Check
Check threshold every minutes

☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the threshold criteria variables and values. You can choose to create a threshold based on discards, errors, or a combination of the two. The default threshold is configured to alert when inbound or outbound interface utilization exceeds 100 discards per minute for more than 20 minutes.
- and / or -
when errors for inbound or outbound interface utilization exceeds 100 errors per minute for more than 20 minutes.



Note: If you select both error and discard thresholds, each error and discard are reported as separate items (rows) in the dashboard report.

- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices where the applicable monitor is enabled.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters. The default threshold check is 10 minutes.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a memory utilization threshold

To configure a memory utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Performance Memory**, then click **OK**. The New/Edit Memory Utilization Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when disk utilization exceeds 95% for more than 1 hour.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a ping availability threshold

To configure a ping availability threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Ping Availability**, then click **OK**. The New/Edit Ping Availability Threshold dialog appears.

New Ping Availability Threshold

Name:

Threshold
This threshold will alert when:
Ping availability average falls below %
for more than

Devices to Monitor
Monitor all devices with ping availability performance data by default

Notification
(No policy)

Threshold Check
Check threshold every minutes
☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when ping availability average falls below 95% for more than 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a ping response time threshold

To configure a ping response time threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Ping Response Time**, then click **OK**. The New Ping Response Time Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when ping response time average exceeds 2 ms for more than 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring passive thresholds

Configuring passive thresholds

Alert Center passive thresholds notify you when WhatsUp Gold passive monitors fall out of the parameters of the thresholds you configure. You can create three passive threshold types:

- § *SNMP trap* (on page 573)
- § *Syslog* (on page 575)
- § *Windows Event Log* (on page 577)

Several things to keep in mind when configuring thresholds for passive monitors:


- § Each Alert Center threshold is associated with a specific passive monitor. The passive monitor associated with the threshold you are creating must be assigned to at least one device. Otherwise, the threshold will not work.
- § When creating a passive threshold, you must select a passive monitor from a list to associate with the threshold. This list contains the passive monitors already configured in the Passive Monitor Library. These monitors are not necessarily assigned to devices, however. To determine which devices have passive monitors assigned to them, you can create a dynamic group. For more information, see *Configuring Dynamic Groups*.
- § It is not possible to monitor unsolicited traps using Alert Center.

Configuring an SNMP trap threshold

To configure an SNMP trap threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **SNMP Trap**, then click **OK**. The New SNMP Trap Threshold dialog appears.



The image shows a Windows-style dialog box titled "New SNMP Trap Threshold". It contains several sections for configuring a threshold:

- Name:** A text input field.
- SNMP Trap type:** A dropdown menu currently showing "Any".
- Threshold:** A section with the text "The threshold will alert when:". It contains two rows of controls: "Number of traps" with a dropdown set to "exceeds" and a text box with "500", and "in the past" with a text box containing "60" and a dropdown set to "minutes".
- Devices to Monitor:** A section with the text "Monitor all devices sending SNMP Traps by default" and a "Select..." button.
- Notification:** A section with a dropdown menu set to "(No policy)" and a browse button (three dots).
- Threshold Check:** A section with the text "Check threshold every" followed by a text box with "5" and the word "minutes". Below this is a checkbox labeled "Automatically resolve items no longer out of threshold".

At the bottom right are "OK" and "Cancel" buttons.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **SNMP Trap type.** Select the SNMP trap type from the list that you want to associate with this threshold. The list is populated with SNMP traps currently configured in the Passive Monitor Library.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of traps exceeds 500 in the past 60 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters. By default, the threshold check is set to every five minutes.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a Syslog threshold

To configure a Syslog threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Syslog**, then click **OK**. The New Syslog Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Syslog type.** Select the Syslog monitor to use with the threshold. This list is populated with Syslog monitors currently configured in the Passive Monitor Library.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of messages exceeds 500 in the past 60 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a Windows Event Log threshold

To configure a Windows Event Log threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Windows Event Log**, then click **OK**. The Windows Event Log Threshold dialog appears.

New Windows Event Log Threshold

Name:

Windows Event Log type:

Threshold
The threshold will alert when:
Number of events
in the past

Devices to Monitor
Monitor all devices sending Windows events by default

Notification

Threshold Check
Check threshold every
☐ Automatically resolve items no longer out of threshold

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Windows event type.** Select the Windows Event Log monitor to use with this threshold. The list is populated with Windows Event Log monitors currently configured in the Passive Monitor Library.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of events exceeds 500 in the past 60 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK** to save the threshold settings.

Configuring Flow Monitor thresholds

Configuring Flow Monitor thresholds

Alert Center Flow Monitor thresholds notify you on WhatsUp Gold Flow Monitor plug-in aspects that fall out of the parameters of the thresholds you create.

You can create five Flow Monitor threshold types:

- § *Flow Monitor Conversation Partners* (on page 583)
- § *Flow Monitor Custom Threshold* (on page 584)
- § *Flow Monitor Failed Connections* (on page 586)
- § *Flow Monitor Interface Traffic* (on page 588)
- § *Flow Monitor Top Sender/Receiver* (on page 590)

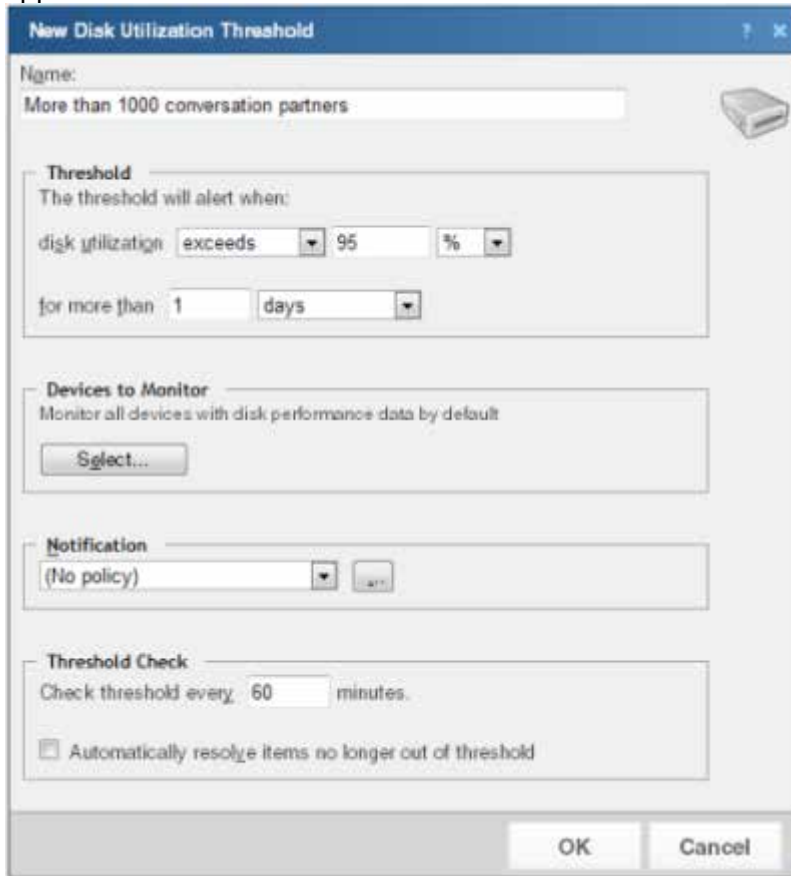
Selecting Flow Monitor threshold hosts

For each Flow threshold that you configure you can include a list of Flow Monitor groups, hosts, or a range of IP addresses to which the threshold will not apply.

To configure a list of Flow threshold exceptions:

- 1** Click the **Alert Center** tab.
- 2** Click **Threshold Library**. The Alert Center Threshold Library dialog appears.

- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select the desired Flow threshold type, then click **OK**. The threshold properties dialog appears.



The image shows a Windows-style dialog box titled "New Disk Utilization Threshold". It contains several sections for configuring a threshold:

- Name:** A text field containing "More than 1000 conversation partners".
- Threshold:** A section with the text "The threshold will alert when:". It contains two rows of settings: "disk utilization" with a dropdown set to "exceeds", a text field with "95", and a dropdown set to "%"; and "for more than" with a text field containing "1" and a dropdown set to "days".
- Devices to Monitor:** A section with the text "Monitor all devices with disk performance data by default" and a "Select..." button.
- Notification:** A section with a dropdown menu set to "(No policy)" and a small "OK" button.
- Threshold Check:** A section with the text "Check threshold every" followed by a text field containing "60" and the word "minutes". Below this is a checkbox labeled "Automatically resolve items no longer out of threshold", which is currently unchecked.

At the bottom right of the dialog are "OK" and "Cancel" buttons.

- 5 In the **Devices to monitor** section, click **Select**. The Threshold Hosts dialog appears.

- 6 Select the hosts to which the threshold applies.
- § To apply the threshold to all hosts except the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ALL hosts EXCEPT**. After you select this option, you will choose the hosts to exclude from the threshold.
 - § To apply the threshold to only the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ONLY the following hosts**. After you select this option, you will choose the hosts to include in the threshold.
- 7 Select the specific hosts to include or exclude from the threshold.
- § To specify a Flow Group to include or exclude from this threshold, in the upper section of the dialog, click **Add**.



Tip: To delete a Flow group, host, or IP range from the list, select it, and then click **Remove**.

- § To specify a single host or IP address to include or exclude from this threshold, enter a **Hostname or IP Address**, and then click **Add**.
 - § To specify an IP address range to include or exclude from this threshold, enter a **Start IP Address** and an **End IP Address**, and then click **Add**.
- 8 Click **OK** to save changes.

Configuring a conversation partners threshold

To configure a Flow Monitor conversation partners threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Click the menu, select **Flow Conversation Partners**, and then click **OK**. The New Flow Conversation Partners Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when a host has sent to or received from more than 1000 conversation partners in the past 15 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a time interval for Alert Center to check the WhatsUp Gold database for items that are out of the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they return to the parameters inside the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a Flow Monitor custom threshold

To configure a Flow Monitor custom threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Flow Monitor Custom Threshold**, then click **OK**. The New Flow Monitor Custom Threshold dialog appears.

The screenshot shows the 'New Flow Monitor Custom Threshold' dialog box. It contains the following fields and sections:

- Name:** A text input field.
- Description:** A text input field with a preview text: "Any host with ... that sent or received more than ... MB of traffic in the past 15 minutes".
- Threshold:** A section titled "This threshold will alert when:" containing three filter rows. Each row has a "Select filter..." dropdown, a "matching" dropdown, and a text input field. Below these is a final condition: "sent or received" dropdown, "more than" text, a text input field, "MB" dropdown, "of data in the past:" text, a text input field, and "minutes" dropdown.
- Traffic to monitor:** A dropdown menu currently showing "All Flow Monitor Sources".
- Hosts to monitor:** A section with a "Select..." button.
- Notification:** A dropdown menu currently showing "(No policy)".
- Threshold Check:** A section with "Check threshold every:" text, a text input field showing "10", and "minutes." text. Below is a checkbox labeled "Automatically resolve items no longer out of threshold".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Description.** As you configure threshold criteria settings, the description automatically updates to include your selections.
 - § **Threshold.** Select the threshold filters and limits, and enter the values to use for each. You can define up to three filters for each Flow Monitor custom threshold.

An example threshold involving multiple filters could state, "This threshold will alert when any host with Protocol matching TCP and Application matching pop3 sent or received more than 100 MB of data in the past 15 minutes."

The default threshold time value is data in the past 15 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a failed connections threshold

To configure a Flow failed connections threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Flow Monitor Failed Connections**, then click **OK**. The New Flow Monitor Failed Connections Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is exceeded when when a host has sent or received more than 1000 failed connections in the past 15 minutes.



Note: WhatsUp Gold Flow Monitor can only find failed connections on sources that are not sending sampled data.

- § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold.

Configuring a Flow Monitor Interface Traffic threshold

To configure a Flow Monitor interface traffic threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Flow Monitor Interface Traffic**, then click **OK**. The New Flow Monitor Interface Traffic Threshold dialog appears.

The screenshot shows the 'New Flow Monitor Interface Traffic Threshold' dialog box. It has a title bar with a question mark and a close button. The dialog is divided into several sections. The 'Name' section has a text input field. The 'Threshold' section has a label 'The threshold will alert when:' and three dropdown menus: 'incoming or outgoing', 'interface traffic', and 'exceeds 90 % for more than 60 minutes'. The 'Traffic to monitor' section has a dropdown menu set to 'All Flow Monitor Sources'. The 'Notification' section has a dropdown menu set to '(No policy)' and a browse button (...). The 'Threshold Check' section has a label 'Check threshold every 5 minutes' and a checkbox 'Automatically resolve items no longer out of threshold'. At the bottom are 'OK' and 'Cancel' buttons.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when incoming or outgoing interface traffic exceeds 90% for more than 60 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor sources from which to monitor traffic; all interfaces on a Flow source are monitored. By default, the threshold is set to monitor traffic from all Flow sources.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a top sender/receiver threshold

To configure a Flow Monitor top sender/receiver threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Flow Monitor Top Sender/Receiver**, then click **OK**. The New Flow Monitor Top Sender/Receiver Threshold dialog appears.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variable and values. The default threshold is configured to alert when a host has sent or received more than 500 MB in the past 15 minutes.
 - § **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.
 - § **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default polling interval is 5 minutes.
- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring system thresholds

Configuring system thresholds

Alert Center system thresholds alert you on aspects of your WhatsUp Gold system according to the threshold parameters you configure. You can create five system threshold types:

- § *Blackout Summary* (on page 593)
- § *VMWare* (on page 595)
- § *Failover* (on page 596)
- § *WhatsConfigured Threshold*
- § *WhatsUp Health* (on page 598)



Note: The thresholds listed in the Threshold Library may vary, depending on your WhatsUp Gold license.

