



User Guide

IPSWITCH

CHAPTER 1 WhatsUp Gold Overview

Welcome to Ipswitch WhatsUp Gold v12	1
WhatsUp Gold editions.....	4
What's new in WhatsUp Gold v12.....	5
Learning about the WhatsUp Gold new application features	6
Finding more information	8
Sending feedback.....	9

CHAPTER 2 Gathering and Viewing Network Data

Gathering network data	11
Viewing network data	12

CHAPTER 3 Installing and Configuring WhatsUp Gold

Installation overview	13
System requirements	14
Installation notes	15
Installing or upgrading	15
Activating WhatsUp Gold for new or upgraded licenses	18
About the Task Tray icon.....	18
Configuring the database	19
About the SQL Server 2005 Express Database.....	19
Upgrading the database engine.....	20
Upgrading the database schema	20
Recovering from a "Version Mismatch" error	26
Using an alternative database setup.....	26
About the Database Utilities	30
Configuring the web server	33
Stopping and starting the internal web server	33
About the default SSL certificates	34
Using IIS on Windows XP or Windows 2003	34
Using IIS on Windows Vista.....	37
Uninstalling Ipswitch WhatsUp Gold v12	41

CHAPTER 4 Using Device Discovery

About Device Discovery	43
Using the Device Discovery wizard	43
About Device Discovery scan types	44

Using Device Discovery wizard SNMP SmartScan option.....	44
Example: discovering devices.....	45
Adding a single device manually	48
Example: manually adding a device to a device group.....	49
Example: clicking and dragging a device to a device group.....	51
About Active Discovery	53

CHAPTER 5 Using the WhatsUp Gold Console

About the console	55
Organizing Devices, Device Groups, and Maps with drag-and-drop	57
About the Device View	58
About device icons	58
About the Map View	59
Organizing device layout and views	59
Adding annotations to a map.....	60
About link lines	61
Using attached lines.....	62

CHAPTER 6 Using the WhatsUp Gold Web Interface

Accessing the web interface.....	63
About the WhatsUp Gold web interface	64
About the GO menu	64
About the Home tab	65
About the Devices tab.....	65
About the Reports tab	67

CHAPTER 7 About Users

About user accounts.....	69
Creating and modifying user accounts	70
About user rights	72
About group access rights.....	74
Enabling group access rights	76
Assigning group access rights.....	76
Propagating group access rights to subgroups.....	77
Determining the highest right	78
Understanding group access rights and user access right	78
About group access rights and users' home groups.....	78
About group access rights and dynamic device groups.....	79

CHAPTER 8 Managing Devices

Device overview	81
About the Device View	82
Learning about the Device Properties	83
About General Device Properties	83
About Device Property Performance Monitors	84
About Active Monitor Device Properties	85
About Passive Monitor Device Properties	86
About Device Property Actions	87
About Device Property Credentials	88
About Device Property Polling	89
About Device Property Notes	90
About Device Property Menus	90
About Device Property Custom Links	92
About Device Property Attributes	93
Adding a new device	94
Adding additional network interfaces to a device	94
Adding attributes to a device	96
Adding notes to a device	96
Changing a device IP address	97
Changing a device name	97
Selecting Device Types	98
Configuring Device Types	99
Changing Device Types	100
Using Acknowledgements	100
Editing multiple devices with Bulk Field Change	101
Using Credentials	103
Creating Custom Context menus	103

CHAPTER 9 Using Device Groups

About device groups	105
Creating device groups	106
About Dynamic Groups	107
Dynamic Group Examples	109
Building Dynamic Groups	114

CHAPTER 10 About Polling

Polling overview.....	115
Changing how you poll devices.....	115
Using Maintenance mode.....	116
Setting how often your devices are polled.....	116
Stopping and starting polling.....	116
Stopping and starting polling on a monitor.....	117
Dependencies overview.....	117
Reading dependencies.....	117
Setting Dependencies.....	119
Viewing Dependencies.....	123
IPX support.....	123

CHAPTER 11 Using Actions

About actions.....	125
About action strategies.....	126
About the Action Library.....	127
About Web Alarms.....	128
Configuring an action.....	130
Creating a Beeper Action.....	130
Creating a Pager Action.....	132
Creating an Email Action.....	134
Creating an SMS Action.....	135
Creating an SMS Direct Action.....	137
Creating a WinPopup Action.....	139
Creating a Syslog Action.....	140
Creating a Text-to-Speech Action.....	141
Creating a Program Action.....	142
Creating an Active Script Action.....	143
Creating a Web Alarm Action.....	144
Creating a Service Restart Action.....	145
Testing an action.....	147
Deleting an action.....	147
Assigning an action to a device.....	147
Creating a Blackout Period.....	148
Percent Variables.....	148
About action policies.....	152
Creating an action policy.....	152

Editing Action Policies	153
Implicit Action Policy	153
Example: getting an Email alert when the Web server fails.....	154

CHAPTER 12 Using Active Monitors

Active monitors overview.....	157
About the Active Monitor Library	158
Supported Active Monitors	159
Assigning active monitors	160
Assigning an action to a monitor.....	161
Deleting active monitors.....	163
Group and Device active monitor reports.....	164
Example: monitoring network printer toner levels	164
Expression Editor	165
Script Syntax	165
Script Syntax: Expect=Keyword	166
Script Syntax: Flow Control Keywords.....	167
Script Syntax: Send=Keyword.....	167
Script Syntax: SimpleExpect Keyword	168
Send to disconnect examples.....	170
Regular Expression syntax	170
Text string example	172
Using Telnet to determine "Expect on Connect" string	173
Using the Active Script Monitor	173
Using the Active Script Monitor context object.....	174
Examples: Active Script Monitor context code.....	177
Using premium monitors.....	187
Monitoring a Microsoft Exchange Server	187
Monitoring Microsoft SQL Server	191
Monitoring WMI-enabled applications	196
Monitoring Mail Servers.....	199

CHAPTER 13 Using Passive Monitors

About Passive Monitors.....	205
Assigning passive monitors	206
Configuring Passive Monitor Listeners	207
About the Passive Monitor Library	209
Group and device passive monitor reports.....	210
Receiving SNMP Traps	210

CHAPTER 14 Using Performance Monitors

Performance Monitor overview.....	213
About the Performance Monitor Library.....	214
Configuring and enabling Performance Monitors	215
Enabling SNMP on Windows devices	218
Adding monitors to the Performance Monitor Library	218
About performance reporting	223
Example: monitoring router bandwidth.....	226
Example: troubleshooting a slow network connection	227
Scenario:	227

CHAPTER 15 Monitoring Performance Data in Real Time

About Real-Time Data features.....	229
Using InstantInfo popups	230
Disabling InstantInfo popups	230
Using Network Tools to view real-time data.....	231
About the Web Task Manager	231
About the Web Performance Monitor.....	232
Using Split Second Graph Workspace Reports	233
Using the Performance Monitor workspace report	233
Viewing Real-time Data in Full Reports	234

CHAPTER 16 Using Active Discovery

About Active Discovery	237
Configuring Active Discovery.....	238
Example: configuring Active Discovery.....	238
Enabling and disabling an Active Discovery task.....	240
Testing Active Discovery tasks.....	241

CHAPTER 17 Using Maps

Using the Map View	243
About the Map View	244
Using map display options.....	245
Using Arrange options.....	246
Organizing devices.....	247
Using device types	247
Using grid properties.....	247
Grouping objects	248

Using the lock position	248
Mapping fonts.....	248
Organizing devices.....	248
Using link lines	249
Using attached lines.....	250
Connecting links.....	251
About unconnected links.....	251
Showing unconnected links.....	251
Creating connected link lines	252

CHAPTER 18 Using the Program Options

Changing the date and time format	253
Changing how long report data is stored.....	254
Changing the device state colors or icons.....	255
Changing clock/regional preferences.....	256

CHAPTER 19 Using Full Reports

Learning about full reports	257
Advantages of full Reports.....	258
About System Reports.....	259
About Group Reports.....	259
About Device Reports.....	260
List of full reports	260
About report refresh intervals.....	263
Printing, exporting, and saving full reports.....	264
Report column sizing and sorting	265
Changing the report date range	265
Adding report to your list of favorites.....	266
Using Recurring Reports	267
Configuring Recurring Reports	267
Testing Recurring Reports.....	268

CHAPTER 20 Understanding and Using Workspaces

Learning about workspaces.....	269
About types of workspaces.....	270
About the Home Workspace.....	270
About the Device Status workspace	271
About the Top 10 workspace.....	273

Managing Workspace Views.....	275
Navigating through workspace views	278
About workspace content	278
Adding workspace reports to a workspace view	279

CHAPTER 21 Using Workspace Reports

Learning about workspace reports	283
List of workspace reports.....	285
About the workspace report menu.....	297
Configuring a workspace report	298
Moving Workspace Reports within a workspace view.....	299
Device Group Mini Status workspace report	300

CHAPTER 22 Using SNMP Features

SNMP overview.....	303
Monitoring an SNMP Service.....	304
About the SNMP Agent or Manager	304
About the SNMP Management Information Base (MIB)	304
About SNMP Object Names and Identifiers	305
Using the SNMP MIB Manager	305
Using the SNMP MIB Manager to troubleshoot MIB files.....	306
About the SNMP operations.....	308
Using a custom name for SNMP device interfaces	309
Configuring a custom name (ifAlias) for an SNMP device interface	309
About SNMP Security	312
Using the Trap Definition Import Tool	312

CHAPTER 23 Using Network Tools

About Network Tools	315
Using the Ping tool.....	316
Using the Traceroute tool.....	317
Using the Lookup tool	318
Using the Telnet tool.....	319
Using the SNMP MIB Walker	319
Using the SNMP MIB Explorer	322
Using the MAC Address Tool	323
Using the Diagnostic Tool	325
Using the Web Performance Monitor	325

Using the Web Task Manager.....	328
Using the Web Task Manager - Process tab.....	329
Using the Web Task Manager - Performance tab	332
Using the Web Task Manager - Interfaces tab	335

Appendix A Using WhatsUp Gold Distributed and MSP Editions

About the WhatsUp Gold Distributed and MSP Edition.....	337
About the Distributed and MSP Edition reporting capabilities.....	338
Installing Central and Remote Sites	338
Step 1: Installing the WhatsUp Gold Central Site	340
Step 2: Configuring the firewall for Remote Site connections.....	343
Step 3: Installing the WhatsUp Gold Remote Site	343
Step 4: Using Reports for WhatsUp Gold Distributed and MSP Edition	347
Advantages of full Reports.....	359
Step 5: Using the Ipswitch Dashboard Screen Manager application	360
Creating and modifying user accounts	362
Learning more about using the WhatsUp distributed solution	364

Appendix B Troubleshooting

Troubleshooting your network.....	367
Database Performance Tool	368
Task Tray Application fails on Windows Vista.....	369
Connecting to a Remote Desktop	369
WhatsUp Gold engine message	369
Troubleshooting SNMP and WMI connections.....	370
False negative returned from WMI monitors.....	371
Re-enabling the Telnet protocol handler.....	371
Passive Monitor payload limitation.....	372
Restarting the WhatsUp Gold services from the command line	372
Recommended SMS modems and troubleshooting tips.....	373

Appendix C About the Dashboard Screen Manager

Ipswitch Dashboard Screen Manager overview	375
How does the Dashboard Screen Manager work?	376
What is a Dashboard playlist?	376
Installing the Dashboard Screen Manager	376
Opening the Dashboard Screen Manager	377
Configuring a Dashboard Screen Manager playlist.....	378

Appendix D Using the SNMP API

CoreAsp.Snmprqst 381
CoreAsp.ComResult 384
CoreAsp.ComSnmprResponse 384
Example scripts using the SNMP API 385

WhatsUp Gold Overview

In This Chapter

Welcome to Ipswitch WhatsUp Gold v12	1
WhatsUp Gold editions	4
What's new in WhatsUp Gold v12	5
Finding more information.....	8
Sending feedback.....	9

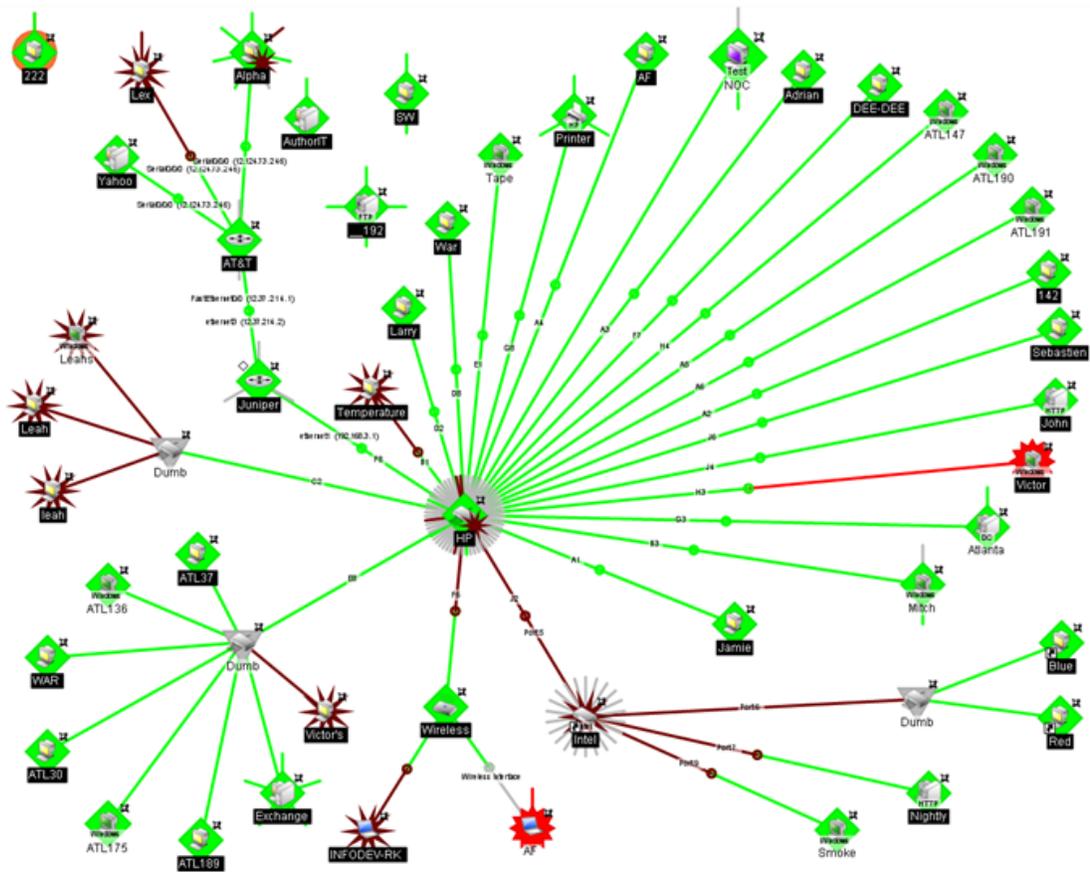
Welcome to Ipswitch WhatsUp Gold v12

Welcome to Ipswitch WhatsUp Gold v12, 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 wizard-based discovery process searches for devices on your network and lets you decide which devices to monitor. You can view monitored devices as a list of devices or as a graphical map.



Polling/Listening

WhatsUp Gold actively polls devices to determine their statuses. You can use pre-configured active monitors, or create your own, to poll services on a device and to 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, or the types of messages received, WhatsUp Gold fires actions to notify you of any change on your network. Actions help with problem resolution through options such as alerting via email or cell phone, or restarting a service.

Reporting and Workspaces

Reports ensure 360° visibility into current status, performance, and historical data for devices and monitors. Workspaces let you focus on segments of the network and create your own views into the report data. These views provide crucial network data in one location, which allows for quick and easy access. WhatsUp Gold offers more than 100 summary reports, or *workspace reports*, that can be used to customize workspaces. Each user can have their own customized workspace views.



WhatsUp Gold Interfaces

WhatsUp Gold offers two user interfaces, the Windows console interface and the web interface, which offer similar functionality. We recommend that you do the initial set up—discovery and mapping—on the console, then use the web interface for additional setup of monitors and workspaces, users and permissions, and for day-to-day monitoring.

- **Windows console interface.** The WhatsUp Gold 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.

WhatsUp Gold editions

WhatsUp Gold is available in four editions. Each edition tailors the features of WhatsUp Gold to meet the diverse needs of WhatsUp Gold users, from small networks to those spanning multiple geographic locations.

- **WhatsUp Gold Standard Edition** provides core network management features.
- **WhatsUp Gold Premium Edition** provides all of the network monitoring capabilities of WhatsUp Gold Standard Edition, plus advanced monitoring for Microsoft® Exchange™, Microsoft® SQL Server™, and SMTP email servers. Premium Edition also includes several features that let you monitor performance data in real time, as well as support for application monitoring using Microsoft's WMI™.
- **WhatsUp Gold MSP Edition** gives managed solution providers the ability to use all of the features of WhatsUp Gold Premium Edition to monitor their customers' remote networks from a central location in the managed solution provider's network operations center. Managing multiple companies' networks at once has never been easier.
- **WhatsUp Gold Distributed Edition** extends the features of WhatsUp Gold Premium Edition to companies whose networks are segmented across multiple geographic locations. WhatsUp Gold Distributed Edition can detect issues at any of the company's sites and can then report the issue to the effected site and to a central location.

Each edition includes a different set of features. The table below shows which features are available in each edition. If a feature is not shown in the table, it is available in all editions.

	Standard Edition	Premium Edition	MSP Edition	Distributed Edition
Application Management				
Monitor Microsoft Exchange		●	●	●
Monitor SQL Server		●	●	●
Monitor applications via WMI		●	●	●
Monitor Email servers		●	●	●
Real-time Monitoring				
View real-time data about devices in reports		●	●	●
Quickly access real-time data via InstantInfo popups		●	●	●
Monitor performance data with the Web Performance Monitor		●	●	●

	Standard Edition	Premium Edition	MSP Edition	Distributed Edition
View real-time information about tasks running on a device using the Web Task Manager		●	●	●
Distributed Monitoring				
Monitor devices on networks segmented across multiple geographic locations			●	●
View report data from multiple remote sites from one central location			●	●

What's new in WhatsUp Gold v12

Ipswitch WhatsUp Gold v12 introduces a number of new features and enhancements that help you manage your network more efficiently than ever. One of the major features, Split Second Graphics (SSG), adds real-time graphs to provide instant feedback about network device performance. This SSG feature, coupled with the existing WhatsUp Gold performance reporting, provides a new level of network device performance intelligence to the already powerful historical performance data reporting capabilities in WhatsUp Gold.

New in WhatsUp Gold Standard, Premium, Distributed, and MSP Editions

- **High Capacity SNMP interfaces** - added support for high capacity SNMP interface counters through the Interface Performance Monitor.
- **NetSNMP MIB** - Unix performance monitoring with NetSNMP agents.
- **Custom names for SNMP interfaces** - SNMP interfaces can be configured with unique identifiers.
- **Cisco MIB support** - includes support for over 200 Cisco MIBs for monitoring Cisco equipment and services.
- **SNMP MIB Walker** - new web-based network tool allows you to browse for SNMP objects that a device supports.
- **SNMP MIB Explorer** - new web-based network tool allows you to browse for SNMP objects defined in MIB files.
- **SNMP MIB Manager** - new web-based network tool for the import and validation of MIB files.
- **Improved SNMP API** - supports enhanced scripting capabilities with both Script Action and Active Script Monitor.
- **Email Actions** - now supports SMTP authentication.
- **SMS Direct** - extended Short Message Service (SMS) support for SMS Direct.
- **Drag-and-Drop Management** - enhanced drag-and-drop capability to include device, group, and map management on the web interface.

- **Upgraded Database Engine** - MSDE 2000 database has been upgraded to Microsoft SQL Server 2005 Express.
- **Passive Monitors** - have been enhanced to use device credentials stored in the Credentials Library.
- **Windows Vista support** - Windows Vista Ultimate or Windows Vista Business (Windows Vista SP1 recommended) both as a WMI monitored OS and as monitoring workstation.
- **New licensing technology** - requires users to enter a serial number to activate all of the WhatsUp Gold products.

New in WhatsUp Gold Premium, Distributed, and MSP Editions

- **InstantInfo** - provides instantaneous access to real-time performance data in enabled reports.
- **Split Second Graphs** - provides real-time graphical data in performance workspace and full reports, the Web Task Manager, and the Web Performance Monitor.
- **Web Performance Monitor** - new web-based network tool that provides insight into processes running on a device or system.
- **Web Task Manager** - new web-based network tool that provides network device overview information about processes that use SNMP or WMI device connections.
- **Email Monitor** - innovative monitor that uses SNMP, POP3, or IMAP by sending emails to servers, with support for encryption and SMTP authentication.
- **Dashboard Screen Manager** - a stand-alone application designed to display a series of Web pages, or a "playlist," on one or multiple monitors.

Learning about the WhatsUp Gold new application features

The matrix below highlights new features that are available in each edition of WhatsUp Gold v12:

New WhatsUp Gold v12 Features	Standard Edition	Premium Edition	MSP Edition	Distributed Edition
SSG (Real-time data)				
Support for instant access to real-time data via InstantInfo popups		●	●	●
Web Performance Monitor network tool which creates Split Second Graphs for use in the Performance Monitor workspace report		●	●	●
Web Task Manager troubleshooting network tool		●	●	●
Support for Split Second Graphs that provide real-time graphical data in performance workspace and full reports, the Web Task Manager, and the Web Performance Monitor		●	●	●

SNMP				
Support for high capacity SNMP interface counters through the Interface Performance Monitor	●	●	●	●
Support for NetSNMP agents for UNIX CPU utilization	●	●	●	●
Support for configurable interface name for SNMP interfaces	●	●	●	●
Includes select Cisco MIBs for use in WhatsUp Gold	●	●	●	●
SNMP MIB Walker network tool which allows you to browse for SNMP objects on a device	●	●	●	●
SNMP MIB File Explorer network tool which allows you to browse for SNMP objects in defined MIB files	●	●	●	●
SNMP MIB Manager network tool which allows you to import and validate MIB files	●	●	●	●
Includes SNMP COM API improvements for enhanced scripting capabilities with the Script Action and Active Script Monitor	●	●	●	●
Email				
Email Monitor with support for encryption and SMTP authentication		●	●	●
Support for SMTP authentication for email actions	●	●	●	●
SMS				
Extended Short Message Service (SMS) support for SMS Direct	●	●	●	●
Drag-and-Drop				
Added support for drag-and-drop device, group, and map management on the web interface	●	●	●	●

SQL Server 2005 Express Database				
Microsoft SQL Server 2005 Express Database	●	●	●	●
Passive Monitors				
Added support for Passive Monitors to use device credentials in the Credentials Library	●	●	●	●
Other Features				
Added the Dashboard application		●	●	●
Added support for Windows Vista	●	●	●	●
Added new licensing technology	●	●	●	●

Finding more information

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.asp>).

- **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.ipswitch.com/WUG120relnotes>).
- **Application Help for the console.** The console help contains 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**.
- **Application Help for the web interface.** The web interface help contains dialog assistance, how-to's that explain how to use features, table of contents, index, and search. Click the **?** icon to access the Help.
- **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.ipswitch.com/WUG120GSG>).
- **New Features Guide.** This guide provides information about the new features in Ipswitch WhatsUp Gold v12. This guide is available on the *WhatsUp Gold web site* (<http://www.ipswitch.com/wug120fbg>).

- **User Guide.** This guide describes how to use the application out-of-the-box. It is also useful if you want to read about the application before installing. To view or download the User Guide, select **Help > WhatsUp Gold User Guide** or download it from the *WhatsUp Gold web site* (<http://www.ipswitch.com/WUG120ug>).
- **WhatsUp Gold Distributed Edition Deployment Guide.** This guide provides instructions on how to plan and deploy the WhatsUp Gold Distributed Edition. This guide is available on the *WhatsUp Gold web site* (<http://www.ipswitch.com/WUG12dsdg>).
- **WhatsUp Gold MSP Edition Deployment Guide.** This guide provides instructions on how to plan and deploy the WhatsUp Gold MSP Edition. This guide is available on the *WhatsUp Gold web site* (<http://www.ipswitch.com/WUG12mspdg>).
- **Translation Guide.** This guide describes how to use the translation features to create a localized version of the WhatsUp Gold web interface. This guide is available on the *WhatsUp Gold web site* (<http://www.ipswitch.com/WUG12Trans>).
- **Licensing Information.** Licensing and support information is available on the *myipswitch.com web portal* (<http://www.myipswitch.com/>). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.
- **User Forum.** Use the online user group forums to interact with other WhatsUp Gold users to share helpful information about the application. The User Forums are available on the *WhatsUp Gold web site* (<http://forums.ipswitch.com/>).
- **Knowledge Base.** Search the Ipswitch Knowledge Base of technical support and customer service information. The knowledge base is available on the *WhatsUp Gold web site* (<http://support.ipswitch.com/kb/>).

Sending feedback

We value your opinions on our products and welcome your feedback.

To provide feedback on existing features, suggest new features or enhancements, or suggest ways to make our products easier to use, please fill out our *product feedback form* (<http://www.ipswitch.com/company/prodfeedback.asp>).

Gathering and Viewing Network Data

In This Chapter

Gathering network data.....	11
Viewing network data.....	12

Gathering network data

There are a few things you need to do before WhatsUp Gold can gather the data you need about the devices on your network.

1. Install the software

First, you need to install your edition of WhatsUp Gold. The User Guide gives step-by-step instructions on how to install each of the four editions of WhatsUp Gold:

- *WhatsUp Gold Standard Edition* (on page 15)
- *WhatsUp Gold Premium Edition* (on page 15)
- *WhatsUp Gold MSP Edition* (on page 338)
- *WhatsUp Gold Distributed Edition* (on page 338)

2. Discover devices

After you have installed WhatsUp Gold, you need to discover devices on your network for the application to monitor. The Device Discovery Wizard allows to choose which devices to add to the database for monitoring.

3. Configure your network

In WhatsUp Gold, devices are organized through device groups. By default, all of the devices on your network are placed into a Dynamic Group named **All devices**. Additionally, each time you discover devices a new device group is created containing the devices found in the scan that you choose to monitor. You can create as many Dynamic and non-Dynamic groups as you want to organize your network in a way that is meaningful to you and your monitoring needs.

4. Configure monitors

WhatsUp Gold comes with several default monitors, but you will need to configure new monitors to gather the specific types of information you seek about your network. There are three types of monitors in WhatsUp Gold:

- *Active monitors* (on page 157)
- *Passive monitors* (on page 205)
- *Performance monitors* (on page 213)

Each of the monitor types gathers a different type of information, so you may use each type of monitor. Before creating monitors, you should figure out what type of network information you need, and configure monitors to gather that specific data.

Viewing network data

After you have configured your network and the appropriate monitors, you can begin viewing the information WhatsUp Gold is gathering for you. There are several ways to view network data with WhatsUp Gold.

1. Device and Map Views

While Device and Map Views are good for viewing device information or the location of a device, they are also useful for viewing the current status of network devices. Devices on both are displayed with device state icons that show the status for devices at the time of the last poll. The Device and Map Views are viewable on both the WhatsUp Gold console and web interface.

2. Workspace views and reports

WhatsUp Gold's workspace views let you organize various workspace reports by the type of information they display or by devices and device groups. Workspace views and reports are viewable from the WhatsUp Gold web interface.

3. Full reports

In WhatsUp Gold, reports are used to troubleshoot and monitor performance and historical data that has been collected during the operation of the application. Reports are viewed from the WhatsUp Gold Reports tab and can be sent on a regular basis to an email address you identify through the Recurring Report feature.

Installing and Configuring WhatsUp Gold

In This Chapter

Installation overview	13
System requirements	14
Installation notes	15
Installing or upgrading	15
Activating WhatsUp Gold for new or upgraded licenses	18
About the Task Tray icon	18
Configuring the database	19
Configuring the web server	33
Uninstalling Ipswitch WhatsUp Gold v12	41

Installation overview

Installing Ipswitch WhatsUp Gold v12 or WhatsUp Gold Premium Edition v12 is straightforward, though the Release Notes are required reading due to possible Service Pack and database issues.

The path you take to a successful installation may differ, depending on the following:

First-time install

If you are installing Ipswitch WhatsUp Gold v12 or WhatsUp Gold Premium Edition v12 for the first time, the installation program does the following with no actions required of you.

- Installs the database server: Microsoft SQL Server 2005 Express (SSE).
- Creates a WhatsUp database in the SSE instance.
- Creates a system Data Source Name (DSN), which tells WhatsUp Gold where to find the WhatsUp database.
- Installs the WhatsUp Gold Edition application.

Read the System requirements, then follow the steps in Installing or upgrading.

Upgrade Notes

If you are upgrading from a previous version of WhatsUp Gold, the installation program detects an existing WhatsUp database and configures the new version to use that database, provided the following conditions are met:

- SQL Server 2005 Express is installed on the computer on which you are installing WhatsUp Gold.
- The WhatsUp database exists on the database server.
- A DSN is configured for the WhatsUp database.

If these conditions are not met, the installation program will notify you and direct you to perform a manual upgrade of the database.

Read the System requirements, then follow the steps in Installing or upgrading. If necessary, configure the database manually. For more information, see *Upgrading the database schema* (on page 20).

If you have an alternative database setup, after completing the WhatsUp Gold installation, you'll need to upgrade the WhatsUp database. For more information, see *Using an alternative database setup* (on page 26).

Custom Database

Though we recommend that you use the default database (SQL Server 2005 Express), if you need to either use another database, or you need to run the database on another computer, you can set it up manually after the WhatsUp Gold or WhatsUp Gold Premium Edition installation has completed. For more information, see *Using an alternative database setup* (on page 26).

System requirements

Minimum software requirements

- Windows XP Professional SP2 (or later), Windows 2003 Server SP1 (or later), Windows Vista Ultimate, or Windows Vista Business (Windows Vista SP1 recommended).
- Microsoft Internet Explorer 6.0 SP1 (or later) or Firefox 2.0 (or later)
- Microsoft .NET Framework v 2.0 or 2.0 SP1
- Microsoft Windows Scripting Host v5.6 or later

Windows Scripting Host is installed with the Windows operating system. To verify your version, run `cscript.exe` at a command prompt.

If you need to update Windows Scripting Host, refer to the *Microsoft Windows Scripting Host site* (<http://www.ipswitch.com/wsh56>).

- Internet connectivity for activation, connecting Central and Remote Sites, and running the web interface.

Minimum hardware requirements

- Intel Pentium-compatible 2 GHz or faster
- 1 GB memory (RAM) (2 GB RAM recommended)
- 256 MB of drive space (up to 4 GB additional for SQL Server 2005 Express Edition database and 7200 RPM drive recommended)
- Display resolution support for 1024 x 768 minimum; recommended display resolution is 1280 x 1024.
- CD-ROM drive
- Network Interface Card (NIC)
- Modem and phone line (for pager, SMS, or beeper actions; modem pooling is not supported)
- GSM modem and active SIM card (for SMS Direct actions)
- SAPI v5.1 and supporting sound card for Text to Speech Actions; SAPI v5.1 can be downloaded from the *Microsoft Speech site* (<http://www.microsoft.com/speech/speech2007/default.mspx>).

Microsoft SQL Server 2005 Express Edition (SSEE) requirements

- SSEE supports up to 4 GB database size and up to 1 GB RAM for the buffer pool. Ensure sufficient disk capacity is available for data storage.



Note: SSEE supports one CPU. In computers with multiple CPUs, SSEE utilizes only one processor.

Installation notes

Read the Release Notes for information about potential installation issues, such as the following:

- Windows XP (SP2) Errors. This Service Pack enables firewall settings that can interfere with Microsoft SQL Server's ability to listen on the network.

Installing or upgrading

The installation program is similar whether you are installing WhatsUp Gold for the first time or upgrading a previous installation. Steps that apply only to a first-time installation, or only to an upgrade, are identified as such.



Note: These installation instructions are intended for WhatsUp Gold Standard Edition and WhatsUp Gold Premium Edition. For installation instructions for WhatsUp Gold Distributed Edition, see the *WhatsUp Gold Distributed Edition Deployment Guide* (<http://www.ipswitch.com/WUG12dsdg>). For installation instructions for WhatsUp Gold MSP Edition, see the *WhatsUp Gold MSP Edition Deployment Guide* (<http://www.ipswitch.com/WUG12mspdg>).

To install or upgrade WhatsUp Gold:

- 1 Log in directly to Microsoft Windows using the Administrator account (or, if you do not have an account called Administrator, use an account that has full administrative privileges to the computer). Do not use Terminal Services or Remote Desktop to install WhatsUp Gold.



Note: When installing on Windows Vista, additional steps are necessary for the Task Tray application to work properly. For more information, see *Task Tray Application fails on Windows Vista* (on page 368).

- 2 Start the installation program:
 - If you purchased a WhatsUp Gold CD-ROM, insert the CD-ROM into the appropriate drive. If it does not run automatically, click **Start**, select **Run**, then enter the CD path followed by `AutoRun.exe`. For example: `D:\AutoRun.exe`
 - If you downloaded WhatsUp Gold Standard Edition or WhatsUp Gold Premium Edition from our Web site, run the downloaded installation application.
- 3 Read the Welcome screen.

The Welcome screen recommends that you disable any running antivirus software, estimates how long it takes to install the application, and displays a button that, when clicked, displays the release notes.

Click **Next** to continue. The License Agreement dialog opens.
- 4 Read the license agreement. Select the appropriate option, then click **Next**.
- 5 **For first-time installation only:** Select the install directories for SQL Server 2005 Express Edition. The application and data files will be installed in default directories. If you want to change the locations, click the browse buttons to find and select a different directory.



Note: If you want to customize your database setup, you need to first complete the installation using Microsoft SQL Server 2005 Express Edition. After installation completes, you can manually configure your database as described in *Using alternative database setups* (on page 26).



Important: Make sure that you have a large capacity drive selected for data storage. Data files can grow up to 4 GB.

The application and data files will be installed in default directories. If you want to change the locations, click the browse buttons to find and select a different directory.

Click **Next**.



Note: The SQL Server 2005 Express Edition installation may take several minutes.

- 6 For new installation only:** Select the installation directory for the WhatsUp Gold application files.

The default path is C:\Program Files\Ipswitch\WhatsUp. We recommend that you use the default path. Some users prefer to put application files on a partition separate from the operating system, which is usually installed on the C: drive, to isolate the application from an operating system crash.

- 7 For upgrade installation only:** Choose whether to backup your current WhatsUp Gold database. We strongly suggest that you do this.
- 8 For upgrade installation only:** Choose how to handle existing Web and Report files.
If you have previously installed WhatsUp Gold, you may already have Web and Report files stored in your installation directory. You can choose to either delete them or back them up during the install. Backup is recommended.
- 9** If a sound card is installed and it has SAPI-compatible drivers, the install program asks whether you want to install Text to Speech capabilities. If you select **No**, you can always return and install Text to Speech at a later date.
- 10 For new installation only:** Choose whether to enable the web server during install and enter a port for this installation. The default port is Port 80.



Note: This dialog will not be displayed during an upgrade if you have already enabled the WhatsUp web server in an older version of WhatsUp.

- 11** Click **Install** to install the WhatsUp Gold application files. The installation program gives you the option to go back and change options or cancel prior to completing the installation.



Important: When you use an alternative database setup, you will need to run the database upgrade scripts when installing a new release of WhatsUp Gold. The installation program will warn you if it detects a non-default database. For information on running the upgrade scripts, see *Upgrading the database schema* (on page 20).

- 12** Make your selections, then click **Finish**.

After the application starts, the Discover Devices wizard appears. This wizard is used to set options on how to discover your network. Follow the wizard dialogs or if you choose to postpone these steps, click the **Cancel**.

Activating WhatsUp Gold for new or upgraded licenses

If WhatsUp Gold is installed using the installation application downloaded from the Web link provided in the purchase confirmation email, the program is fully functional immediately after installation.

If the WhatsUp Gold v12 license is not automatically activated during the installation or if you are upgrading from a previous WhatsUp Gold version, you can manually activate WhatsUp Gold using the activation program in the WhatsUp Gold group of the Windows Start menu.



Important: Make sure that you activate WhatsUp Gold before starting the application. The WhatsUp Gold polling engine will be turned off and a message tells you that the license has expired. The application is not functional until after it has been activated.

To activate WhatsUp Gold manually:



Note: Before you start the manual activation process, make sure that you have your product serial number available to use in the activation program.

- 1 Click **Start > Programs > Ipswitch WhatsUp Gold > Manage WhatsUp Gold License**. The activation program appears.
- or -
If you run the WhatsUp Gold console at the end of the installation, it displays an Invalid License dialog. Click the **Purchase/Unlock** to start the license activation process.
- 2 Follow the onscreen instructions to complete the product activation.