Configuring a Blackout Summary threshold

To configure a **Blackout Summary** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.

- 3 Select **Blackout Summary** from the menu, then click **OK**. The New/Edit Blackout Summary Threshold dialog appears.

New Blackout Summary Threshold

Name:

Threshold
The threshold will alert when a blackout period has ended
and an action would have been triggered by a passive monitor
or state change.

Devices to Monitor
Monitor all devices with blackout schedules by default

Notification
(No policy)

Threshold Check
Check threshold every minutes.

- 4 Specify or select the appropriate information in the dialog box:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** The threshold alerts you when a blackout period has ended and an action would have been triggered by a passive monitor or state change.



Note: You cannot configure threshold criteria for the Blackout Summary threshold.

- § **Devices to Monitor.** Click Select to select the devices to which the threshold applies. By default, the threshold applies to all devices. Use this dialog to select groups to which this threshold does not apply.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.
- § **Threshold check.** Enter a time interval for Alert Center to check the WhatsUp Gold database for actions that were not triggered because of a scheduled blackout period that has finished.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold settings.

Configuring a VMware threshold

To configure a VMware threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **VMware** from the menu, then click **OK**. The New/Edit Blackout Summary Threshold dialog appears.

- 4 Complete the box with the appropriate information:
 - § **Name.** Enter a name for the VMware threshold. The name entered here is displayed as the threshold's dashboard report title on the Alert Center Home page.
 - § **Virtualization Events type.** Select the event type for which you want to create a threshold. The following options are available:

- § **All HA (High Availability) error events**
- § **All Virtual machine migration events**
- § **All security related events**
- § **Other events**



Note: When **Other events** are collected from the vCenter server, and you select **Other events** in the threshold configuration, you only see those events that were selected when event collection was configured in the Device Properties - Virtualization menu.



Note: For more information about event types and event type selection, see the Configure VMware event listener dialog help.

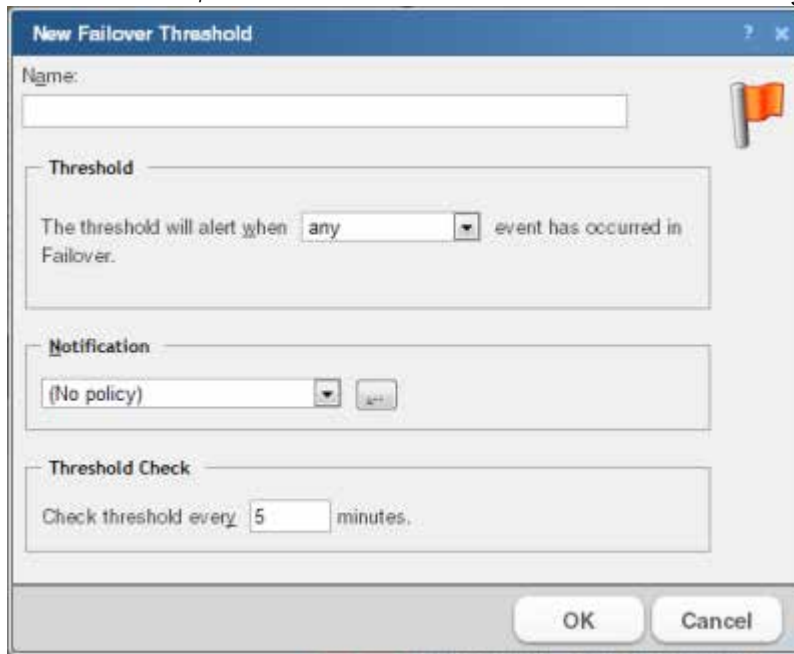
- 5 Select one of the following alert criteria:
 - § **The threshold will alert immediately if an event occurred within the last Threshold Check of *<Threshold_Check_Period>* minutes.** Select this option if you want alerts to occur immediately when an event has occurred within the threshold check period, where *<Threshold_Check_Period>* is the value defined in the Threshold Check area of this dialog.
 - § **The threshold will alert when:** Select this option if you want to define a number of events and time range for the threshold alert.
 - § **Number of events *<exceeds_or_falls_below>* *<number>*.** Use this setting to configure the number of events of the selected event type that must be received before firing the alert, where *<exceeds_or_falls_below>* determines if the number should **Exceed** or **Fall Below** the threshold value, and *<number>* is the threshold value.
 - § **in the past *<number>* *<unit_of_time>*.** Use this setting to configure the number and units of time that the threshold check should check for events, where *<number>* is the number of units of time, and *<unit_of_time>* is the unit of time.
- 6 Select the policy you want to apply to the threshold from the **Notification** boxes. Use the browse (...) button to access the Alert Center Notification Policies dialog. You can create new policies or edit existing policies from the Alert Center Notification Policies dialog.
- 7 Enter the number of minutes to wait between threshold checks in the **Threshold Check** area of the dialog.
- 8 Click **OK** when you have completed your configuration.

Configuring a Failover threshold

To configure a failover threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.

- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Failover**, then click **OK**. The New Failover Threshold dialog appears.



- 4 Specify or select the appropriate information in the dialog box.
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select the desired threshold criteria variables and values. You can configure the threshold to alert you when any event occurs, when an error occurs, or when an informational event occurs. By default, the threshold is configured to alert you when any event has occurred in Failover.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 5 Click **OK** to save the threshold.

Configuring a WhatsUp Health threshold

To configure a WhatsUp Health threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **WhatsUp Health**, then click **OK**. The New WhatsUp Health Threshold dialog appears.
- 4 Enter a **Name** for the threshold. This name is displayed as the threshold dashboard report title on the Alerts Home page.
- 5 Click the **Database** tab. Enter the appropriate threshold information:
 - § **Database size exceeds ____ %/GB/MB**. Select this option to have the threshold alert when the database size exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- § **Total performance monitors exceed ____**. Select this option to have the threshold alert when the total number of performance monitors exceeds the number you specify. The default number of total performance monitors is 3,000.
- § **Total performance monitor records exceed ____**. Select this option to have the threshold alert when the total number of performance monitor records exceeds the number you specify. The default number of total performance monitor records is 2,000,000.
- § **Total passive monitor records exceed ____**. Select this option to have the threshold alert when the total number of passive monitor records exceeds the number you specify. The default number of total passive monitor records is 1,000,000.
- § **Total expired records exceed ____**. Select this option to have the threshold alert when the total number of expired records exceeds the number you specify. The default number of total expired records is 500,000.
- § **Total devices being monitored exceeds ____ % of license limit**. Select this option to have the threshold alert when the total number of devices being monitored exceeds the percentage of the license limit you specify. The default percentage of the license limit is 90%.



Tip: Click **View WhatsUp database** to view a graph of the current WhatsUp database usage.

- 6 Click the **Services** tab. Enter the appropriate threshold information:
 - § **WhatsUp polling service is down ____ minutes.** Select this option to have the threshold alert when the WhatsUp service has been down for the number of minutes you specify. The default threshold value is 5 minutes.
 - § **WhatsUp discovery service is down ____ minutes.** Select this option to have the threshold alert when the WhatsUp discovery service is down the number of minutes that you specify. The default number is 5 minutes.



Note: Web service threshold checks do not apply to users running IIS.



Note: If you are experiencing a high volume of errors from your WhatsUp Health threshold service checks, please see Troubleshooting the WhatsUp Health Threshold.

- 7 Click the **Flow Monitor** tab. Enter the appropriate threshold information pertaining to the WhatsUp Gold Flow Monitor.
 - § **Netflow database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the Netflow database exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- § **NfArchive database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the NfArchive database size exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- § **Flow collector service is down ____ minutes.** Select this option to have the threshold alert when the Flow collector service is down for the number of minutes you specify. The default threshold value is 5 minutes.
- § **Any bounce traffic occurs.** Select this option to have the threshold alert when bounce traffic occurs on a Flow Monitor source.
- § **Host records exceed ____.** Select this option to have the threshold alert when the number of host records exceeds the amount you specify. The default threshold value is 2,000,000 records.
- § **Raw, hourly, or daily records exceed ____.** Select this option to have the threshold alert when the number of raw data records exceeds the amount you specify. The default threshold value is 10,000,000 records.

- § **Total sources sending data exceeds ____ % of license limit.** Select this option to have the threshold alert when the total sources sending data exceeds the percentage of license limit that you specify. The default threshold value is 90% of license limit.



Tip: Click View Netflow database usage to view a graph of the current Netflow database usage. Click View NfArchive database usage to view a graph of the current NfArchive database usage.

- 8 After selecting the desired options for each tab and entering the appropriate threshold variables and values, specify your choices for the Notification and Polling sections of the dialog.

- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alerts Home page.

- § **Threshold check.** Enter a value for the polling interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items out of the threshold's parameters. The default polling interval is 5 minutes.
Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time, as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is not advised.

- 9 Click **OK** to save the threshold settings.

Configuring wireless thresholds

Configuring wireless thresholds

You can use WhatsUp Gold Alert Center to configure wireless thresholds to alert you about the health of your Wireless infrastructure devices according to the threshold parameters you configure. There are multiple wireless threshold types:

- § *Wireless Access Point RSSI* (on page 601)
- § *Wireless Banned Client MAC Address* (on page 602)
- § *Wireless Client Bandwidth* (on page 604)
- § *Wireless CPU* (on page 603)
- § *Wireless Device Over Subscription* (on page 605)
- § *Wireless Excessive Rogues* (on page 606)
- § *Wireless Memory* (on page 606)
- § *Wireless Rogue Access Point MAC Addresses* (on page 607)
- § *Wireless Rogue Hidden SSID* (on page 608)
- § *Wireless Rogue Specific SSID* (on page 609)
- § *Wireless Rogue Unknown* (on page 609)

Configuring a Wireless Access Point RSSI threshold

To configure a new **Wireless Access Point RSSI** (Received Signal Strength Indication) threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Access Point RSSI** from the list, then click **OK**. The New Wireless Access RSSI Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when RSSI falls below 20% for more than 30 minutes. Additionally, specify the minimum number of clients to user in the averaging. The default minimum is 3.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Banned Client MAC Addresses threshold

To configure a new **Wireless Banned Client MAC Address** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Banned Client MAC Addresses** from the list, then click **OK**. The New Wireless Banned Client MAC Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Enter any banned MAC addresses separated by commas and select an interval time range. The default range is 30 minutes. The threshold will alert when any MAC addresses listed are connected to the network in the given time interval.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.

- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless CPU Utilization threshold

To configure a new Wireless CPU Utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless CPU** from the list, then click **OK**. The New Wireless CPU Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when CPU utilization exceeds 90% for more than 30 minutes.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. The user has the option to specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Client Bandwidth threshold

To configure a new Wireless Client Bandwidth threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.

- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Client Bandwidth** from the list, then click **OK**. The New Wireless Client Bandwidth Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Select and enter the desired threshold criteria variables and values. The threshold will alert when clients that are connected to the specified SSID(s) exceed their bandwidth quota for the specified traffic direction, in the given time range. The default criteria is 20 MB transmitted and received in a time range of 30 minutes.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. The user has the option to specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Device Over Subscription threshold

To configure a new Wireless Access Point Oversubscription threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Access Point Over Subscription** from the list, then click **OK**. The New Wireless Access Point Over Subscription Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.

- § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the average number of clients attached exceeds the 'Client Count' for more than the specified 'Time Range'.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 10 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Excessive Rogues threshold

To configure a new **Wireless Excessive Rogues** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Excessive Rogues Alert** from the list, then click **OK**. The New Wireless Excessive Rogues Alert Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired rogue alert threshold criteria. The default time range interval is 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Memory Utilization threshold

To configure a new Wireless Memory Utilization threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Memory** from the list, then click **OK**. The New Wireless Memory Utilization Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when memory utilization exceeds 90% for more than 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items

that are out of the threshold's parameters. The default check interval is every 5 minutes.

- § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.