Note: When the activation is complete, a confirmation page indicates the license has been activated. If the activation does not complete successfully, you may be behind a proxy or firewall that is blocking the activation request. In this case, click the **Offline** button, then follow the onscreen instructions.

For more help and information about licensing, go to the *Ipswitch licensing portal* (<http://www.myipswitch.com/>).

About the Task Tray icon

WhatsUp Gold installs a task bar icon on your computer. This icon is constantly running, and alerts you to the status of the application as a whole.

WhatsUp Gold Icons

During normal operation, the WhatsUp Gold icon displays the worst state of all devices on your map. In addition, you can enable tooltips to have the icon display any state change that occurs on the system. To do this, right-click on the icon and select or clear **Enable Tooltips**.



When the WhatsUp Gold polling engine is not running (the service is stopped) this icon appears:



If this is the case, you need to restart the Ipswitch WhatsUp Gold Engine service. If the polling engine is not running, then WhatsUp Gold is not connected to the database, and nothing in the application will function properly.

To turn off the Task Tray Application and icon, right-click on the icon and select **Close Task Tray Application**.

Configuring the database

WhatsUp Gold requires a database to store information about the devices it monitors. By default, WhatsUp Gold installs and configures SQL Server 2005 Express Edition to use as its data store. WhatsUp Gold also supports using Microsoft SQL Server 2005 installed either on the same computer as WhatsUp Gold or on a separate computer.

If you want to use SQL Server 2005 installation to host the WhatsUp Gold database, you must complete the WhatsUp Gold installation and then migrate the WhatsUp database to your SQL instance.

About the SQL Server 2005 Express Database

The WhatsUp Gold installation program installs the SQL Server Express Edition (SSEE) database server and configures the WhatsUp database. SSEE provides several benefits over Microsoft SQL Desktop Engine (MSDE 2000), which was used by previous versions of WhatsUp Gold.

SSEE provides the following benefits over MSDE 2000:

- Doubles database size limit from 2 GB to 4 GB.
- Removes workload governor, greatly improving database performance.
- Supports Microsoft Windows Vista.
- Support for SQL Server 2005 as a database.

For more information, see the *Microsoft SQL Server Express Web site* (<http://www.microsoft.com/sql/editions/express/default.mspx>).

Upgrading the database engine

New features in Ipswitch WhatsUp Gold v12 mandate an update of the original database engine from Microsoft SQL Server 2000 Desktop Engine to SQL Server 2005 Express Edition. The WhatsUp Gold installation program will automatically upgrade the database engine, provided the database is in the default configuration. A default configuration is one that meets the following conditions:

- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) is installed on the same computer on which you are installing WhatsUp Gold.
- The instance name for the MSDE 2000 installation is `WhatsUp`.
- A `WhatsUp` database instance exists in this MSDE 2000 instance.
- A DSN named `WhatsUp` is configured to point to the WhatsUp database in this MSDE 2000 instance.

All other configurations are considered non-default configurations. The WhatsUp Gold installation program will notify you, during the installation, if you have a non-default configuration. This will necessitate a manual upgrade of the database schema before the WhatsUp Gold application will function correctly. If you prefer, you may also upgrade your database engine to SQL Server 2005 before upgrading the database schema.



Warning: An SQL Server 2005 Express Edition database cannot be imported to Microsoft SQL Server 2000. You may continue to use Microsoft SQL Server 2000 as your database engine, but only if you were already using it before upgrading to WhatsUp Gold v12. Beginning with WhatsUp Gold v12, users that want to move from the SQL Server 2005 Express Edition Database Engine must migrate to Microsoft SQL Server 2005. For more information, see *Using an alternative database setup* (on page 26).

Upgrading the database schema

Changes to the WhatsUp Gold v12 application require the database schema to be upgraded. If you are running a default database configuration, the WhatsUp Gold v12 upgrade automatically upgrades your database schema for you. If not, you must manually upgrade your database schema after installing WhatsUp Gold v12 before you can use the application.

You must first complete the WhatsUp Gold installation, then upgrade the database schema. This section steps through how to upgrade the database schema for an installation of WhatsUp Gold that is a non-default configuration.

To upgrade the database from WhatsUp Gold v11.x or WhatsUp Professional 2006:

- 1 Make a backup of your WhatsUp database.



Warning: Ipswitch Technical Support may not be able to recover your network data from a database which has failed an upgrade attempt. It is imperative to make a backup copy of the database, in case any portion of the database schema upgrade encounters a problem.

- 2 Copy the `<WUG_Install_Folder>\DB Scripts` folder to the computer running the SQL Server that hosts the WhatsUp database.



Important: You must copy the entire DB Scripts folder to the computer running the SQL Server. This includes any files and sub-directories it may contain.

- 3 Make note of the fully qualified path to the DB Scripts directory, it may be required in the steps that follow.
- 4 Run the upgrade scripts, either by running the Visual Basic (VB) script which automatically runs each script in sequence or by running each script individually using the SQL Management tools.



Warning: The upgrade scripts should be run only once. If an upgrade script is interrupted or errors occur, you must restore your database before running the scripts a second time.



Important: Before running the scripts, close the WhatsUp Gold application; then, stop the Ipswitch WhatsUp Engine and the Ipswitch Web Server service, for more information see *Stopping and starting the Ipswitch WhatsUp Engine* and *Stopping and starting the internal web server in the Help*. If you are running IIS as your web server, stop IIS, then restart it.

To upgrade the database automatically using the VB Script:

- 1 On the computer on which the SQL server hosting the WhatsUp database is installed, open the command prompt window, then go to the location where you copied the <WUG_Install_Folder>\DB Scripts directory. Navigate to the Upgrade Scripts directory inside it.



Warning: The VB script must be executed locally on the SQL Server. If SQL Server is installed on another computer, attempting to run the VB script from the WhatsUp computer will cause the database upgrade to fail.



Note: If running the VB script on a Windows Vista computer, be sure to run the command prompt with administrative privileges. For more information, see the *Microsoft Command Prompt FAQ article* (<http://windowshelp.microsoft.com/Windows/en-US/help/81242f3c-c9bf-442c-a49d-e18b02f72e691033.mspx>).

- 2 Execute the VB script using the following case-sensitive command:
`cscript upgrade_db.vbs -S "<sql_server_name>" -d "WhatsUp"`
Replace <sql_server_name> with the machine name or machine name and database instance name.

For example:

If you have a default instance of SQL installed on a computer named SQLBOX:

```
cscript upgrade_db.vbs -S "SQLBOX" -d "WhatsUp"
```

If you have a named instance of SQL installed on a computer named SQLSYSTEM and the instance name is WUG:

```
cscript upgrade_db.vbs -S "SQLSYSTEM\WUG" -d "WhatsUp"
```

For assistance in determining whether your SQL instance is a default or named instance, please contact your database administrator.



Note: Arguments are case-sensitive (-d is not the same as -D).



Tip: Optional: If you prefer to use SQL authentication to execute the VB script, you can use the `-U` and `-P` switches to provide an SQL user and that user's password.

```
cscript upgrade_db.vbs -S "<sql_server_name>" -d "WhatsUp" -U  
<sql_user_name>" -P "<sql_password>"
```

Replace `<sql_user_name>` with the SQL username and `<sql_password>` with that user's password.

For example:

```
cscript upgrade_db.vbs -S "SQLSERVER" -d "WhatsUp" -U "sa" -P  
"WhatsUp_Gold"
```

The VB script will execute the appropriate upgrade scripts, based on the existing WhatsUp Gold database schema. As each upgrade script is executed, a log file is created in the `DB Scripts\Upgrade Scripts` directory. If errors occur during the execution of an upgrade script, the corresponding log file for the script will be displayed in a Notepad window.

- 3 After the database upgrade is complete, start the Ipswitch services (**Ipswitch Web Server\$WhatsUp** and **Ipswitch WhatsUp Engine**) and run the WhatsUp Gold application normally. If you are running IIS as your web server, stop IIS, then restart it.



Note: We recommend that you make a backup of your SQL database after the upgrade has completed. This will be useful for any disaster recovery mechanisms in place at your company.

To manually run the upgrade scripts:

The alternative to using the VB script is to manually execute the upgrade scripts using Query Analyzer (SQL 2000), SQL Management Studio (SQL 2005), or the SQL command-line utilities (`osql.exe` or `sqlcmd.exe`). If you need assistance using the management tools for SQL 2000 or SQL 2005, contact your database administrator or consult the online documentation for each tool.



Important: Be sure to run all of the queries, in the instructions below, against the WhatsUp database.

Using Query Analyzer (SQL 2000) and Management Studio (SQL 2005):

- 1 Determine your current database version by executing the following query against the WhatsUp database. The value returned should be a six digit number.

```
SELECT sValue FROM DatabaseProperty WHERE sName = N'Version'
```
- 2 Using a text-editor of your choice, open the `Transform.ini` file located in the `DB Scripts\Transforms` directory. In the `[VERSIONS]` section, locate the version that matches the version of your database.
For example, database version 110302 corresponds to transform version 39. Make a note of the transform version, which we will refer to as the "starting transform version."
- 3 Find the `[SCRIPTS]` section in `Transform.ini` file. Make note of all the Transform entries which appear **after** your starting transform version.

For example, if your starting transform version is 39, the first upgrade script you need to run is transform 40 (`upgrade_from_110302_to_120001.sql`) and the last is `FinalUpgradeScript.sql`.

- 4 Open each upgrade script needed to complete your schema upgrade in a text editor of your choice. Replace every occurrence of the `<DATAFILESPATH>` variable with the absolute path to the `DB Scripts` directory. Some scripts may have several `<DATAFILESPATH>` variables that need replacement, some scripts may have none.



Note: Be sure to exclude any trailing slashes from the directory path when replacing the text.

For example, in an upgrade script, we see the following text:

```
BULK INSERT WorkspaceReport FROM  
'<DATAFILESPATH>\WorkspaceReport.txt'
```

If we copied the `DB Scripts` directory to a `WUG` directory at the root of the `C` drive on the SQL Server, we would change it to the following:

```
BULK INSERT WorkspaceReport FROM 'C:\WUG\DB  
Scripts\WorkspaceReport.txt'
```



Important: The path you replace the `<DATAFILESPATH>` variable with must be local to the SQL Server hosting the WhatsUp database. It must be a directory on a local drive, not a network share or mapped drive. If you are running Query Analyzer Management Studio from another computer, be sure to use the path that would be "seen" by the SQL Server, not your remote computer.

- 5 Save each updated file.
- 6 Run each upgrade script using Query Analyzer or Management Studio. The script should be run in the order specified in `Transform.ini`. Check for any errors or warnings returned by the SQL tool before continuing to the next upgrade script. If any script should fail, restore your database backup and repeat any previously successful upgrade scripts before attempting to run the failing script again.



Warning: Do not stop the script upgrade process before it has completed. Stopping the process before it is complete will corrupt the database. The time to complete the upgrade process will vary. It is possible that it could take several hours, depending on the database size. A message will display at the end of the process to confirm that the database upgrade process is finished.

- 7 After the last upgrade script is complete, you may start the Ipswitch services (**Ipswitch Web Server\$WhatsUp** and **Ipswitch WhatsUp Engine**) and run the WhatsUp Gold application normally. If you are running IIS as your web server, stop IIS, then restart it.



Tip: Optional: We recommend making another backup of your SQL database once the upgrade has completed. This will be useful for any disaster recovery mechanisms in place at your organization.

Using the osql utility (SQL 2000) and the sqlcmd utility (SQL 2005):

An alternative to using the Query Analyzer or Management Studio tools is using the SQL command-line tools to execute the upgrade scripts. If your database is SQL 2000, use the *osql* utility. If you are running SQL 2005, you should use the *sqlcmd* utility. For more information, see the Microsoft web site for information about the *osql utility* ([http://msdn2.microsoft.com/en-us/library/aa214012\(SQL.80\).aspx](http://msdn2.microsoft.com/en-us/library/aa214012(SQL.80).aspx)) and the *sqlcmd utility* (<http://msdn2.microsoft.com/en-us/library/ms162773.aspx>).

Each utility needs connection and authentication information specific to your environment in order to connect to the WhatsUp database and issue queries and schema updates. Your specific connection and authentication information may vary from the examples below. Contact your database administrator for information about using these command-line utilities. These examples assume that that Windows user running the utility has administrative access to the DB, and that the SQL Server is a default instance on a computer named `SQLSYSTEM`.

- 1 Determine your current database version by executing the following case-sensitive query against the WhatsUp database. The value returned should be a six-digit number.

SQL 2000 (osql):

```
osql -E -S "SQLSYSTEM" -d "WhatsUp" -Q "SET NOCOUNT ON SELECT sValue
FROM DatabaseProperty WHERE sName = N'Version'"
```

SQL 2005 (sqlcmd):

```
sqlcmd -E -S "SQLSYSTEM" -d "WhatsUp" -Q "SET NOCOUNT ON SELECT
sValue FROM DatabaseProperty WHERE sName = N'Version'"
```



Note: Arguments are case-sensitive (-d is not the same as -D).

- 2 Using a text-editor of your choice, open the `Transform.ini` file located in the `DB Scripts\Transforms` directory. In the `[VERSIONS]` section, locate the version that matches the version of your database. For example, database version 110302 corresponds to transform version 39. Make a note of the transform version, which we will refer to as the "starting transform version."
- 3 Find the `[SCRIPTS]` section in `Transform.ini`. Make note of all the *Transform* entries which appear **after** your starting transform version. For example, if your starting transform version is 39, the first upgrade script you'll need to run is transform 40 (`upgrade_from_110302_to_120001.sql`) and the last is `FinalUpgradeScript.sql`.
- 4 Open each upgrade script needed to complete your schema upgrade in a text-editor of your choice. Replace every occurrence of the `<DATAFILESPATH>` variable with the absolute path to the `DB Scripts` directory. Some scripts may have several that need replacement, some may have none. Be sure to exclude any trailing slashes from the directory path when replacing the text.
For example, in an upgrade script, we see the below text:

```
BULK INSERT WorkspaceReport FROM
'<DATAFILESPATH>\WorkspaceReport.txt'
```

If we copied the `DB Scripts` directory to a `WUG` directory at the root of the `C` drive on the SQL Server, we would change it to the following:

```
BULK INSERT WorkspaceReport FROM 'C:\WUG\DB
Scripts\WorkspaceReport.txt '
```



Note: The path you replace <DATAFILES_PATH> variable with must be local to the SQL Server hosting the WhatsUp database. It must be a directory on a local drive, not a network share or mapped drive. If you are running the command-line tools from another computer, be sure to use the path that would be "seen" by the SQL Server, not your remote computer.

- 5 Save each updated file.
- 6 Run each upgrade script using the appropriate command-line tool. The script should be run in the order specified in `Transform.ini`. Check for any errors or warnings returned by the SQL tool before continuing to the next upgrade script. If any script fails, restore your database backup and repeat any previously successful upgrade scripts before attempting to run the failing script again.

SQL 2000 (osql):

```
osql -E -S "<sql_server_name>" -d "WhatsUp" -i
"<upgrade_script_name.sql>"
```

SQL 2005 (sqlcmd):

```
sqlcmd -E -S "<sql_server_name>" -d "WhatsUp" -i
"<upgrade_script_name.sql>"
```

For example:

SQL 2000 (osql):

```
osql -E -S "SQLSYSTEM" -d "WhatsUp" -i
"upgrade_from_110302_to_120001.sql"
```

SQL 2005 (sqlcmd):

```
sqlcmd -E -S "SQLSYSTEM" -d "WhatsUp" -i
"upgrade_from_110302_to_120001.sql"
```



Tip: Optional: You can specify to create a log file for each upgrade script using the `-o` switch and by specifying a filename. We recommend creating a separate log file for each upgrade script. For example:

```
sqlcmd -E -S "SQLSYSTEM" -d "WhatsUp" -i
"upgrade_from_110302_to_120001.sql" -o
"upgrade_from_110302_to_120001.log"
```

- 7 After the last upgrade script is complete, you may start the Ipswitch services (**Ipswitch Web Server\$WhatsUp** and **Ipswitch WhatsUp Engine**) and run the WhatsUp Gold application. If you are running IIS as your web server, stop IIS, then restart it.



Note: We recommend that you make a backup of your SQL database after the upgrade has completed. This will be useful for any disaster recovery mechanisms in place at your company.

Recovering from a "Version Mismatch" error

When starting the WhatsUp Gold application, you may see a "Version Mismatch" error if the program version does not match the database version. The WhatsUp Gold application can only use a database that is compatible with the version of the software currently installed. For example, WhatsUp Gold v12 cannot use a database containing the WhatsUp Professional 2006 schema.

This problem most often occurs when the WhatsUp Gold application was upgraded and the database was in a non-default configuration, but the WhatsUp database schema was not upgraded. It may also occur if you restore a WhatsUp Gold database from an earlier version of the application.

To resolve this problem, upgrade the database schema to match the version of the currently installed application with the instructions in the *Upgrading the database schema* (on page 20).

The WhatsUp Gold Polling Engine will not run, nor can the WhatsUp Gold application or web interface be used until this database version mismatch error is corrected.

Using an alternative database setup

We recommend using the default database, which is Microsoft SQL Server 2005 Express Edition (SSEE), and letting the installation program set up the database for you.



Important: If you want to migrate to SQL 2005, you must first install WhatsUp Gold and its SSEE instance and then migrate to the SQL 2005 Database Engine.

You can manually configure WhatsUp Gold to:

- Use Microsoft SQL Server 2005 instead of Microsoft SQL Server 2005 Express Edition (SSEE). SSEE is essentially a scaled down version of Microsoft SQL Server 2005. It can support up to 4 GB of data. If you need to use more space, you can purchase Microsoft SQL Server 2005 to use with WhatsUp Gold.
- Run the database on a computer separate from the one on which you have installed WhatsUp Gold. This may result in improved database performance by allowing separate resources to be used by both the database engine and the WhatsUp Gold application.



Warning: While WhatsUp Gold supports the SQL Server 2000 Database Engine, you cannot migrate from the SSEE database engine to SQL Server 2000. The SQL Server database engines are not forward compatible and SQL Server 2000 cannot read the database data stored in a SQL Server 2005 database.

Either of these options requires manually configuring the database, so you need to have knowledge of how to manage and configure SQL Server 2005. There are several points to consider before deciding to move from a default database environment that uses SSEE to a non-default configuration:

- When upgrading WhatsUp Gold in the future, you will be required to manually *upgrade your database schema* (on page 20). In the default database configuration, the upgrade wizard will complete this database upgrade automatically.
- For most WhatsUp Gold users, 4 GB of drive space is adequate to store network data for at least one year. If you find that you are running out of database space in the default WhatsUp database, you may need to adjust your data collection or retention settings. Migrating to SQL Server 2005 because of the database size may be unwarranted in many cases.
- Previous versions of WhatsUp Gold were limited by the Microsoft SQL Server 2000 Desktop Edition workload governor. When polling a large number of devices or monitors, this could lead to performance problems that could only be solved by a migration to a version of SQL that did not have the governor. SQL Server 2005 Express Edition now removes this governor and significantly increases the database performance thresholds.
- After migrating to a non-default SQL instance of the WhatsUp database, the database management requires manual maintenance on a routine basis. In most organizations, this is managed by a professional database administrator (DBA) or someone familiar with maintaining databases and optimizing them for best performance. If your organization does not have a DBA or someone with similar skills, it may be best to continue using the SQL Server 2005 Express Edition database that ships with WhatsUp Gold.

Supported databases

- Microsoft SQL Server 2005 Enterprise Edition
- Microsoft SQL Server 2005 Standard Edition
- Microsoft SQL Server 2005 Workgroup Edition
- Microsoft SQL Server 2005 Express Edition

Database pre-requisites:

- Microsoft SQL Server 2005 English (with Service Pack 2) installed on the WhatsUp Gold host computer or another computer. If SQL Server is installed on another computer, remote connections to the SQL Server must be allowed. For more information, see *How to configure SQL Server 2005 to allow remote connections* (<http://support.microsoft.com/kb/914277>).



Important: WhatsUp Gold does not support non-English versions of SQL Server 2005.

- We recommend using an SQL account as the WhatsUp database user. However, if the SQL Server 2005 database exists on the same computer or both computers are members of the same domain, you may use Windows authentication. For more information about enabling mixed mode authentication in SQL Server 2005, see the Microsoft article about *Authentication Mode* <http://msdn2.microsoft.com/en-us/library/ms144284.aspx>.



Note: When using Windows Authentication, the WhatsUp Gold services and applications must run as the database user.

- A database user with the following privileges:
 - Full administrator privileges to the WhatsUp database. WhatsUp Gold v12 only supports accessing the database via an account with full administrator rights to the database. We do not support a limited access account.
 - User's language is (United States) English. This can be set in the properties for the login used by WhatsUp Gold.

If you need assistance configuring or verifying these prerequisites, contact your database administrator or refer to the *Microsoft SQL 2005 documentation* (<http://support.microsoft.com/ph/2855>).

Part I - Backing up the WhatsUp Database

- 1 From the WhatsUp computer, make a backup of the database. From the main menu in the WhatsUp Gold console, select **Tools > Database Utilities > Back Up SQL Database**. For this example, we will save our database as `database.dat` in the root of D:\
(D:\database.dat).
- 2 Close the WhatsUp Gold application; then, stop the **Ipswitch WhatsUp Engine** and the **Ipswitch Web Server\$WhatsUp**, for more information see *Stopping and starting the Ipswitch WhatsUp Engine* and *Stopping and starting the internal web server in the Help*. If you are running IIS as your web server, stop IIS, then restart it.
- 3 If open, close the Ipswitch Task Tray application. Right-click on the icon and select **Close Task Tray Application**.
- 4 If the SQL server to which you will be migrating the database is on another computer, copy the `.dat` file, created in Step 1, to the SQL server. Otherwise, proceed to Part II.

Part II - Importing the WhatsUp Database into SQL 2005

- 1 Create a database in SQL 2005 which has the following properties:
 - a) Database name is `WhatsUp`.
 - b) Default collation is `SQL_Latin1_General_CP1_CI_AS`.
- 2 Find the location of the Data and Log file for this new database. This information is required later in the migration process.
In SQL Server Management Studio, right-click the database, select **Properties**, then select the **Files** page. You can identify which file is the Data file by the value in the **File Type** column. The locations for the Data and Log files are under the **Path** column. In our example, the Data file is located in `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\WhatsUp.mdf` and the Log file is located in `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\WhatsUp.ldf`.
- 3 Close Management Studio and any other applications which may be accessing the WhatsUp database on the SQL server.
- 4 Open a command prompt on the SQL server and execute the following case-sensitive command to import the database into SQL.
In our example, we have a default instance installed on a computer named `SQL_1`. If your SQL install is a named instance, rather than the default instance, specify your SQL server name as `SQL_server_name\Instance_name`.

```
sqlcmd -E -S "<SQL_server_name>" -Q "RESTORE DATABASE [WhatsUp] FROM DISK='<location of .dat file>' WITH REPLACE, MOVE 'WhatsUp_dat' TO '<location of data file for SQL database>', MOVE 'WhatsUp_log' TO '<location of log file for SQL database>'"
```

In our example, this becomes:

```
sqlcmd -E -S "SQL_1" -Q "RESTORE DATABASE [WhatsUp] FROM  
DISK='D:\database.dat' WITH REPLACE, MOVE 'WhatsUp_dat' TO  
'C:\Program Files\Microsoft SQL  
Server\MSSQL.1\MSSQL\Data\WhatsUp.mdf', MOVE 'WhatsUp_log' TO  
'C:\Program Files\Microsoft SQL  
Server\MSSQL.1\MSSQL\Data\WhatsUp.ldf' "
```

- 5 After you receive the response that the database was successfully restored, close the command prompt.

Part III - Configuring the DSN



Important: Make sure that the instructions below are completed on the computer that WhatsUp Gold is installed on.

- 1 On the WhatsUp computer, open the Data Sources (ODBC) control panel (**Control Panel > Administrative Tools > Data Sources (ODBC)**).
- 2 Select the **System DSN** tab.
- 3 Click **Add...**, select **SQL Server**, then click **Finish**.
- 4 Specify a name for the DSN. It cannot be `WhatsUp` or any other in-use user or system DSN name. In this example, we will call ours DSN **WhatsUp2**.
- 5 In the **Server** box, enter the IP Address or name of the SQL Server. You can browse for it from the menu or enter it manually. If you are using a named SQL instance, be sure to also enter the Instance Name. Click **Next**.
- 6 Click to select the **SQL Server authentication...** option, then enter the credentials for the SQL user on your SQL server. Click **Next**.
- 7 Click to select the **Change the default database to** option and select **WhatsUp** from the menu. Click **Next**.
- 8 Click **Finish**.
- 9 Click **Test Data Source...** and verify that no errors are listed. Click **OK**, then click **OK** again.

Part IV - Configuring WhatsUp to use the new database

- 1 Run the Connection String Configuration Utility. This application is located in your WhatsUp installation directory (usually `C:\Program Files\Ipswitch\WhatsUp\NmConfig.exe`).
- 2 Change the text in the **Database connection string (DSN)** field to match the new DSN created in Part III. In our example, it will read `DSN=WhatsUp2`.
- 3 Enter the **Username** and **Password** for your SQL user from Part III, Step 6. Click **OK**.
- 4 Click **Yes** to restart the Ipswitch services.



Note: A dialog opens and tells you that you need to restart the WUG Engine. When you click **Yes**, not only are you restarting the WUG Engine, you are restarting the WUG Web Server. If you are running IIS as your web server, stop IIS, then restart it.

- 5 On the WhatsUp computer, open the Windows Registry Editor (`regedit.exe`), and browse to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ipswitch
WhatsUp Engine. Make a backup of this key.
- 6 Delete the `DependOnGroup` and `DependOnService` values.
- 7 Restart the WhatsUp computer.



Note: If you prefer, you can now change the properties for the `MSSQL$WHATSUP` service so that it does not run automatically at boot. We do not recommend that you uninstall SQL Server 2005 Express Edition from the WhatsUp machine.

About the Database Utilities

You can use the WhatsUp database utilities to back up and restore the database and to perform database maintenance and troubleshooting.

To access the database utilities:

From the WhatsUp Gold console main menu, select **Tools > Database Utilities**.

Using the database backup and restore backup utility

Through this feature, you can back up your complete WhatsUp Gold SQL Server database to any mapped directory you have on your network. The file is saved as a `.dat` file and can be restored at any time. Using Backup, your data is saved to a `.dat` file. Restore reverses this process, overwriting your current database with the data in a `.dat` file.



Caution: You cannot use this feature to back up from, or restore to a remote database, (meaning the SQL/SQL Express server is located on a remote server) or to a local database that has an instance name other than `WHATSUP`.

If you want to back up the SQL database to a mapped drive, you may need to change the Logon settings for the `MSSQL$Whatsup` service (or your customized SQL service). The account must have write access to the mapped drive for the backup to be successful.

To change the SQL database logon settings:

- 1 Click **Start > Control Panel > Administrative Tools > Services**, then double click `MSSQL$WHATSUP` (SQL Server (WhatsUp)). The Web Server Properties dialog opens.
- 2 Click the **Log On** tab on the Properties dialog.
- 3 Change the account logon settings as required.



Important: This is a complete backup and restore, so any change that you make after the backup will be overwritten if a restore process is done.

To access the **Database Utilities Backup and Restore** features:

From the main menu in the WhatsUp Gold console, select **Tools > Database Utilities > Back Up SQL Database**

- or -

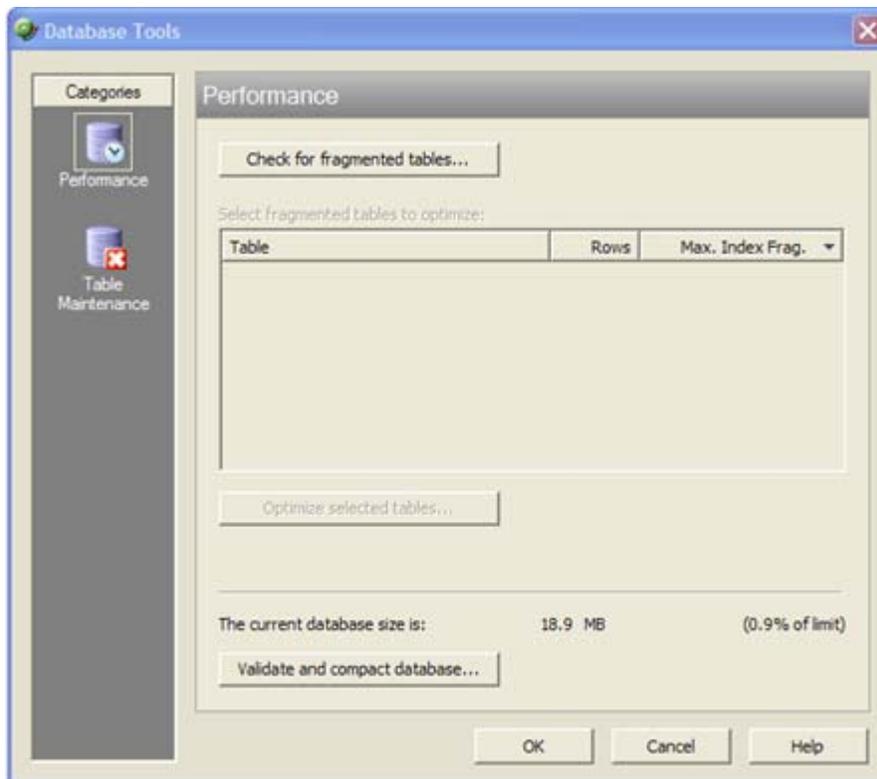
Tools > Database Utilities > Restore SQL Database.

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, select **Tools > Database Utilities > Tools**. The Database Tools dialog opens.



- 2 Select one of the tools:
 - Performance
 - Table Maintenance

Database Performance Tool

The Database Performance Tool is used to monitor the size of your database, and to manage the index fragmentation percentage of the individual tables. Fragmented indexes can cause database operations to slow down considerably, in much the same way that disk fragmentation causes your computer to run slower.

Click **Check for fragmented tables** to begin. This may take a considerable amount of time (up to a few minutes), depending on how many records are in your database.

- **Select fragmented tables to optimize.** This list shows all database tables with greater than 10% index fragmentation, along with the total number of data rows in that table.
- **Optimize selected tables.** Select the tables in the list above to defragment those database tables. WhatsUp Gold automatically stops and restarts the WhatsUp Service. The status of the operation appears on the dialog, next to this button.
- **The current database size is.** This section of the dialog shows the total amount of space used by the database. If you are using SQL Server 2005 Express as the WhatsUp Gold database, this section also displays the percentage of the 4 GB file size limit currently in use.
- **Validate and compact database.** Click this button to execute commands that validate the database, index, and database links, and to compact the database. WhatsUp Gold automatically stops the WhatsUp Service and restarts it once the operation is complete.

The validation phase executes the SQL Server commands `DBCC CHECKCONSTRAINT`, `DBCC CHECKCATALOG`, and `DBCC CHECKDB`. These commands check the integrity of all constraints in the database, check for consistency in and between system tables in the database, and check the allocation and structural integrity of all the objects in the database.

The compacting phase executes the SQL Server command `DBCC SHRINKDATABASE`, which shrinks the size of the data files in the database. Note that no compression is used; the database is simply compacted by removing empty space.

For more information on validating or compacting the database, see *Getting Started with SQL Server* (http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp) on the Microsoft Web site..

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.

Click **Purge Expired Rows** to remove those records from the database.

Configuring the web server

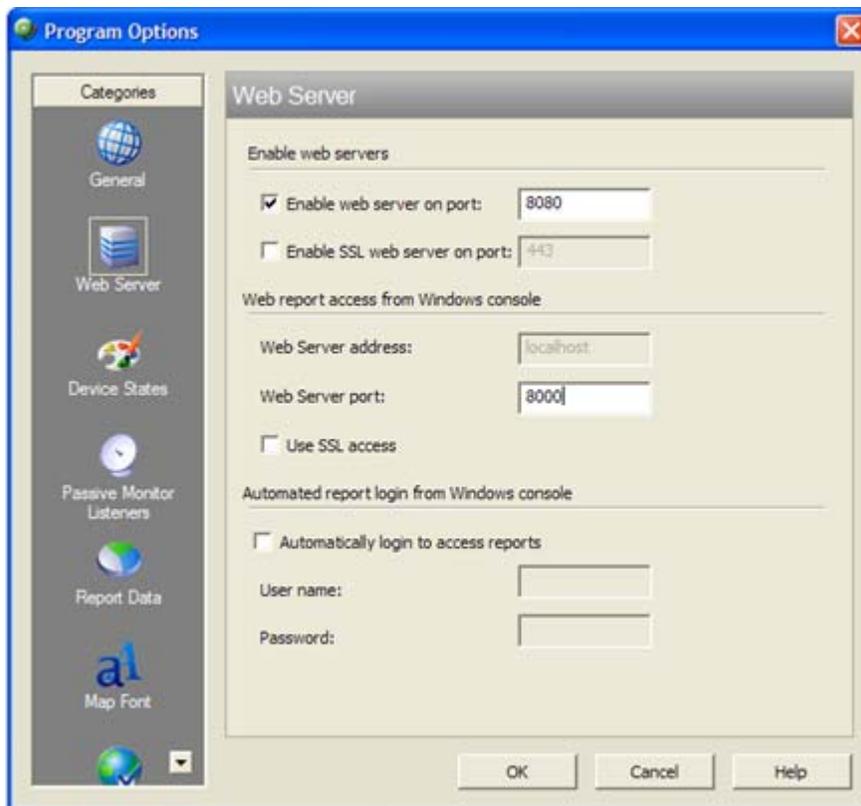
By default, WhatsUp Gold delivers and configures a lightweight web server to serve the web interface over regular HTTP or SSL-encrypted HTTPS.

Alternatively, you can configure Microsoft Internet Information Services as the web server for the WhatsUp Gold web interface.

Stopping and starting the internal web server

To start or stop the WhatsUp Gold web server:

- 1 On the WhatsUp Gold console, select **Configure > Program Options**.
- 2 On the Program Options dialog, select **Web Server**.



- 3 Select **Enable web server on port** to start the server, or clear the option to stop the server.
- 4 Click **OK** to save your changes.

You can change the port that the server runs on by changing the port number next to the **Enable web server on port** option.



Tip: To restart the web server, clear **Enable web server on port** and click **OK** to close the dialog. Then, open Program Options dialog again and select **Enable web server on port** again.



Tip: You can also restart the web server using the `NmServiceRestart.exe` command line utility. For more information, see *Restarting the WhatsUp Gold services from the command line* (on page 372).

About the default SSL certificates

WhatsUp Gold install the SSL certificates and keys needed to immediately begin connecting to the SSL web server using 128 bit encryption.

The SSL files included with WhatsUp Gold (`root.pem` and `server.pem`) are installed with every copy of WhatsUp Gold as a demonstration of how SSL can be used to encrypt web traffic. If you choose to use these default files, your encrypted session can be intercepted and decrypted by anyone who has access to these files.

You should replaced the default certificates with new SSL certificates that you generate and sign. These sample files reside in the `<WhatsUp Gold Install Directory>\data\SSL` directory.

Also, since the sample certificate is issued with `Ipswitch` as the Common Name, it will generate a Domain Name Mismatch Security Error every time a new browser session is established.

Using IIS on Windows XP or Windows 2003

Follow these steps to run the WhatsUp Gold web interface through an IIS (Internet Information Services) Web server on Windows XP or Windows 2003. This procedure assumes that you are using the default instance of SQL Server 2005 Express that is delivered with WhatsUp Gold and that WhatsUp Gold, SQL Server 2005 Express, and Internet Information Server are all installed on the same server.



Important: This procedure is for use with Windows XP and Windows 2003 only. For instructions on how to configure IIS as the web server for the WhatsUp Gold web interface on Windows Vista, see *Using IIS on Windows Vista* (on page 37).

To use IIS as the web server for the WhatsUp Gold web interface on Windows XP or Windows 2003:

- 1 Stop the following services and applications:
 - Ipswitch WhatsUp Engine service
 - Ipswitch Web service
 - Task Tray application
 - WhatsUp Gold console

- 2 Specify a username and password for WhatsUp Gold to use when connecting to SQL Server 2005 Express (SSE).
 - a) From the Windows Start menu, select **Control Panel > Administrative Tools > Data Sources** and select the **System DSN** tab.
 - b) Select the WhatsUp DSN and click **Configure**. The Configuration wizard opens.
 - c) Verify that the fields in the first dialog are correct for your SQL Server authentication preferences, then click **Next**.
 - d) On the second dialog, verify that the **With SQL Server authentication using login ID and password entered by the user** option is selected. In the **Login** field, enter the SQL username. In the **Password** field, enter the SQL user's password. Click **Next**.



Note: For the default instance of SSE installed with WhatsUp Gold, the default **username** is sa and the **password** is WhatsUp_Gold.

- e) On the third dialog, verify that the first option is selected and that the WhatsUp database appears in the drop-down menu. Click **Next**.
 - f) Continue to click **Next** until you come to the final dialog, then click **Finish**. The ODBC Microsoft SQL Server Setup dialog opens. You can click **Test Data Source** to test the configuration or click **OK**.
 - g) Browse to the WhatsUp Gold install directory and run NmConfig.exe. Specify sa as the username and WhatsUp_Gold as the password, then click **OK**. Restart the polling engine if prompted.
- 3 Stop the Web site under which you want to run the WhatsUp Gold web interface.
 - a) From the Windows Start menu, select **Control Panel > Administrative Tools > Internet Information Services**. The Internet Information Services (IIS) Manager appears.
 - b) Right-click on the Web site under which you want to run the WhatsUp Gold web interface and select **Stop**.
- 4 Create a virtual directory for the WhatsUp Gold web interface.
 - a) Right-click on the Web site on which you want to run the WhatsUp Gold web interface and select **New > Virtual Directory**. The Virtual Directory Creation Wizard appears.
 - b) Click **Next**. The Virtual Directory Alias dialog appears.
 - c) In **Alias**, enter NmConsole. Click **Next**. The Web Site Content Directory dialog appears.
 - d) In **Path**, enter or browse to select <WhatsUp Gold install path>\HTML\NmConsole\. Click **Next**. The Virtual Directory Access Permissions dialog appears.
 - e) Enable **Read** and **Run scripts (such as ASP)**, then click **Next**.
 - f) Click **Finish** to close the wizard.
- 5 Enable the parent paths feature for the NmConsole virtual directory.
 - a) In the Internet Information Services (IIS) Manager, right-click on the newly created NmConsole virtual directory and select **Properties**.
 - b) Select the **Virtual Directory** tab, then click **Configuration**.

- c) On the Options tab, select **Enable parent paths**. Click **OK**.
- 6 Configure authentication methods for the NmConsole virtual directory.
 - a) In the NmConsole Properties dialog, select the **Directory Security** tab.
 - b) Under **Anonymous access and authentication control** (in Windows XP) or **Authentication and access control** (in Windows 2003), click **Edit**. Verify that **Enable anonymous access** is enabled.
 - c) By default, IIS uses a restricted account named IUSR_<machine_name> for anonymous access. Under **Account used for anonymous access**, change the user listed in the **User name** field to a local administrator.



Note: In Windows XP, if you wish to use a domain user with local administrator rights, you must disable the **Allow IIS to control password** option and enter the password for the domain user.

- or -

Specify permissions for the IUSR_<machine_name> on the Windows Registry and the appropriate folders.

- In the Windows Registry, grant IUSR_<machine_name> user the Full Control permission to the HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\WebServer\WhatsUp key.
 - In Windows Explorer, grant IUSR_<machine_name> user the Full Control permission to the <WhatsUp Gold install path>\HTML\ folder and all of the files and folders located beneath it.
 - In Windows Explorer, grant IUSR_<machine_name> user the Full Control permission to the <WhatsUp Gold install path>\Data\Mibs folder.
- d) Click **OK** to close the Authentication Methods dialog, then **OK** to close the NmConsole Properties dialog.
- 7 On Windows 2003 (IIS 6) only, you must enable and configure Active Server Pages.
 - a) In the **Internet Information Services (IIS) Manager**, select the **Web Services Extensions** folder. The Web Services Extensions pane appears.
 - b) Select **Active Server Pages**, then click **Allow**.
 - c) Enable ASP response buffering and increase the buffer limit as follows:
 - From the Windows desktop, select **Start > Run**. The Run dialog appears.
 - Enter `cmd.exe`, then click **OK**.
 - Enter the following commands:

```
cd /d %systemdrive%\inetpub\adminscripts
cscript.exe adsutil.vbs SET w3svc/AspBufferingLimit 8000000
cscript.exe adsutil.vbs SET w3svc/AspMaxRequestEntityAllowed 8000000
```
- 8 Restart IIS. To do this, in the Internet Information Services (IIS) Manager, right-click on the Web site on which you want to run the WhatsUp Gold web interface and select **Start**.

- 9 Disable the Ipswitch web server. This can be done on the WhatsUp Gold console at **Configure > Program Options > Web Server**. After disabling the Ipswitch Web server, verify that reports still load correctly by right-clicking a device in the console and selecting **Device Reports**. If the reports do not load properly, verify that the **Web server port** in the **Web report access from Windows console** section of the contains the port number used by IIS.
- 10 Restart the services and applications you stopped in Step 1.
- 11 Connect to the WhatsUp web interface by opening a browser and entering the following address in the Address box:

`http://<ip_address - or - hostname>/NmConsole/`

Examples

`http://192.168.1.200/NmConsole/`

`http://demo.whatsupgold.com/NmConsole/`



Important: When adding a device through IIS, an issue with IIS may cause you to receive an error that says, "Error scanning device." For information on how to resolve this issue, see *"Error scanning device XXXXX. Probable cause is it does not exist" when using IIS as the Web Server* (<http://support.ipswitch.com/kb/WP-20061130-es01.htm>).

Using IIS on Windows Vista

Follow these steps to run the WhatsUp Gold web interface through an IIS (Internet Information Services) Web server on Windows Vista. This procedure assumes that you are using the default instance of SQL Server 2005 Express that is delivered with WhatsUp Gold and that WhatsUp Gold, SQL Server 2005 Express, and Internet Information Server are all installed on the same server.



Important: Throughout the procedure below, Windows Vista may periodically ask you to confirm that you want to perform certain tasks that require administrative privileges. If this occurs, select **OK**.



Important: This procedure applies to Windows Vista with Service Pack 1 only. For instructions on how to configure IIS as the web server for the WhatsUp Gold web interface on Windows XP or Windows 2003, see *Using IIS on Windows XP or Windows 2003* (on page 34).

- 1 Stop or close the following services and applications:
 - Ipswitch WhatsUp Engine service
 - Ipswitch Web service
 - WhatsUp Gold Task Tray application
 - WhatsUp Gold console application
 - Internet Information Services (which appears as the World Wide Web Publishing Service in the Services applet of the Control Panel)

- 2 Specify a username and password for WhatsUp Gold to use when connecting to SQL Server 2005 Express (SSE).
 - a) From the Windows Start menu, select **Control Panel > Administrative Tools > Data Sources** and select the **System DSN** tab.
 - b) Select the WhatsUp DSN and click **Configure**. The Configuration wizard opens.
 - c) Verify that the fields in the first dialog are correct for your SQL Server authentication preferences, then click **Next**.
 - d) On the second dialog, verify that the **With SQL Server authentication using login ID and password entered by the user** option is selected. In the **Login** field, enter the SQL username. In the **Password** field, enter the SQL user's password. Click **Next**.



Note: For the default instance of SSE installed with WhatsUp Gold, the default **username** is `sa` and the **password** is `WhatsUp_Gold`.

- e) On the third dialog, verify that the first option is selected and that the WhatsUp database appears in the drop-down menu. Click **Next**.
 - f) Continue to click **Next** until you come to the final dialog, then click **Finish**. The ODBC Microsoft SQL Server Setup dialog opens. You can click **Test Data Source** to test the configuration or click **OK**.
 - g) Browse to the WhatsUp Gold install directory and run `NmConfig.exe`. Enter the **username** and **password** for your SQL user, then click **OK**. Restart the polling engine if prompted.
- 3 Create a Windows user to serve as the user context under which the WhatsUp Gold web interface runs.
 - a) Open **Control Panel > Administrative Tools > Computer Management**. The Computer Management application appears.
 - b) Select **Local User and Groups**, then select the **Users** folder.
 - c) From the menu, select **Action > New User**. The New User dialog appears.
 - d) Enter the information for the new user. We recommend using a name that is easily identifiable as the WhatsUp Gold user, such as `WhatsUpUser` or `WUGUser`.
 - e) Clear **User must change password at next logon**.
 - f) Click **Create**. The new user is created.
 - g) Click **Close** to close the New User dialog.
 - h) Double-click the new user. The Properties dialog for the user appears.
 - i) Select the **Member Of** tab. A list of groups to which this user belongs appears.
 - j) Verify that the user is a member of the Users group.
 - k) Click **OK**, and then close the Computer Management window.
 - l) The user is now ready to be used by the WhatsUp Gold web interface.



Tip: If unexpected errors occur in WhatsUp Gold with IIS 7.0, try using the `Administrator` user login to resolve the issue.

- 4 Verify that IIS is installed and properly configured.
 - a) Open **Control Panel > Programs and Features**.
 - b) From the Tasks pane on the left side of the window, select **Turn Windows Features on or off**. The Windows Features dialog appears.
 - c) Verify that **Internet Information Services** is selected.
 - d) Expand **Internet Information Services > World Wide Web Services > Application Development Features**.
 - e) Select **ASP**, then click **OK**.
- 5 Create an IIS application pool for WhatsUp Gold to use.
 - a) Open **Control Panel > Administrative Tools**. The Administration Tools window appears.
 - b) Double-click **Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) Manager appears.
 - c) In the **Connections** pane on the left side of the window, expand the item that corresponds to the name of the server on which you are working.
 - d) Right-click on **Application Pools** and select **Add Application Pool**. The Add Application Pool dialog appears.
 - e) In **Name**, enter `NmConsole`.
 - f) Under **.NET Framework version**, select the highest version available.
 - g) Under **Managed pipeline mode**, select **Classic**.
 - h) Click **OK**. The new application pool is created.
- 6 Configure advanced settings on the `NmConsole` application pool.
 - a) Right-click the **NmConsole** application pool from the list, then select **Advanced Settings** from the right-click menu. The Advanced Settings dialog appears.
 - b) Expand **Process Model**, then select the **Identity** row. Click the browse (...) button that appears in the second column. The Application Pool Identity dialog appears.
 - c) Select **Custom account**, then click **Set**. The Set Credentials dialog appears.
 - d) Enter the name and password of the user you created for the WhatsUp Gold web interface to run as, then click **OK**.
 - e) Make sure the **Maximum Worker Processes** are set to `1`.
 - f) Click **OK** to exit the Advanced Settings dialog.
- 7 Create an IIS application for the WhatsUp Gold web interface.
 - a) In the **Connections** pane on the left side of the screen, under Sites, locate the Web site under which you want WhatsUp Gold to run. Right-click it and select **Add Application**. The Add Application dialog appears.
 - b) In **Alias**, enter `NmConsole`.

- c) Click the **Select** button next to **Application pool**. The Select Application Pool dialog appears.
- d) Select the NmConsole application pool, then click **OK**.
- e) In Physical path, enter (or use the browse button to select) the path to the WhatsUp Gold web interface. This should be located at <WhatsUp Gold install path>\HTML\NmConsole\.
- f) Click **Connect As**. The Connect As dialog appears.
- g) Select **Specific user**, then click **Set**. The Set Credentials dialog appears.
- h) Enter the name and password of the user you created for the WhatsUp Gold web interface to run as, then click **OK**.
- i) Click **OK** to close the Connect As dialog.



Tip: After configuring the settings for the application, click **Test Settings** to verify that everything is configured correctly.

- j) Click **OK**. The new application is created.
- 8** Modify the ASP settings for the **NmConsole** application.
- a) In the **Connections** pane on the left side of the window, select the **NmConsole** application.
 - b) In the center section of the screen, under the **IIS** heading, double-click **ASP**.
 - c) Under **Enable Parent Paths**, select **True**. This option is required to support use of the relative paths used to navigate in the WhatsUp Gold web interface.
 - d) Expand **Limit Properties**.
 - e) Change the value of **Maximum Requesting Entity Body Limit** to 8000000.
 - f) Change the value of **Response Buffering Limit** to 8000000.
 - g) In the **Actions** pane on the right side of the window, click **Apply**.
- 9** On the Windows Registry and the appropriate folders, specify permissions for the user you created for the WhatsUp Gold web interface to run as.
- In the Windows Registry, grant the user the Full Control permission to the HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\WebServer\WhatsUp key.
 - In Windows Explorer, grant the user the Full Control permission to the <WhatsUp Gold install path>\HTML\ folder and all of the files and folders located beneath it.
 - In Windows Explorer, grant the user the Full Control permission to the <WhatsUp Gold install path>\Data\Mibs folder.

- 10** To prevent a port conflict, the internal web server must be set to use another port, such as 8080, or must be disabled. This can be done on the WhatsUp Gold console at **Configure > Program Options > Web Server**.



Note: If you configure the Web Server to run on a port other than the port you specified during the installation of WhatsUp Gold, you must configure the Windows Firewall to allow traffic on that port.

If you disable the WhatsUp web interface, verify that reports still load correctly by right-clicking a device in the WhatsUp Gold console and selecting Device Reports. If not, double-check the settings on the **Program Options > Web Server** panel and verify the **Web server port** in the **Web report access from Windows console** section contains the port number used by IIS.

- 11** Restart the services and applications you stopped in Step 1.
- 12** Connect to the WhatsUp web interface by opening a browser and entering the following address in the Address box:

`http://<ip_address - or - hostname>:port/NmConsole/`

Examples

`http://192.168.1.200/NmConsole/`

`http://192.168.1.200:8080/NmConsole/`

`http://www.ipswitch.com:8080/NmConsole/`

Uninstalling Ipswitch WhatsUp Gold v12

To uninstall Ipswitch WhatsUp Gold v12:

- 1** Select **Start > Settings > Control Panel**, then select **Add or Remove Programs**.
- 2** Select Ipswitch WhatsUp Gold v12.
- 3** Select **Remove**.

You can also run the Ipswitch WhatsUp Gold v12 installation program, then select **Remove**.

Select one of the following dialog options:

- Remove the WhatsUp Gold application, but leave network data I have collected intact.
- Remove both the WhatsUp Gold Premium application, and all network data I have collected.
- Also, remove the "WhatsUp" copy of SQL Server Express Edition.

Using Device Discovery

In This Chapter

About Device Discovery	43
Using the Device Discovery wizard	43
About Device Discovery scan types	44
Using Device Discovery wizard SNMP SmartScan option	44
Adding a single device manually	48
About Active Discovery	53

About Device Discovery

WhatsUp Gold provides you the capability called Device Discovery that allows you to discover devices connected to your network.

There are three ways to use Device Discovery:

- 1 Through the Device Discovery Wizard in the WhatsUp Gold console
- 2 Through single Device Discovery
- 3 Through Active Discovery

Using the Device Discovery wizard

The Device Discovery wizard scans your network for devices, using the protocol(s) and settings you choose. After devices and monitors are found, you select the ones you want to monitor and WhatsUp Gold creates devices in the database for each item you choose.

The wizard begins by default after installation. After this initial Discovery, you can run another Discovery at any time from the console by clicking **File > Discover Devices**.



Note: The Device Discovery Wizard is only available in the console application.

Device groups are created based on subnetworks found during the scan. You may notice that some group folders may be empty. This is because a subnet was found, but the devices in that subnet were not scannable or you chose not to monitor them.

About Device Discovery scan types

There are four options for device discovery. They are:

- **SNMP SmartScan:** SmartScan discovers devices by reading SNMP information on your network. This scan type uses an SNMP enabled router to identify both network devices and subnetworks. We recommend using SmartScan as your primary Discovery method.
- **IP Range Scan:** WhatsUp Gold scans a range of IP addresses and finds the devices that respond to one or more of the chosen services. The Discover Devices wizard prompts you to enter a range of the IP addresses in your network. You should use IP Range Scan if SNMP is either unavailable or does not meet your needs.
- **Network Neighborhood:** Scanning a Network Neighborhood creates a list of devices by scanning the Windows network to which your computer is connected, and finding the other systems on the network. Use this type of scan if you only want to discover Windows devices.
- **Hosts File Import:** WhatsUp Gold imports devices from the system's Hosts file, which is a text file that lists host names and their IP addresses on a network. For small networks, the Hosts file is an alternative to DNS. The Hosts file may also be called a host table by some TCP/IP vendors.

For more information, see *Example: discovering devices* (on page 45).

Using Device Discovery wizard SNMP SmartScan option

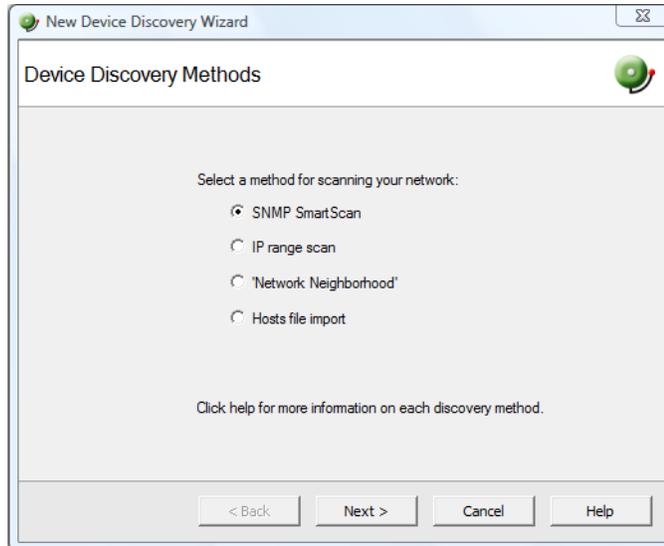
This section describes how to use the Device Discovery wizard with the SNMP SmartScan option to discover devices. In this example, you want to discover all of the devices attached to a specific SNMP-enabled router on your network. To accomplish this, you need to:

- Know the IP address of the SNMP-enabled router whose network you want to discover.
- Know the Read Community name assigned to the devices on the network.

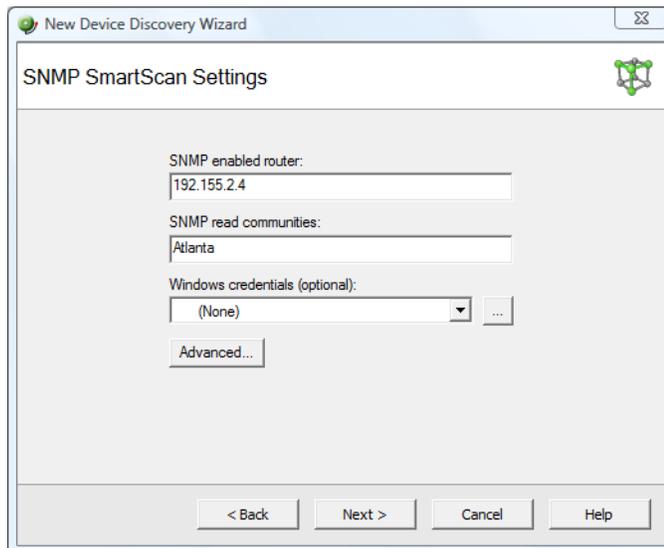
Example: discovering devices

To discover devices:

- 1 Select **File > Discover Devices**. The New Device Discovery Wizard appears.



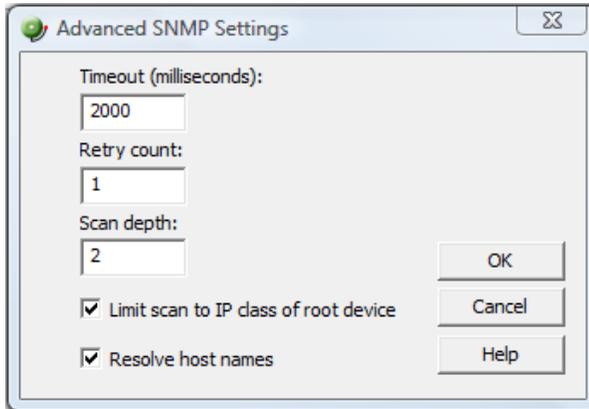
- 2 Select **SNMP SmartScan** as the method for scanning your network, then click **Next**. The SNMP SmartScan settings dialog appears.



- 3 In the **SNMP enabled router** box, enter the IP address of the SNMP enabled router you want to use for this scan.
- 4 In the **SNMP read communities** box, enter the proper read community string for that router. If an incorrect string is entered, WhatsUp Gold will be unable to scan the network. Additional community strings may be entered, separated by commas, if there are multiple SNMP enabled devices on your network that use different strings.

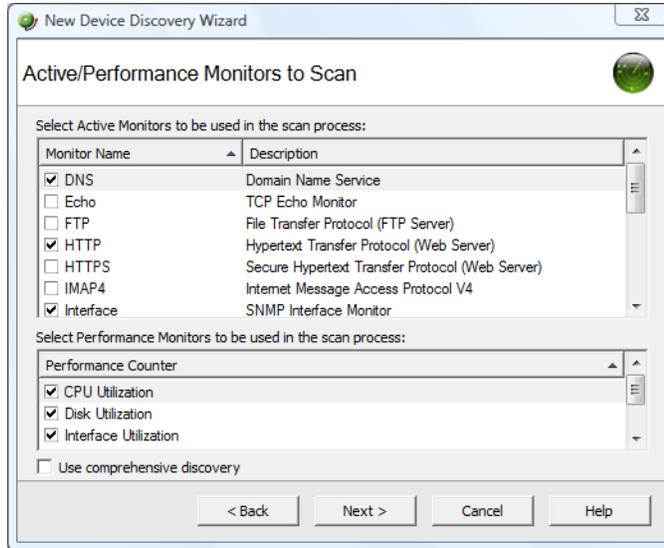
Optionally, select the Windows credential that you want to use during discovery. These credentials are configured in the Credentials Library, and store Windows authentication information (username and password) for those devices that require a logon for discovery or monitoring. Click the browse (...) button next to this box to access the Credentials Library. You can select a specific credential, select **All** to try all credentials that are configured or select **None** to ignore those devices that require you to log on. The credential that is successful is associated with each device.

- 5 Click the **Advanced** button if you want to change the scan's default timeouts in milliseconds, retry counts, and scan depth.



- Click to select the **Limit scan to IP class of root device** option if you want to limit the scan to the network class (A, B, or C) defined by the IP address of the root device. If the IP address is within the network class of the root device, the scan proceeds. Otherwise, the scan skips to the next IP address.
- Click to select the **Resolve host names** option if you want to populate the list of discovered devices with host names in addition to IP addresses.
- Click **OK** to save changes and return to the SNMP SmartScan settings dialog.

- 6 Click **Next**. The Active/Performance Monitors to Scan dialog opens. Select the type of Active Monitor(s) and Performance Monitor(s) you want to use in this scan process. In this example, select DNS, HTTP, and Interface as our Active Monitors (Ping is selected by default) and CPU, Disk, and Interface Utilization as our Performance Monitors to be used in the scan process.



- The *Ping monitor* polls the device on a regular basis to establish whether it is Up or Down. By default, WhatsUp Gold sends a ping command to each viable IP address in the range configured during the first section of this wizard. If the device responds, WhatsUp Gold scans for the monitors listed on this dialog. If the device does not respond, discovery moves on to the next IP address. You can select **Use comprehensive discovery** to have device discovery scan each IP address for all of the selected monitors without first sending the ping command to the device. Discovery takes longer if this option is selected.



Note: If you want a Ping monitor created for the devices found in discovery, you must select **Ping** as an active monitor to scan even if you have cleared the **Use comprehensive discovery** option.



Note: If a device only has one interface, WhatsUp Gold intentionally does not add the Interface Active Monitor during discovery. Doing so with the Ping Active Monitor would be redundant.

- The *HTTP monitor* polls a web server (if one is discovered) on the device on a regular basis to establish if it is Up or Down.



Tip: To see how a monitor is configured, you can go to the Active Monitor Library (**Configure > Active Monitors**), select a monitor, then click **Edit**.

- The *Disk Utilization monitor* monitors and reports on the available disk space for the selected device. Data collected is displayed in the Disk Utilization Report.
- 7 Click **Next**. The Device Discovery displays the estimated remaining scan time and the scan's progress. You can cancel the Device Discovery by clicking **Stop**.

- 8 When the Discovery is completed, the **Devices to Monitor** window opens, listing all of the devices just discovered and the active and passive monitors that were applied. Note that if any of the devices have already been entered into the database, a shortcut to the device will be created in the device list. To add all of the devices to the database, click **Next**. To remove specific devices to be monitored from this list, clear the checkbox next to the device you want to remove.



Note: Additional Active Monitors and Performance Monitors that are already in the database will not be added to devices.

- 9 Click **Next**. The Action Policy Selection dialog appears. For more information about Action Policies, see *About Action Policies* (on page 152).

- 10 Complete the remaining screens in the wizard.

The Results summary shows the number of selected new devices, number of active and performance monitors, whether or not an Action Policy is applied, and the number of selected device shortcuts.

- 11 Click **Finish** to begin monitoring the devices. A progress bar appears while devices are added to the database, then the Device View opens with a list of new devices found in the device discovery process. For more information about Device Views, see *About the Device View* (on page 58).



Note: If some device group folders are empty, it is due to the fact that although a subnet was found, the devices in the subnet were either not scannable, or you chose not to monitor them.

Adding a single device manually

There are three ways to add devices, individually, to the monitoring database:

- In the Map View or Device View, in the console or the web interface, right-click and select **New > New Device**.
 - From the console, you can display the Device Types (list of device icons) in the left pane, then click and drag one to the Device or Map view.
 - From the console, click **File > New > New Device**.
- or -
- From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Devices > New Device**.

Adding a device without scanning

You can add a "bare bones" device to the database immediately without scanning. The new device is generically categorized as a workstation.

This option is sometimes useful for testing purposes, as it allows you to add the same device to a database multiple times. At this time there no limit for the number of times you can add the same device to your database.



Examples

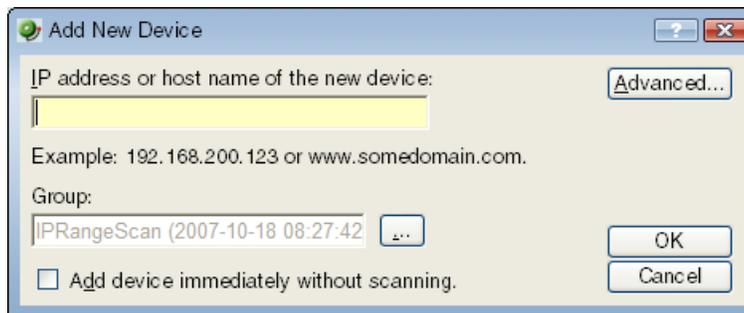
- Example: manually adding a device to a device group (on page 49)
- Example: clicking and dragging a device to a device group (on page 50)

Example: manually adding a device to a device group

When you manually add a device, you are prompted to enter the IP address or host name. WhatsUp Gold attempts to resolve the IP address or hostname, then scans the device for Active Monitors. When the scan is complete, you can further configure the device as needed. To demonstrate, we'll add a workstation to a device group.

To manually add a device to a device group:

- 1 Select the Device Group from the left hand pane to which you want to add a new device. Click the **Map View** tab (at the bottom of the console) to display the map for the group.
- 2 Right-click in the Map View, then click **New > New Device**. The Add New Device dialog opens.



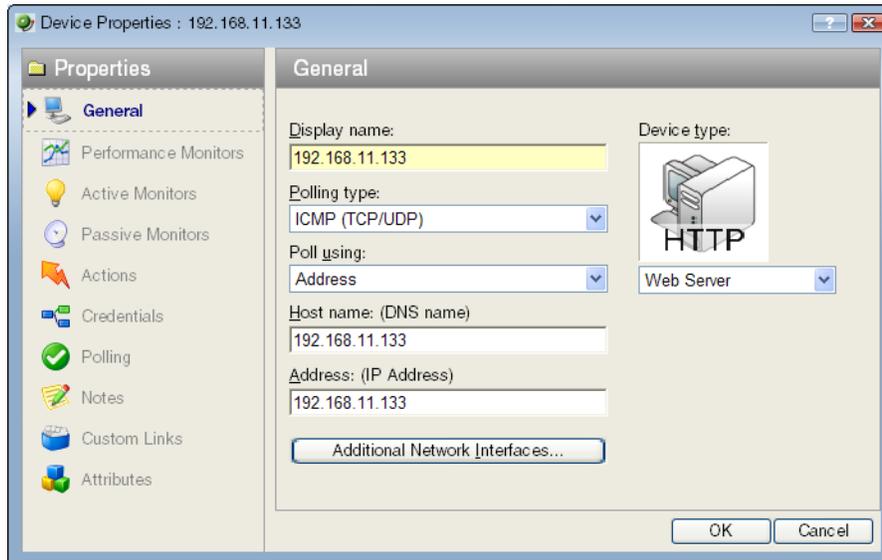
- 3 Enter the IP address or host name for the device into the box.
Optionally, select **Add device immediately without scanning** to add a device without scanning for the device.



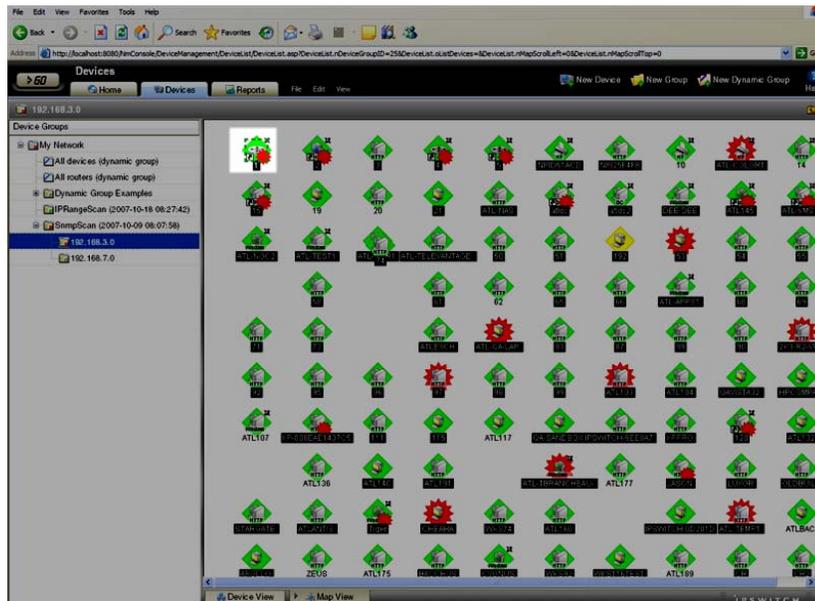
Note: Any monitors for which the **Use comprehensive discovery** option is selected will be checked when the device is added.

Using WhatsUp Gold v12

- Click **OK** to add the device. If the device already exists in another group, you will get a message to that effect. If you want to add a short cut for the device in this new group, click **Yes**. The Device Properties dialog opens.



- You can either accept the default Properties populated when you added the device, or modify them. If you accept them, click **OK**. The new device icon appears in the Map View.

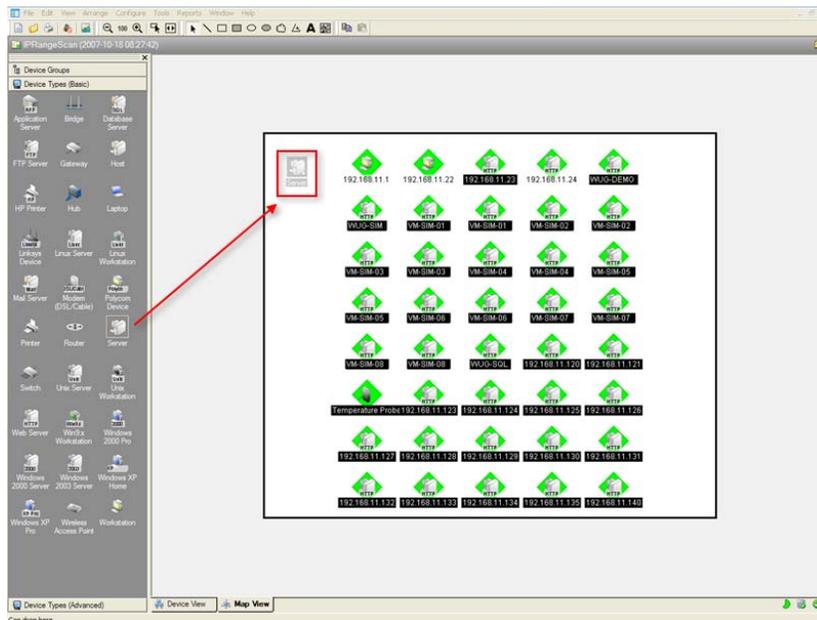


For more information about the Device Properties dialog, see *Learning about the Device Properties* (on page 82).

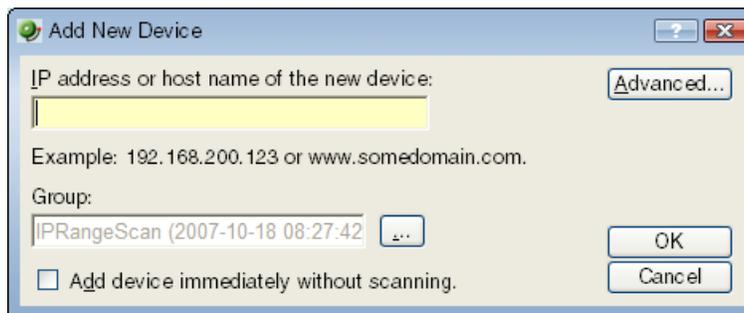
Example: clicking and dragging a device to a device group

To click and drag a device to a device group:

- 1 In the left pane of the console, select **Device Types (Basic)** or **Device Types (Advanced)**, depending on which device type you desire.
- 2 Drag the device icon to the Map View.



The Add New Device dialog opens.



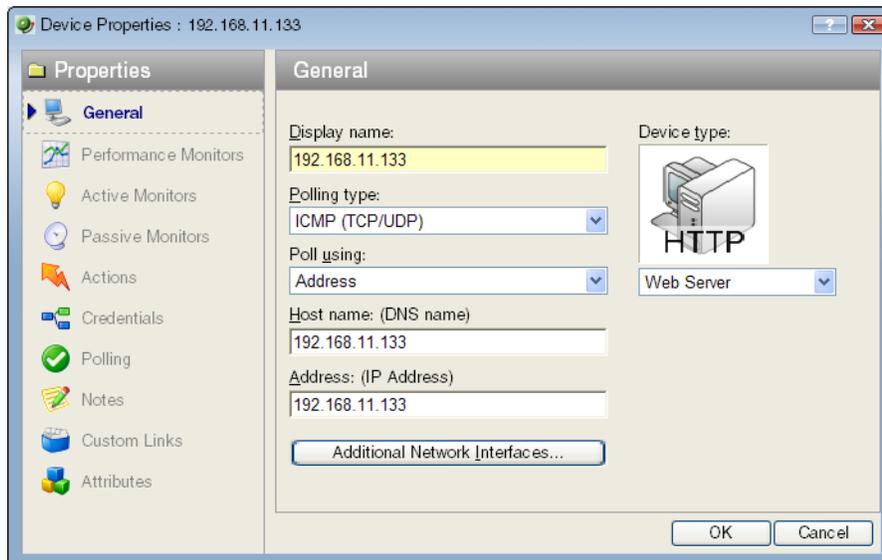
- 3 Enter the IP address or host name for the device into the box.
Optionally, select **Add device immediately without scanning** to add a device without scanning for the device.



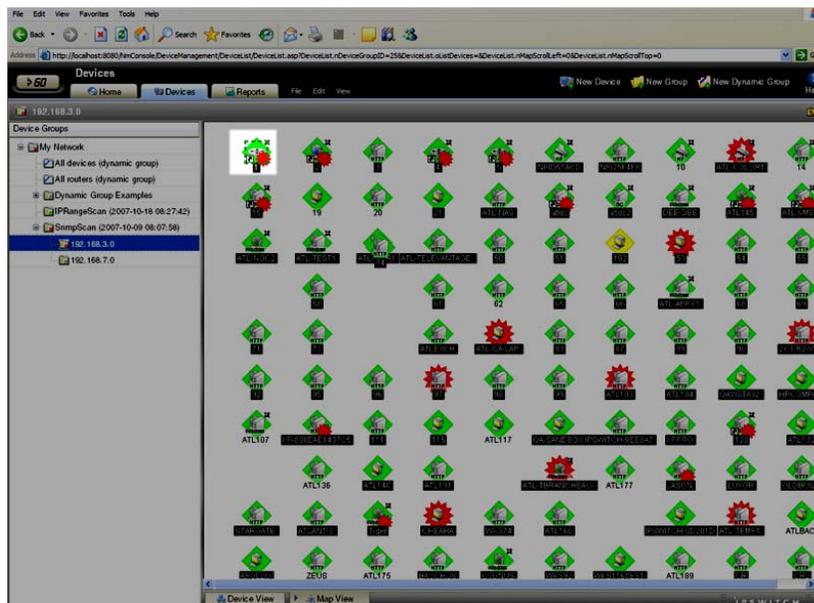
Note: Any monitors for which the **Use comprehensive discovery** option is selected will be checked when the device is added.