5 Click **OK**.

Configuring a Wireless Rogue Access Point MAC Addresses threshold

To configure a new **Wireless Rogue Access Point MAC Addresses** threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Access Point MAC Addresses** from the list, then click **OK**. The New Wireless Access Point MAC Addresses dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Enter any rogue MAC addresses separated by commas and select an interval time range. The default range is 30 minutes. The threshold will alert when any MAC addresses listed here broadcast SSID's in the given time interval.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Hidden SSID threshold

To configure a new Wireless Rogue Hidden SSID threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Hidden SSID** from the list, then click **OK**. The New Wireless Rogue Hidden SSID Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold**. Click the hyperlink to edit the list of acceptable rogues and select an interval time range. The default range is 30 minutes.
 - § **Devices to Monitor**. Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification**. Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check**. Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Specific SSID threshold

To configure a new Wireless Rogue Specific SSID threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Specific SSID** from the list, then click **OK**. The New Wireless Rogue Specific SSID Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name**. Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.

- § **Threshold.** Enter one or more SSIDs and select an interval time range. The threshold is configured to alert when any of the listed SSIDs are detected in the specified time range. The default range is 30 minutes.
- § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
- § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Configuring a Wireless Rogue Unknown SSID threshold

To configure a new Wireless Rogue Unknown SSID threshold:

- 1 From the WhatsUp Gold web interface, go to **Alert Center > Threshold Library**. The Alert Center Threshold Library dialog appears.
- 2 Click **New**. The Select Threshold Type dialog appears.
- 3 Select **Wireless Rogue Unknown SSID** from the list, then click **OK**. The New Wireless Rogue Unknown SSID Threshold dialog appears.
- 4 Specify or select the appropriate information in the dialog boxes:
 - § **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - § **Threshold.** The threshold is configured to alert when any new or previously unseen SSIDs are detected in the specified time range. The default range is 30 minutes.
 - § **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. The Threshold Devices dialog appears. Specify to which devices the threshold applies by adding them or to which devices the threshold does not apply by excluding them using this dialog. Additionally, groups can also be added or excluded from the threshold using this dialog. Click **OK**.
 - § **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits.

If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- § **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default check interval is every 5 minutes.
 - § Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 5 Click **OK**.

Admin

In This Chapter

Using WhatsUp Gold Admin features858

Home860

Scheduling.....861

System Administration.....865

Options897

Using WhatsUp Gold Admin features

In This Chapter

Using Admin features.....858

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	860
Opening NM Console from the Web interface.....	860

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.

Scheduling

In This Chapter

Adding and editing a recurring action	861
Managing scheduled reports	863

Adding and editing a recurring action

Recurring actions allow users to fire actions based on a regular schedule, independent of the status of devices. Recurring actions can perform tasks such as sending heartbeat messages through email or SMS text, letting users know a system is up and running.

After an action is configured through the *Action Library* (on page 612), 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 612).

- 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

In This Chapter

Scheduling a Recurring Action	863
Scheduling maintenance	863

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	865
Using the SNMP MIB Manager.....	865
Setting LDAP or Cisco ACS credentials.....	868
Translation Groups.....	871
Managing users and groups.....	874
Using the Polling Configuration Library.....	888
Using the Task Library.....	892

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 866).

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.

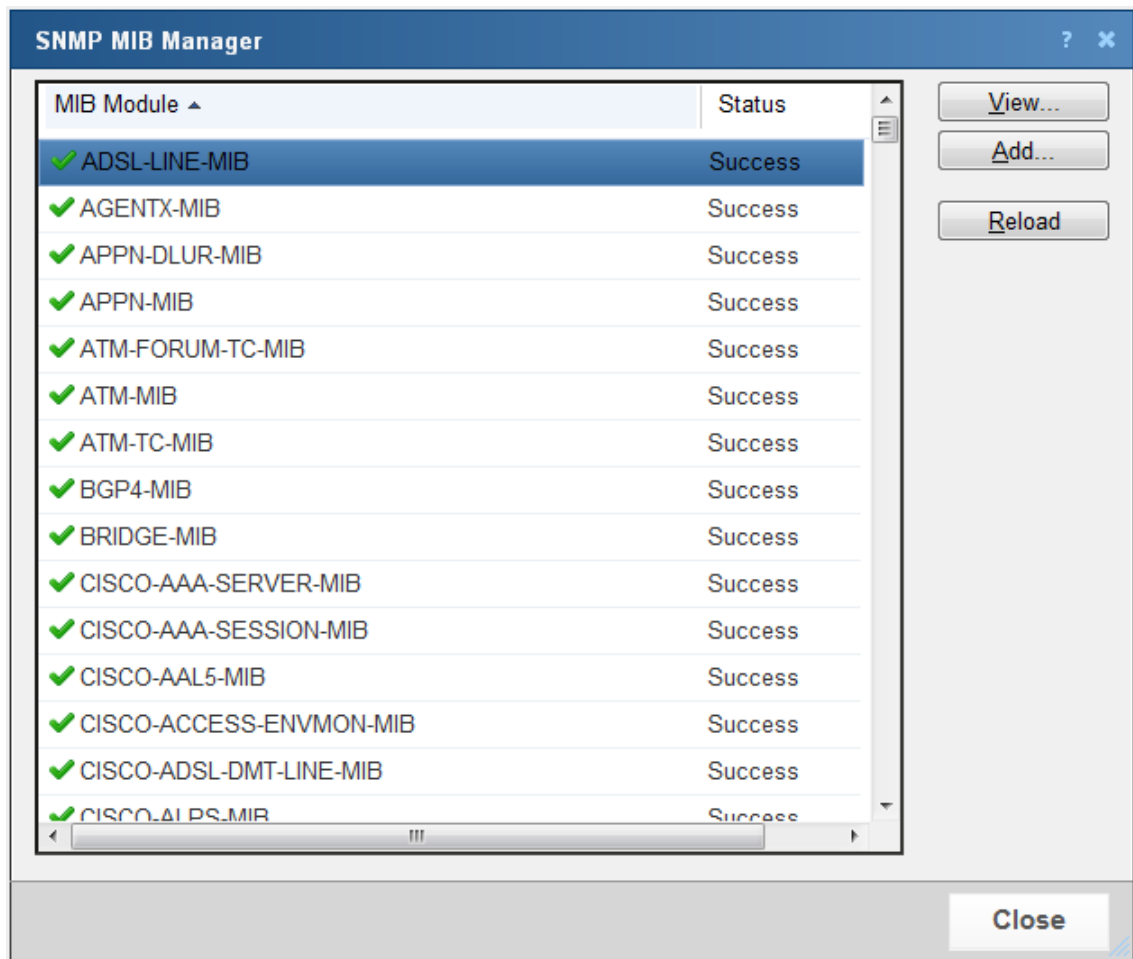
- § After you import a new MIB file or are troubleshooting code in a MIB file, click **Reload** to refresh the MIB Module list and the Status list.



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.





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:

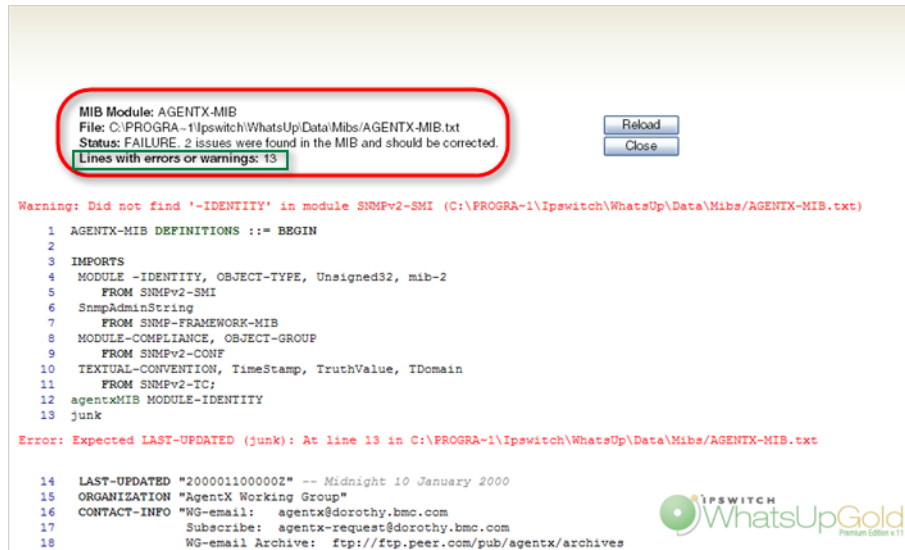
Cannot find module (IANA-RTPROTO-MIB).

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 865) 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.



- 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 if 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 or Cisco ACS credentials

Use the Configure External Authentication 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.

-or-

- § Configure Cisco ACS credentials and configure WhatsUp Gold to connect with a Cisco ACS server.

To configure WhatsUp Gold to use Windows Active Directory for authentication:

- 1 From the WhatsUp Gold web interface, go to **Admin > External Authentication**. The Configure External Authentication dialog appears.
- 2 Select the **Active Directory / LDAP** tab.
- 3 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 SSL (Default port: 636).
- 4 In the Server Type area, select **Active Directory** to enable Active Directory domain credentials. The **Logon Domain** box is activated.
 - 5 Enter the Active Directory **Logon Domain** from which you want to access and import AD groups.
 - 6 (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 870).
 - 7 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 existing WhatsUp Gold user groups. For more information, see *Browse Active Directory* (on page 871).



Note: Authentication for nested Active Directory groups are not supported.

- 8 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 882) 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 871) 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.

- 9 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 SSL (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.

To configure WhatsUp Gold to use Cisco ACS for authentication:

Use the Cisco ACS tab to configure Cisco ACS credentials and to configure WhatsUp Gold to connect with a Cisco ACS server. Before configuring in WhatsUp Gold, make sure to enable the UCP interface on the respective Cisco ACS device and make sure the device uses a valid certificate.

To configure WhatsUp Gold to use Cisco ACS credentials for authentication:

- 1 From the WhatsUp Gold web interface, go to **Admin > External Authentication**. The **Configure External Authentication dialog** appears.
- 2 If not already active, select the **Cisco ACS** tab.
- 3 Enter or select the appropriate information:
 - § **Cisco ACS server hostname / IP address.** Enter the server hostname or IP address for the Cisco ACS server.
 - § **Cisco ACS server port number.** Enter the port the Cisco ACS server uses to listen for connections (Default: 431).
- 4 (Optional) Click **Test** to open the Test Cisco ACS Authentication dialog. The Test dialog allows you to verify that your credentials are configured correctly. For more information, see *Test credentials* (on page 870).
- 5 Click **OK** to save changes. WhatsUp Gold saves the Cisco ACS credentials and the Configure External Authentication dialog closes.

Test LDAP credentials

Test the credentials you have entered.

To test credentials:

- 1 Click **Test**.
- 2 Enter the appropriate information:
 - § **User name**. Enter a valid user name that has access to the server for which you are testing credentials.
 - § **Password**. Enter the password associated with the user name.
- 3 Click **Test**. WhatsUp Gold attempts to connect using the credentials and returns a test success or failure message.
- 4 Click **Close**.
- 5 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 868).

- 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

WhatsUp Gold User Guide

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 user accounts and user groups.....	874
About user rights	877
Adding and editing user accounts.....	880
Adding and editing user groups.....	882
About device group access rights.....	883

Managing user accounts and user groups

Use the Manage Users dialog to manage user accounts and user group access to application features such as the WhatsUp Gold Console, Account Administration, System Administration, Monitoring, Devices, and Reports.

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 with the authentication type set to LDAP. The user will log in to WhatsUp Gold using the credentials they use to authenticate with their LDAP server. For 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 from the Configure External Authentication dialog. For more information, see *Setting LDAP or Cisco ACS credentials*. (on page 868)
- § **Cisco ACS.** The user account is created when a user with a Cisco ACS authentication server has been configured to authenticate with Cisco ACS from WhatsUp Gold. The user will log in to WhatsUp Gold using their Cisco ACS credentials, which must be configured from the Configure External Authentication dialog. For more information, see *Setting LDAP or Cisco ACS credentials* (on page 868).

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.

- § To permit a locked user to perform a log on attempt before the designated time delay has expired, click **Unlock**. The lock icon next to the user account will disappear and the user will be able to perform a log on attempt.

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.

To set the password policy settings:

- § Click **Change**. The Password Policy Settings dialog appears.
- § **Account Lockout Duration (minutes)**. Enter the time in minutes that the system should delay before allowing a locked out user from performing a log on attempt.
- § **Minimum number of days between password changes**. Enter the minimum number of days required between password changes.
- § **Password expires after (days)**. Enter the number of days before a password expires.
- § **Retain passwords for at least (days)**. Enter the number of days to retain previously used passwords.
- § **Ensure password not reused against previous**. Enter the number of passwords that are not to be reused against previous passwords.
- § **Warn when (days) left before password expiration**. Enter the number of days to warn user before password expiration.
- § **Minimum complex password length**. Enter the minimum number of characters required for the password policy. The default minimum complex password requirement is one special character, one capital (upper case) letter, one lower case letter, and one number.
- § Click **OK**. The new password policy values appear in the 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.

WhatsUp Gold Console	
Access WhatsUp Gold Console	Enables users to access the WhatsUp Gold Admin Console application (NMConsole.exe) when FIPS 140-2 is enabled. Important: If FIPS 140-2 is disabled, the Access WhatsUp Gold Console user right does not apply. For more information, see Program Options - General in the WhatsUp Gold console application.

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 access 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.
Access Virtualization Actions Menu	Enables users to perform VM actions (stop, pause, restart, etc) on any virtual host within WhatsUp Gold.
Email Settings	Enables users to configure WhatsUp Gold email settings from the Email Settings dialog (Admin > Email Settings).
Configure Flow Monitor	Enables users to create, edit and delete WhatsUp Gold Flow Monitor sources, collection intervals and data intervals for reports.
Access APM	Enables users to access the APM features.
Configure APM Application Instance	Enables users to create, modify, and delete application profiles.
Configure APM Application Profiles	Enables users to create, modify, and delete application instances.
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.
Access Tools	Enables users to access and use the Tools menu from the right-click menu when a device is selected. Also enables access to the web interface Tools menu.
Access WhatsVirtual	Enables users to access WhatsVirtual features.
Access WhatsVirtual Map	Enables users to access WhatsVirtual maps.
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 and Edit User dialog to create a new user account or to edit existing user accounts.

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 is created for that user. They are added to the group that was mapped to the AD group of which the user account is a member.



Important: As 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.



Note: Once a user account has been added, this field will be unavailable for editing by the user. Only edits by a different user with "manager users" rights will be allowed to edit another account's user name.

§ **Authentication type.**

- § **Internal.** Select this option for internal authentication using a password entered on this dialog.
- § **LDAP.** Select this option for remote authentication using an LDAP server (other than an Active Directory server) configured on the LDAP credentials dialog.
- § **Cisco ACS.** Select this option for Cisco ACS server authentication.



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.
- § **Apply Account Lockout Policy.** If your Authentication type is either **Internal** or **Cisco ACS**, select this option to provide the user with three successive log on attempts. After the third failed attempt, the user will be locked out of the system until a designated time period has expired. If you want to grant the user the ability to log on before the designated time period has elapsed, the user must contact the Administrator to unlock the account.



Note: The Apply Single Session Policy is not compatible with the Ipswitch Dashboard Screen Manager stand-alone application. Please do not select this option if you're using the Dashboard Screen Manager.

- § **Apply Single Session Policy.** Select this option to allow the user to log on to the system once, and not allow multiple sessions running at the same time.
- § **Apply Password Aging Policy.** If your Authentication type is Internal, select this option to apply a password aging policy for the user. The user will be subject to a minimum number of days between password changes, password expiration after a given number of days, and a password history check to ensure a given number of previous passwords are not reused.
- § **Apply Password Complexity Policy.** If your Authentication type is Internal, select this option to apply a password complexity policy for the user. The complexity requirements are driven by the internal WhatsUp Gold password policy. The default minimum complex password requirement is one special character, one capital (upper case) letter, one lower case letter, and one number. The password must also not match a password stored in the dictionary.
- § **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 882).



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*.



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

Close

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	<input checked="" type="checkbox"/>
Group Write	<input type="checkbox"/>
Device Read	<input checked="" type="checkbox"/>
Device Write	<input type="checkbox"/>

☒ Apply changes to all sub Device Groups recursively for: guest

OK Cancel



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 883).

Propagating group access rights to subgroups

Group access rights are passed from parent group to subgroup: when a new 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 887).

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 35).



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 35).

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 poller is installed on a remote machine, 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 this machine using the same user credentials used during the poller installation. You can also run the remote machine 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* (on page 37) 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 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*.

- 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.....	892
Create/Edit a WhatsUp Gold task	893
Configuring task schedules.....	894

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:

- § Alert Center DB Maintenance which cleans the AlertCenterItems and AlertCenterLog tables.
- § APM Hourly Availability Rollup which handles hourly rollup of application instances, component instances, and group instances availability data.
- § Defrag Performance Tables which defrags all Statistical table indecies.
- § Group Updater which updates device group state and status based on the state and status of the devices and child devices groups within the group.
- § Purge expired action activity data which cleans up all expired data and configuration related to the action manager.
- § Purge expired APM data which cleans up all expired data and configuration for APM.
- § Purge Log Tables which cleans various 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.

Task pass and fail events are logged in the Logger report.



Note: Some tasks cannot be copied or deleted and therefore, the **Copy** and **Delete** buttons are 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 727)
General Error Log Expiration Time Limit	General Error Log (on page 729)
Passive Monitor Error Log Expiration Time Limit	Passive Monitor Error Log (on page 730)
Performance Monitor Log Expiration Time Limit	Performance Monitor Error Log (on page 730)
Recurring Report Log Expiration Time Limit	Recurring/Scheduled Report Log (on page 734)
Remote Server Log Expiration Time Limit	Remote Site Log
System Activity Log Expiration Time Limit	Activity Log (on page 734)
Web Alarm Log Expiration Time Limit	N/A
Web User Activity Log Expiration Time Limit	Web User Activity Log (on page 735)
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 730)
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 > Tasks**. 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.

- § **Description.** (Optional) Enter additional information about the task. This description displays next to the monitor in the Task Library.
 - § **Enable this schedule.** Select this option to begin configuring the task's schedule. For more information, see *Configuring tasks* (on page 894).
 - § **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 > Tasks**. 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.
 - § **Description.** (Optional) Enter additional information about the task. This description displays next to the monitor in the Task Library.
 - § **Enable this schedule.** Select this option to begin configuring the task's schedule. For more information, see *Configuring tasks* (on page 894).
 - § **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.....	897
Changing preferences.....	897
Managing dashboard views.....	899
Using the Program Options.....	901

Configuring Email settings

Use this dialog to configure the default global settings for Email actions.

To configure Email settings:

- 1 From the WhatsUp Gold web interface, go to **Admin > Email**. The Configure Email Settings dialog opens.
- 2 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.** Enter 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.
- 3 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* (on page 47) should refresh.
- § **Full report.** Enter a time (in seconds) for how often *monitor reports* (on page 682) 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 303).



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.

WUGSpace Community

If you enter your community credentials in this dialog, they will be saved and used to automatically log into the community each time you download, import, or publish application profiles in WhatsUp Gold APM.

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:

- 1 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.
- 2 Click **New**. The New Dashboard View dialog appears.
- 3 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 one 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).
- 4 Click **OK** to save changes.

To edit an existing dashboard view:

- 1 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.
- 2 Select a view from the list, then click **Edit**. The Edit Dashboard View dialog appears.
- 3 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).

4 Click **OK** to save changes.

To copy an existing dashboard view:

1 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

2 Select a view from the list, then click **Copy**. The Edit Dashboard View dialog appears.

3 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).

4 Click **OK** to save changes.

To copy a dashboard view to another WhatsUp Gold user:

1 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

2 Click **Copy to**. The Edit Dashboard View dialog appears.

3 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.

4 Click **OK** to save changes.

To delete a dashboard view:

1 From the WhatsUp Gold web interface, go to **Admin > Dashboard Views**. The Manage Dashboard Views dialog appears.

2 Select a view from the list, then click **Delete**. A confirmation dialog appears.

3 Click **Yes** to confirm the deletion.

Using the Program Options

In This Chapter

Enabling the polling engine	901
Enabling actions.....	902
Enabling performance monitors.....	902
Enabling WhatsVirtual event collection.....	902
Enabling Ping Throttle.....	903
Enabling the SNMP Trap Listener	903
Enabling the Windows Event Log listener	904
Enabling the Syslog listener.....	904
Enabling FIPS 140-2 mode.....	905
Changing the device state colors or icons	906
Passive Monitor Listeners.....	906
Changing how long report data is stored	907
Selecting a display font.....	907
Changing clock/regional preferences.....	907
Changing the date and time format	907
Using the WhatsUp Services Controller	909

There are a number of administrative features available in the WhatsUp Gold console Program Options.



Note: Program Options are only available from the WhatsUp Gold console.

To access the WhatsUp Gold console Program Options:

- 1 Click **Start > Programs > Ipswitch WhatsUp Gold > WhatsUp Gold**. The WhatsUp Gold console application appears.
- 2 Click **Configure > Program Options**. The Program Options dialog appears.
- 3 Select options as required.

Enabling the polling engine

To enable or disable the WhatsUp polling engine:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable polling engine** to turn on polling. Clear the selection to turn polling off.
- 4 Click **OK** to save changes.



Tip: In the bottom right corner of the WhatsUp Gold console, the Polling icon shows if the engine is active.

Enabling actions

To enable or disable the WhatsUp Gold actions:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable actions** to enable actions. Clear the selection to disable all actions.



Important: If you disable WhatsUp Gold actions, any configured actions or action policies do not run.

- 4 Click **OK** to save changes.

Enabling performance monitors

To enable or disable WhatsUp Gold performance monitors:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable performance monitors** to enable WhatsUp Gold performance monitors. Clear the selection to disable all performance monitors.



Important: If you disable performance monitors, WhatsUp Gold ceases to gather device data using any of the default or custom performance monitors that exist in the Performance Monitor Library.

- 4 Click **OK** to save changes.

Enabling WhatsVirtual event collection

To enable or disable WhatsVirtual event collection:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable WhatsVirtual event collection** to enable the collection of events from all of the configured vCenter servers. Clear the selection to disable the collection of events.



Note: The **Enable WhatsVirtual event collection option** is selected by default, enabling event collection for all configured vCenter servers.

- 4 Click **OK** to save your changes, or click **Cancel** to discard your changes.

Enabling Ping Throttle



Note: Increasing the time between consecutive pings generated by the ping engine lowers the bandwidth required to support the ping engine, but increases the amount of time required to ping monitored devices. Decreasing the time between consecutive pings increases bandwidth requirements, but decreases the amount of time needed to ping monitored devices.



Note: The **Throttle pings by x msec** selection persists only if you have selected an option other than the default. The default setting is 20 msec.

To enable ping throttle:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon. The General options appear.
- 3 Select **Throttle pings by x msec** option and select the number of milliseconds you want the ping engine to wait between consecutive pings.
- 4 Click **OK**. The Program Options dialog closes.

Enabling the SNMP Trap Listener

You must enable the SNMP Trap listener to collect data for the *SNMP Trap Log* (on page 731) report.



Important: The SNMP Trap Listener cannot be enabled through the web interface; it must be enabled in the WhatsUp Gold console.

Important: The Microsoft SNMP Trap Listener must be disabled to enable the WhatsUp Gold SNMP Trap Listener.

To enable the SNMP Trap listener:

- 1 In the WhatsUp Gold console, select **Configure > Program Options**. The Program Options dialog appears.
- 2 Select **Passive Monitors Listeners**.
- 3 Select **SNMP Trap**, then click **Configure**. The SNMP Trap Listener Configuration dialog opens.
- 4 Select **Listen for messages on port** and enter a port number to enable the SNMP Trap Listener (default port is 162).
- 5 To collect data on unsolicited events as well, select **Accept Unsolicited SNMP Traps**.



Note: Do not select this option when using SNMP v3 credentials.

- 6 Click **OK** to close the SNMP Trap Listener Configuration dialog. Click **OK** again to close the Program Options dialog.

To disable the Microsoft SNMP Trap Listener:

- 1 Click **Start** and type `services.msc` in the search box. The Services console appears.
- 2 Locate **SNMP Trap Service** in the list of services.
- 3 Right-click **SNMP Trap Service**, and select **Properties** from the menu.

- 4 Verify that the service status is **Stopped**. If the service status is Started, click the **Stop** button.
- 5 Verify that the Startup type is **Manual** or **Disabled**. If the startup type is set to another type, select **Manual** from the Startup type menu.
- 6 Click **OK** to close the SNMP Trap Properties dialog.

Enabling the Windows Event Log listener

You must enable the Windows Event Log listener to collect data for the *Windows Event Log* (on page 733).

To configure the Windows Event Log Listener:

- 1 From the WhatsUp Gold console main menu, select **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.

Enabling the Syslog listener

You must enable the Syslog listener to collect data for the *Syslog* (on page 732) report.

To configure the Syslog Passive Monitor Listener:

- 1 From the WhatsUp Gold console main menu, select **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 Syslog Trap listener, 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, as when another application needs to use the same port.
 - § **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 device Syslog reports and are able to trigger actions.

- 5 Click **OK** to save changes.

Enabling FIPS 140-2 mode



Note: For information about operating WhatsUp Gold in FIPS-140-2 mode, please see *About operating WhatsUp Gold in FIPS 140-2 mode* (on page 905).

If WhatsUp Gold is being installed on an operating system that is currently running in FIPS140-2 mode, WhatsUp Gold will detect the FIPS compliant operating system and automatically place WhatsUp Gold in FIPS 140-2 mode upon initial installation and start-up. However, if WhatsUp Gold is installed on an operating system that is not running in the FIPS compliant mode and the operating system has the FIPS compliant mode enabled after a WhatsUp Gold install occurs, then you must manually enable the **Operate in FIPS 140-2 mode** option in the WhatsUp Gold console application Program Options General dialog.