Using WhatsUp Gold v12

- 4 Click **OK** to add the device. If the device already exists in another group, you will get a message to that effect. If you want to add a short cut for the device in this new group, click **Yes**. The Device Properties dialog opens.



- 5 You can either accept the default Properties populated when you added the device, or modify them. If you accept them, click **OK**. The new device icon appears in the Map View.



- 6 For more information about the Device Properties dialog, see *Learning about the Device Properties* (on page 82).

About Active Discovery

You can use Active Discovery to schedule WhatsUp Gold to scan your network for new monitors (active monitors and performance monitors) and devices on a regular basis. Newly discovered items are added to the Active Discovery Results report, and WhatsUp Gold notifies you that a new device was found, or a new monitor was found on an existing device. You can then review the report and select the items you want to add to your device list.

For more information, see *Using Active Discovery* (on page 237).

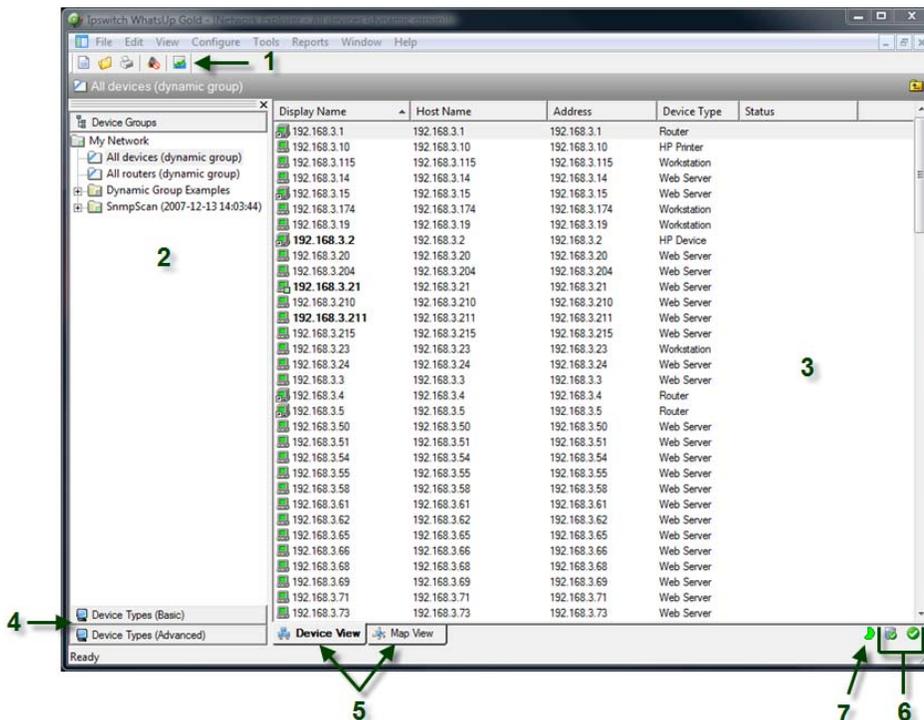
Using the WhatsUp Gold Console

In This Chapter

About the console.....	55
Organizing Devices, Device Groups, and Maps with drag-and-drop.....	57
About the Device View.....	58
About the Map View.....	59

About the console

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



- 1 The WhatsUp Gold Toolbar.** The icons on this toolbar change according to the view you are currently using. 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 Device Types Groups.** Click the **Basic** or **Advanced** tab to view the device types contained in the group selection. These types can be dragged into the view pane to create a new device based on the selected device type.
- 5 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.
- 6 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

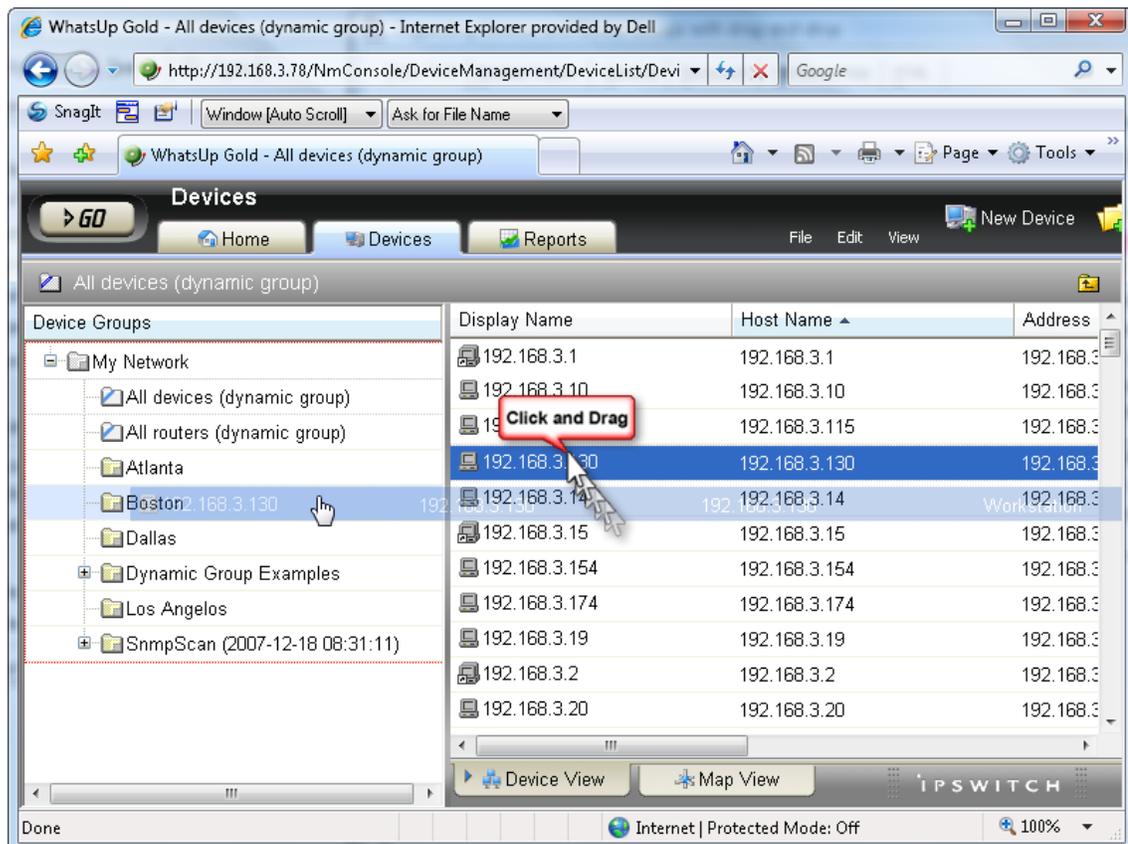


Polling is disabled

- 7 Database Size Indicator Icon.** This icon shows the current size of your database. The color and shape changes according the database size thresholds:
 - Green - 49% and below.
 - Yellow - 50% to 74%
 - Red - 75% and above.

Organizing Devices, Device Groups, and Maps with drag-and-drop

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



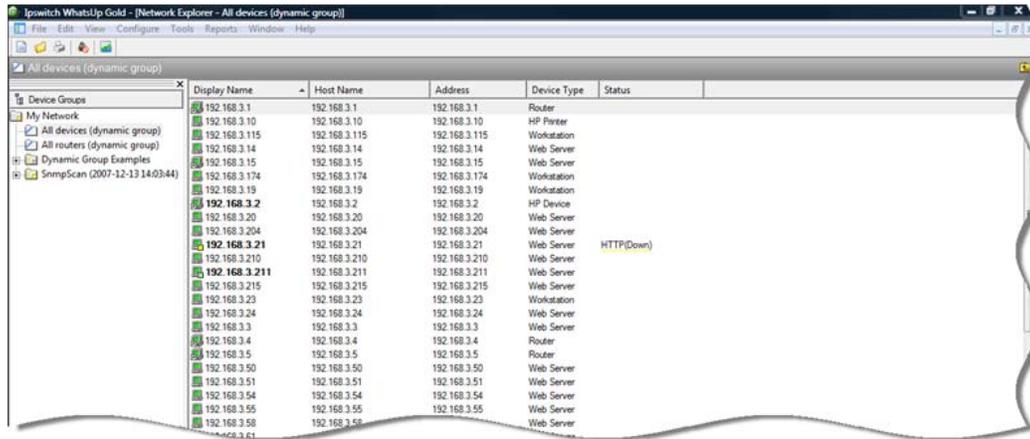
After you drop the icon or icons, a menu appears, asking if you want to move or copy the devices. If you move the devices, they are deleted from the previous device group. If you copy the devices, the devices appear in both device groups.



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 Device View

With a similar look and feel to Windows Explorer, the Device View gives you another option to help you keep your complex network organized and performing properly. In this view, devices are organized by device group, and appear in the list in alphabetical order based on the name of the folder or the display name of the device.



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

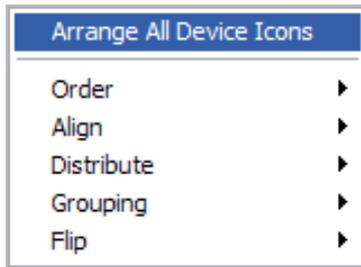
When the entry in the Device list is a group folder, the Status column shows the number of devices in the group with a breakdown of how many devices are in each device state.

About device icons

The following icons appear in the Device View when viewing the contents of a device group.

Icon	Description
	(Green) All monitors on the device are considered up.
	(Red) Device is considered down, because one or more monitors are down. The green square shows that at least one monitor is responding.
	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. For more information about Acknowledgements, see <i>Device overview</i> (on page 81).

Try the different Arrange menu features until you are satisfied with the device layout. Be aware that there is no undo option for the arrange tool.



To clean up a map after completing Discovery:

- 1 Select a device group, then click the **Map View** tab.
- 2 Right-click in the Map View, then select **Display > Clip Device Names**. This removes the domain part of the device name and shows only the host name.
- 3 Select all devices in the view by clicking and dragging a selection box around all devices. Then, from the Arrange menu, select **Distribute > Device Icons in Rows**.

If you have a large set of devices or want to represent a topology specific to your network, you can also use the graphics annotations (such as lines, text, circles) and attached lines to create custom map views.

You can select object(s) in the map, right-click and select **Lock Position** from the menu. Lock Position keeps an object from moving as you move other items around, or when adding devices to the map. If you want an object to be able to change positions on the map, remove the Lock Position selection. It is very useful to lock images you may place in the background, or text you want to protect.



Note: Locking an object on the console prevents you from moving that same object on the web interface.

Adding annotations to a map

Annotations are graphical objects that let you customize a map view. You can add text, shapes, lines, and graphics to visually organize a set of devices.



To use the Annotation (Draw) tools:

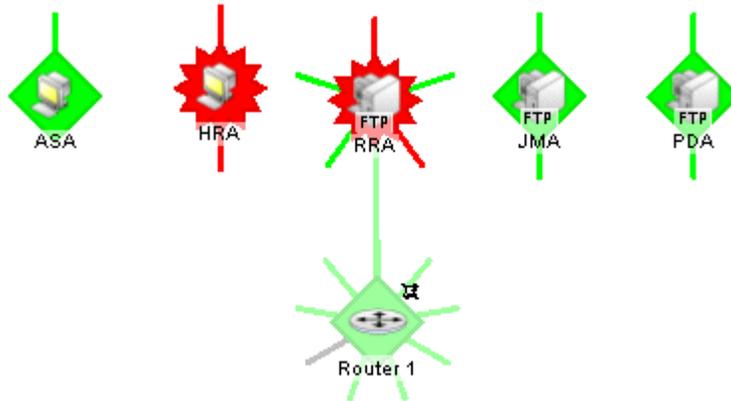
- 1 In the Map View toolbar, click an Annotation (Draw) icon to make it the active tool.
- 2 Drag the cursor onto a map to create a line, rectangle, circle, polygon, text, file image, or network cloud.

To change Annotation (Draw) tool properties, such as border width and color, select the annotation, then click **Properties** from the right-click menu.

About link lines

You can use Link lines to get a graphical view of the network link (the Interface service) between two devices. Link lines can also show the status of any service which has an Active Monitor on the device.

The following example shows a map with link lines displayed.



- Router 1 shows a connecting link to device RRA and this link is currently up. Also shown are eight unconnected links, all of which represent interfaces on the router. One of the unconnected links is disabled.
- JMA is a workstation that shows two unconnected links that are currently up. These are Ping and FTP monitors, found under **Device Properties > Active Monitors**.
- RRA is an FTP Server that is currently down and shows five unconnected links, two of which are down.

By default, links are rendered in one of four colors:

- **Green** indicates an Active Monitor that is up (for example, but not limited to, Interface). This includes services that have not yet been polled.
- **Red** indicates a down Active Monitor.
- **Gray** indicates a service listed in the device's Active Monitors list, but not currently monitored.
- **Orange** indicates that the device is currently in maintenance mode.



Note: These colors are subject to change if a user changes the colors of the default device states.

For more information, see *Using link lines* (on page 249).

Using attached lines

Attached lines show an arbitrary connection between devices. When you move two devices that are connected by attach lines, the attach lines also move. Attach lines are visual representations assigned by the user, and not a reflection of a true connection between the two devices. The true connection between the two devices is done with Link lines.

To draw an attached line:

- 1 In the Map View, right-click a device. The right-click menu appears.
- 2 Click **Attach > Attach to**. A line displays next to the cursor.
- 3 Click the device icon you want to attach to. WhatsUp Gold draws an attached line between the two devices.



Note: Each device can attach to up to five other devices.

Using the WhatsUp Gold Web Interface

In This Chapter

Accessing the web interface..... 63
About the WhatsUp Gold web interface..... 64

Accessing the web interface

You can connect to the WhatsUp Gold web interface from any supported browser by entering its web address. This web address consists of the hostname of the WhatsUp Gold host and the web server port number. The default port number is 80.

For example, if your WhatsUp Gold host is named `monitor1.ipswitch.com`, then the web address will be: `http://monitor1.ipswitch.com:80`.



Note: When you use the default port number (80), you do not have to include the port number in the address.

There are two default users on the Web server:

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

By default, the web server is disabled in the console. You have the option to enable the web server during installation, or on the console by going to **Configure > Program Options > Web Server**. Select **Enable web server on port**.



Note: You can also use Microsoft Internet Information Services (IIS) as the web server for WhatsUp Gold. For more information, see *Using IIS on Windows XP or Windows 2003* (on page 34) or *Using IIS on Windows Vista* (on page 37).

About the WhatsUp Gold web interface

The web interface allows you to view and modify almost all aspects of WhatsUp Gold using a web browser. From the web interface, you can add devices, view or modify device groups, view device maps, and access reports about your devices.

The web interface includes two features that are not available through the console:

- In WhatsUp Gold Premium, Distributed, and MSP Editions, Split Second Graphs display up-to-the-second information on SNMP and WMI performance counters for the devices on your network. Split Second Graphs can be viewed on the WhatsUp Gold Web Performance Monitor, the Web Task Manager, device and group performance reports, and several workspace reports.
- Full and workspace reports are only available through the web interface. From the console, you can launch a web browser to view reports in the web interface, but you cannot view the reports directly in the console.

There are also some features that are available in the console but are not available through the web interface:

- Advanced mapping features, such as annotations, link lines, and automatic arrangement of device icons are not available in the web interface.
- Device discovery is not available in the web interface, but you can add specific devices by IP address.

The web interface is organized into four main sections: the GO menu, the Home tab, the Devices tab, and the Reports tab.

About the GO menu

The main menu for the web interface is accessed using the GO button. The GO menu is similar to the Microsoft Windows Start menu. The GO menu allows navigation to other areas of the web interface with only a few clicks. It is always present in the top-left corner of the browser window, except when viewing dialogs.



With the GO menu, you can navigate to the areas you will use most in WhatsUp Gold, including your customized Home workspace views; your monitored devices list; Network Tools; the configuration of the Passive, Active, and Performance Monitor libraries; and the WhatsUp Gold Help.

About the Home tab

The Home Workspace is the first screen you see after logging in to the web interface. The Home Workspace is your customizable home page. It displays important information about the health of monitored servers and network devices in a way that can be tailored to your specific needs.

For more information on your Home Workspace, see *Customizing workspace views* (on page 275).

The Workspace Toolbar

- **Add Content.** Use this button to add workspace reports to your workspace views.
- **Workspace View.** Use this drop-down menu to edit your workspace views and to switch between workspace views.
- **Help.** Use this button to view the WhatsUp Gold Help for the window you are currently viewing.



About the Devices tab

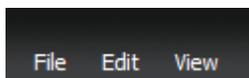
The Devices tab is used to view and manage the lists of devices you have added to WhatsUp Gold. The Devices tab has two modes:

- **Device View** shows a list of devices and groups formatted like a table.
- **Map View** shows the map that you configured for the current device group in the console.

You can add devices in either mode by using the Devices Menu or the Devices Toolbar located along the top edge of your browser.

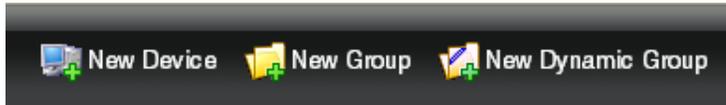
The Devices Menu bar

- **File.** Use this section of the menu to add new devices, device groups, and dynamic groups.
- **Edit.** Use this section of the menu to copy, move, edit, and delete devices and device groups. You can also access Device Status and Device Properties from this section.
- **View.** Use this section to switch between Device and Map views, to navigate to device groups, and to refresh the screen.



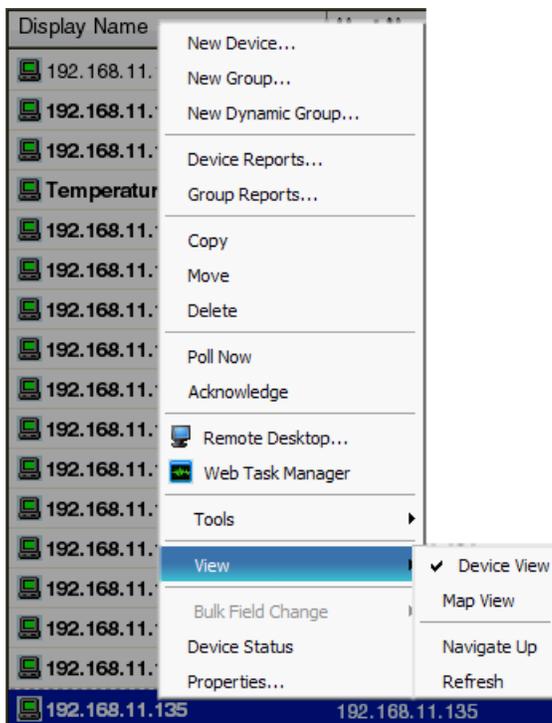
The Devices Toolbar

- **New Device.** Use this button to add a new device to your list of monitored devices.
- **New Group.** Use this button to add a new device group to your list of monitored devices.
- **New Dynamic Group.** Use this button to add a new dynamic group to your list of monitored devices.



The Right-Click Menu

You can also manage groups using the right-click menu, which includes quick links to many common tasks, tools, and reports.

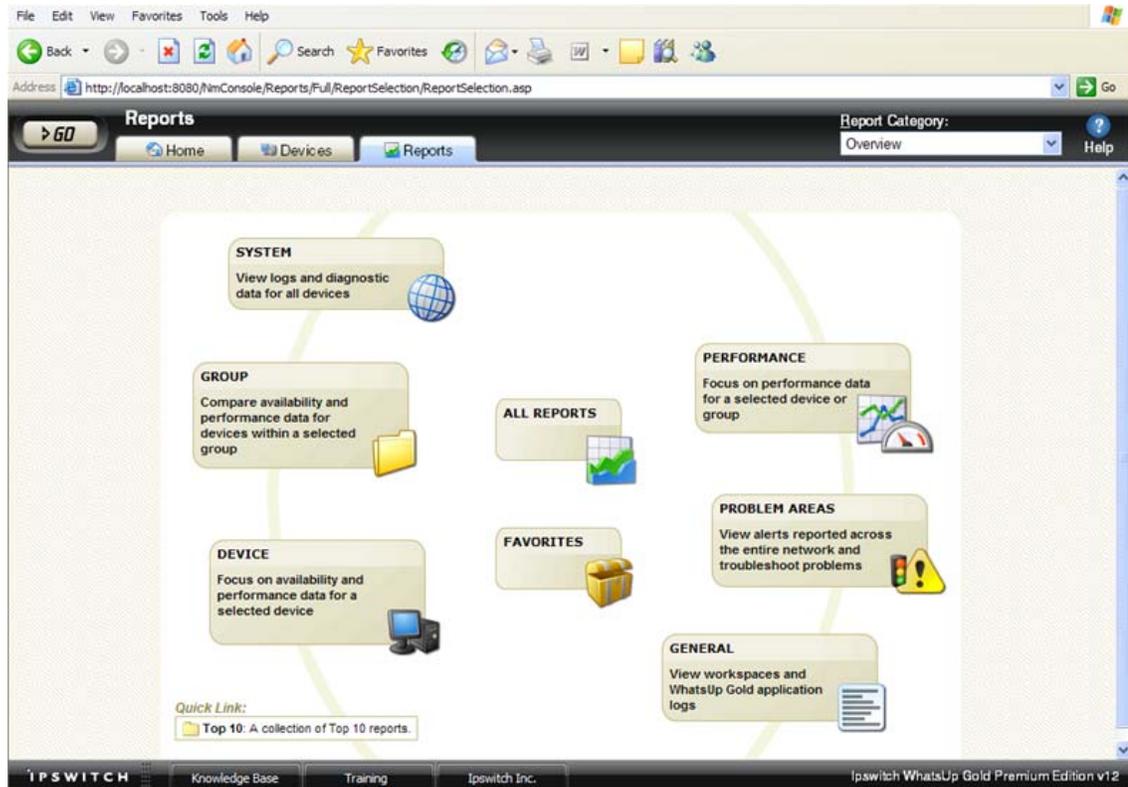


Drag and Drop

Just like in the console and most Windows applications, you can use your mouse to organize devices and groups using drag and drop in the web interface. You can drag devices from the device view or map view into device groups in the device groups list, in the list of devices and groups contained in the current group, or on a map.

About the Reports tab

The Reports tab is the starting point for launching Full Reports. When you select the Reports tab, the Reports Overview screen appears.

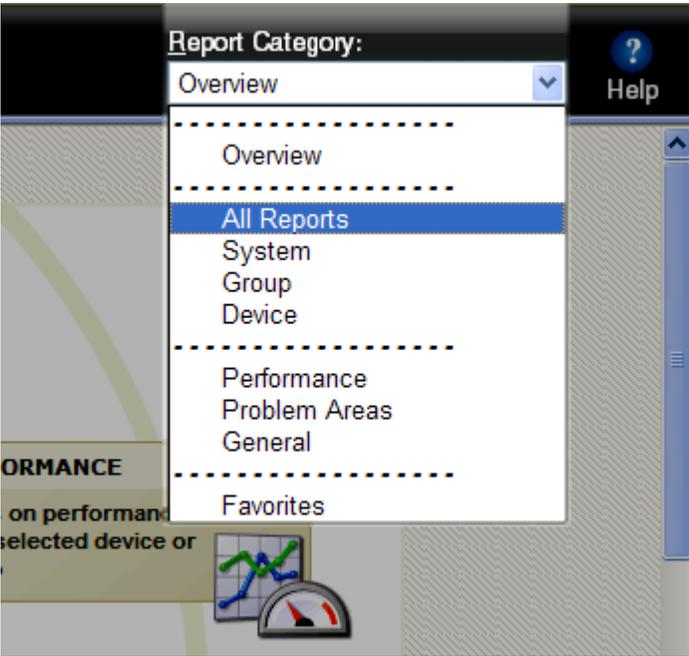


This screen divides the reports into several categories.

- **System** reports show logs and diagnostic data for all devices.
- **Group** reports allow you to compare availability and performance data for devices within a group.
- **Device** reports give a view into availability and performance data for a single device.
- **Performance** reports allow you to view historical performance data for a device or group.
- **Problem Area** reports provide an indication of typical problems that may be occurring on your network.
- **General** reports give you access to your workspaces and show you data logged by WhatsUp Gold during its operation (such as logs from active discovery).
- **All Reports** opens a page with links to every available report.
- **Favorite** reports is a customizable list of reports that you find useful.

Report Category menu

The Report Category drop-down menu allows you to jump to report category screens from where to choose reports for viewing.



About Users

In This Chapter

About user accounts	69
About user rights	72
About group access rights	74

About user accounts

User accounts in WhatsUp Gold define a person's role and determine what actions the person can perform.

Default user accounts

There are two default user accounts:

- 1 **Administrator account.** The Administrator 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 account.** The Guest account allows people 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 things in the application. The Administrator (or anyone else with **Manage User** rights) can modify the Guest account rights using the Manage Users dialog.

Additional user accounts

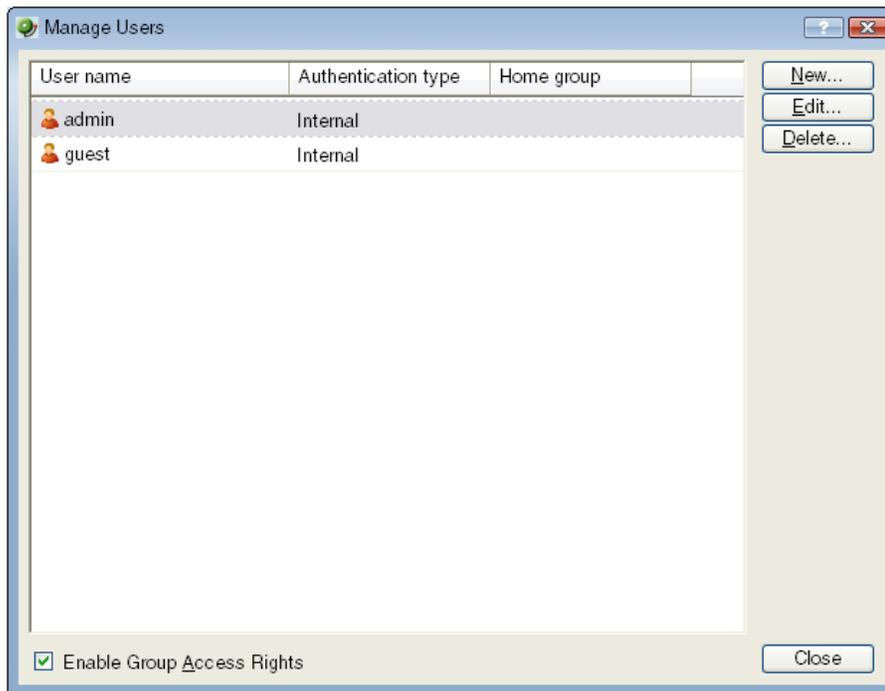
The Administrator can create additional user accounts as needed. There is no limit to the number of user accounts allowed on the system, though each additional account does increase the maintenance overhead for WhatsUp Gold. Each time permissions and rights are modified, the Administrator should verify that each user has only the intended rights.



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.

Creating and modifying user accounts

User accounts that are granted the **Manage User** right can create and edit user accounts.



To create a new or edit a WhatsUp Gold user account:

- 1 From the WhatsUp Gold web interface, select **GO**. The GO menu appears.
- 2 On the **WhatsUp** section of the **GO** menu, select **Configure > Manage Users**. The Manage Users dialog appears.
- 3 Click **New**. The Add User dialog appears.

- or -

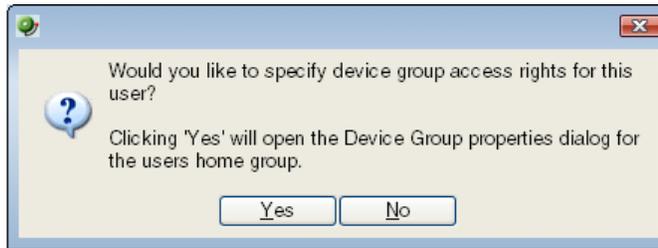
Select a user account and then click **Edit**. The Edit User dialog appears.

The screenshot shows the 'Add User' dialog box with the following details:

- User name:** Mitch
- Authentication type:** Internal
- Language:** English
- Internal password:** [masked]
- Confirm password:** [masked]
- Home group:** My Network
- User rights:**
 - General:**
 - Change Your Password
 - Configure Workspaces
 - Manage IP Security
 - Manage Web Server
 - Translations
 - Manage Workspace Views
 - Manage Users
 - Configure LDAP Credentials
 - Manage SNMP MIBs
 - Monitors / Actions:**
 - Configure Active Monitors
 - Configure Performance Monitors
 - Configure Actions
 - Configure Passive Monitors
 - Configure Action Policies
 - Manage Recurring Actions
 - Devices:**
 - Manage Groups
 - Access Active Discovery Results
 - Manage Devices
 - Configure Credentials
 - Reports:**
 - Check all rights

- 4 Enter the appropriate information.
 - **User Name.** Enter the name of the user.
 - **Authentication Type.** Select the method of authenticating the user.
 - **Internal.** Use the internal user database built in to WhatsUp Gold.
 - **LDAP.** Use an external LDAP database.
 - **Language.** Select the language to display for the user.
 - **Internal Password.** Enter a password for the user. This option is disabled if **Authentication Type** is set to LDAP.
 - **Confirm Password.** Confirm the user's password. This option is disabled if **Authentication Type** is set to LDAP.
 - **Home Group.** Select the device group that the user will see when they log into the WhatsUp Gold web interface. If they have the correct group access rights, they will be able to navigate out of this group.
 - **User Rights.** Select the rights that correspond to the actions you want to allow the user to complete.
 - **Check all rights.** Select this option grant the user rights to perform all of the actions listed.

- 5 Click **OK** to save changes.
- 6 If you have enabled Group Access Rights, you will be prompted if you would like to specify Group Access Rights for the new user account.



Select **Yes** to open the Device Group Properties dialog for the user's home group.

- or -

Select **No** to close the dialog and return to the Manage Users 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 can manage user rights on the Add/Edit User dialog in the web interface.



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.

General	
Change Your Password	Enables users to change their own password.
Configure Workspaces	Enables users to add workspace views as well as configure, move, and delete workspace reports within workspace views.
Manage IP Security	Enables users to control access to the web interface based on specific IP addresses.
Manage Web Server	Enables users to change the configuration of the web server.
Translations	Enables users to view the translation system as well as import and export languages.
Manage Workspace Views	Enables users to add, delete, and copy workspace views, as well as edit the properties of a specific workspace view.
Manage Users	Enables users to create and edit users for the web interface. This option also allows users to specify Group Access Rights.

Configure LDAP Credentials	Enables users to configure LDAP credentials for connecting to an LDAP server for user authentication in the web interface.
Manage SNMP MIBs	Enables users to download and delete SNMP MIBs through the SNMP MIB Manager.
Monitors/Actions	
Configure Active Monitors	Enables users to create, edit, and remove active monitors 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 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.
Configure Action Policies	Enables users to create, edit, and remove action policies 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.
Devices	
Manage Groups	Enables users to create, edit, or remove device groups on the network.
Access Active Discovery Results	Enables users to access the Active Discovery Results dialog. Granting users access to this dialog also enables users to add devices to the network and to add Active Monitors, and Performance Monitors to a device.
Configure Credentials	Enables users to configure SNMP and Windows credentials.
Manage Devices	Enables users to add new devices and edit existing devices in the groups in which the user has access.
Reports	
Access Group and Device Reports	Enables users to view group and device reports for the groups the user has access.
Access System Reports	Enables users to view system reports.
Access Split Second Graph Reports	Enables users to view Split Second Graph reports in workspace and full reports.
Remote	
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.

About Remote User Rights

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.

About group access rights

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.

Group access rights are useful when users need to view and edit only those groups that matter to them, as would be the case with a large network with multiple network administrators. Group access rights allow an administrator to grant each user rights to only the devices on the network for which that user is responsible.

Types of group access rights

There are four types of group access rights:

- 1 **Group Read.** This right allows users to view items within the selected group and pertaining to that group, including the group's reports, map, and device list.
- 2 **Group Write.** This right allows users to edit group properties and add, edit, and delete devices and subgroups within the selected group.
- 3 **Device Read.** This right allows users to view the device properties and device reports of all devices within the selected group.
- 4 **Device Write.** This right allows users to edit the device properties of any device within the selected group and to delete the device from the group.



Note: To add a device to a group, a user must have Group Write rights to the group. Device Write rights allow users to modify and delete existing rights, but do not allow them to add new devices to the group.



Tip: When enabled, group access rights are applied throughout WhatsUp Gold. Device and group pickers, reports, and group views all respect what a user account is granted permission to view and edit.

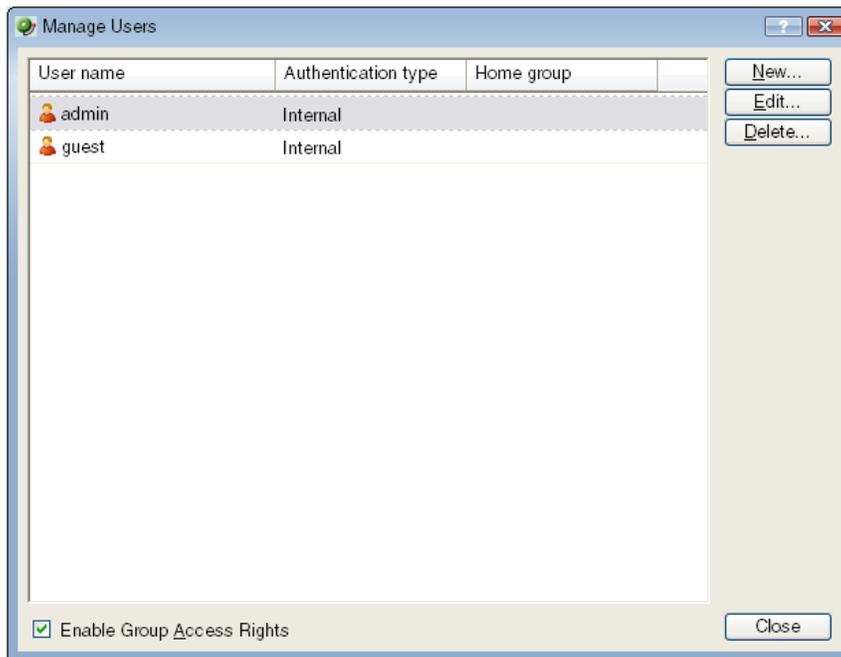
The following is a list of operations and the group access rights that must be assigned for the user to perform that task:

- List, Map, and Group reports 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 and Device Reports requires **Device Read**.

Modifying Device Properties, Bulk Field Change, and Acknowledgement require **Device Read** and **Device Write**.

Enabling group access rights

Group access rights may be enabled and disabled from the Manage Users dialog.



To enable group access rights:

- 1 From the WhatsUp Gold web interface, select **GO**. The GO menu appears.
- 2 On the **WhatsUp** section of the **GO** menu, **Configure > Manage Users**. The Manage Users dialog appears.
- 3 Select **Enable Group Access Rights** at the bottom of the dialog. The setting is immediately saved.

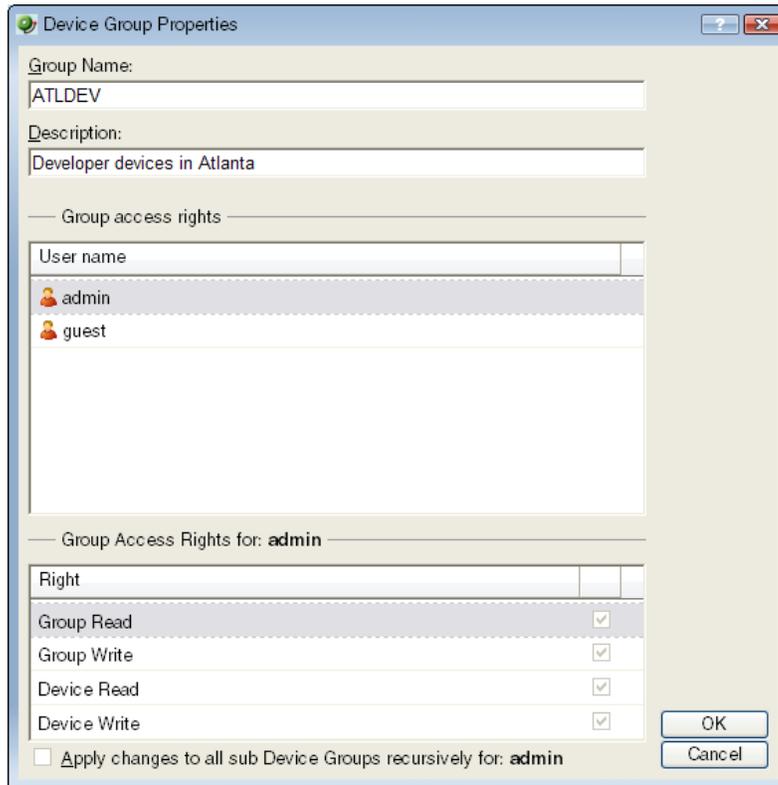
Simply enabling group access rights does not ensure that the rights are set up the way that you want. You also need to assign group access rights to each group on your network.