To enable or disable FIPS 140-2 mode:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Operate in FIPS 140-2 mode** to enable FIPS 140-2 mode. Clear the selection to stop WhatsUp Gold from operating in FIPS 140-2 mode.



Note: When the FIPS 140-2 mode is selected (enabled), WhatsUp Gold prompts users for the web interface user credentials to log into the console application.



Note: This option is disabled if any of the configured credentials in the Credentials Library are not FIPS-compliant. In order for this option to be available, you must go to the Credentials Library and either modify or remove the non-compliant credentials.

- 4 Click **OK** to save changes.

About operating WhatsUp Gold in FIPS 140-2 mode

There are several *important* things to take into consideration if you plan to operate WhatsUp Gold in FIPS 140-2 mode:

- § When the FIPS 140-2 mode is selected (enabled), WhatsUp Gold prompts users for the web interface user credentials to log into the console application. For more information, see Program Options - General in the WhatsUp Gold console application.
- § If WhatsUp Gold is being installed on an operating system that is currently running in FIPS140-2 mode, WhatsUp Gold detects the FIPS compliant operating system and automatically places WhatsUp Gold in FIPS 140-2 mode upon initial installation and start-up.
However, if WhatsUp Gold is installed on an operating system that is not running in the FIPS compliant mode and the operating system has the FIPS compliant mode enabled after a WhatsUp Gold install occurs, then you must manually enable the **Operate in FIPS 140-2 mode** option in the WhatsUp Gold console application Program Options General dialog.
- § If you plan to use FIPS 140-2, we recommend that you use credentials and SSL certificates that use strong encryption.
- § If you plan to use FIPS 140-2, make sure that devices with SSH-based monitoring are configured to use SSHv2.
- § SNMPv3 credentials using MD5 and/or DES56 are prohibited; you are unable to enable FIPS if SNMPv3 credentials using MD5 and/or DES56 exist in the Credentials Library. You must modify or remove such credentials in order to enable FIPS.

The following may occur when you try to enable FIPS 140-2 mode in the Program Options dialog:

If a message is presented that you have non-compliant SNMPv3 credentials:

This option is disabled because the SNMPv3 credentials are not FIPS compliant. Go to the Credentials Library to edit or remove the SNMP credentials. After editing or removing the credentials, you can enable this option in the Program Options dialog.

For more information about the FIPS 140-2 specification, see the *U.S. Department of Commerce documentation* (http://www.whatsupgold.com/wug_USDOC_FIPS).

Changing the device state colors or icons

To change the device state colors or icons:

- 1 From the main menu, click **Configure > Program Options**.
- 2 In Program Options, click **Device States**.
- 3 To change an existing icon or state, select the entry from the list and click **Edit**.
- 4 Adjust the shape and color of the icon using the settings in the **Device State Editor**.
- 5 Click **OK** to save changes.

If the default settings do not fit your needs, click **Add** to create a new device state, using the internal state and state time that you need.

Passive Monitor Listeners

Passive Monitor Listeners are applications that listen for specific information being passed across your network, or events that occur on one of your devices, then notifies WhatsUp Gold when the information matches what it is listening for. Use this dialog to configure those

servers according to your specific needs. For more information, see *Using Passive Monitors* (on page 436).

WhatsUp Gold provides the following Passive Monitor Listeners:

- § **SNMP Trap**. This listener monitors SNMP information being passed across your network.
- § **Syslog**. This listener monitors a computers Syslog.
- § **Windows Event Log**. This listener monitors the Windows Event Log.

Changing how long report data is stored

Ping Active Monitor data is stored in the WhatsUp Gold database to populate the performance logs available in the application.

To configure WhatsUp Gold report data:

- 1 From the main menu, click **Configure > Program Options**.
- 2 In Program Options, click **Report Data**.
- 3 On the Report Data section, you can change the data settings for performance monitors, active monitors, and passive monitors.
- 4 Click **OK** to save the changes.

You can see how many rows in the database that the data takes up by viewing the numbers under the time settings.

Selecting a display font

Use the Map Font to select a font for the device labels in your map views and log graphs. The fonts in the list are fonts that are currently installed and available on your computer.

To select a display font for WhatsUp Gold:

- 1 From the main menu bar on the WhatsUp Gold console, click **Configure > Program Options**. The Program Options dialog appears.
- 2 Click **Map Font**, then select the font and font size you want to use in WhatsUp Gold.

Changing clock/regional preferences

To use a 24-hour clock instead of the default 12-hour clock:

- 1 From the WhatsUp Gold main menu, click **Configure > Program Options**.
- 2 Click the **Regional** section.
- 3 Select the **Use 24 hour clock** option.
- 4 Click **OK**.

Changing the date and time format

To change the date and time format:

- 1 From the WhatsUp Gold main menu, click **Configure > Program Options**.
- 2 Select the **Regional** section.
- 3 For each of the three date formats, select the one that best suits your needs.
- 4 Click **OK**.

These formats can be seen in use on several of the logs available on the WhatsUp Gold web interface.

Using the WhatsUp Services Controller

In This Chapter

Managing services.....909

Managing services

The WhatsUp Gold Admin Panel allows you to manage all Ipswitch WhatsUp Gold services.



Note: Some services are optional. If the associated product is not licensed and enabled, you may not be able to start, stop, or restart the service. Your license file determines whether you can access a plug-in. To update your license visit the *WhatsUp Customer Portal* (<http://www.whatsupgold.com/wugCustPortal>).

- § Polling Engine (`nm-service.exe`)
- § Flow Collector (`bwcollector.net.exe`)
- § Alert Center (`alertcenterservice.exe`)
- § Configured (`networkconfigservice.exe`)
- § Discovery (`discoveryservice.exe`)
- § Failover Manager (`nmfailover.exe`)
- § API (`nmapi.exe`)
- § Connected Data Service (`networkviewerdataservice.exe`)
- § Virtual Service (`whatsvirtualservice.exe`)
- § Service Bus (`nm-servicebus.exe`)
- § Polling Controller (`nmpollingcontroller.exe`)
- § Data Collector (`nmdatacollector.exe`)
- § Active Monitor Manager (`nmmanagers.exe`)
- § Poller (`nmpoller.exe`)
- § Task Controller (`nmtaskcontroller.exe`)
- § APM State Manager (`apmstatemanager.exe`)
- § Wireless Poller (`nmwireless.exe`)
- § WhatsUp Configuration API (`nmconfigurationmanager.exe`)
- § WhatsUp Message Server (`nm-messageserver.exe`)
- § Action Manager (`nmactionmanager.exe`)
- § Drone Manager (`dronemanager.exe`)
- § APM Discovery (`apm-discovery-service-host.exe`)

The Admin Panel communicates with the Ipswitch Service Control Manager service (`ServiceControlManager.exe`) to issue start, stops, and restarts to the services used by WhatsUp Gold and its plug-in applications.

The following information is displayed:

- § **Description.** Lists the description of the WhatsUp service, as gathered by the Ipswitch Service Control Manger service.
- § **Process Name.** Lists the WhatsUp process .exe as listed in the Windows Task Manager Process tab.
- § **Status.** Lists the current state of the service.

To stop a WhatsUp Gold or plug-in service:

- 1 Go to **Admin > Admin Panel**.
- 2 Select the service you want to stop by clicking its service **Description**.
- 3 Click **Stop**. The results appear in the Services Log.

To start a WhatsUp Gold or plug-in service:

- 1 Go to **Admin > Admin Panel**.
- 2 Select the service you want to start by clicking its service **Description**.
- 3 Click **Start**. The results appear in the Services Log.

To restart a WhatsUp Gold or plug-in service:

- 1 Go to **Admin > Admin Panel**.
- 2 Select the service you want to restart by clicking its service **Description**.
- 3 Click **Restart**. The results appear in the Services Log.

To manually stop all WhatsUp Gold services:

- 1 Close all WhatsUp Gold applications.
- 2 From the Windows **Administrative Tools > Computer Management** application, under **Services and Applications > Services**, select the **Ipswitch Service Control Manager** service, then click **Stop**.
- 3 Stop all the pollers that may be running on local system or remote computers. From the Windows Task Manager, click the **Processes** tab, select the `ServiceControlManager.exe` process in the **Image Name** list, then click **End Process**.

Using SNMP

In This Chapter

SNMP overview	911
Enabling SNMP on Windows devices.....	912
Monitoring an SNMP Service.....	912
About the SNMP Agent or Manager	913
About the SNMP Management Information Base.....	913
About SNMP Object Names and Identifiers.....	914
Using the SNMP MIB Manager.....	914
Using the SNMP MIB Manager to troubleshoot MIB files.....	915
About the SNMP operations.....	917
Using a custom name for SNMP device interfaces.....	917
About SNMP security	918
Using the Trap Definition Import Tool.....	919

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 911).

To install SNMP Monitoring:

- 1 From the Windows Control Panel, click **Add or Remove Programs** (Programs and Features).
- 2 Click **Add/Remove Windows Components** (Turn Windows features on or off).
- 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 430).

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 917) and *Enabling SNMP on Windows devices* (on page 912).

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.

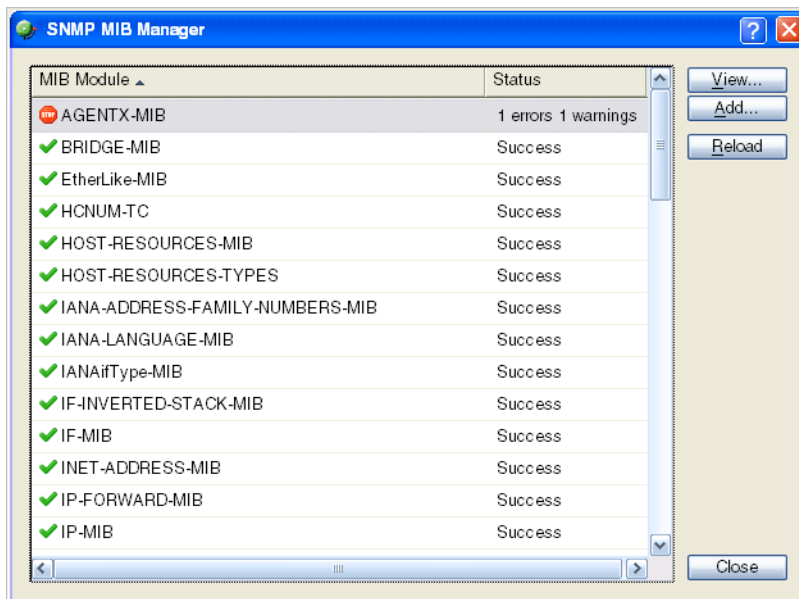


Note: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

- § **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.



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.



- 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 if 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 In the WhatsUp Gold web interface, select **Devices** from the **Dashboard** tab.
- 2 Right-click on the target device and select **Properties** to launch the Device Properties dialog.
- 3 Select the **Performance Monitors** tab.
- 4 Select **Interface Utilization**, then click **Configure**. The Configure Interface Data Collection dialog appears.
- 5 In the **Collect data for** list, select **Specific Interfaces**.
- 6 Choose the specific interfaces for which you want to collect data.
- 7 Click **OK**.

To add an Active Monitor for a newly renamed device interface:

- 1 From the admin console, access the Device Properties dialog for the target device, then select the **Active Monitors** tab.
- 2 If the target device had existing active monitors configured and enabled prior to renaming the interface, select the old instance, then click **Remove**.
- 3 Click **Rescan** to refresh the interface list. If a device has performance monitors set up prior to renaming the device's interface(s), the device interface names are automatically updated.
- 4 Click **OK**.

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.

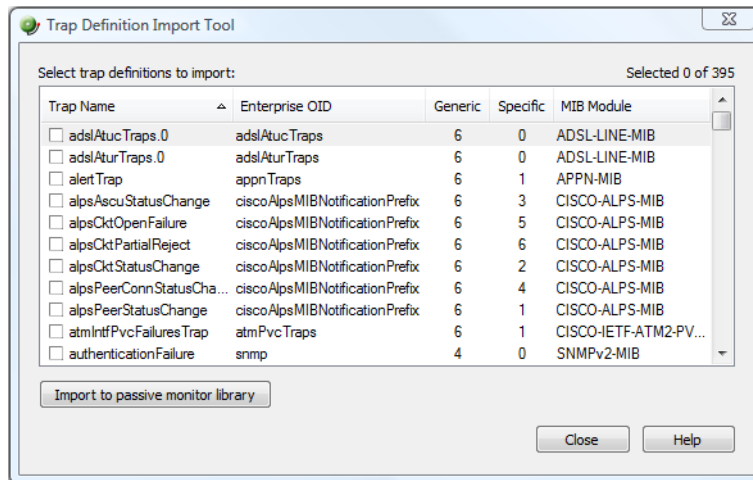
Devices need SNMP credentials assigned to them before SNMP-based Active Monitors will work.

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.



- 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	920
Scripting Active Monitors	921
Scripting Performance Monitors.....	937
Scripting Actions.....	947
Using the SNMP API.....	952

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 921).
- § **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 937).
- § **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 947).