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 Group Properties dialog, you can add and edit the access rights for the selected group.



Important: You must enable 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 will have to enable group access rights in the Manage Users dialog (On the **GO** menu, from the **WhatsUp** section, **Configure > Manage Users**).



Note: 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 group access rights* (on page 74).

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 group access rights and user access right

When group access rights are enabled, WhatsUp Gold determines effective rights by first negotiating user rights, then group access rights. This means that, while 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 78).

Managing Devices

In This Chapter

Device overview.....	81
About the Device View	82
Learning about the Device Properties	82
Adding a new device.....	94
Selecting Device Types.....	98
Using Acknowledgements	100
Editing multiple devices with Bulk Field Change	101
Using Credentials	103
Creating Custom Context menus	103

Device overview

In WhatsUp Gold, devices are virtual representations of resources (computers/workstations, servers, routers, switches, etc.) that are connected to your computer through a LAN (Local Area Network), a wireless network, or even over the Internet. WhatsUp Gold watches these devices through a network connection. When those network resources are cannot be reached by WhatsUp Gold, the device is considered down and an action can be configured to fire.

Device Services

WhatsUp Gold associates Active Monitors with devices on your network. Active monitors query the network services installed on a device and then wait for a response. These monitors query the services running on a network resource, checking to make sure that the FTP server, web server, email server, etc., is up and responding. Active Monitors include DNS, SNMP, Telnet, Ping, TCPIP, and NT Service. If a response is either not received or is not what is expected, the service is considered down. If the query is returned as expected, the service is considered up.

For a more information about service monitors, see *Active monitors overview* (on page 157).

About the Device View

This view provides an overview of each device in a selected group. Each device's icon provides information about its status. In addition, the Status column indicates which specific active monitor is down and the duration of the interruption. When the entry in the Device list is a group folder, the Status column shows the number of devices in the group with a breakdown of how many devices are in each device state.



Note: Dynamic groups will not show information about the number of devices in a group or a breakdown of how many devices are in each device state in the Status column. For more information, see Using Dynamic Groups.

Following is an example of a device list.

Display Name	Host Name	Address	DeviceType	Status
Routers NorthPoint HRA ASA JMA RRA JTA Hub1	NorthPoint HRA ASA JMA RRA JTA Hub1	156.21.50.130 156.21.50.15 156.21.50.129 156.21.50.107 156.21.50.27 156.21.50.182 156.21.50.100	Server Workstation HP Device Wireless Access Point Workstation Workstation Workstation	 <u>Interface[35:E3](Down at least 20 min)</u> <u>FTP(Down)</u>

The indicators in the Display Name column show the current state of the items in this group.

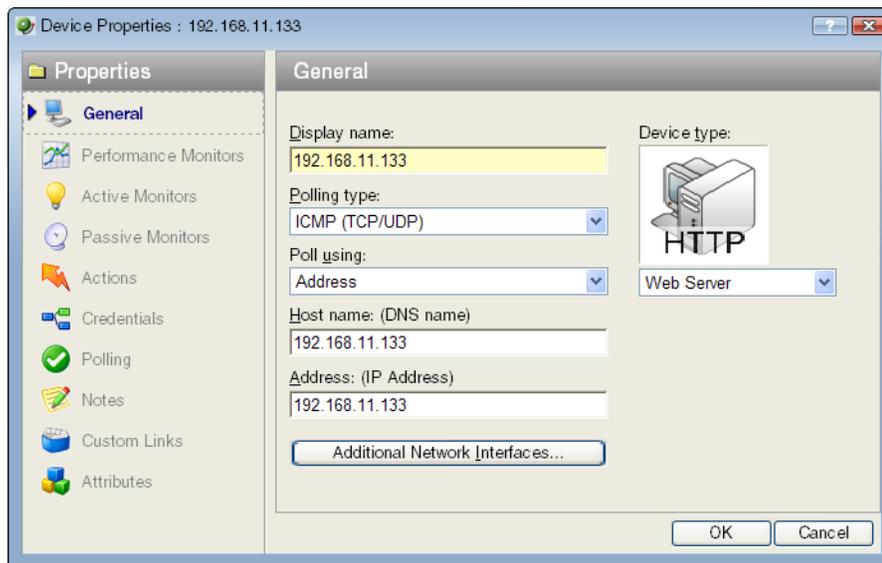
- Routers is a dynamic group.
- Device NorthPoint is a server that is currently up. The icon shows that this device is also in another device group.
- Device HRA is a workstation that is currently up.
- Device ASA is an HP Device that is up, but one of the interfaces (E3) is not responding.
- Device JMA is a wireless access point that is currently in maintenance mode.
- Device RRA is a workstation that is currently up. Its icon shows that this device is also in another device group.
- Device JTA is a workstation that is currently responding to polls, but it has a monitor (FTP) that is down.
- Device Hub 1 is in an unknown status because the device has not been polled. In this case, it is due to a down dependency set on the Router.

Learning about the Device Properties

You can modify individual device properties by right-clicking a device icon in either the **Device View** or **Map View**, then selecting **Properties**. Following is an overview of the device properties available to use in WhatsUp Gold.

About General Device Properties

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.

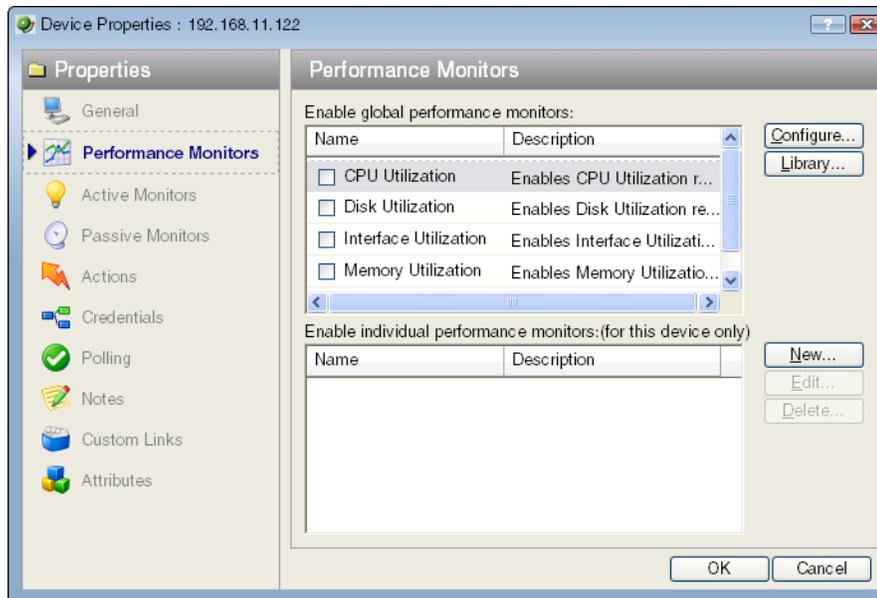
- **Host name (DNS).** This should be the official network name of the device if the polling method is ICMP. The network name must be a name that can be resolved to an IP address. If the polling method is NetBIOS or IPX, this must be the NetBIOS or IPX name.
- **Address.** Enter an IP or IPX address.
- **Additional Network Interfaces.** Click this button to configure an additional Network Interface for the current device.
- **Device Type.** Select the appropriate device type from the pull-down menu. The icon displayed will represent the device in all views.

About Device Property Performance Monitors

Use Performance Monitors dialog to configure and manage performance monitors for the selected device.



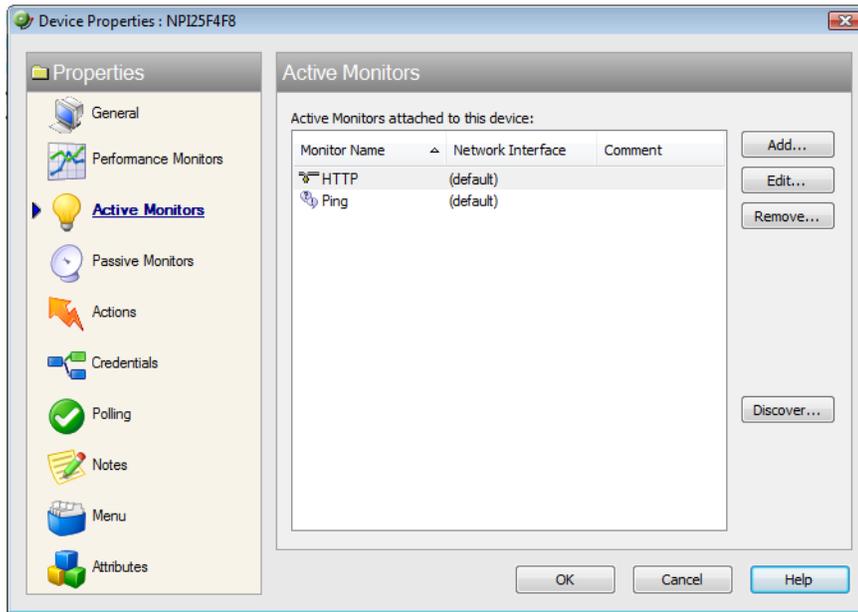
Note: For some performance monitors, the SNMP credential on the device must be configured. For WMI performance monitors, the Windows credential is required.



For more information, see *Performance monitor overview* (on page 213).

About Active Monitor Device Properties

Use the Active Monitors dialog to display and manage Active Monitors for this device. There are several ways an Active Monitor can be added to this list: You can manually add the monitor by clicking the **Add** button on this dialog, click the **Discover** button to have WhatsUp Gold scan the device for all Active Monitors. Monitors may have been added during initial discovery, when WhatsUp Gold first added the device to the database.

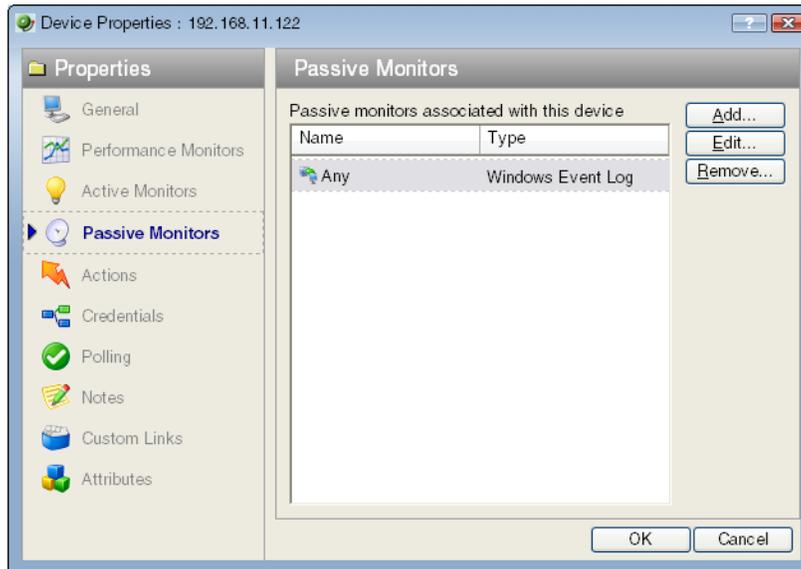


- Click **Add** to configure a new Active Monitor.
- Select an Active Monitor and click **Edit** to change the configuration.
- or -
Double-click an Active Monitor to edit the configuration.
- Select an Active Monitor and click **Remove** to remove the monitor from the device.
- On the WhatsUp Gold console, you can click **Discover** to have WhatsUp Gold scan the device for Active Monitors on the device.

For more information, see *Active monitors overview* (on page 157).

About Passive Monitor Device Properties

Some elements on a network may not provide a clear up or down status when queried. For example, a message may get logged to the system's Event log by another application (such as an antivirus application alerting when a virus is found). Because these messages/events can occur at any time, a Passive Monitor Listener listens for them, and notifies WhatsUp Gold when they occur.



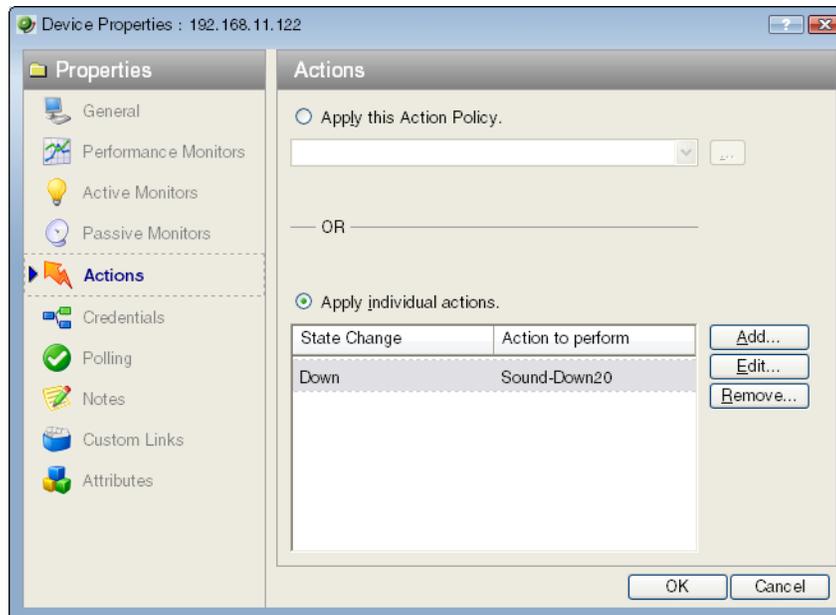
This dialog displays all Passive Monitors configured for this device.

- 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.

For more information, see *Passive monitor overview* (on page 205).

About Device Property Actions

You can select an Action Policy to use on this device or configure alerts specifically for this device.



Select a policy from the **Apply this Action policy** pull-down menu. You can also create a new, or edit an existing action policy by clicking the **Browse** button next to the pull-down menu box.

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.

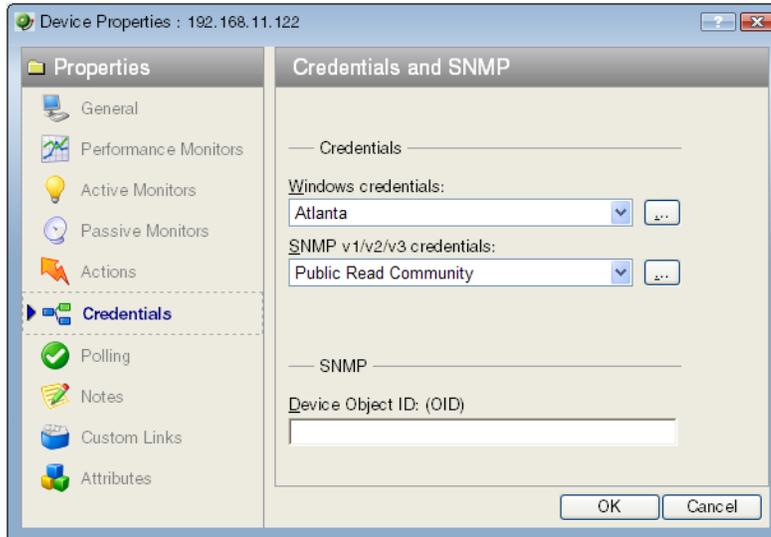
This dialog displays all Actions configured for this device.

- 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.

For more information, see *About actions* (on page 125).

About Device Property Credentials

The Credentials dialog displays **Windows and SNMP credentials** information for the current device.



Devices that are SNMP manageable devices appear on the map view with an icon with a white star in the top right corner.

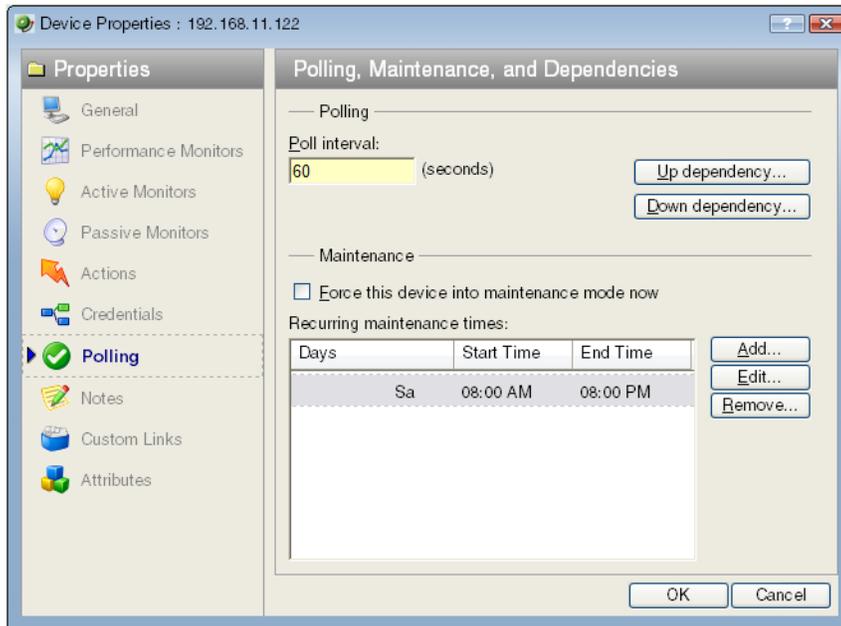


- **Windows credentials.** Select the Windows credential to connect to this device. Click the browse (...) button to browse the Credentials Library.
- **SNMP v1/v2/v3 credentials.** Select the SNMP credentials to connect to this device. If the **Identify devices via SNMP** option was selected during 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. Click the browse (...) button to browse the Credentials Library.
- **Device Object ID (OID).** The SNMP object identifier for the device. This identifier is used to access a device and read other SNMP data.

For more information, see *Credentials overview* (on page 103).

About Device Property Polling

Polling is the term used for monitoring discovered devices in WhatsUp Gold. The Polling dialog lets you configure polling options and/or schedule maintenance times for the selected device.



Polling

- **Poll interval.** This number determines how often WhatsUp Gold will poll the selected device. Enter the number of seconds you want to pass between polls.
- **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 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, but it remains in the device list with an identifying icon. By default, the maintenance state is represented by an orange background color.

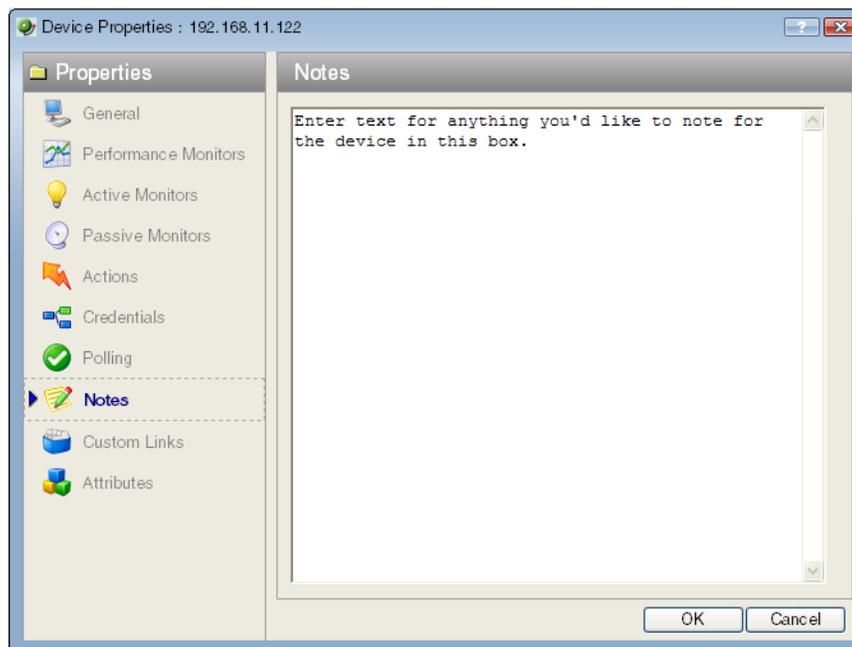
- **Force this device into maintenance mode now.** Select this option to put the selected device in maintenance mode. Clear the option to resume polling the device.
- **Recurring maintenance times.** This box displays all scheduled maintenance times for the device.
 - Click **Add** to schedule a new 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 115) and *Dependencies overview* (on page 117).

About Device Property Notes

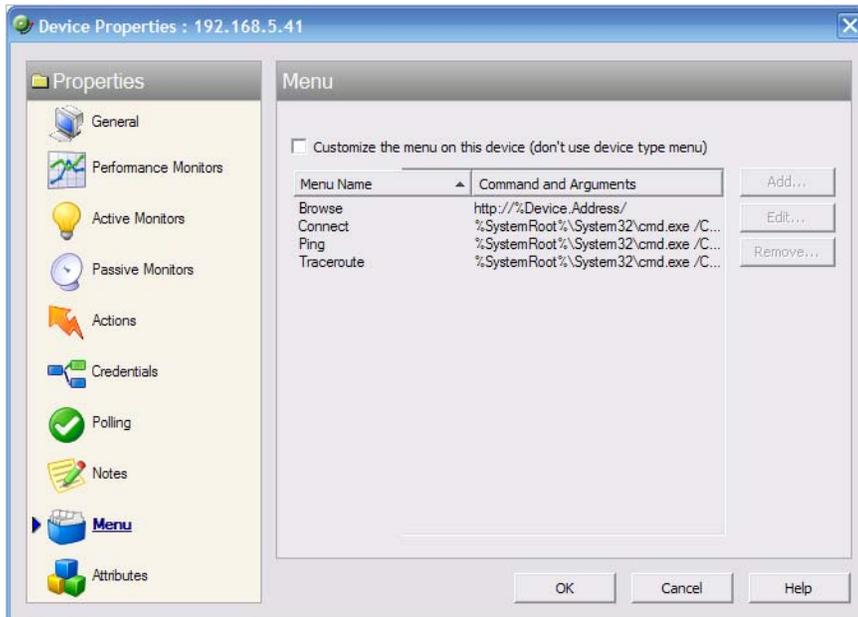
The Notes dialog provides an option to enter free-form messages to the device database.



About Device Property Menus

In the WhatsUp Gold console, you can use the Menu dialog to create a custom context menu for a device. After a new option has been configured, it appears on the context menu when you right-click the device in the device list.

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.



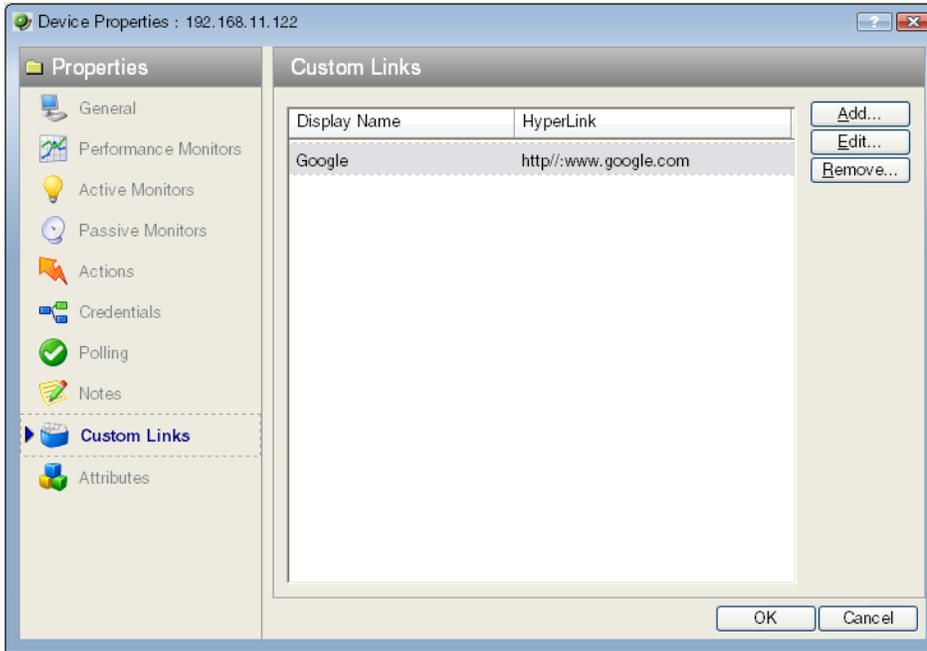
- **Customize the menu on this device (don't use device type menu).** Select this option to create and/or modify a context menu for this device. This will override any separate context menu that has already been created for the device type of the device.
- **Menu list.** This box displays the commands 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.



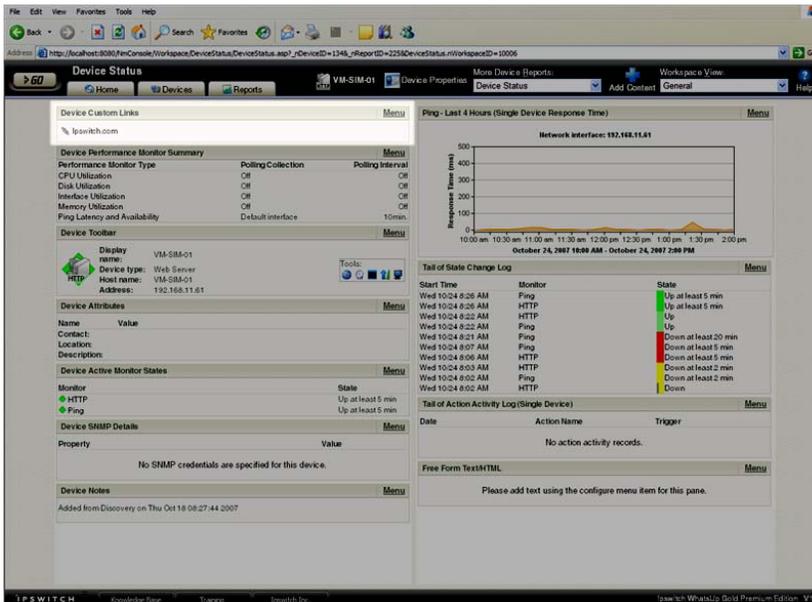
Important: Menu items can only be configured on the WhatsUp Gold console.

About Device Property 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 workspace report to its Device Status workspace view. For more information, see *Adding workspace reports to a Device Status workspace* (on page 278).



- 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.

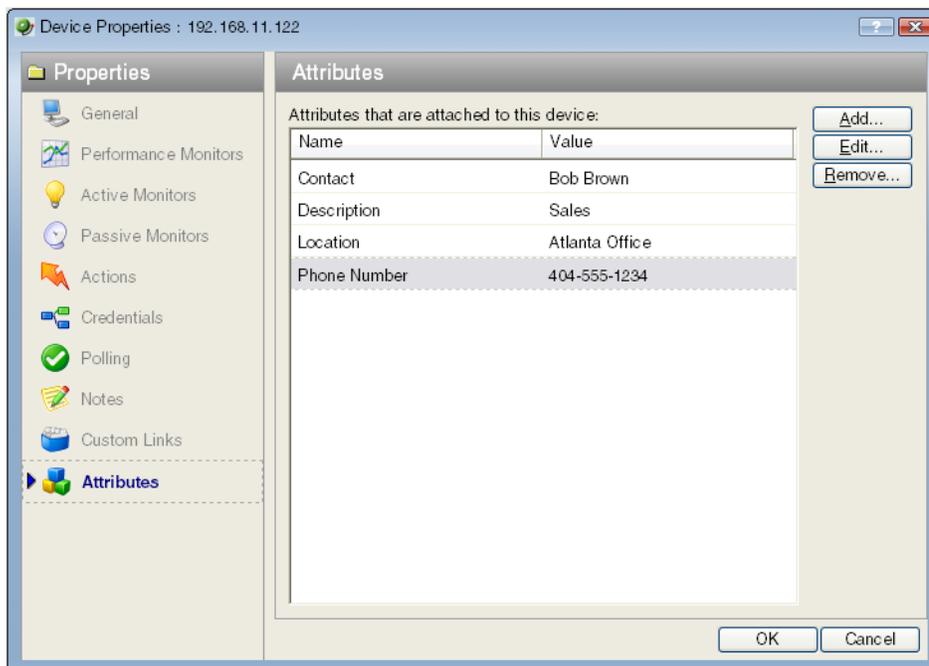
- Select a custom link in the list, then click **Remove** to remove it from the list.



Important: Custom links are only configurable and viewable in the web interface.

About Device Property Attributes

The Attributes dialog lists attributes that are associated with a 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.



- Click **Add** to add a new attribute.
 - Select an attribute on the list, then click **Edit** to change the settings.
- or -
- Double-click an attribute to edit its configuration.
- Select an attribute in the list, then click **Remove** to remove it from the list.

Adding a new device

There are two ways to add devices to the monitoring database:

- Discover devices automatically. For more information, see *Using the Device Discovery wizard* (on page 43).
- Manually add devices.

To manually add a new device:

- 1 In the Device view, right-click, then select **New Device**. The Add New Device dialog opens.



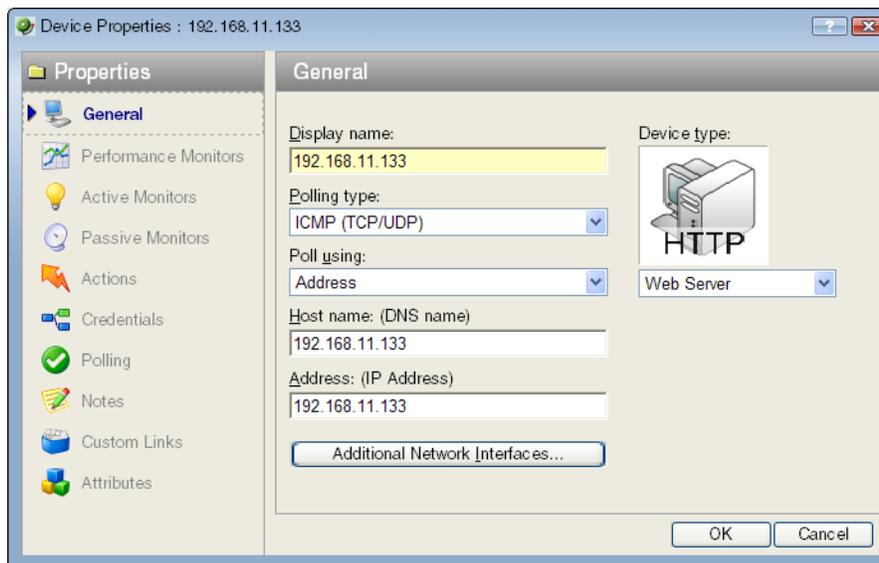
- 2 Enter the IP address or hostname for the device you want to add.
- 3 Click **Advanced** to select a number of additional options for which to scan the device.
- 4 If you want to add a device without scanning, select **Add device immediately without scanning**. This immediately adds a "bare-bones" device, generically categorized as a workstation.
- 5 Click **OK** to save changes. The WhatsUp Gold attempts to resolve the IP address or hostname, then scans that device for Active Monitors. When the scan is complete, Device Properties dialog opens, allowing you to further configure the device as needed.

Adding additional network interfaces to a device

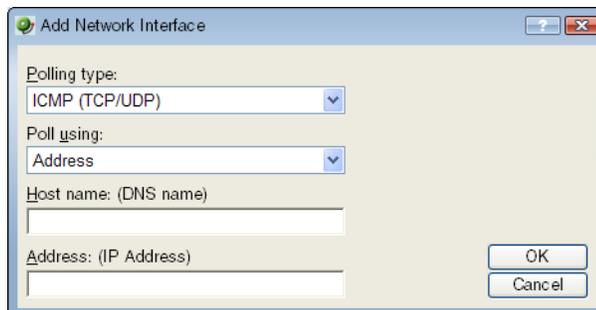
To configure a network interface:

- 1 Right-click a device, then click **Properties**. The Device Properties dialog appears.

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



- 3 Click **Additional Network Interfaces**. The Add Network Interfaces dialog appears.
- 4 Click **Add**. The Add Network Interfaces dialog appears.



- 5 Enter the network information for the new interface.
- 6 Click **OK** to return to the General section.

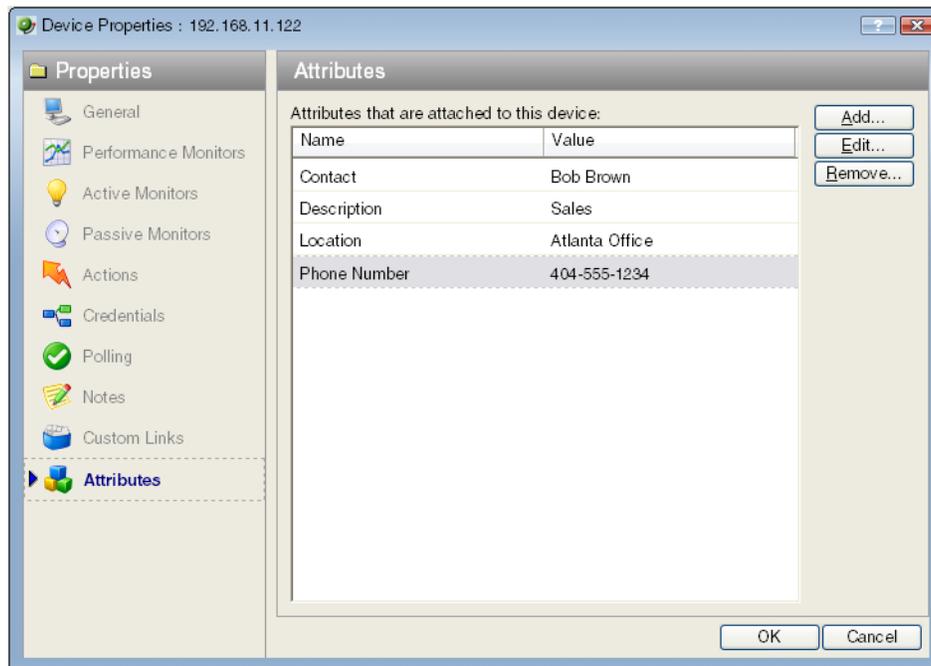
To change the default network interface on a device:

- 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 attributes to a device

To add attributes to a device:

- 1 Right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Attributes**. The Attributes dialog appears.



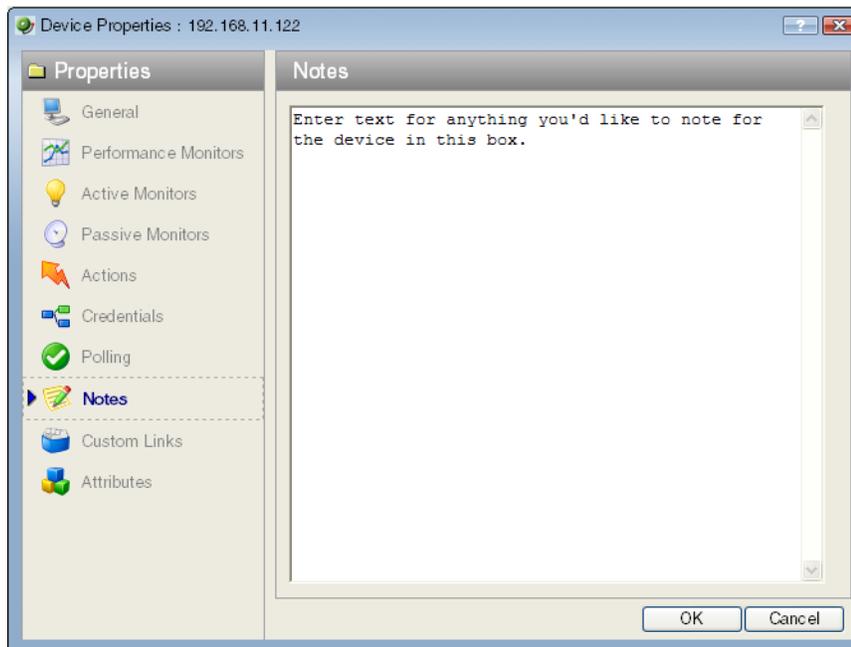
- 3 Use the following options:
 - Click **Add** to add a new device attribute. The Add Attribute dialog appears.
 - Select a device attribute in the list, then click **Edit** to change the settings.
 - Select a device attribute in the list, then click **Remove** to remove it from the list.
- 4 Enter information in the **Attribute name** and **Attribute value** boxes.
- 5 Click **OK** to save changes.

Adding notes to a device

To add a note to a device:

- 1 Right-click a device, then click **Properties**. The Device Properties dialog appears.

- 2 Click **Notes**. The Notes dialog opens.



- 3 Enter the note in the **Notes** box.

Notes. The first line of the notes box displays information about when the device was added to the database.

You can customize the notes with any information you want to include about the device. For example, you may want to record historical information about a device, physical location information, or perhaps 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.

Changing a device IP address

To change a device IP address:

- 1 In Device view, right-click a device. In the context menu, select **Properties > General**.
- 2 Enter the new IP address in the **Address** box.
- 3 Click **OK** to save changes.

Changing a device name

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

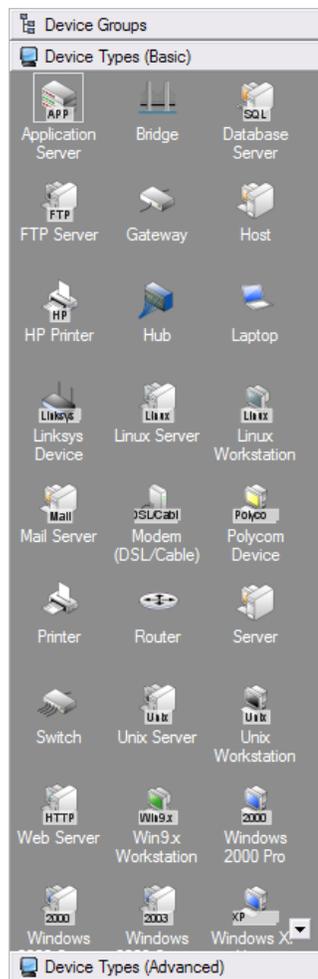
To change a device name:

- 1 In Device view, right-click a device. In the context menu, click **Properties > General**.

- 2 In the General section of Device Properties, enter the new name in the **Display Name** box.
- 3 Click **OK** to save changes.

Selecting Device Types

In the left-hand pane of the WhatsUp Gold console interface, the Device Types (icons representing the types of devices you may have on your network) appear.



Click the tab at the bottom of the pane to switch from **Device Types (Basic)** to **Device Types (Advanced)**.

You can select a device type in the Device Properties General dialog on the console or web interface. For more information about selecting a specific device types for existing devices, see *About General Device Properties* (on page 83).

Configuring Device Types

To create a device type:

If you want Device Discovery to use a special icon when it finds this device, make sure you have run the MIB extractor.

- 1 From the console, click **Configure > Device Types > New**.
- 2 Enter a **Device Type Name** for the new device.
- 3 In the **Icon filename** box, browse to a graphic file to represent the device.
- 4 In the **Overlay text** box, you can enter a word or two which will overlay the device icon to help differentiate this device. For example, `HP Laser` to help differentiate this device from other printers which use the same icon.
- 5 Select the device **Polling type**.
- 6 (Optional) In the **SNMP Object ID** text box, enter an SNMP identifier (or use the browse button `...` to find one) that corresponds to a vendor device type; this is usually found in the **private > enterprises** section of the MIB tree, under the vendor name.

Device discovery finds and maps devices using the SNMP identifiers to locate the specified devices. To scan for devices, you must also enter the proper Community name.

You can use multiple identifiers. For example, suppose a manufacturer named Acme makes three devices: the Acme 4500, the Acme 4501, and the Acme 4502. You could define one device type to represent any Acme device in the 4500 series; in the SNMP Object box, you would enter the three SNMP identifiers for the Acme 4500, 4501, and 4502. The Scan tool will use the icon for any of the three devices.

You need to separate multiple SNMP object identifiers by using semi-colons. The last number in the identifier can be an asterisk, a range using hyphens, or contain multiples separated by commas. For example:

1.3.6.1.4.1.311.1.1.3.1.3

1.3.6.1.4.1.311.1.1.3.1.3;1.3.6.1.4.1.311.1.1.3.1.4

1.3.6.1.4.1.311.1.1.3.1.3,4

1.3.6.1.4.1.311.1.1.3.1.1,3-4

1.3.6.1.4.1.311.1.1.3.1.*

- 7 Click **Next** to save the new device type, and access the Active Monitor dialog for device types.
- 8 Click **Add** to add an active monitor for the device type.
- 9 Click **Next** to access the Passive Monitor dialog for device types.
- 10 Click **Add** to add a passive monitor for the device type.
- 11 Click **Next** to access the Context Menu dialog for device types.
- 12 Click **Add** to add a context menu for the device type.
- 13 Click **Next** to access the Action Policy dialog for device types.
- 14 Associate an action policy, or click the browse button to create or edit an action policy.
- 15 Click **Finish** to save the new device type.

Changing Device Types

Device Types act like templates for new devices, containing device properties (such as active and passive monitors, menu items, etc.) and represented by different icons in Device Properties and on the Map view.

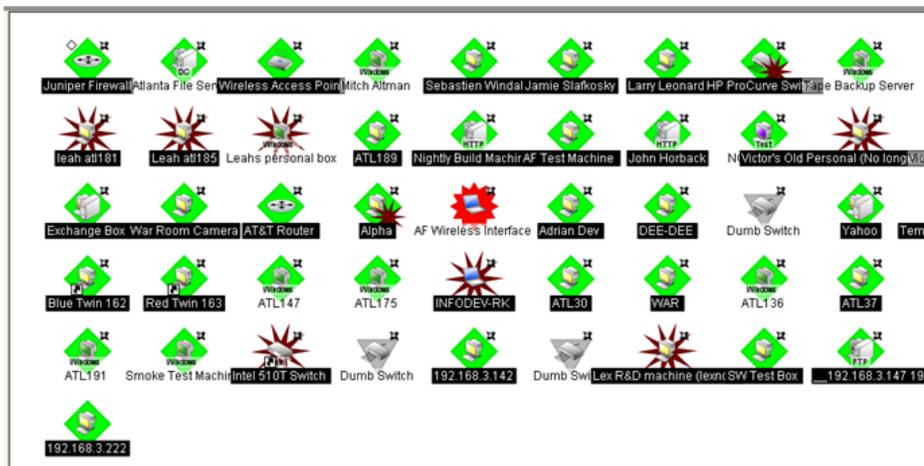
When you change a device type on an existing device, you are only changing the icon that represents the device, and not adding additional information and settings to the device. All other changes will have to be done manually.

To change a device type icon on an existing device:

- 1 In Device view, right-click on a device, then select **Properties > General** from the context menu.
- 2 In the **Device type** list, select a new device type.
- 3 Click **OK** to save changes.

Using Acknowledgements

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



After the device is in Acknowledgement mode, it will remain 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.

To acknowledge a state change:

- Select the device or devices you want to acknowledge, right-click, then click **Acknowledge**.



- or -

- Access the State Change Acknowledgement report and select the devices you want to acknowledge. After the devices are selected, click **Clear** to remove the devices from the report, thereby acknowledging the state change.

Editing multiple devices with Bulk Field Change

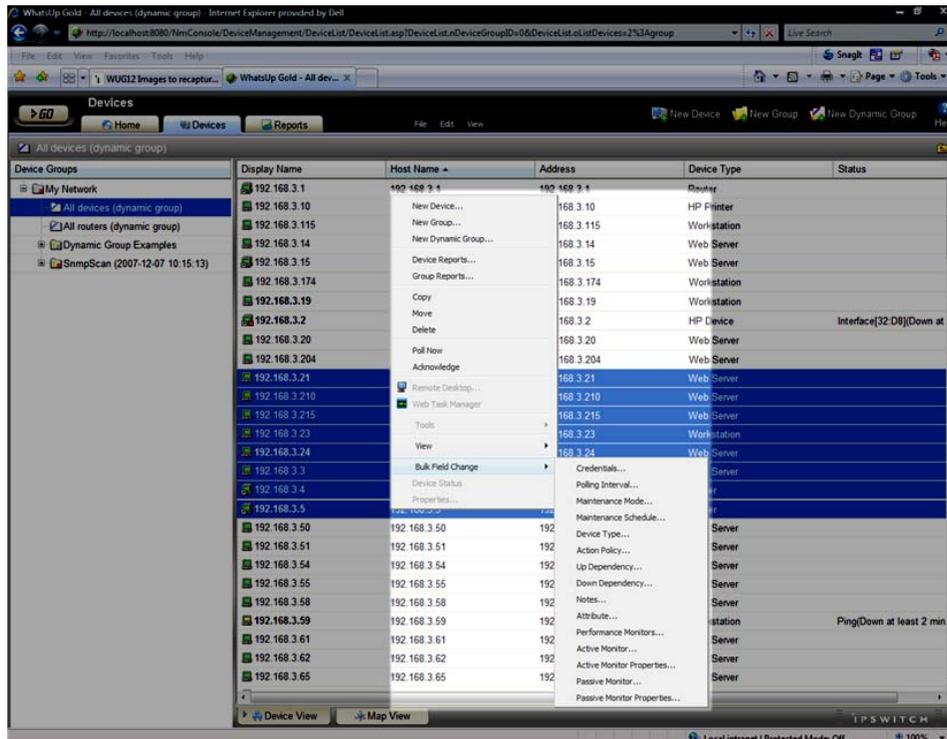
The Bulk Field Change feature gives you the ability to make changes to multiple devices and device groups. You must have administrative privileges to the devices or device groups that you want to make changes to.

To edit multiple devices:

- 1 Select the devices or device groups you want to change, right-click and select **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 field 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 that you want set.
 - 4** Click **OK** to save changes.

Using Credentials

The Credentials system stores login or community string information for Windows (WMI Active Monitors, WMI Performance Monitors, and the Web Task Manager) and SNMP devices in the WhatsUp Gold database. The system supports SNMP v 1, 2, and 3.

Credentials are configured in the Credentials Library (found on the web interface menu in the **WhatsUp** section of the **GO** menu at **Configure > Credentials Library**) and used in several places throughout the application. They can be associated to devices in **Device Properties > Credentials**, or through the **Credentials Bulk Field Change** option.

A device needs SNMP credentials applied to it before SNMP-based Active Monitors will work. Similarly, NT Service Checks must have Windows credentials applied.

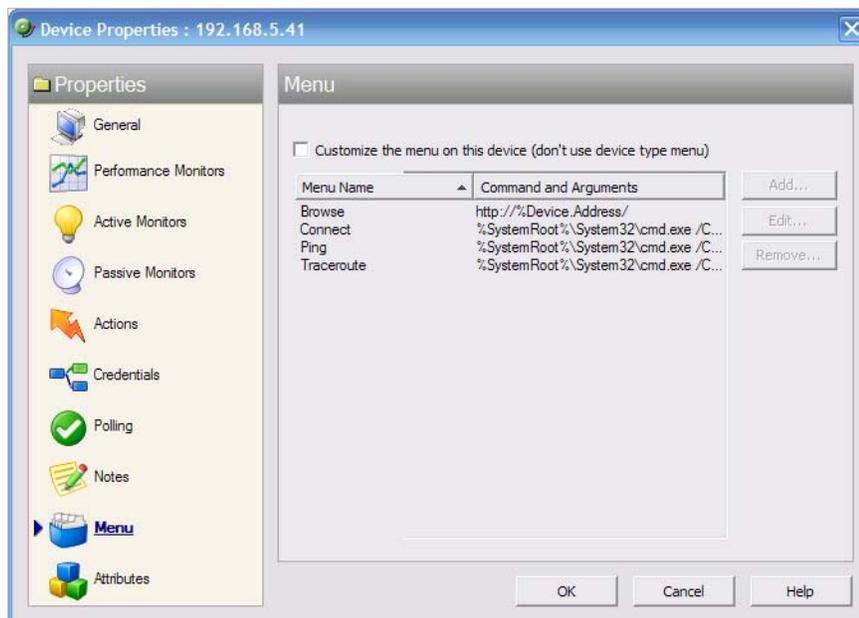
Creating Custom Context menus

You can create custom context menus for WhatsUp Gold in the console. When you create a custom context menu, it is available in the right-click menu for devices. When the menu item is selected, the associated command is executed with the arguments that were entered in the menu configuration options.

To create a custom menu:

- 1** Double-click the device you want to edit, the Device Properties appear.

- 2 Click **Menu**. The Device Properties Menu dialog appears.



- 3 Click to select the **Customize the menu on this device (don't use device type menu)** option.
- 4 Click **Add**. The Add Menu Item dialog appears.
- 5 Enter information in the **Display name**, **Command**, and **Arguments** boxes.
- 6 Click **OK** to save changes. The custom menu is added to the device's context menu.

Using Device Groups

In This Chapter

About device groups.....	105
About Dynamic Groups.....	107
Building Dynamic Groups.....	114

About device groups

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

Device group types

Two types of device groups exist in WhatsUp Gold:

- Non-dynamic groups
- Dynamic groups

Non-dynamic groups are simply referred to as "device groups." Each time you discover devices on your network, a new device group is created containing the devices found in the scan that you choose to monitor. The group is named using the type of scan you used during discovery, and the date and time the scan took place. For example, "SNMPScan (2007-08-03 10:24:37)." Devices that are already in the database are added to the new group as a shortcut to the original device reference. This is only to relay that there are more than one reference in the My Network tree, as you configure devices by clicking either the original reference icon or the shortcut. Functionally, they serve the same purpose and display the same device status.

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

Device group icons

Just as devices in WhatsUp Gold, device groups use icons to display the current state of the group, or to indicate the type of device group.

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

Device group maps

The Map View is based on device group folders, meaning that each device group will have a separate map. If a device group folder contains a subfolder, or subgroup, you can double-click on the folder in Map View to display the subfolder's map.

Device group reports

Device groups are particularly important when you are viewing full and workspace reports pertaining to a specific group, or group reports. When viewing Group Reports, you choose one specific device group in which to view network data. It's a good idea to think of ways to easily distinguish device groups from one another for this reason. An easy way to distinguish groups is using group names that are meaningful, such as "Atlanta Developers" and "Atlanta Tech Support." As a result, you can easily tell what each device group is when choosing a group on which to view Group Report information.

Device Group Access Rights

Similar to user rights are the WhatsUp Gold group access rights which link permissions to device groups. For more information, see *About group access rights* (on page 74).

Creating device groups

To create a new device group:



Important: You cannot create a new device group within a dynamic group.



Note: There is a separate procedure for creating new dynamic groups.

On the WhatsUp Gold console

- 1 Select **File > New Group**. A new device group appears in the My Network Tree named "New Device Group." You will need to rename this group.
- 2 To rename the group, select the new group and right-click. The right-click menu appears. Select **Rename** and enter a new name for the group.

On the WhatsUp Gold web interface

- 1 From the Devices tab, click the **New Group** button.



- or -

From the Devices tab, select **File > New Group**.

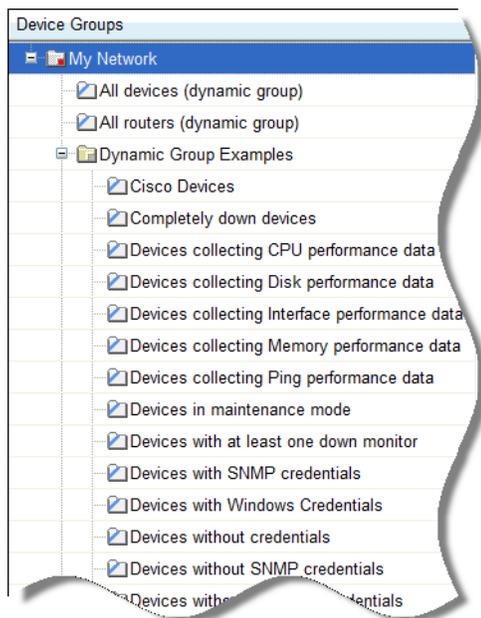
The Create Group dialog appears.

- 2 Enter a title and short description for the group in the **Group Name** and **Description** fields.
- 3 Click **OK** to add the group to the My Network tree.

About Dynamic Groups

This feature provides the ability to create device groups based on whatever criteria users choose, without having to create device shortcuts. Dynamic groups can be created for specific device types, device attributes, active monitors, or anything else that is stored for individual devices in the database. Dynamic groups act as SQL queries that run on the WhatsUp Gold database, and can display real-time data if viewed through a report that is set to automatically refresh.

WhatsUp Gold is pre-configured with dynamic group examples, which you can see in the Devices view, under Device Groups.



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

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



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

To configure Dynamic Groups:

- 1 In the WhatsUp Gold web interface, right-click on the device view, then select **New Dynamic Group**. The SQL Dynamic Group dialog appears.
- 2 From here, you must select a method for configuring the new Dynamic Group. You can either use the WhatsUp Gold Dynamic Group Builder, or the SQL dialog. If you are an advanced SQL user, you should choose the second option. Otherwise, we recommend selecting the Dynamic Group Builder.

To use the Dynamic Group Builder:

- 1 In the first part of the dialog, enter the appropriate information into the following fields:
 - **Group Name.** Enter a name for the Dynamic Group as it will appear in the WhatsUp Gold Device List.
 - **Description.** (Optional.) Enter a short description for the new Dynamic Group.
- 2 In the second part of the dialog, you will create and edit rules to form an SQL filter for the Dynamic Group.

To begin writing the rules for your SQL filter, click **Add**. The Dynamic Group Editor appears.
- 3 In the Dynamic Group Editor, enter the appropriate information (for more information, see the help topic for this dialog). As you create rules, they are added to the Dynamic Group Builder dialog where you can add more rules, edit, or delete existing rules by clicking the **Add**, **Edit**, or **Delete** buttons.

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

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

Validating your filter code

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

Converting your filter code

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

To use the SQL Dynamic Group dialog:

- 1 Enter a **Display name** for the group, enter the group **Description**, and enter an SQL query in the **Filter** box that identifies the devices you want to appear in that group.

- 2 Click **OK** to add the group to the device list. SQL validation occurs as soon as you click **OK**. If the filter fails, an error message appears.

In addition to the pre-configured dynamic groups, we have provided several sample filters for you to create some very interesting dynamic groups.



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

Dynamic Group Examples

WhatsUp Gold is pre-configured with dynamic group examples, which you can see in the Devices view, under Device Groups. For more information on these groups, see Using Dynamic Groups.

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



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

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

```
SELECT DISTINCT Device.nDeviceID
FROM Device
    JOIN PivotActiveMonitorTypeToDevice
        ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID
    JOIN ActiveMonitorStateChangeLog
        ON
PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID=
ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID
WHERE Device.bRemoved = 0
    AND DATEDIFF(Hh,ActiveMonitorStateChangeLog.dStartTime,GETDATE())
<= 3
```

To show all devices with multiple interfaces:

```
SELECT DISTINCT NetworkInterface.nDeviceID
FROM Device
    JOIN NetworkInterface
        ON Device.nDeviceID = NetworkInterface.nDeviceID
WHERE Device.bRemoved = 0
GROUP BY NetworkInterface.nDeviceID
HAVING COUNT(NetworkInterface.nDeviceID) > 1
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM Device
    JOIN PivotActiveMonitorTypeToDevice
        ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID
    JOIN ActiveMonitorStateChangeLog
        ON
PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =
ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID
    JOIN MonitorState
        ON Device.nWorstStateID = MonitorState.nMonitorStateID
WHERE Device.bRemoved = 0
    PivotActiveMonitorTypeToDevice.bDisabled = 0
    AND DATEDIFF(hh, ActiveMonitorStateChangeLog.dStartTime,
GETDATE()) <= 2
    AND MonitorState.nInternalMonitorState = 1
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM Device
    JOIN ActionActivityLog
        ON Device.nDeviceID = ActionActivityLog.nDeviceID
    JOIN PivotDeviceToGroup
        ON Device.nDeviceID = PivotDeviceToGroup.nDeviceID
    JOIN DeviceGroup
        ON PivotDeviceToGroup.nDeviceGroupID =
DeviceGroup.nDeviceGroupID
WHERE Device.bRemoved = 0
    AND DATEDIFF(Dd, ActionActivityLog.dDateTime, GETDATE()) <= 2
    AND DeviceGroup.sGroupName = 'My Key Resources Group'
```

To show all devices that need acknowledgement:

```
SELECT DISTINCT Device.nDeviceID
FROM Device
    JOIN PivotActiveMonitorTypeToDevice
        ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID
    JOIN ActiveMonitorStateChangeLog
        ON
PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =
ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID
WHERE Device.bRemoved = 0
    AND ActiveMonitorStateChangeLog.bAcknowledged = 0
    AND PivotActiveMonitorTypeToDevice.bRemoved = 0
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN PivotStatisticalMonitorTypeToDevice
          ON Device.nDeviceID =
PivotStatisticalMonitorTypeToDevice.nDeviceID
      JOIN StatisticalDiskIdentification
          ON
PivotStatisticalMonitorTypeToDevice.nPivotStatisticalMonitorTypeToDevice
ID =
StatisticalDiskIdentification.nPivotStatisticalMonitorTypeToDeviceID
      JOIN StatisticalDiskCache
          ON
StatisticalDiskIdentification.nStatisticalDiskIdentificationID =
StatisticalDiskCache.nStatisticalDiskIdentificationID
WHERE  Device.bRemoved = 0
      AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1
      AND StatisticalDiskCache.nDataType = 1
      AND ((nUsed_Avg / nSize) > 0.90)
      AND (NOT nSize = 0
          OR nSize IS
            NULL))
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN MonitorState
          ON Device.nWorstStateID = MonitorState.nMonitorStateID
WHERE  Device.bRemoved = 0
      AND MonitorState.nInternalMonitorState IN (1,2)
      AND Device.nDeviceTypeID IN (3,4,38,63,64,65,66,67,68,71,72)
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN MonitorState
          ON Device.nWorstStateID = MonitorState.nMonitorStateID
WHERE  Device.bRemoved = 0
      AND MonitorState.nInternalMonitorState = 1
      AND Device.nWorstStateID = Device.nBestStateID
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN PivotActiveMonitorTypeToDevice
          ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID
```

```
        JOIN ActiveMonitorStateChangeLog
          ON
PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =
ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID
        JOIN MonitorState
          ON PivotActiveMonitorTypeToDevice.nMonitorStateID =
            MonitorState.nMonitorStateID
WHERE Device.bRemoved = 0
      AND PivotActiveMonitorTypeToDevice.bRemoved = 0
      AND PivotActiveMonitorTypeToDevice.bDisabled = 0
      AND MonitorState.nInternalMonitorState = 1
      AND DATEDIFF(Mi, ActiveMonitorStateChangeLog.dStartTime, GETDATE())
>= 20
      AND Device.nWorstStateId = Device.nBestStateId
```

To show devices whose Actions (or whose Active Monitors' Actions) have a specific word in their name:



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

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN ActionPolicy
        ON Device.nActionPolicyID = ActionPolicy.nActionPolicyID
      JOIN PivotActionTypeToActionPolicy
        ON ActionPolicy.nActionPolicyID =
          PivotActionTypeToActionPolicy.nActionPolicyID
      JOIN ActionType
        ON PivotActionTypeToActionPolicy.nActionTypeID =
          ActionType.nActionTypeID
WHERE  Device.bRemoved = 0
      AND ActionType.sActionTypeName LIKE '%Critical%'

UNION

SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN PivotActiveMonitorTypeToDevice
        ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID
      JOIN ActionPolicy
        ON PivotActiveMonitorTypeToDevice.nActionPolicyID =
          ActionPolicy.nActionPolicyID
      JOIN PivotActionTypeToActionPolicy
        ON ActionPolicy.nActionPolicyID =
          PivotActionTypeToActionPolicy.nActionPolicyID
      JOIN ActionType
        ON PivotActionTypeToActionPolicy.nActionTypeID =
          ActionType.nActionTypeID
```

```
WHERE Device.bRemoved = 0
      AND PivotActiveMonitorTypeToDevice.bRemoved = 0
      AND ActionType.sActionTypeName LIKE '%Critical%'
```

To show devices to which a particular Performance Monitor is assigned:

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN PivotStatisticalMonitorTypeToDevice
          ON Device.nDeviceID =
PivotStatisticalMonitorTypeToDevice.nDeviceID
      JOIN StatisticalMonitorType
          ON StatisticalMonitorType.nStatisticalMonitorTypeID =
PivotStatisticalMonitorTypeToDevice.nStatisticalMonitorTypeID
WHERE  Device.bRemoved = 0
      AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1
      AND StatisticalMonitorType.sStatisticalMonitorTypeName
      LIKE '%Interface Utilization%'
```

To show devices to which a particular Passive Monitor is assigned:

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN PivotPassiveMonitorTypeToDevice
          ON Device.nDeviceID = PivotPassiveMonitorTypeToDevice.nDeviceID
      JOIN PassiveMonitorType
          ON PassiveMonitorType.nPassiveMonitorTypeID =
          PivotPassiveMonitorTypeToDevice.nPassiveMonitorTypeID
WHERE  Device.bRemoved = 0
      AND PivotPassiveMonitorTypeToDevice.bRemoved = 0
      AND PassiveMonitorType.sMonitorTypeName LIKE '%Cold Start%'
```

To show devices to which a particular Active Monitor is assigned:

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN PivotActiveMonitorTypeToDevice
          ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID
      JOIN ActiveMonitorType
          ON ActiveMonitorType.nActiveMonitorTypeID =
          PivotActiveMonitorTypeToDevice.nActiveMonitorTypeID
WHERE  Device.bRemoved = 0
      AND PivotActiveMonitorTypeToDevice.bRemoved = 0
      AND ActiveMonitorType.sMonitorTypeName LIKE '%Ping%'
```

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

```
SELECT DISTINCT Device.nDeviceID
FROM   Device
      JOIN NetworkInterface
          ON Device.nDeviceID = NetworkInterface.nDeviceID
          AND Device.nDefaultNetworkInterfaceID =
```

```
        NetworkInterface.nNetworkInterfaceID
JOIN DeviceType
    ON Device.nDeviceTypeID = DeviceType.nDeviceTypeID
WHERE (Device.sDisplayName LIKE '%Mail Server%'
    OR NetworkInterface.sNetworkName LIKE '%server1.ipswitch.com%'
    OR NetworkInterface.sNetworkAddress LIKE '%1.2.3.4%')
AND Device.bRemoved = 0
```

Building Dynamic Groups

- 1 In the first part of the dialog, enter the appropriate information into the following fields:
 - **Group Name.** Enter a name for the Dynamic Group as it will appear in the WhatsUp Gold Device List.
 - **Description.** (Optional.) Enter a short description for the new Dynamic Group.
- 2 In the second part of the dialog, you will create and edit rules to form an SQL filter for the Dynamic Group.

To begin writing the rules for your SQL filter, click **Add**. The Dynamic Group Editor appears.
- 3 In the Dynamic Group Editor, enter the appropriate information (for more information, see the help topic for this dialog). As you create rules, they are added to the Dynamic Group Builder dialog where you can add more rules, edit, or delete existing rules by clicking the **Add**, **Edit**, or **Delete** buttons.

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

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

Validating your filter code

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

Converting your filter code

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

About Polling

In This Chapter

Polling overview	115
Dependencies overview	117
IPX support	123

Polling overview

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

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

Changing how you poll devices

After a device is added to the database, WhatsUp Gold begins watching that device using ICMP (Internet Control Message Protocol). WhatsUp Gold 'bounces' a message off of the device, then waits for the echo reply. If the reply is not returned, WhatsUp Gold considers it unresponsive device and changes the status color of the device.

By default, WhatsUp Gold uses the IP address of the device to send this message. You can change this to use the Host name or the Windows name of the computer, and you can change the means it uses to poll the devices.

To change how you poll a device:

- 1 Double-click on the device you want to edit to view Device Properties.
- 2 Click the **General** icon.
- 3 Select the type of poll you want to check the device with in the **Polling type** list box.
- 4 Select IP address or Host name from the **Poll using** list box.
- 5 If you select Host name in the **Poll using** box, you must complete the **Host name** box.
- 6 Click **OK** to save changes.

This is useful if you want to monitor a device that has a dynamic IP address instead of an address assigned to that device. You will need to choose Poll using **Host name** so the DNS will be able to find the device on the network.

Using Maintenance mode

This feature lets you place devices in Maintenance mode, where they will not be polled by the engine.

Any device placed in maintenance mode is not polled, and actions are not fired for it, but it remains in the device list and historical data is preserved. By default, the maintenance state is represented by an orange color in both the device list view and the map view.



Device view



Map view

The mode can be set in two ways:

- **Force this device into maintenance mode now.** Set this device options manually by selecting **Device Properties > Polling**.
- **Scheduled maintenance times.** Schedule maintenance times 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.

Setting how often your devices are polled

The default polling interval is 60 second. You can change this on a per-device basis.

- 1 Double-click on the device you want to edit to view Device Properties.
- 2 Click the Polling icon to view the Polling section of Device Properties.
- 3 Change the interval in the **Poll Frequency** box.
- 4 Click **OK** to save changes.

Stopping and starting polling

To stop or start the polling on all devices by turning the polling engine off or on:

- 1 From the main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select the **Enable polling engine** to turn on polling. Clear the selection to turn polling off.
- 4 Click **OK** to save changes.

In the bottom right corner of the WhatsUp Gold console, the Polling icon shows if the engine is active.

Stopping and starting polling on a monitor

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

- 1 Double-click on the device you want to edit to view Device Properties.
- 2 Click the **Active Monitor** icon.
- 3 Select the Active Monitor you want to change the polling on.
- 4 Click **Edit** to view the Monitor Properties for that monitor.
- 5 Click the **Polling** icon.
- 6 Select **Enable polling for this Active Monitor** to turn polling on, clear the option to turn it off.
- 7 Click **OK** to save changes.

Dependencies overview

By default, WhatsUp Gold polls all devices and active monitors in your device list, unless you manually turn off polling for the system as a whole, or at the device and monitor level. The dependency feature gives you the ability to avoid turning off polling to devices, and instead makes polling dependent on the status of another device's active monitor(s).

Setting dependencies on one device's active monitors will place another device up or down depending on the type of dependency you configure.

There are two types of dependencies:

- **Up Dependency** can be thought of as something is "behind" something else. The dependant device will only be polled if the device "in front" of it is up.
- **Down Dependency** can be thought of as something is "in front of" something else. The dependant devices in front will not be polled unless the device further down the line is down.

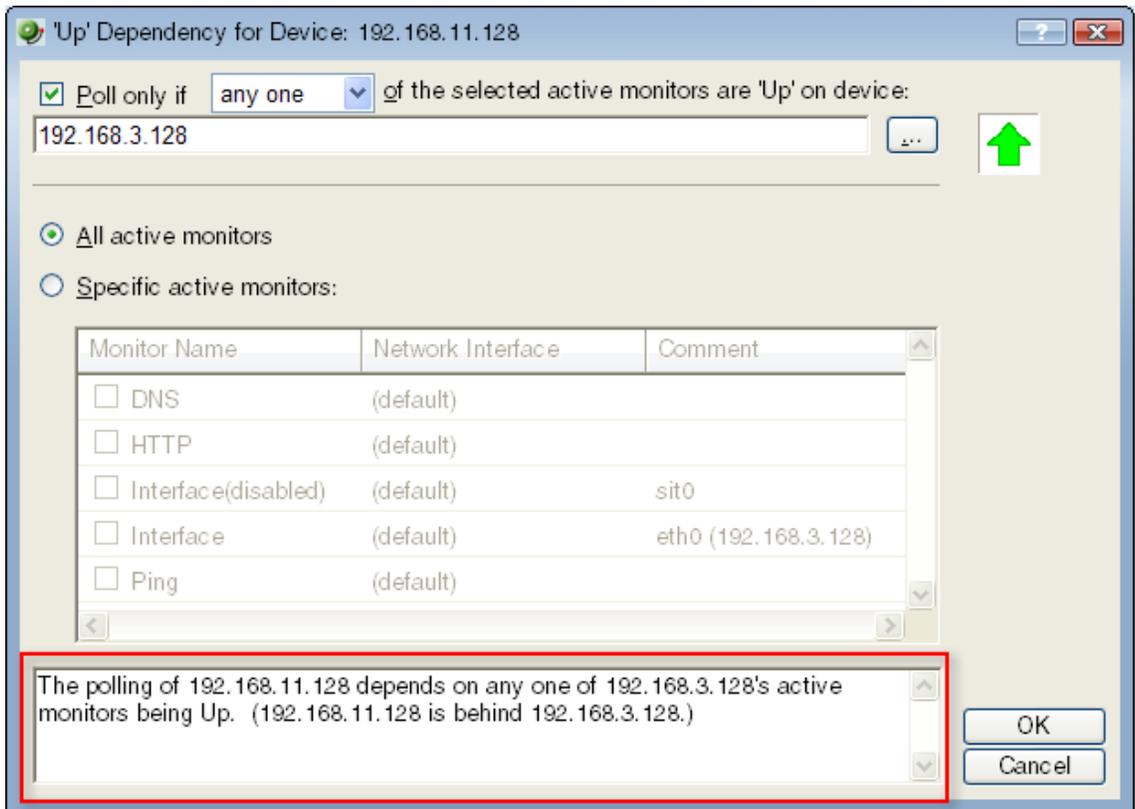
Example

If you make devices behind a router, up dependant on the router's ping active monitor, those devices will not be polled unless the dependent router's ping attempts are successful. If the router's ping active monitor fails, the devices behind the router are placed in the unknown state. Without the dependency, the devices behind the router would fire off actions when they became unavailable due to the router's failed ping attempts. With the dependency, only actions on the router will fire.

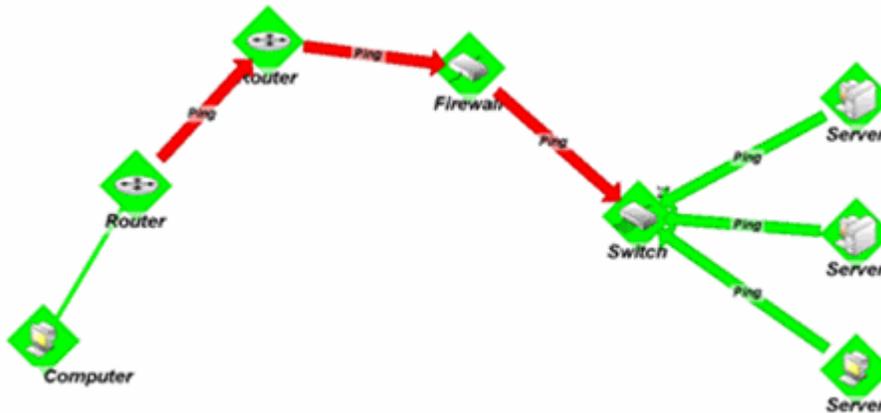
Reading dependencies

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

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



- 2 Read the dependency arrows in the Map View.

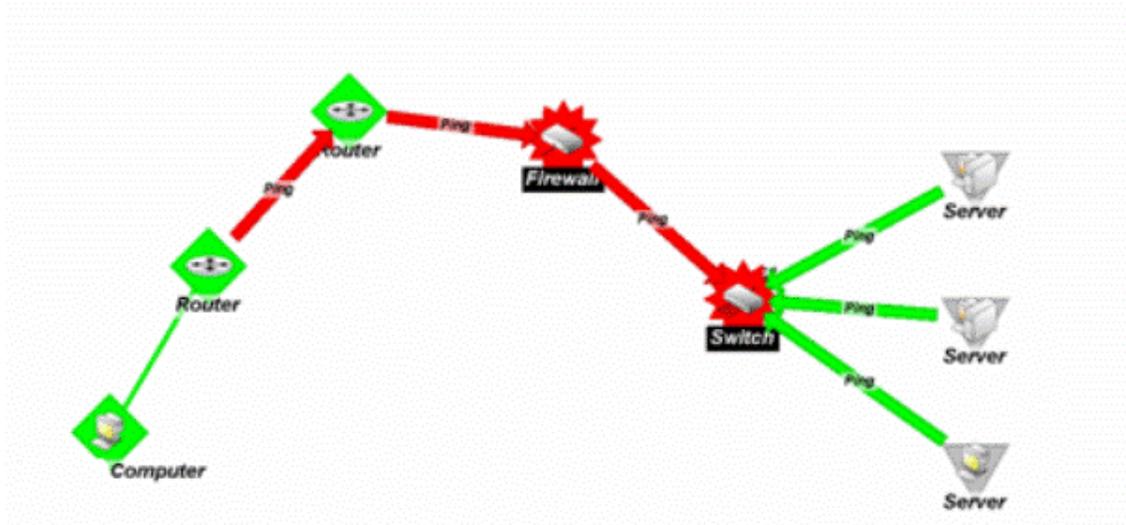


The map above displays several Up and Down dependencies. The green arrows indicate an Up dependency, and the red arrows indicate a Down dependency.

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.

Using WhatsUp Gold v12

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.