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.

New Active Script Monitor

Name: ☐ Use in discovery

Description:

Timeout: (seconds) Script type:

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
```

OK Cancel Help

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

`LogMessage(sText);`

Method description

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 = parseInt(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 924)
- § *Alert when temperature exceeds or drops out of range* (on page 925)
- § *Determine invalid user account activity* (on page 926)
- § *Monitor bandwidth utilization on an interface* (on page 931)
- § *Monitor an SNMP agent running on a non standard port* (on page 934)
- § *Monitor for unknown MAC addresses* (on page 935)

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 interface 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 DOT1DTONFDBPORT_OID = "1.3.6.1.2.1.17.4.3.1.2";
    var DOT1DTONFDBADDRESS_OID = "1.3.6.1.2.1.17.4.3.1.1";
    var sOid = DOT1DTONFDBPORT_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(DOT1DTONFDBPORT_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(DOT1DTONFDBPORT_OID.length+1, sOid.length);

        // get it in hex format...
        oComResult = oSnmpRqst.Get(DOT1DTONFDBADDRESS_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

Edit Active Script Performance Monitor

Name: Script type:

Description: Timeout (sec):

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

Buttons: Add, Edit, Remove

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.
```

Buttons: OK, Cancel, Help

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 698) full and dashboard reports.
- \$ Errors from this performance monitor are displayed in the *Performance Monitor Error log* (on page 730) 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

`LogMessage(sText);`

Method description

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 = parseInt(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.

This method allows you to graph a value.

Example

JScript

```
Context.SetValue(245)
```

```
SetValue(nValue);
```

`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 942)
- § *Poll a reference variable and perform a calculation* (on page 943)
- § *Graph a temperature monitor* (on page 944)
- § *Poll the storage table using SNMP GetNext* (on page 945)
- § *Poll multiple reference variables* (on page 946)

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);
}
```

}

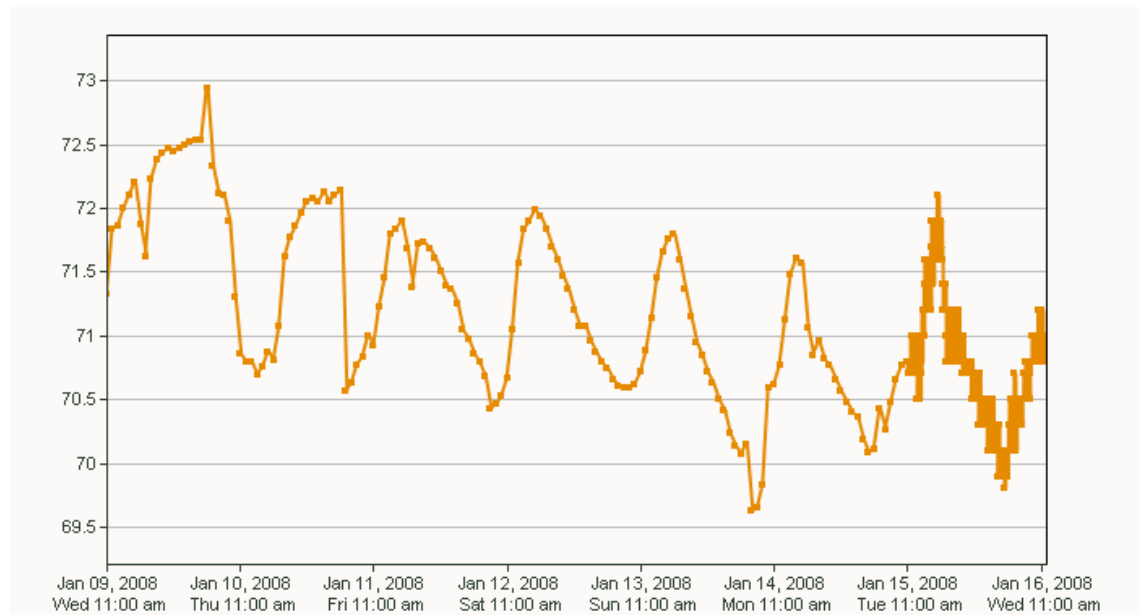
Graph a temperature monitor



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 + ".9999999999"))
{
    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.

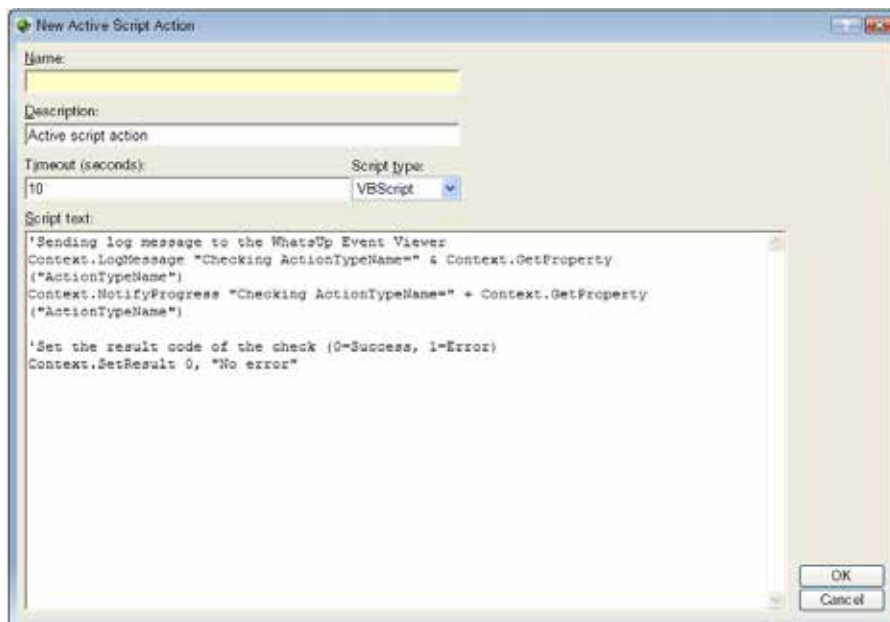
```
// This script is a JScript that will allow you to graph the percentage of retransmitted
TCP
//' segments over time on a device.
// For this script, we use two SNMP reference variables:
//' The first Reference variable RVtcpOutSegs is defined with OID 1.3.6.1.2.1.6.11 and
instance 0. It polls the
//' 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.



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

`LogMessage(sText);`

Method description

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. These 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

"CredWindows:DomainAndUserid"	Windows NT Domain and User ID
-------------------------------	-------------------------------

This context object is only available if impersonations are enabled.

"CredWindows:Password"	Windows NT Password
------------------------	---------------------

This context object is only available if impersonations are enabled.

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 950)

§ *Acknowledge all devices* (on page 951)

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 959).

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 `ComSnmprResponse` 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
<code>Initialize(nDeviceID)</code>	Initializes the <code>Snmprqst</code> object for the device with the device ID specified in <code>nDeviceID</code> . If a device is not configured with a valid SNMP credential, the operation will fail. § <code>nDeviceID</code> . A positive integer corresponding to the device ID of a device configured in WhatsUp Gold.	<code>ComResult</code> object

Method	Description	Returns
	<p>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:</p> <pre>Context.GetProperty("DeviceID")</pre>	
Initialize2 (sDeviceAddress, nCredentialID)	<p>Initializes the <code>SnmpRqst</code> 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 <code>SnmpRqst</code> for a device that is not configured in WhatsUp Gold as long as the credentials for the device are configured in the credential library.</p> <p>§ sDeviceAddress. The address or hostname of the device to be queried.</p> <p>§ nCredentialID. A positive integer corresponding to the credential ID of a credential configured in WhatsUp Gold.</p>	ComResult object
SetTimeoutMs (nTimeoutInMilliSec)	<p> Sets the timeout value in milliseconds. If not specified, the timeout defaults to 2000 milliseconds.</p> <p> nTimeoutInMilliSec. A positive integer representing the number of milliseconds after which unresolved requests should be terminated.</p> <p> Note: This method returns a value if the method fails and requires an object variable to capture this value. For example: <code>varComResult = SnmpRqst.SetTimeoutMs(5000);</code> where <code>varComResult</code> is a <code>ComResult</code> object.</p>	ComResult object
SetNumRetries (nNumberRetries)	<p>Sets the number of times to retry a request that has timed out. If not specified, failed requests are retried one time.</p> <p>§ nNumberRetries. A positive integer representing the number of times to retry timed out requests.</p> <p>Tip: To send only one SNMP packet per request,</p>	ComResult object

Method	Description	Returns
	Set <code>nNumberRetries</code> to 0 (zero).	
SetPort (<code>nPort</code>)	Sets the TCP/IP port to be used by <code>SnmpRqst</code> . If not specified, port 161 is used. § <code>nPort</code> . A positive integer between 1 and 65535 corresponding to the port to be used.	ComResult object
Get (<code>sOid</code>)	Issues an SNMP Get command to retrieve the value of the specified object. § <code>sOid</code> . A string containing a valid OID.	ComSnmpResponse object
GetNext (<code>sOid</code>)	Issues an SNMP GetNext command to retrieve the value of the object that follows the specified object in lexicographic order. § <code>sOid</code> . A string containing a valid OID.	ComSnmpResponse object
GetMultiple (<code>sListOfOids</code>)	Issues an SNMP Get command for each of the objects specified. <code>GetMultiple</code> sends all commands in a single SNMP protocol data unit, so it is more efficient than issuing multiple <code>Get</code> commands independently. § <code>sListOfOids</code> . A comma-separated list of valid OIDs.	ComSnmpResponse object
Set (<code>sOid</code> , <code>sType</code> , <code>sValue</code>)	Issues an SNMP Set command to set an OID value on a device. § <code>sOid</code> . A string containing a valid OID for the object for which you want to set the value. § <code>sType</code> . 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 § <code>sValue</code> . 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 <code>true</code> if this object contains a failure and <code>false</code> if the object contains a success.
GetErrorMsg	If Failed is <code>true</code> , 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 <code>SnmpRqst.GetMultiple</code> . Note: This member is only useful when used with <code>SnmpRqst.GetNext</code> . It can be used with <code>SnmpRqst.Get</code> and <code>SnmpRqst.Set</code> , 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 (<code>SnmpRqst.Get</code> , <code>SnmpRqst.GetNext</code> and <code>SnmpRqst.Set</code>)
Failed	If the request succeeded, returns <code>false</code> . If the request failed, returns <code>true</code> . Note: When polling multiple objects, <code>Failed</code> returns <code>true</code> if even one error exists in the results returned by <code>GetPayload</code> .
GetErrorMsg	If <code>Failed</code> returns <code>true</code> , 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 <code>VarBindList</code> node which contains one or many <code>SnmpVarBind</code> nodes. <pre><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" /></pre>

	</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 `ComSnmprResponse` 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 function 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.

Using the Dashboard Screen Manager

In This Chapter

Ipswitch Dashboard Screen Manager overview	960
How does the Dashboard Screen Manager work?	961
Installing the Dashboard Screen Manager	961
Configuring a Dashboard Screen Manager playlist	962

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 962).

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

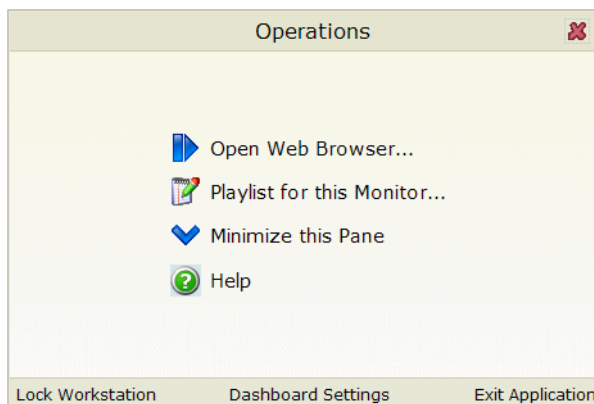
After successfully installing the Dashboard, you can access the application from your Windows Start Menu by clicking **Ipswitch Dashboard > Dashboard**.



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 962).



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.

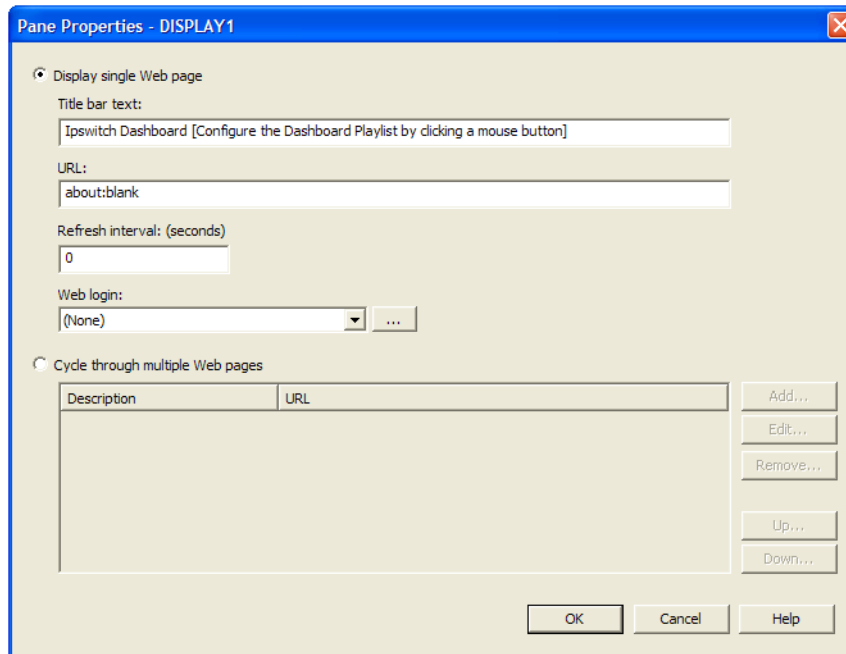
To configure a single Web page playlist:

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.