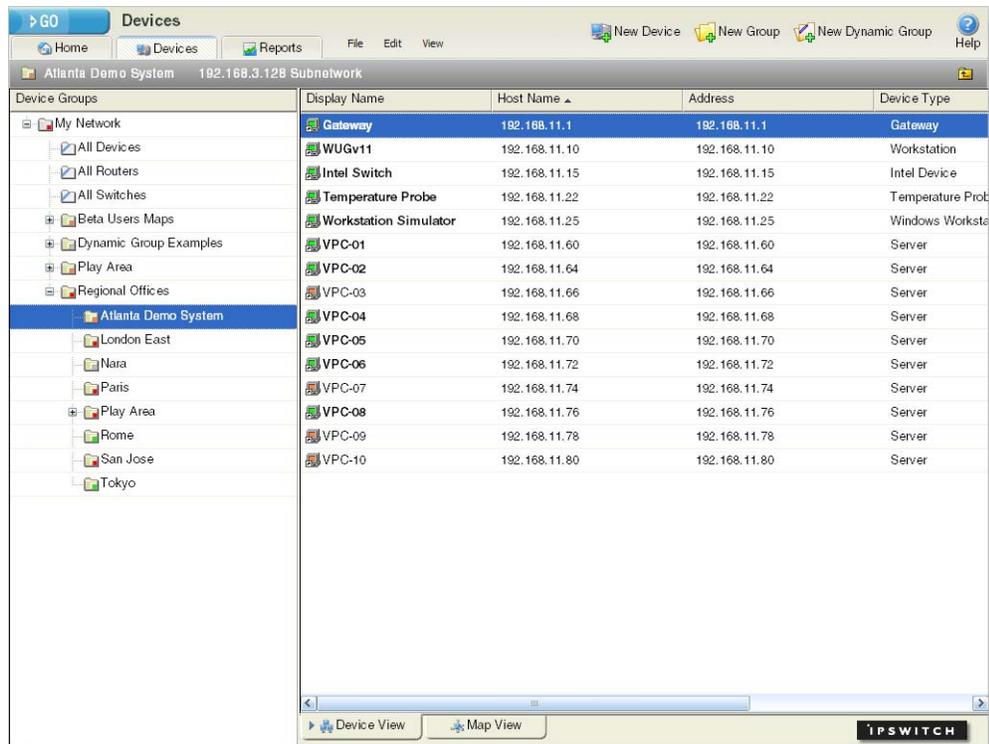
Setting Dependencies

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 Double-click a device in My Network view (**View > Device View**). The Device View appears.

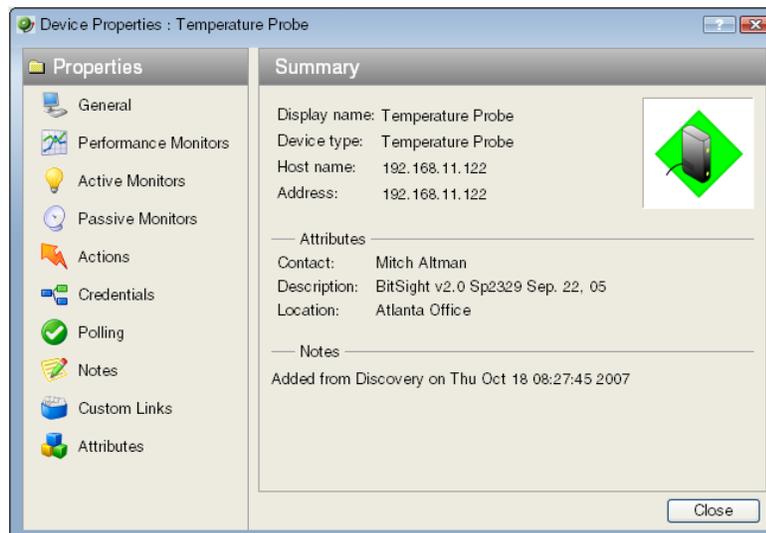


- 2 Double-click a device.

In the console, the Device Properties dialog appears.

- or -

In the web interface, the Device Status page appears. Click Device Properties. The Device Properties dialog appears.

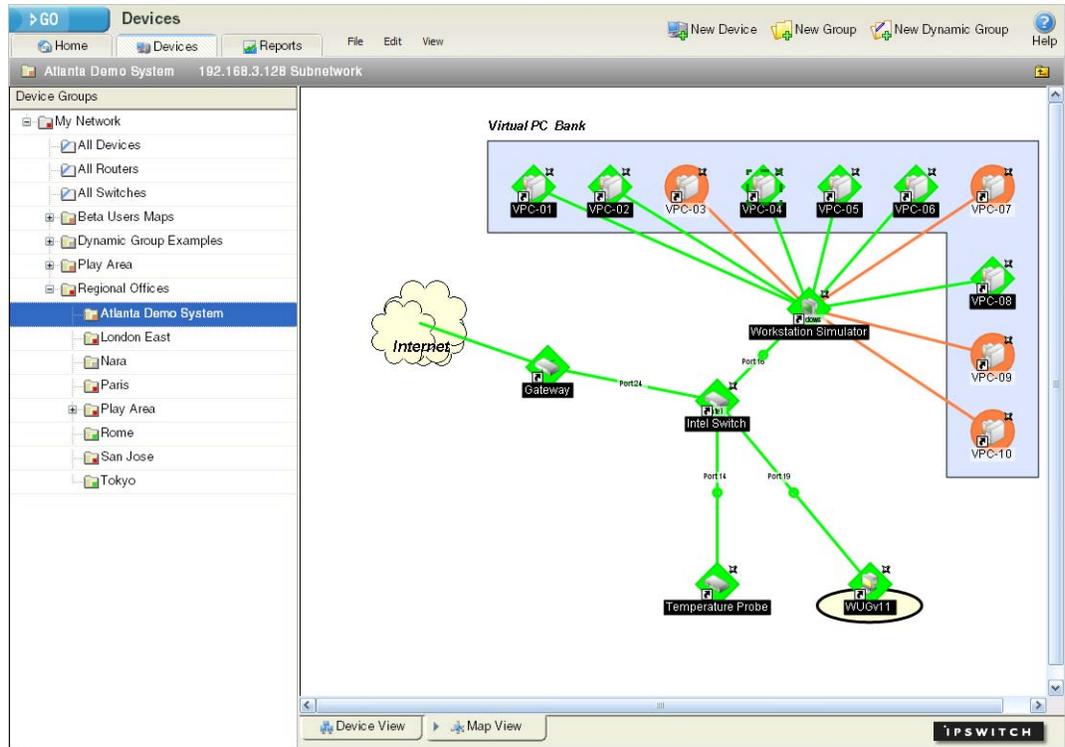


Using WhatsUp Gold v12

- 3 Click **Polling**. The Polling, Maintenance, and Dependencies dialog appears.
- 4 Click either the **Up Dependency...** or the **Down Dependency...** button to bring up the Device Dependencies dialog and configure the up or down dependency.

To set dependencies in the Map View:

- 1 In the console, double-click a device in My Network view (**View > Map View**). The 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. For information about using the Device Dependencies dialog, see the *Using the Device Dependencies dialog* topic below.

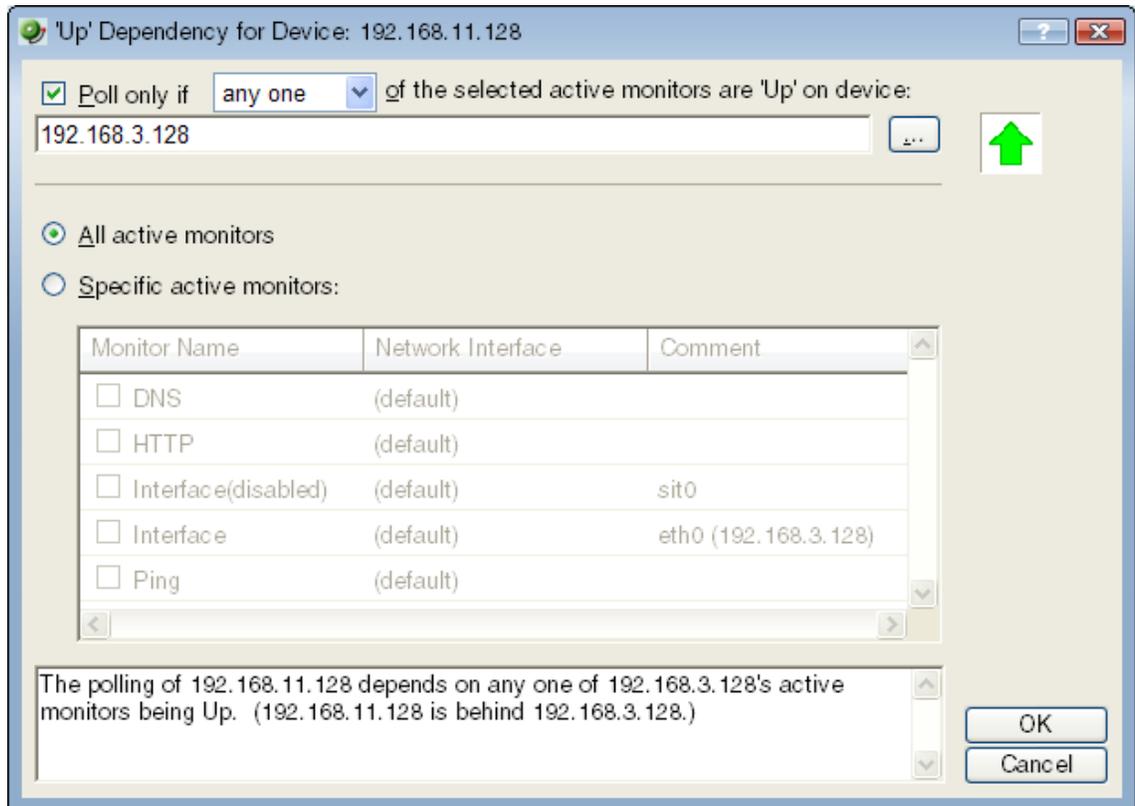


Note: You cannot set a dependency across groups. However, you can make shortcuts to the devices you want to set a dependency on in a group, then set the dependency to the shortcut.

To view the dependency between the two devices, click **Display > Polling Dependency Arrows** In the Map View,

Using the Device Dependencies dialog

The Device Dependencies dialog is the same for both up and down dependencies with the exception that one sets up dependencies and the other sets down dependencies. Up dependencies are indicated with an upward green arrow icon, while down dependencies are indicated with a downward red arrow.



- Click to select the **Poll only if** check box to either poll only if **Any one** or **Every one** of the active monitors selected below are up or down on device, depending on the type of dependency you want to set.
- Click the browse (...) button to select a device for the dependency.
- Select either **All active monitors** or **Specific active monitors** and check the active monitors you want to associate with the dependency.

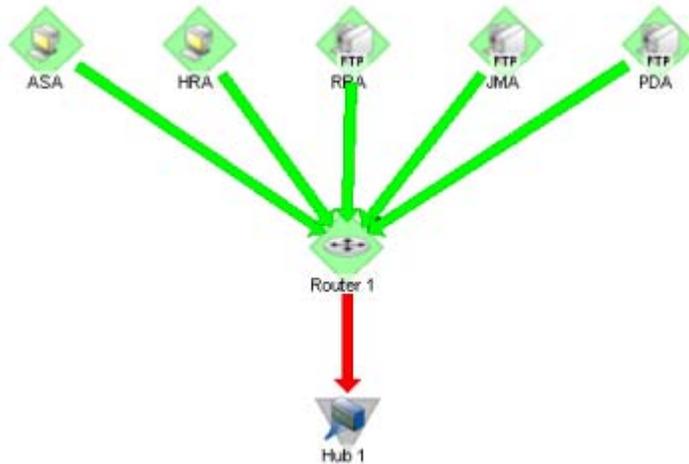
The statement at the bottom of the dialog is generated to help you understand the type of dependency you have created.

An example statement would read:

The polling of Workstation Simulator depends on every one of Intel Switch's active monitors being 'Up'. (Workstation Simulator is 'behind' Intel Switch).

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 section of Device Properties 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.

IPX support

To poll IPX devices, Microsoft's NWLink IPX/SPX Compatible Transfer Protocol must be installed and running on the computer on which you installed WhatsUp Gold.

To add the IPX protocol:

- 1 Open the Network applet in the Windows Control Panel.
- 2 In the **Select Network Component** dialog box, select Microsoft, then select the IPX/SPX-compatible Component and follow the online instructions.

Using Actions

In This Chapter

About actions.....	125
About action strategies	126
About the Action Library	127
About Web Alarms	128
Configuring an action	130
Testing an action	147
Deleting an action.....	147
Assigning an action to a device.....	147
Creating a Blackout Period.....	148
Percent Variables	148
About action policies	152

About actions

When a device or monitor state change occurs, WhatsUp Gold can perform an action to try to correct the problem, notify someone of the state change, or launch an external application.

For example, you can set up an action that sends you an email alert when your Web server device is down.

You can configure actions on a single device or monitor, or define an Action Policy to use across multiple devices or monitors.

WhatsUp Gold provides the following action types:

- **Beeper Action.** Activates a beeper.
- **Pager Action.** Sends a message to a pager.
- **Program Action.** Runs another program (executable) to take some action.
- **Email Action.** Sends an SMTP mail message.
- **Winpop Action.** Displays a message in a pop-up window on a Windows NT system.
- **SMS Action.** Sends a Short Message Service (SMS) notification to a pager or cell phone using an email or dialup gateway

- **SMS Direct Action.** Sends an SMS message to pager or cell phone directly using an SMS modem.
- **Service Restart Action.** Stops or restarts a Windows NT system.
- **Syslog Action.** Sends a message to a host that is running a Syslog server.
- **Text to Speech Action.** Sends a text-to-speech notification to a speaker.
- **Sound Action.** Sounds an alarm by playing a sound file on the WhatsUp Gold console.
- **Active Script Action.** Allows you to write either VBScript or JScript code to perform a check on a device. If the script returns an error code, the monitor is considered down.



Note: Ipswitch does not support the scripts that you create, only the ability to use them in the Active Script Action.

- **Web Alarm.** Sounds an alarm by playing a sound file on the WhatsUp Gold web interface.

About action strategies

When configuring actions for your devices and monitors, you should take a few things into consideration.

- Large lists of devices have the potential of sending out very large amounts of external notifications (email, SMS, beeper, etc).
Imagine the number of messages sent if external notifications are placed on a router and every device and monitor that uses that router for their connection to the Internet. If the router goes down, it will appear as if all of the devices are down, and messages will be sent for each of them. Consider using dependencies and limiting the external notifications to the router and the most important of the devices in the group.
- Do not rely on sound actions when there is not someone around to hear the notification. Sound notifications are safe to use in almost any situation, but is not the best choice for items that are monitored overnight.
- If the device states do not fit what you need, change them, or add new ones.
You may want to add device states for longer periods of downtime. Perhaps creating a **Down at least 60 mins** state, and sending an escalated message to show that the device is still down after an hour.
- Action policies are easier to manage than lists of actions built on a device.
Whenever possible, it is a good idea to use action policies over actions configured for a single device. That way, you can reuse the work you put into the list, and can keep better watch over the actions that are being fired.
- Visual notifications are usually enough for most of the devices on your network.

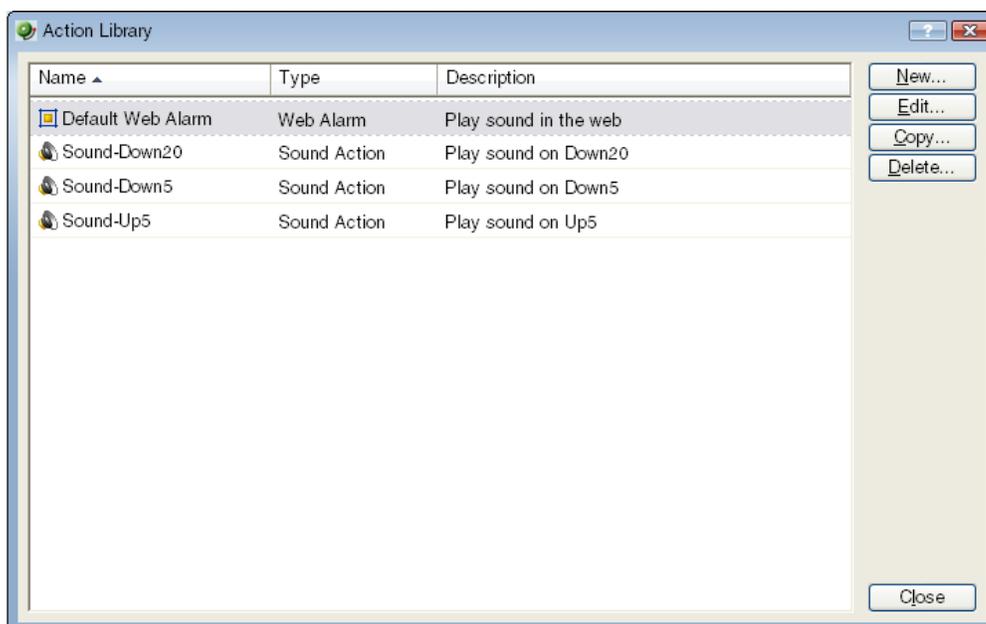
Unless the device is vital to the daily-operation of the business or office, the state change color and shape should be enough to let you know what is going on with your monitored devices.

- An action can be assigned to a device or to a specific monitor. If you want to be notified if any or all of the monitors on a device goes down, assign the action to the device. If you are concerned with specific monitors on a device, assign the action to the monitor itself. Remember that if you assign the action to both the monitor and the device, both actions will fire if the monitor goes down.
- You can check on the status of firing alerts via Running Actions. Here, you can cancel single alerts, or all currently firing alerts.

About the Action Library

The Action Library shows all of the actions configured for your network. These actions can be assigned to any device or monitor, or included in an action policy. When you assign the action to a device or monitor, you specify the state change that will trigger the action.

To open the Action Library, from the main menu of the WhatsUp Gold console, select **Configure > Action Library**.



From this dialog, you can:

- **Create a new action.** Click **New**. After the action has been created, it can be assigned to one or multiple devices or monitors. You can create the following types of actions to send a message or take an action when the status of a device or monitor changes.
 - Beeper
 - Sound
 - Pager

- Program
 - Service Restart
 - SMS
 - SMS Direct
 - SMTPMail
 - Syslog
 - Text to Speech
 - WinPopup
 - Web Alarms
 - Active Script Action
- **Make changes to an action.** Select the action you want to modify and click **Edit**. Changes made here effect each instance of the action.
 - **Copy an action.** To create a copy of an action so you can base a new action on the setup information of an existing one, select the action and click **Copy**. You can then edit the new copy as needed.
 - **Remove an action from the Action Library, devices, and monitors.** To remove an action from both the Action Library and any device or monitor to which it is assigned, select the action, then click **Delete**. This is a global delete of the selected action; the action is removed from any action policy, device, or active monitor to which the action is associated.

If you need to remove an action from a specific action policy, device, or monitor, open the properties for the policy, device, or monitor and delete it there. This removes only the specified instance of that action; the action remains in the Action Library and on other devices to which it is assigned.



Note: Be aware that when you remove an action from the Action Library, you are removing that action from all action policies, as well as all devices and monitors on which the action is assigned. In addition, all statistics relating to that action are also deleted from the database. When you first open the Action Library, if you have not yet defined an Action, you will see the default Web Alarm, which you can assign to any device or monitor.

About Web Alarms

A Web Alarm is a type of Action that can be applied to a device, or through an Action Policy. On the WhatsUp Gold web interface, when Web Alarms are enabled and a device goes down, or a state changes, a window pops up and an audible alarm sounds. In the Web Alarm popup window, the current Web Alarms are listed. You can mute or dismiss these alarms.



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 v12.

Configuring a Web Alarm Action

A Web Alarm can be configured to apply to a device as an individual Action on a specific device, or to multiple devices using an Action Policy. Before you can assign an Action to a device or group of devices, you must first configure it in the Action Library.

For more information, see *Creating a Web Alarm Action* (on page 144).

The Web Alarm popup window

When a Web Alarm Action is fired, and you are logged in to the WhatsUp Gold web interface, the Web Alarm popup box appears in your browser. From here, you dismiss one or all of the alarms listed. You can also mute them. Muting an alarm leaves the alarm listed, but stops the alarm from sounding.



Note: You cannot disable Web Alarms from the popup window.

If you'd like more information on one of the devices listed in the popup window, you can double-click the device to bring up its Device Status Workspace.

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 here. Instead, you enable and disable Web Alarms on the web interface on the User Preferences dialog (Select **GO**. From the **WhatsUp** section, select **Configure > Preferences**). Also from the User Preferences dialog, you can adjust the Web Alarms refresh interval. The refresh interval indicates the number of seconds WhatsUp Gold waits until checking for new Web Alarms.

By default, Web Alarms are enabled on the web interface with a refresh interval of 120 seconds.

Accessing Web Alarms on the web interface

There are two places users can access Web Alarms from the WhatsUp Gold web interface:

- 1 The Web Alarm window. This appears when Web Alarms are enabled and a Web Alarm Action is fired. You can also access this window by selecting **GO**, then from the **WhatsUp** section, selecting **Devices > Web Alarms**.
- 2 The Web Alarm workspace report. This is a default workspace report located on the Problem Areas 1 workspace view of the Home Workspace.

Another way of listing and accessing your network's Web Alarms is creating a Dynamic Group which lists all of the current Web Alarms. For more information on Dynamic Groups in WhatsUp Gold, please see Using Dynamic Groups.

Configuring an action

There are two aspects of fully configuring an action. The first is to 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).

After the action is created, the second step is to 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 147)
- *Assigning an action to a monitor* (on page 161)
- *Creating a custom action policy* (on page 152)

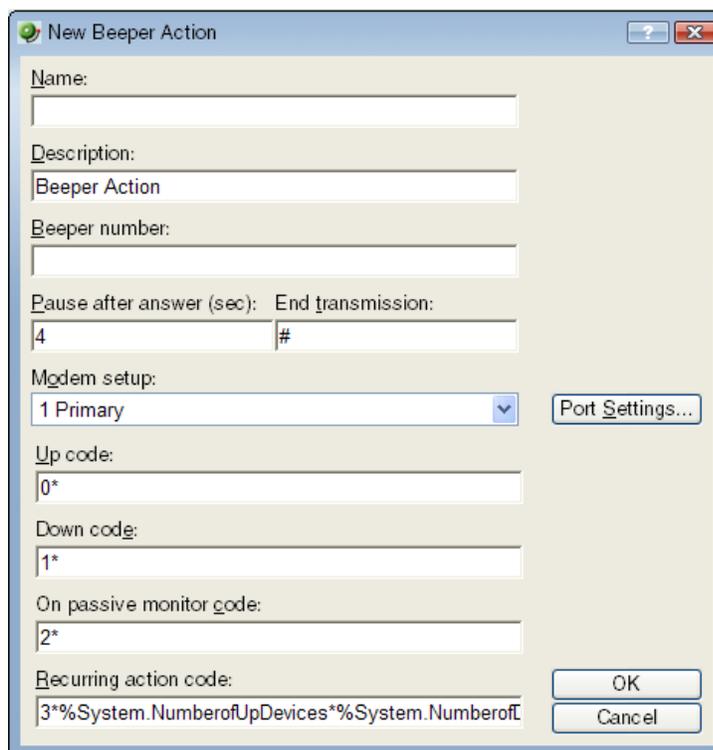
After the actions have been completely configured, WhatsUp Gold launches the action as soon as the proper state change is reached.

Creating a Beeper Action

To create a Beeper Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Beeper Action**.
 - or -
 - Select an existing Beeper Action, then click **Edit**.

The action properties page appears.



3 Set the appropriate options.

- **Name.** The name of the action as it appears in the Action Library.
- **Description.** Enter a short description of the action. This is displayed in the Action Library dialog along with the entry in **Name**.
- **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.** Enter a number of seconds the modem should pause before sending the signal codes once a connection has been 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 either 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'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 will affect ALL uses of that setting.

- **Up code.** Specifies the characters sent to the beeper to indicate that the device has come back 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 codes are:
 - %System.NumberofUpDevices
 - %System.NumberofDownDevices
- 4 Click **OK** to save this action. The action now appears in the Action Library.
 - 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a Pager Action

To create a Pager Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Pager Action**.
 - or -
 - Select an existing Pager Action, then click **Edit**.

The action properties page appears.

- 3 Set the appropriate options.
 - **Name.** Enter an identifying name for this pager action.
 - **Description.** Enter a short description of the action. This is displayed along with the Names 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.
 - 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 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 will affect ALL uses of that setting.

- **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 Click **OK** to save this action. The action now appears in the Action Library.
 - 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating an Email Action

To create an Email Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Email Action**.
 - or -
 - Select an existing Email Action, then click **Edit**.

The action properties page appears.

The screenshot shows a dialog box titled "New Email Action". It contains the following fields and controls:

- Name:** An empty text input field with a "Mail Content..." button to its right.
- Description:** A text input field containing "E-mail Action".
- SMTP Server:** An empty text input field.
- Port:** A text input field containing "25".
- Timeout (sec):** A text input field containing "5".
- Mail to:** An empty text input field.
- SMTP server requires authentication
- Username:** An empty text input field.
- Password:** An empty text input field.
- Use an encrypted connection (SSL/TLS)
- OK** and **Cancel** buttons at the bottom right.

- 3 Enter the email destination information.
 - **Name.** Enter a unique name for this action.
 - **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.

- **SMTP Mail Server.** Enter the IP address or Host (DNS) name of your email server (SMTP mail host).
- **Port.** Enter the port number that the SMTP server is installed on.
- **Timeout.** Enter the amount of time (in seconds) to wait for user authentication on the SMTP server. The authentication fails if this time limit is exceeded.
- **Mail To.** Enter the email addresses you want to send the alert to. Email 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.
- **SMTP server requires authentication.** Check this option if your SMTP server uses authentication. This enables the Username and Password fields.

The Email action supports three authentication types:

- CRAM-MD5
- login
- plain

The authentication type is not configurable. It is negotiated with the SMTP server automatically.

- **Username.** Enter the username to be used with SMTP authentication.
 - **Password.** Enter the password of the username to be used with 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).
- 4 Click **Mail Content.** Enter the content of the email alert.
- **From.** Enter the email address that will appear in the From field of the email that is sent by the Email action.
 - **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.
- 5 Click **OK** to save this action. The action now appears in the Action Library.
- 6 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating an SMS Action

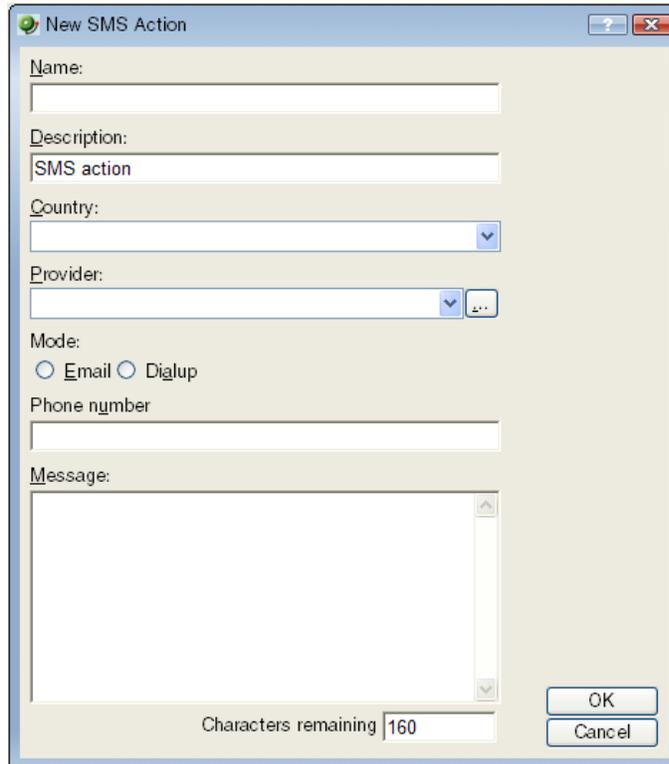
To create an SMS Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.

2 In the Action Library, do one of the following:

- Click **New**, then select **SMS Action**.
- or -
- Select an existing SMS Action, then click **Edit**.

The action properties page appears.



3 Set the appropriate options.

- **Name.** Enter a unique display name to identify the SMS notification.
- **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
- **Country.** Using the list box, select the country for the SMS provider.
- **Provider.** Using the list box, select the desired provider.



Note: If the provider list is incomplete and/or incorrect, you can click the **Providers** button to add, edit, or delete providers in this list.

- **Connection Settings.** Mode is 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, so you can enter many numbers.



Note: Non-numeric characters such as "-" and "." will be ignored.

- **Message.** 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.).
- 4** Click **OK** to save this action. The action now appears in the Action Library.
 - 5** Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

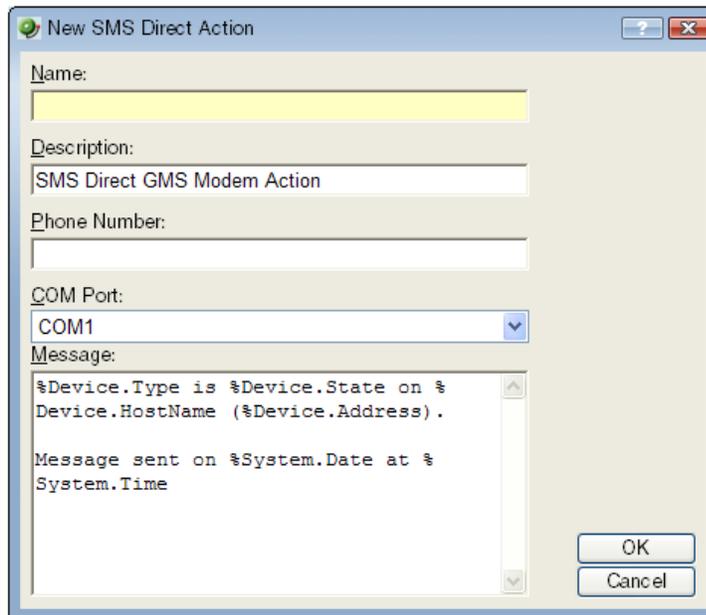
Creating an SMS Direct Action

SMS Direct Actions send SMS messages directly through an SMS modem, unlike SMS actions, which use email gateways or dial-up modems. If you want to send an SMS message and do not have an SMS modem, see *Creating an SMS Action* (on page 135).

To create an SMS Direct Action:

- 1** Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2** In the Action Library, do one of the following:
 - Click **New**, then select **SMS Direct**.
 - or -
 - Select an existing SMS Direct Action, then click **Edit**.

The action properties page appears.



The screenshot shows a dialog box titled "New SMS Direct Action". It contains the following fields and values:

- Name:** (Empty text box)
- Description:** SMS Direct GMS Modem Action
- Phone Number:** (Empty text box)
- COM Port:** COM1 (Selected from a dropdown menu)
- Message:**
%Device.Type is %Device.State on %
Device.HostName (%Device.Address).

Message sent on %System.Date at %
System.Time

Buttons: OK, Cancel

3 Set the appropriate options.

- **Name.** Enter a name for this notification. This name is for your reference only and will never be displayed to the notification recipient.
- **Description.** Enter or modify the description. This description appears in the Action Library and is for your reference only.
- **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 ".", will be ignored.

There is a 2,000 character limit in this field, 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.

- **Message.** Enter the text message you want to send with this notification plus any desired percent variable codes. Keep in mind that if you use percent variables, this will greatly increase the character count.



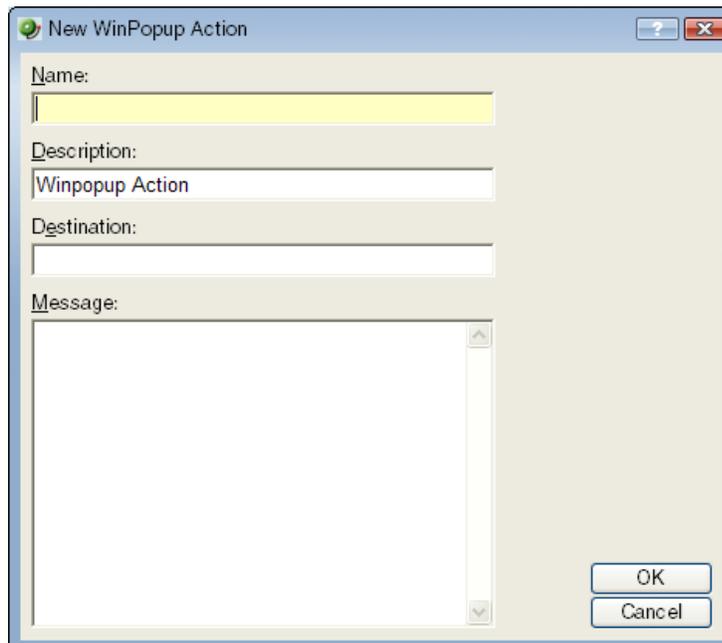
Note: If the message exceeds 140 characters, the message may be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.), each message containing up to 140 characters, for a total of up to 420 characters. Spaces are counted in the total number of characters.

- 4 Click **OK** to save this action. The action now appears in the Action Library.
- 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a WinPopup Action

To create a WinPopup Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **WinPopup Action**.
 - or -
 - Select an existing WinPopup Action, then click **Edit**.The Action Properties page appears.



The screenshot shows a dialog box titled "New WinPopup Action". It has a standard Windows-style title bar with a question mark icon and a close button. The dialog contains four input fields: "Name:" (empty), "Description:" (containing "Winpopup Action"), "Destination:" (empty), and "Message:" (empty text area). At the bottom right, there are two buttons: "OK" and "Cancel".

- 3 Set the appropriate options.
 - **Name**. Enter an identifying name for this winpopup action.
 - **Description**. Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
 - **Destination**. Specify the Windows NT host or domain that you want to receive this notification.

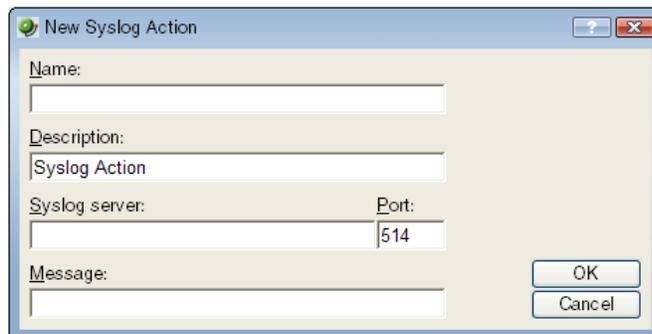
- **Message.** Enter a text message using percent variables if needed.
 - **Refresh.** Click this button to refresh the **Destination** list. This populates the list with all of the targets you can choose in which to send a winpop action.
- 4 Click **OK** to save this action. The action now appears in the Action Library.
 - 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a Syslog Action

To create a Syslog Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Syslog Action**.
 - or -
 - Select an existing Syslog Action, then click **Edit**.

The action properties page appears.



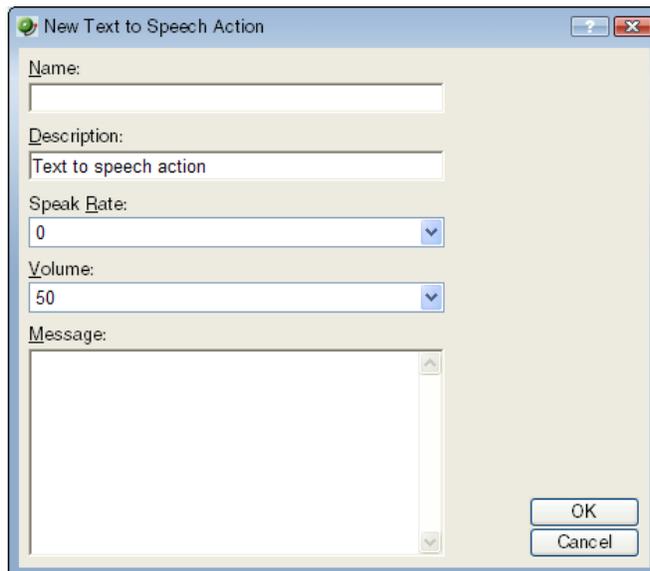
- 3 Set the appropriate options.
 - **Name.** Enter a name for the action. This will appear in the Action Library.
 - **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
 - **Syslog Server.** Enter the IP address of the machine 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 be sent 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 will be limited to 1023 bytes, in order to comply with the Syslog protocol. Non-visible ASCII characters such as tabs and linefeeds will be replaced by space characters.

- 4 Click **OK** to save this action. The action now appears in the Action Library.
- 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a Text-to-Speech Action

To create a Text-to-Speech Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Text-to-Speech Action**.
 - or -
 - Select an existing Text-to-Speech Action, then click **Edit**.The action properties page appears.



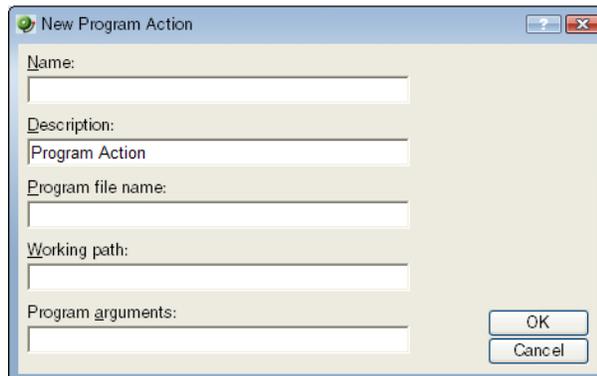
- 3 Set the appropriate options.
 - **Name**. Enter a unique name for this action.
 - **Description**. Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
 - **Speak Rate**. Select how fast the voice speaks the message.
 - **Volume**. Select the volume of the message.
 - **Message**. Enter any text message you want audibly repeated. Your own text can be used in addition to percent variables.