- 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.

Troubleshooting and Maintenance

In This Chapter

Troubleshooting your network	966
Maintaining the Database	967
Group Policy Object 503 Service Unavailable Error	969
Recovering from a "Version Mismatch" error	970
Task Tray Application fails on Windows Vista	971
Co-located SQL Server and WhatsUp Gold server clocks must be synchronized	971
Connecting to a remote desktop	972
WhatsUp Gold engine message	972
Troubleshooting SNMP and WMI connections	972
False negative returned from WMI monitors	973
Re-enabling the Telnet protocol handler	974
Passive Monitor payload limitation	975
Receiving entries in the SNMP Trap Log	975
Recommended SMS modems and troubleshooting tips	975
Troubleshooting IIS configuration	977
Uninstalling Ipswitch WhatsUp Gold	978
Troubleshooting the WhatsUp Health Threshold	979

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.

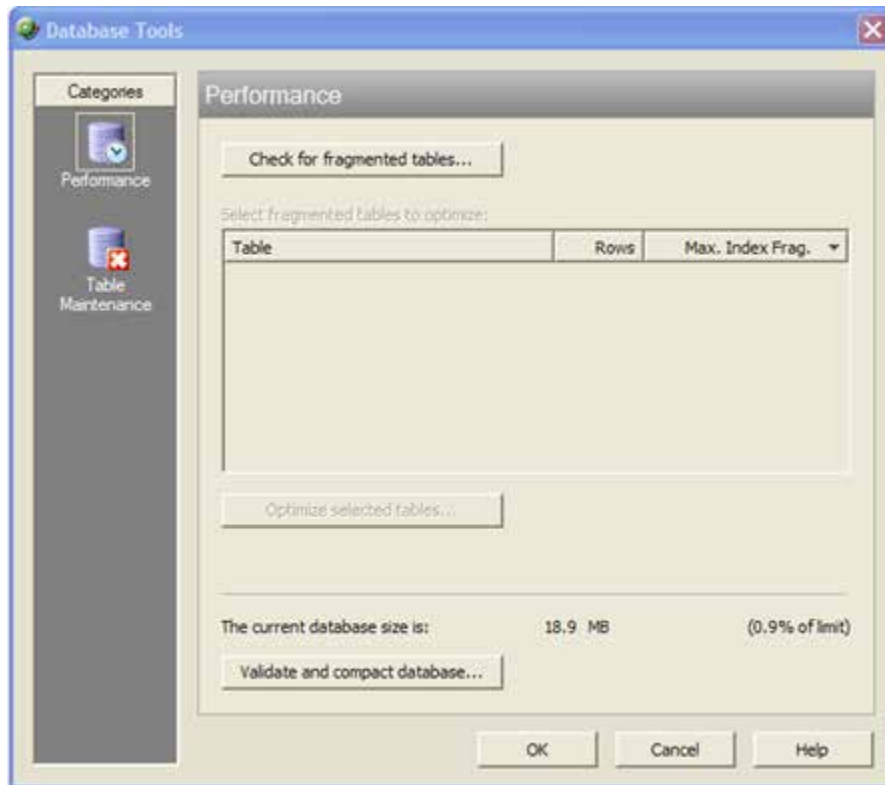
To access the database utilities, open the WhatsUp Gold console, then click **Tools > Database Utilities** from the main menu.

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.



- 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 Microsoft SQL Server 2008 R2 Express Edition as the WhatsUp Gold database, this section also displays the percentage of the 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 CHECKCONSTRAINTS`, `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 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 267). 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 `RPCPingTimeout` to 10000 (decimal).

To edit the `RPCPingTimeout` 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 `ieexplore.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.whatsupgold.com/coniugomodems>
- § *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.
- § *Vodafone 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

Troubleshooting IIS configuration

If you experience an IIS configuration error when attempting to install WhatsUp Gold, there are a number of troubleshooting procedures you can perform that, in most cases, will correct the issue eliminating the need to call technical support.

- § First, if you are installing WhatsUp Gold for the first time or if you are upgrading from version 15.x or earlier, restart your computer and run the WhatsUp Gold installation program again.
- § In the event the IIS configuration error persists, close all browser window instances, clear your browser cache, open a new browser instance, and attempt to access WhatsUp Gold.
- § If this does not correct the issue, reset IIS by opening a command line on your WhatsUp Gold server and issuing the following command: `iisreset`.

If you are still experiencing IIS configuration issues, perform the following procedures to check for the proper account settings in IIS and then repair IIS as a last option, if needed.

To check for correct WhatsUp Gold account settings using IIS 6:

- 1 Launch Internet Information Services (IIS) Manager from the Administrative Tools section of the Windows Control Panel. Search for `inetmgr` from the Windows Start menu to locate the application, if needed.
- 2 Select **Application Pools** from the navigation tree at left and confirm that **NmConsole** is present and running.
- 3 Right-click **NmConsole** and select **Properties** to launch the NmConsole Properties dialog.
- 4 Select the **Identity** tab and confirm the `WhatsUpGold_User` account, or the account name you entered during WhatsUp Gold installation, is in use.
- 5 Click **Apply** to apply any IIS configuration changes you made, if applicable, then click **OK** to close the dialog.
- 6 Return to the navigation tree and expand the Web Sites folder.
- 7 Right-click the **WhatsUp Gold virtual directory**, then select **Properties** to launch the WhatsUp Gold Properties dialog.
- 8 Click the **Directory Security** tab.
- 9 Click **Edit** to launch the Authentication Methods dialog.
- 10 Confirm that the `WhatsUpGold_User` account is in use.
- 11 Click **OK** to close the Authentication Methods dialog.
- 12 Right-click **NmConsole**, then click **Properties** to launch the NmConsole Properties dialog.
- 13 Confirm that the `WhatsUpGold_User` account is in use.

To check for correct WhatsUp Gold account settings using IIS 7/7.5:

- 1 Launch Internet Information Services (IIS) Manager from the Administrative Tools section of the Windows Control Panel. If needed, search for `inetmgr` from the Windows Start menu to locate the application.
- 2 Select **Application Pools** from the navigation tree at left and confirm that NmConsole is present and running.

- 3 Right-click **NmConsole**, then select **Properties** to launch the NmConsole Properties dialog.
- 4 Select the **Identity** tab and confirm the `WhatsUpGold_User` account is in use.
- 5 Click **Apply** to apply any IIS configuration changes you made, if applicable, then click **OK** to close the dialog.
- 6 Return to the navigation tree and expand the Sites folder.
- 7 Select the **WhatsUp Gold virtual directory**, then click the **Basic Settings** hyperlink at right.
- 8 Click **Test Settings**. Results should indicate `Connect as 'WhatsUpGold_User'`. Verify two successful results.
- 9 Select **NmConsole**, then click the **Basic Settings** hyperlink at right.
- 10 Click **Test Settings**. Results should indicate `Connect as 'WhatsUpGold_User'`. Verify two successful results.

To repair IIS:

- 1 Launch Internet Information Services (IIS) Manager from the Administrative Tools section of the Windows Control Panel. If needed, search for `inetmgr` from the Windows Start menu to locate the application.
- 2 Delete the WhatsUpGold website and the corresponding NmConsole Application Pool from within the IIS Configuration Manager.
- 3 Delete the following key from the registry using `regedit.exe`:
 - § On 64-bit Operating Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ipswitch\Network Monitor\WhatsUp Gold\Setup\IIS`
 - § On 32-bit Operating Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Network Monitor\WhatsUp Gold\Setup\IIS`
- 4 Re-launch the WhatsUp Gold Installer and select all "repair" options when prompted.

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 configuration 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.

Frequently Asked Questions

The following sections answer frequently asked questions about WhatsUp Gold features and procedures.

Monitors and actions (on page 980)

Alert Center (on page 981)

Dashboards (on page 982)

Wireless (on page 982)

User accounts and permissions (on page 982)

Flow Monitor (on page 984)

Administrative tasks (on page 985)

WhatsConfigured (on page 987)

Monitors and actions FAQ

1 *Where do I configure monitors?*

All monitors (Active, Passive, Performance) are configured in the Monitors Library, accessed from **Admin > Monitors**.

2 *What do each of the monitor types do?*

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.

Passive monitors listen for device events. As active monitors actively query or poll devices for data, passive monitors passively listen for device events.

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.

3 *Where do I assign monitors to devices?*

All monitors are assigned to devices on the Device Properties dialog, accessed by right-clicking a device in either Device or Map View, then clicking **Properties**.

4 *Can I assign monitors to more than one device at a time?*

Yes. The Bulk Field Change feature allows you to assign monitors to multiple devices. To use the Bulk Field Change feature, select the devices to which you want to add a monitor, right-click, then click **Bulk Field Change**. The Bulk Field Change menu displays the available monitor commands. Click the monitor type you want to add.

- 5 *Where do I configure Passive Monitor Listeners? I don't see this option on the web interface.*

Passive Monitor Listeners are configured on the WhatsUp Gold admin console from the Program Options dialog, accessed from the **Configure** menu.

- 6 *What is a global performance monitor?*

A global performance monitor can be applied to all network devices. These performance monitors are the default, base monitors that cannot be removed from the Performance Monitor Library.

- 7 *What are actions?*

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.

- 8 *Where do I configure actions?*

Actions are configured in the Actions Library, accessed from **Admin > Actions**.

- 9 *Where do I assign actions to devices?*

Actions are assigned to devices on the Device Properties dialog, accessed by right-clicking a device in either Device or Map View, then clicking **Properties**.

- 10 *What is an action policy?*

Action policies allow you to group multiple actions for use on a device or monitor. For example, you can create an action policy to restart a particular service if a service stops on a device and to email you if the device shuts down.

- 11 *Where are action policies configured?*

Action policies are configured in the Action Policy Library, accessed from **Admin > Action Policies**.

Alert Center FAQ

- 1 *What is Alert Center?*

Alert Center is a feature in WhatsUp Gold that handles alerting on performance monitors, passive monitors, system health, Flow Monitor, and Wireless through user-defined thresholds and notification policies.

- 2 *Why doesn't Alert Center do alerts on active monitors?*

WhatsUp Gold actions were designed to work with active and passive monitors and currently cannot be applied to performance monitors. Alert Center was designed to alert on performance monitors as well as other WhatsUp Gold features and plug-ins.

- 3 *What is the difference between an action and a threshold notification?*

Alert Center's threshold notifications come in the form of alerts that are displayed on the Alert Center home page and in emails. While alerts can also send email notifications, they can also perform a number of tasks. Used together, Alert Center and actions help you stay informed and thoroughly manage your network.

4 *What are notification policies?*

Notification policies allow you to sequence Alert Center notifications. For example, you can email the QA lab manager in step 1 if a device in the QA lab goes down, you can email an IT representative in step 2 if multiple devices in the QA lab go down, and you can email the IT manager in step 3 if all devices in the QA lab go down.

5 *Where do I configure Alert Center notifications?*

In the Notification Library, accessed from **Alert Center > Notification Library**.

6 *Where do I configure Alert Center notification policies?*

In the Notification Policy Library, accessed from **Alert Center > Notification Policy Library**.

7 *Where do I configure Alert Center thresholds?*

In the Threshold Library, accessed from **Alert Center > Threshold Library**.

8 *What are running notification policies?*

Running notification policies are notification policies that are currently running. These policies are displayed at the top of the Alert Center home page and can be stopped at any time.

9 *How do I assign thresholds to devices?*

When you configure a threshold, you choose the device to which you want to assign the threshold in the "Devices to Monitor" section of the threshold configuration dialog.

Dashboard FAQ

1 *What exactly is a dashboard?*

Dashboards display various types of network information in the form of network views dashboard reports and can be customized to display the information you find m

2 *How do I create new dashboards?*

You create new dashboards and manage existing dashboards from the Manage Dashboard Views dialog, accessed from **Admin > Dashboard views**.

Wireless FAQ

1 *I did a device discovery, but the scan did not find any of my wireless devices. What should I do?*

Make sure the "Gather information for wireless topology and performance" option is selected on the Discovery Console (Settings > Advanced Settings) and perform a new discovery scan. Also, ensure that relevant SNMP credentials (SNMPv2 and higher) are included in your discovery scan and assigned/enabled on your wireless devices prior to doing a discovery scan. Lastly, do not use single device discovery to add wireless devices to WhatsUp, as devices discovered are not recognized as wireless devices.

2 *Where do I configure Wireless settings?*

On the Wireless Applications Settings page, accessed from the Wireless tab by clicking the gear icon in the right corner of the menu bar and clicking Application Settings. From the Applications Settings page you can configure the Global Settings, Data Collection settings, and manage your Excluded rogues list.

3 *What is a rogue device?*

A rogue device is an unauthorized device that is connected to your network that could potentially be a risk. The Wireless Rogues page displays a list of foreign wireless devices connected to your network and gives you the opportunity to categorize the devices as either non-threatening or potentially harmful—you can exclude the devices you see as non-threatening and focus on possible threats.

User accounts and permissions FAQ

1 *Where do I go to create user accounts for my team members?*

You create user accounts on the Manage Users dialog, accessed from **Admin > Users**.

2 *How are user account permissions handled?*

When the WhatsUp admin user account creates new user accounts, user rights are selected for the new user account. These user rights govern the actions the account can perform in WhatsUp. The WhatsUp administrator account has every right enabled. It is up to the administrator's discretion to choose the rights given to other accounts carefully, taking into consideration the amount of access each account requires and should be given.

3 *Can I create user groups?*

Yes. You can create user groups on the Manage Users dialog, accessed from **Admin > Users**.

4 *Are specific permissions needed to edit device groups?*

Yes. Along with user rights, accounts need specific device group access rights to see devices within particular device groups and to manage these devices and groups. By default, only the administrator user account can see and manage all network devices. As the administrator sees fit, these rights can be enabled on a per-right basis for other user accounts.

5 *How are device group rights carried from group to group?*

Each group has its own access rights, except in the case of subgroups. Group access rights are passed from parent group to subgroup—when a new group is created, all 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 subgroups within it by selecting Apply changes to all sub Device Groups recursively on the Device Group Properties dialog.

6 *What happens when a device belongs to more than one device group?*

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 it belongs.

7 *How do user rights and device group access rights work together?*

When device group access rights are enabled, WhatsUp 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 access rights are considered. If a user does not have the Manage Devices user right, for example, then the Device Write group access rights are not honored.

8 *How do device group access rights work with dynamic 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 device 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 device groups to which the device belongs—if a device is granted one right in one group, it has the right in every group to which it belongs.

9 *Where do users go to change their password after initial login?*

Passwords are managed from the Preferences dialog, accessed from **Admin > Preferences**.

Flow Monitor FAQ

1 *What is Flow Monitor?*

Flow Monitor is a network traffic monitor that lets you gather, analyze, and report on network traffic patterns and bandwidth utilization in real-time.

2 *What is NetFlow?*

NetFlow is a protocol used to collect data about network IP traffic and is used to monitor and record network usage, give indications of traffic routes and provide data in support of traffic accounting, usage-based billing and other network related activities. This data is classified using the concept of a network flow.

3 *How does Flow Monitor work?*

Flow Monitor uses the 1) NetFlow exporter to observe packet data and create records from the observed data to transmit to the 2) NetFlow collector that collects records sent from the exporter and stores them in a database to be forwarded to the 3) Netflow analyzer which analyzes the records for information of interest.

4 *Can all devices transmit NetFlow data automatically to Flow Monitor?*

No. Only network devices such as routers and switches can transmit NetFlow data.

5 *Do network devices automatically transmit flow data to Flow Monitor?*

No. You must manually configure your network devices to export flow data to Flow Monitor. For more information, see [Manually configuring devices to export data to Flow Monitor](#) and [Configuring sFlow enabled devices to export flow data to Flow Monitor](#).

6 *What is Flexible NetFlow?*

Flexible NetFlow is a Cisco IOS that is used to monitor network traffic. You can configure Flexible NetFlow on Cisco network devices to send flow information to Flow Monitor.

7 *What is NetFlow v9 (Lite)?*

NetFlow v9 (Lite) is based on NetFlow v9 and is packet-based sampled data configurable to a range of packet samples. You can configure NetFlow v9 (Lite) on network devices to send sampled flow data to Flow Monitor.

8 *What is NBAR?*

Network Based Application Recognition (NBAR), is a Cisco-developed application classification engine used to recognize a wide variety of applications. You can configure NBAR on Cisco network devices to work in conjunction with Flexible NetFlow.

9 *What is CBQoS?*

Class-based quality of service (CBQoS) is the ability of a network to provide improved services to identified classes of network traffic. These services include supporting dedicated bandwidth, improving loss characteristics, managing network congestion, traffic shaping and setting traffic priorities. CBQoS involves two major components, traffic classes, and traffic policies. You can configure CBQoS on Cisco network devices to support your network traffic health.

Admin FAQ

1 *What is the Monitors Library?*

The Monitors Library is where all WhatsUp Gold monitors (Passive, Active, and Performance) are stored and configured.

2 *What is the Actions Library?*

The Actions Library is where all WhatsUp Gold actions are stored and configured.

3 *What is the Action Policies Library?*

The Action Policies Library is where all WhatsUp Gold action policies are stored and configured.

4 *What is an action policy?*

Action policies allow you to group multiple actions for use on a device or monitor. For example, you can create an action policy to restart a particular service if a service stops on a device and to email you if the device shuts down.

5 *What is the Credentials Library?*

The Credentials Library is where all credentials are stored and configured. Credentials are required for WhatsUp Gold to discover devices, to monitor devices, and to perform actions on devices.

6 *What are recurring actions?*

Recurring actions allow you to fire actions based on a schedule, independent of device statuses. Recurring actions can perform tasks such as sending current system status messages through email or text message.

7 *What are scheduled reports?*

Scheduled reports allow you to have report information sent on a schedule via email, Microsoft Excel, or Adobe .pdf.

8 *What can I configure using the WhatsUp Gold server options?*

Using the server options, you can configure the number of passive monitor records WhatsUp Gold stores on the server and the max height and width of graphical maps. Additionally, you can enable and disable access to WhatsUp Gold from mobile devices.

9 *What does the SNMP MIB Manager do?*

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.

10 *What is the LDAP Credentials dialog for?*

Use the LDAP Credentials dialog to configure LDAP or Active Directory (AD) credentials and to configure WhatsUp Gold to connect with an AD server to import group information from a Microsoft Domain Controller into WhatsUp Gold.

11 *What are the translation options?*

You can translate selected dialog groups or the entire WhatsUp Gold web interface using the Translation dialog. Any language on the list can be selected. The list is populated by language XLIFF files stored in the Language Library.

12 *What is the Users dialog used for?*

Use the Manage Users dialog to manage user accounts and user groups. From this dialog you can create and delete user accounts and user groups, and enable and disable group access rights.

13 *What is the Polling Configuration Library?*

The Polling Configuration Library displays all pollers configured for use with WhatsUp Gold. Use this library to configure new or existing pollers.

14 *What are WhatsUp Gold pollers?*

15 In WhatsUp Gold, pollers are used to gather information from your network devices. Beginning in WhatsUp Gold v16, network administrators can configure WhatsUp Gold to use multiple pollers to increase the number of devices WhatsUp Gold can poll and monitor, this is called 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.

16 *What is the WhatsUp Gold Task Library?*

The Task Library allows you to schedule tasks through the WhatsUp Gold web interface. You can perform many tasks, such as clean the cache for performance monitors, update device groups, and perform database table maintenance. You can configure new and existing tasks using this dialog.

17 *What are the Email Settings used for?*

WhatsUp Gold uses these settings to send action alerts and scheduled report information. Typically, you should enter the network administrator's email information in the Configure Email Settings dialog.

18 *Where does the admin account set its password?*

The admin account password is changed on the Preferences dialog (**Admin > Preferences**).

19 *Where can WhatsUp Gold web interface refresh and display options be set?*

Use the Preferences dialog (Admin > Preferences) to configure refresh intervals for reports, dashboards, and the device list; to set the number of records displayed for reports; to enable and disable web alarms as well as set how often they should be checked; and to select where to display Instant Info popups.

20 *Where can dashboard views be configured?*

Use the Manage Dashboard Views dialog (**Admin > Dashboard Views**) to create, modify, and delete WhatsUp Gold dashboard views.

WhatsConfigured FAQ

1 *How does the WhatsConfigured plug-in for WhatsUp Gold differ from the WhatsConfigured standalone application?*

We have gone to great lengths to make the WhatsConfigured plug-in as similar as possible to the standalone application. WhatsConfigured's main functionality has been carried over to the standalone, allowing you to perform nearly all WhatsConfigured tasks and procedures on the WhatsUp Gold web interface.

2 *What are WhatsConfigured tasks?*

Tasks dynamically gather configuration data from your network devices using task scripts. These tasks are applied to devices and then can be scheduled to run on a regular basis or can be manually ran as needed to upload, download, and backup configuration files, manage device credentials, and much more.

3 *Where are tasks configured?*

Tasks are configured and stored in the Task Library (**Configured > Task Library**).

4 *Where are tasks applied to devices?*

Tasks can be applied to devices on the Device Properties dialog or when configuring tasks in the Task Library.

5 *How do I run a task immediately, rather than waiting for it to run during its configured schedule?*

You can run a task on demand using the **Run Now** option in the Task Library.

6 *What are task scripts?*

Task scripts login to devices through SSH or Telnet and run command-line interface (CLI) commands on devices. These tasks can perform a number of operations, such as restoring or backing up a running or startup configuration, or changing an application password.

7 *Are task scripts configurable?*

Yes and no. WhatsConfigured comes with two pre-configured tasks, which can not be edited or deleted. However, you can copy these pre-configured tasks and modify them. You can also create custom scripts from scratch using the WhatsConfigured Custom Script Language.

8 *Where are task scripts configured?*

Task scripts are configured and stored in the Task Script Library (**Configured > Task Script Library**).

9 *What are policies?*

WhatsConfigured policies search through archived configuration files for strings that are either expected or not expected within the file(s).

10 *Where are policies configured?*

Policies are configured in the Policy Library (**Configured > Policy Library**).

11 *What are templates?*

Templates allow network admins to automatically push device configurations to devices of the same type by replacing device-specific information (IP address, hostname) with variables, saving time and reducing the possibility of error from one manual device configuration to another.

12 *Where are templates configured?*

Templates are configured in the Template Library (**Configured > Template Library**).

13 *What are system scripts?*

System scripts allow you to create scripts to override WhatsConfigured's pre-configured, global scripts for specific functions, such as backup running config scripts. For example, you can create a script for backing up the running config for Cisco devices by copying an existing backup script and modifying the script to map to a Cisco OID. As such, the script would serve as the new default backup config script for Cisco devices, backing up the running config for all devices that support the Cisco OID you specified in the script.

14 *Where are system scripts configured?*

System scripts are configured in the System Script Library (**Configured > System Script Library**).

15 *What is the CLI Settings Library?*

WhatsConfigured allows you to override the default CLI settings used to carry out configuration tasks by creating custom CLI settings for devices from a particular vendor or for specific IP addresses. The CLI Settings Library is where CLI Settings are stored and configured.

16 *What does the Archive Search tool let me do?*

The Archive Search tool lets you search the content of device configuration archives. A configuration archive is any device output captured when running a configuration task/script. When a configuration script is run, the output from one or more commands may be captured and stored in a user or system specified key. The output is saved to the device using the key name and the time-stamp as a look-up key.

17 *What does the VLAN Manager do?*

The VLAN Manager allows you to easily and dynamically update VLAN configurations. Using the VLAN Manager, you can add, edit, and delete VLANs from individual devices. Additionally, you can copy and move single or multiple VLANs from one network device to other VLAN capable network devices.

APM FAQ

1 Is there a limit to the number of components I can add to an application?

No. You are only limited by the number of components your APM license supports.

2 Can I use the same application instance name throughout the different type and profile categories?

No. Each application instance name must be unique throughout the APM system.

- 3 Why are there no components to choose from when configuring a critical component group with an application instance?

The component of interest may already have its critical property enabled, or the component of interest does not exist within the same list as the critical component group. For example, if the component was inherited rather than added as a unique component.

- 4 Why are some Windows services in a stopped state not displayed within the Services Selection dialog when configuring a Service Check (SNMP) component?

Only the Service Check (WMI) component displays both running and stopped Windows services within the dialog.

- 5 Why is the Delete command disabled when attempting to delete a component?

The component of interest currently belongs to a critical component group; either the component needs to be removed from said critical component group or the group needs to be deleted prior to deleting the component.

Copyright notice

©1991-2015 Ipswitch, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the expressed prior written consent of Ipswitch, Inc.

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc., also assumes no liability for damages resulting from the use of the information contained in this document.

IMail, the IMail logo, WhatsUp, the WhatsUp Gold logo, WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Portions of Telerik Extensions for ASP.NET MVC ©2002-2012 by Telerik Corporation. All rights reserved. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

This document was published on Monday, May 18, 2015 at 14:34.