- 4 Click **OK** to save this action. The action now appears in the Action Library.
- 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a Program Action

To create a Program Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Program Action**.
 - or -
 - Select an existing Program Action, then click **Edit**.The action properties page appears.



- 3 Set the appropriate options.
 - **Name.** Enter a name for the action you are creating. This is the name that appears in the Action Library.
 - **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
 - **Program filename.** Enter or browse to the executable of the application you want to launch.
 - **Working path.** Enter or browse to the directory 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 this action. The action now appears in the Action Library.

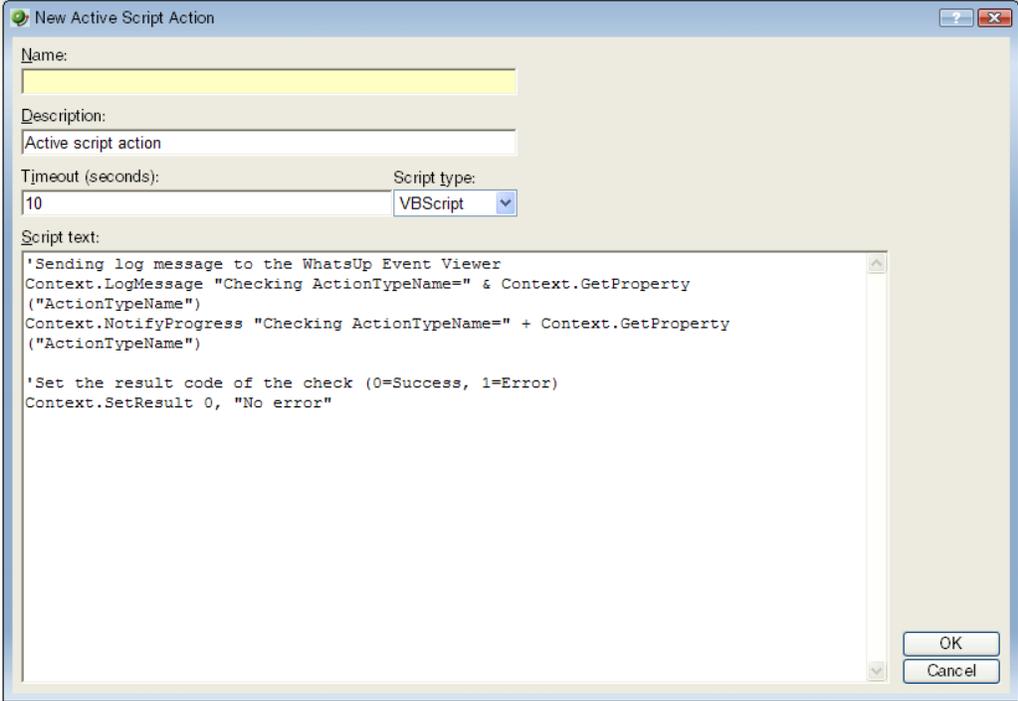
- 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating an Active Script Action

To create an Active Script Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Active Script Action**.
 - or -
 - Select an existing Active Script Action, then click **Edit**.

The action properties page appears.



The screenshot shows a dialog box titled "New Active Script Action". It contains the following fields and values:

- Name:** (empty, highlighted in yellow)
- Description:** Active script action
- Timeout (seconds):** 10
- Script type:** VBScript
- Script text:**

```
'Sending log message to the WhatsUp Event Viewer
Context.LogMessage "Checking ActionTypeName=" & Context.GetProperty
("ActionTypeName")
Context.NotifyProgress "Checking ActionTypeName=" + Context.GetProperty
("ActionTypeName")

'Set the result code of the check (0=Success, 1=Error)
Context.SetResult 0, "No error"
```

Buttons for "OK" and "Cancel" are located at the bottom right of the dialog.

- 3 Set the appropriate options.
 - **Name.** The name of the action as it appears in the Action Library.
 - **Description.** The description of the action as it appears in the Action Library.

- **Timeout.** The amount of time (in seconds) WhatsUp Gold should wait for the action script to run.



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.** Write or insert your action code here.
- 4 Click **OK** to save this action. The action now appears in the Action Library.
 - 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a Web Alarm Action

To create a Web Alarm Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.

- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Web Alarms Action**.

- or -

Select an existing Web Alarms Action, then click **Edit**. The Action Properties page appears.

The screenshot shows a dialog box titled "New Web Alarm Action". It has a title bar with a question mark and a close button. The dialog contains the following fields and controls:

- Name:** An empty text input field.
- Description:** A text input field containing "Web Alarm Action".
- Message:** An empty text input field.
- Play Sound:** An unchecked checkbox.
- Sound file name:** A dropdown menu showing "Alarm1.wav".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

- 3 Set the appropriate options.
 - **Name.** The name identifies the Web Alarm action in the Action Library list.

- **Description.** A short description of the action. The description appears in the Action Library list.
- **Message.** Enter a short message to send to the visual cue part of the Web Alarm in the web interface.
- **Play Sound.** Select this option to play the sound file whenever a web alarm action is fired. Clear this option to only have the visual cue appear in the Web Interface.
- **Sound file name.** Select a sound file that has been installed in your `\Program Files\Ipswitch\WhatsUp\HTML\1033\NMconsole\WebSounds` directory. Custom sounds added to this directory appear in the drop-down list.



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

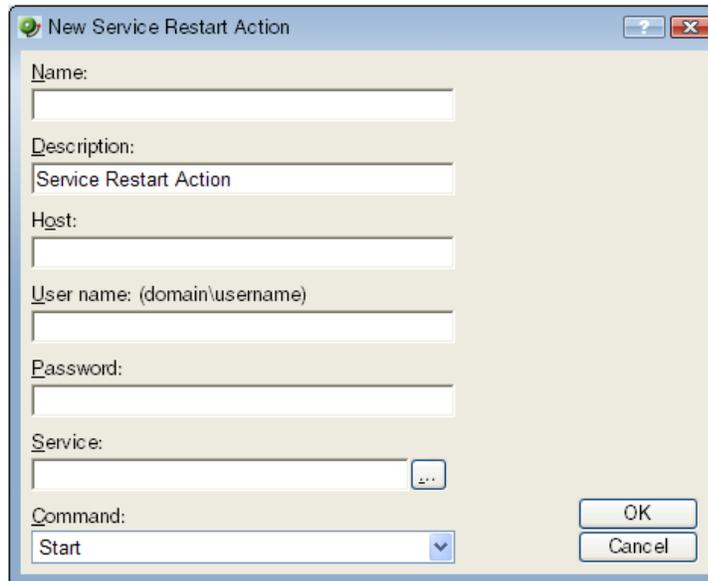
- 4 Click **OK** to save this action. The action now appears in the Action Library.
- 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Creating a Service Restart Action

To create a Service Restart Action:

- 1 Go to the Action Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Library**. The Action Library appears.
 - or -
 - From the main menu bar of the console, select **Configure > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **Service Restart Action**.
 - or -
 - Select an existing Service Restart Action, then click **Edit**.

The action properties page appears.



- 3 Set the appropriate options.
 - **Name.** Enter the name of the action as you would like it to appear in the Action Library.
 - **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry **Name**.
 - **Host.** Click the browse button to select the desired host from your Network Neighborhood.
 - **User name (domain\username).** Enter a user login to use with this monitor. In order to monitor the service on another machine, the WinEvent monitor has to be configured with the correct user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, then the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user. No user name and password is needed for local services (services on the machine where WhatsUp Gold is running).
 - **Password.** Enter the password for the login used above. To monitor NT services on a XP machine with an account that has empty password, the XP's Local Security Settings might have to be modified. From **Administrative tools > Local Security Settings**, click on **Security Settings > Local Policies > Security Options**. Then right click on the setting: **Account: Limit local account use of blank passwords to console logon only** and click **Properties**, and select **Disable**.
 - **Service.** Click the browse button to select the desired service associated with your host.
 - **Command.** Use the list box to 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 this action. The action now appears in the Action Library.
- 5 Assign the action to a device or a monitor. For more information, see *Assigning an action to a device* (on page 147) or *Assigning an action to a monitor* (on page 161).

Testing an action

After an action has been created, you can test that action to make sure it works properly.

To test an action:

- 1 Select **Configure > 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.

Deleting an action

Actions that were added at the device or monitor level can be removed by selecting the action in the Actions dialog of the Device or Monitor Properties, and clicking **Remove**. This does not effect any other item in the database.

If you have assigned action policies to your devices, you can remove the action from the policy itself.

To remove an action from the database completely, you must access the Action Library, select the action and click **Delete**. When an action is removed from the Library, it is also removed from all items configured to use that action.

Assigning an action to a device

You can assign one or more individual actions to a device, or assign an action policy that may contain multiple actions used across your device list.

To assign actions to a device:

- 1 Right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Actions dialog appears.
- 3 Select the **Apply individual actions** option.
- 4 Click **Add** to access the Action Builder wizard.
- 5 Follow the directions in the Action Builder wizard.
- 6 At the end of the wizard, click **Finish** to add the action to the device.
- 7 If you need to add more actions to the device, click **Add** and repeat these directions.
- 8 When you have completed adding actions, click **OK**.

To assign an action policy to a device:

- 1 Right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Actions dialog appears.
- 3 Select the **Apply this Action Policy** option.
- 4 Select the action policy you want to use for this device. If you need to create a new action policy first, click **Add** to access the Action Builder dialog.

- 5 Click **OK** to save the changes.

After an action has been added to the device, the action fires when that device reaches the specified state.

Creating a Blackout Period

You can create a Blackout period to have WhatsUp Gold suspend specific actions during the scheduled period of time. Use this feature to keep from sending a notification to someone who is on vacation, or to keep from sending email when there is no one to receive it.

To create a Blackout period:

- 1 Access the Action Builder Wizard.
 - Select **Device Properties > Actions**, then click **Add**.
 - Select **Device Properties > Active Monitors > Monitor Properties > Actions**, then click **Add**.
 - On the Actions Policies dialog, then click **Add**.
- 2 Within this wizard, click the **Blackout period** button.
- 3 On the Weekly Blackout Schedule dialog, set the times you want the blackout to occur. The schedule that is set is repeated weekly.
- 4 Click **OK**.
- 5 Complete the wizard.

Percent Variables

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.

Using WhatsUp Gold v12

<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>	<p>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.</p>

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).

<p><code>%Device.Attribute. [Attribute Name]</code></p>	<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 · Custom. If you have created a custom attribute you can use the name of that custom attribute in the percent variable. <p>Example: <code>%Device.Attribute.Phone</code> <code>%Device.Attribute.RackPosition</code></p> <p>To avoid an error, when placing <code>%Device.Attribute</code> in quotation marks, place a space between the last letter and the closing quotation mark.</p> <p>Example: <code>"%Device.Attribute.Contact "</code>; correct <code>"%Device.Attribute.Contact"</code>; incorrect</p>
<p><code>%Device.DatabaseID</code></p>	<p>Returns the database ID of a device.</p>
<p><code>%Device.DisplayName</code></p>	<p>Display Name (from General of device properties)</p>
<p><code>%Device.HostName</code></p>	<p>Host Name (from General of device properties)</p>
<p><code>%Device.Notes</code></p>	<p>Notes. (Notes are from the device properties Notes)</p>
<p><code>%Device.SNMPOid</code></p>	<p>SNMP Object identifier.</p>
<p><code>%Device.State</code></p>	<p>The state's description (such as "Down at least 2 min" or "Up at least 5 min")</p>
<p><code>%Device.Status</code></p>	<p>This shows the name of the active monitor, preceded by the device state id : 10 DNS</p>
<p><code>%Device.Type</code></p>	<p>Device Type (from General of device properties)</p>

<p>Passive Monitor Variables</p>	<p>Description</p>
<p><code>%PassiveMonitor.DisplayName</code></p>	<p>The name of the monitor as it appears in the Passive Monitor Library.</p>

Using WhatsUp Gold v12

<code>%PassiveMonitor.LoggedText</code>	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.)
<code>%PassiveMonitor.Payload.*</code>	Payload generated by a passive monitor.
<code>%PassiveMonitor.Payload.EventType</code>	The type of passive monitor (Syslog, Windows Event, or SNMP Trap)

System Variables	Description
<code>%System.Date</code>	The current system date. Configure the date format in Regional Options (from Program Options)
<code>%System.DisplayNamesDownDevices</code>	Display names of devices with down monitors
<code>%System.DisplayNamesDownMonitors</code>	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
<code>%System.DisplayNamesUpDevices</code>	Display names of up devices
<code>%System.DisplayNamesUpMonitors</code>	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
<code>%System.InstallDir</code>	Displays the directory on which WhatsUp Gold is installed
<code>%System.NumberofDownDevices</code>	Number of down devices on your network
<code>%System.NumberOfDownMonitors</code>	Shows the number of down monitors on your network
<code>%System.NumberofUpDevices</code>	Number of up devices on your network
<code>%System.NumberOfUpMonitors</code>	Shows the number of up monitors on your network
<code>%System.Time</code>	The current system time. The format is hh:mm:ss

About action policies

You can use action policies to stack multiple actions together in a single policy. You can then assign the action policy to any device or monitor. If you later need to edit an action, you can edit the action policy and the changes will be applied to all of the devices that use that particular action.

For more information, see:

- *Creating an action policy* (on page 152)
- *Editing action policies* (on page 153)
- *Implicit Action Policy* (on page 153)

Creating an action policy

This feature gives you the ability to stack multiple actions together in a single policy. You can then assign those actions to any device or monitor in your device list. Once assigned, you can edit the policies in the Action Policies dialog without having to make changes to all of the devices that use that particular action.

To create an action policy:

- 1 Open the Action Policies dialog.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Policies**.
- or -
 - From the main menu bar on the console, select **Configure > Action Policies**. The Action Policies dialog appears.
- 2 On the Action Policies dialog, click **New**.
- 3 In the New Action Policy dialog, 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 will help you remember what is contained in that 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 the **Up** and **Down** buttons above the action list.

If you select **Only execute first action**, WhatsUp Gold executes the actions in the list, starting at the top, and stops as soon as an action successfully fires.
- 8 Once all of the actions have been added, click **OK** to create the policy and add it to the active list.

- 9 Assign the action policy to a device or monitor. For more information, see:
 - *Assigning an action to a device* (on page 147)
 - *Assigning an action to a monitor* (on page 161)



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.

Editing Action Policies

When you make changes to an action policy, you change the operation of all items that are currently assigned to use the policy.

To edit an action policy:

- 1 Open the Action Policies dialog.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Action Policies**.
- or -
From the main menu of the console, **Configure > Action Policies**. The Action Policies dialog appears.
- 2 On the Action Policies dialog, select the policy you want to edit.
- 3 Click **Edit**.
- 4 Make changes to the policy as necessary.
- 5 Click **OK**.

Implicit Action Policy

With the Implicit Action policy, WhatsUp Gold automatically assigns actions to all devices in your database. There is no way to opt out of the Implicit Action policy, so any action in that policy will be used by all devices. The Implicit Action Policy is not used for active monitors, just devices.

The Implicit Action policy is configured through the Action Policies dialog. 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 too.



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 v12. For more information on the Web Alarm Action, see *About Web Alarms* (on page 128).

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:

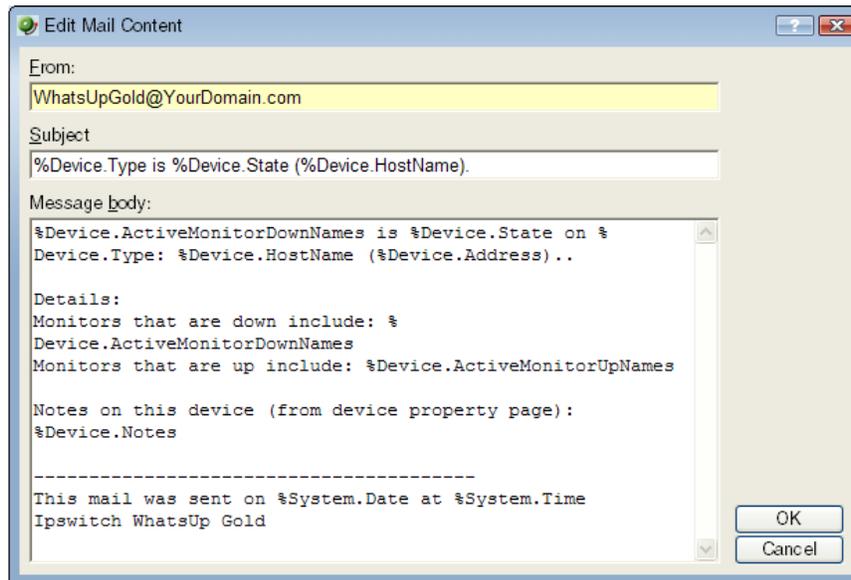
- 1 Open device properties for your Web server device (right-click a web server device, then click **Properties**). The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Active Monitors dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.
- 4 Use the following 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 screen, select **HTTP**, then click **Next**. The Set Polling Properties dialog appears.
 - b) 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 opens.
 - 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 the **Down** option in the **Execute the action on the following state change** list, then click **Finish**. The New Email Action dialog appears.
 - g) Enter the information as shown:

The screenshot shows the 'New Email Action' dialog box with the following fields and values:

- Name: MailtoWebmaster
- Description: E-mail Action
- SMTP Server: 192.168.5.5
- Port: 25
- Timeout (sec): 5
- Mail to: webmaster@yourdomain.com
- SMTP server requires authentication
- Username: EmailUserAccount
- Password: [masked with dots]
- Use and encrypted connection (SSL/TLS)

Buttons: Mail Content..., OK, Cancel

- h) Click **Mail Content**. The following information is included in the Edit Mail Content dialog and can be customized as required:



- i) Click **OK** to save changes and return to the previous screen. Click **OK** again to return to the Setup Actions for Monitor State Changes screen, then click **Finish**.

Setting up an HTTP Content Active Monitor with an email alert:

- 1 Open device properties for your Web server device (right-click the same Web server device you used for the email alert, then click **Properties**). 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 Use the same process to add the HTTP Content 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 screen, select **HTTP Content**, then click **Next**. The Set Polling Properties dialog appears.
 - b) 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.
 - 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) In the **Select an action from the Action Library** list, select **MailtoWebmaster**. In the **Execute the actions on the following state change** list, select **Down**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes screen.
 - f) On the Select Action and State screen, select **MailtoWebmaster**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.
 - g) Click **Finish**.

The two active monitors and resulting email actions are now enabled. When the Web server is down, HTTP Active Monitor will fail, triggering 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 could not return web content, the Email Action would report:

```
HTTP Content is down on server: web1.YourDomain.com (192.168.5.5)
```

Any details or notes specified in the action will also be reported.

Using Active Monitors

In This Chapter

Active monitors overview.....	157
About the Active Monitor Library.....	158
Assigning active monitors.....	160
Assigning an action to a monitor	161
Deleting active monitors	163
Group and Device active monitor reports.....	164
Example: monitoring network printer toner levels.....	164
Expression Editor	165
Using the Active Script Monitor	173
Using premium monitors	187

Active monitors overview

Active monitors query network services installed on a device, then wait on the response. If a response is not received or if the response does not match what is expected, the service is considered down, and a state change occurs on the device.

If the query is returned with the expected response, the service is considered up. The following Active Monitor types are available in WhatsUp Gold:

- Active Script Monitor
- DNS Monitor
- Email Monitor
- NT Service Monitor
- Ping Monitor
- SNMP Monitor
- TCPIP Monitor
- Telnet Monitor
- WMI Monitor (WhatsUp Gold Premium)
- Microsoft® Exchange™ and Microsoft SQL Server Monitor (WhatsUp Gold Premium)



Note: There are several types of TCPIP Monitors that are configured using the same dialog.

For more information about the Active Monitor types, see *Supported active monitors* (on page 159).

About the Active Monitor Library

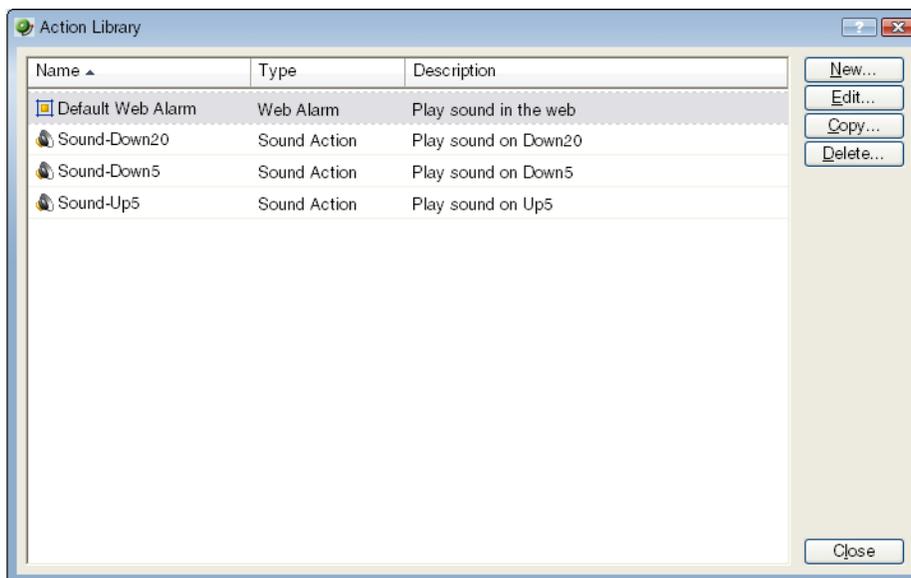
The Active Monitor Library is the central storehouse of all active monitors that have been configured for your network.

The Active Monitor Library dialog is used to configure active monitor types. It includes a list of Active Monitors that are available by default, on an out of the box installation. As you configure new active monitor types, they are listed here.

It's important to note that when you make changes to the active monitors listed in this dialog, the changes affect each instance of that particular monitor across your device groups.

To access the Active Monitor Library:

- On the console, click **Configure > Active Monitor Library**.
- On the web interface, on the **WhatsUp** section of the **GO** menu, click **Configure > Active Monitor Library**.



Use this dialog to configure new or existing active monitor types:

- Click **New** to configure a new type.
- Select an existing type, then click **Edit** to change its configuration.
- Select an active monitor type, then click **Copy** to make a copy of that type.

- Select an active monitor type, then click **Delete** to remove it from the list.
- In the WhatsUp Gold console, you can select an active monitor, then click **Test** to test the selected Active Monitor on a device.

Supported Active Monitors

The following is a list of all of the Active Monitor types that are supported by WhatsUp Gold.

Active Script Monitor. The Active Script Monitors let you write either VBScript or JScript code to perform a check on a device. If the script returns an error code, the monitor is considered down.



Note: Please be aware that Ipswitch does not support the scripts that you create, only the ability to use them in the Active Script Monitor.

- **DNS Monitor.** The DNS monitor is a simple service Monitor that checks for the DNS (Domain Name Server) on port 53. If no DNS service responds on this port, then the service is considered down.

Email Monitor. 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.
- **SNMP Monitor.** The Simple Network Management Protocol is the protocol governing network management and monitoring of network devices and their functions. This monitor queries the SNMP device and tries to match the expected returned value.
- **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.
- **Ping Monitor.** The Ping monitor sends an ICMP (ping) command to a device. If the device does not respond, the monitor is considered down.
- **TCP/IP Monitor.** The TCPIP monitor is used to monitor a TCPIP service that either does not appear in the list of standard services, or uses a non-standard port number.

NT Service Monitor. The NT Service Monitor checks the status of a service on a Windows machine and attempts a restart of the service (if the appropriate Administrator permissions exist).



Note: A running Windows Management Instrumentation (WMI) service on the targeted machine is required for this NT Service Monitor to work properly. Windows 2000 Service Pack 2 or higher, XP, and 2003 are installed with the WMI service. WMI is not installed with Windows NT, but can be downloaded from Microsoft and installed on Windows NT.

WhatsUp Gold Premium supports additional Active Monitor types:

- **Microsoft® Exchange™ and Microsoft SQL Server Monitor** manages the availability of key application services, rather than just the network visibility of the host server.
- **General application monitoring using Microsoft's WMI** monitors any performance counter value you specify, and triggers an alarm if the value changes, goes out of range, or undergoes an unexpected rate of change.

For more information, see *Using WhatsUp Gold Premium Edition* (on page 187).

Assigning active monitors

There are two steps in assigning an active monitor to a device. The first is to configure the active monitor in the Active Monitor Library, and the second is to add that Monitor to a device. For most users, the default configuration is sufficient and there is no need to make any changes to the active monitors in the library.

To configure (add/edit) an active monitor:

- 1 Open the Active Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**.
- 2 Click **New** to configure a new Active Monitor,
- or -
Select a monitor from the list and click **Edit** to make changes to an existing configuration.
The configuration dialog for the selected monitor type appears.
- 3 After you make the necessary changes, click **OK** to add the monitor to the list, or to save the changes you made to one already on the list.

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, make sure that the device has credentials assigned before creating an active monitor for it. For more information, see *Using Credentials* (on page 103).

There are a number of ways to assign Active Monitors to devices:

- Select the Active Monitors you want to scan for during Device Discovery. When you select the discovered devices and add them to your database, WhatsUp Gold creates a monitor for each network service found.
- In the Device Properties Active Monitor dialog, click **Discover**. WhatsUp Gold scans the device and creates a monitor for each network service found.

- 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 Setup actions for the monitor state changes.
 - 5 Click **Finish** to add the monitor to the device.
- Add when you create a new device:
 - 1 In the console click **File > New > New Device**. The Add New Device dialog appears.
- or -
In the web interface, from the **WhatsUp** section of the **GO** menu, click **Devices > New Device**. The Add New Device dialog appears.
 - 2 Click **Advance**. The Device Discovery Properties dialog appears.
 - 3 In the **Select Active Monitors to be used in the scan process** section, select the Active Monitors type you want to assign to the device.
 - 4 Click **OK**.
- 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, select **Bulk Field Change > Active Monitor**.
 - 3 Select the active monitor type you want to add.
 - 4 Click **OK**.

Assigning an action to a monitor

You can assign one or more individual actions to a monitor, or assign an action policy that may contain multiple actions.

To assign an action to an active monitor:



Note: During the configuration of a new monitor, you are presented with the Action Builder as part of the wizard. The following set of directions is for existing monitors.

- 1 Right-click the device the active monitor is configured on, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Active Monitors dialog appears.
- 3 Double-click the monitor on which you want to add actions.
- 4 Go to the actions properties:
 - From the web interface, in the Active Monitor Properties wizard, click **Next**.
 - or -
 - From the console, in the Active Monitor Properties dialog, select **Actions**.
- 5 Select the **Apply individual actions** option.
- 6 Click **Add** to access the Action Builder wizard.
- 7 Follow the directions in the Action Builder wizard.
- 8 At the end of the wizard, click **Finish** to add the action to the monitor.
- 9 If you need to add more actions to the monitor, click **Add** and repeat these directions.
- 10 Click **OK** after all actions have been added.

To assign an action policy to an active monitor:



Note: During the configuration of a new device, you are presented with the Action Builder as part of the wizard. The following instructions are for existing devices.

- 1 Right-click the device on which the active monitor is configured, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Active Monitors dialog appears.
- 3 Double-click the monitor on which you want to add actions.
- 4 Go to the actions properties:
 - From the web interface, in the Active Monitor Properties wizard, click **Next**.
 - or -
 - From the console, in the Active Monitor Properties dialog, select **Actions**.
- 5 Select the **Apply this Action Policy** option.
- 6 Select the action policy you want to use for this device. If you need to create a new action policy first, click the browse button to access the Action Policies dialog.
- 7 Click **OK** to save the changes.

To assign an action to a passive monitor:

- 1 Right-click the device the on which the passive monitor is configured, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Passive Monitors**.
- 3 Double-click the monitor on which you want to add actions. The Passive Monitor Properties appear.
- 4 Go to the actions properties:
 - From the web interface, in the Passive Monitor Properties wizard, click **Next**.
 - or -
 - From the console, the Passive Monitor dialog appears.
- 5 Click **Add** to access the Action Builder wizard.

- 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 If you need to add more actions to the monitor, click **Add** and repeat these directions.
- 9 Click **OK** after all actions have been added.



Note: You cannot assign an action policy to a passive monitor.

After an action has been added to the monitor, the action fires when that state reaches the assigned down state.

Deleting active monitors

Unless you are absolutely sure you need to remove an active monitor Type from the Active Monitor Library, you should never have to delete an item from this list. If you do, and you find you need it later, you will have to configure it completely again. This includes the default types that were added during initial installation of WhatsUp Gold. We recommend that you only delete the custom monitors that you create.



Caution: When you remove an active monitor type from the library, all active monitors of that type are deleted from the devices you are monitoring, and all related report data is lost.

The best course of action is to remove the monitors at the device level or to disable the monitor by clearing the selection on the Device Properties.

To remove a monitor from a device:

- 1 Right-click the device you want to remove the monitor from, then click **Properties**. The Device Properties dialog opens.
- 2 Click **Active Monitors**. The Active Monitors attached to the selected device displays in the list.
- 3 Select the monitor you want to remove.
- 4 Click **Remove**. A warning dialog opens, stating that all data for that monitor will be deleted if the monitor is removed.
- 5 Click **Yes** to remove the monitor.



Note: If you want to stop monitoring an Active Monitor on a device, but want to keep the historical data, then you must disable the monitor instead of deleting it from a device.

Using the Bulk Field Change feature

To remove an active monitor from multiple devices:

- 1 Select the devices in the Device View or Map View, then right-click on one of the selected items. The context menu appears.
- 2 Select **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog box appears.

- 3 In the **Operation** list, click **Remove**.
- 4 In the **Active Monitor type** list, select the active monitor that you want to remove.
- 5 Click **OK** to remove the monitor from the selected devices.

Group and Device active monitor reports

The following reports display information for devices or device groups that have active monitors configured and enabled. Access these reports from the Reports tab on the web interface. For more information, see *Using Full Reports* (on page 257).

- State Change Acknowledgement
- Active Monitor Availability
- Active Monitor Outage
- Health
- State Change Timeline
- State Summary
- Device Status

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 will notify you when toner levels are low.

To configure the printer monitor:

- 1 From the WhatsUp Gold web interface, click **Go > Configure > Active Monitor Library**. The Active Monitor Library 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.

- 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, TonerMonitor and Toner monitor for the Hewlett Packard LaserJet 4050N.

For the **Object ID** and **Instance**, click the browse (...) button; then locate and find 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
```

- 4 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 will fail when the printer toner level reaches 99.
- 5 Test the newly created active monitor and make appropriate changes if needed.

- 6 Assign the active monitor to the printer device, click **Device Properties > Active Monitors**.
- 7 In the active monitor dialog, click **Add**.
- 8 During the configuration wizard, create or select an action to notify you when the printer's toner levels are low.
- 9 Repeat steps 6-8 for each network printer that requires monitoring.

Expression Editor

WhatsUp Gold knows the proper connecting commands for checking the *standard* services listed on the Services dialog box, but to monitor a *custom* service, you may want to specify what commands to send to the service and what responses to expect from the service in order for WhatsUp Gold to consider the service up. It is up to you 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.

Script Syntax

You create a script using keywords. In general the Script Syntax is `Command=String`. 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 checking.

Keywords

- To send a string to a port, use the `Send=` keyword.
- To expect a string from a port, use the `SimpleExpect=` or the `Expect=` keyword.
- To comment out a line, use the `#` symbol as the first character of the line.
- To receive conditional responses for errors and successes, use *Flow Control Keywords* (on page 167).

Examples

If you have a TCP service to check where you needed to do the following:

- expect something on connection
- send a command
- check for a response
- send something to disconnect

Script Syntax: Expect=Keyword

This provides you a great amount of flexibility to accept variable responses and pick out only the information you need. This is accomplished using special control characters and regular expressions. If you do not need all this flexibility or are new to writing your own custom TCP/UDP scripts then you may want to start off using the SimpleExpect keyword first.

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 has the form `Expect=Response` where the Response is either specified as an exact text string or a mixture of regular expression rules and text. The **Add/Edit Expect Rule** button will help you construct and test a regular expression response string. It will automatically choose the variation of Expect for you based on options you select in that dialog. The **Add/Edit Expect Rule** button 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 will be converted automatically.

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
```

Script Syntax: Flow Control Keywords

The script language has been expanded to have conditional responses on "error" or "success" of a step within the scripts. This is done by using the following keywords.

- **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`

Script Syntax: Send=Keyword

To Send command on a connection, use a `Send=keyword`. The form 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
```

Script Syntax: SimpleExpect Keyword

The SimpleExpect Keyword lets you specify expected responses from your server. 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 the information you need. If you need additional flexibility you may want to consider using the regular expression syntax available in the Expect Keyword.

The SimpleExpect form is `SimpleExpect=Response`. Where the response is just 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 Hexidecimal) 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
```

Send to disconnect examples

For a service like FTP, this 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
```

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
<code>[...]</code> character class	Matches any character inside the brackets. Example, <code>[abc]</code> matches "a", "b", and "c"
<code>[^...]</code> negated character class	Matches any character except those inside the brackets. Example, <code>[^abc]</code> matches all characters except "a", "b", and "c". See below for alternate use - the way <code>^</code> is used controls its meaning.
<code>-</code> dash	Used within a character class. Indicates a range of characters. Example: <code>[2-7]</code> matches any of the digits "2" through "7". Example: <code>[0-3a-d]</code> is equivalent to <code>[0123abcd]</code>
<code>\</code> escaped character	Interpret the next character literally. Example: <code>3\.14</code> matches only "3.14". whereas <code>3.14</code> matches "3214", "3.14", "3z14", etc.
<code>\xnn</code> binary character	Match a single binary character. <code>nn</code> is a hexadecimal value between 00 and FF. Example: <code>\x41</code> matches "A" Example: <code>\x0B</code> matches Vertical Tab

Quantifiers

Meta-character	Matches
? question	One optional. The preceding expression once or not at all. Example: colou?r matches "colour" or "color" Example: [0-3][0-5]? matches "2" and "25"
* star	Any number allowed, but are optional. Example: .* Zero or more occurrences of any character
+ plus	One required, additional are optional. Example, [0-9]+ matches "1", "15", "220", and so on
??, +?, *?	"Non-greedy" versions of ?, +, and *. Match as little as possible, whereas the "greedy" versions match as much as possible Example: For input string <html>content</html> <.*?> matches <html> <.*> matches <html>content</html>

Matching Position

Meta-character	Matches
^ caret	Matches the position at the start of the input. Example: ^2 will only match input that begins with "2". Example: ^[45] will only match input that begins with "4" or "5"
\$ dollar	At the end of a regular expression, this character matches the end of the input. Example: >\$ matches a ">" at the end of the input.

Other

Meta-character	Matches
alternation	Matches either expression it separates. Example: H Cat matches either "Hat" or "Cat"
(...)	Provides grouping for quantifiers, limits scope of alternation via precedence. Example: (abc)* matches 0 or more occurrences of the the string abc Example: WhatsUp (Gold) (Professional) matches "WhatsUp Gold" or "WhatsUp Professional"
\0, \1, ... backreference	Matches text previously matched within first, second, etc, match group (starting at 0). Example: <{head}>.*?</\0> matches "<head>xxx</head>".
! negation	The expression following ! does not match the input Example: a!b matches "a" not followed by "b".

Abbreviations

Abbreviations are shorthand Meta-characters.

Abbreviation	Matches
\a	Any alphanumeric character: ([a-zA-Z0-9])
\b	White space (blank): ([\t])
\c	Any alphabetic character: ([a-zA-Z])
\d	Any decimal digit: [0-9]
\D	Any non decimal digit [^0-9]
\h	Any hexadecimal digit: ([0-9a-fA-F])
\n	Newline: (\r \r?\n)
\p	Any punctuation character: ,\!:\;"'?!@#\$\$%^&*(){}- _+= <>!~
\P	Any non-punctuation character
\q	A quoted string: (\("[^"]*" '[^']*')
\s	WhatsUp Gold style white space character [\t\n\r\f\v]
\S	WhatsUp Gold style non-white space character [^\t\n\r\f\v]
\w	Part-of-word character ([a-zA-Z0-9_])
\W	Non-word character ([^a-zA-Z0-9_])
\z	An integer: ([0-9]+)

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 to find the proper value for **SimpleExpect**, or an **Expect** string for a particular service. Packet Capture tools can also be very useful.

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 see what comes back. 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 will not provide you with a simple response string to use. You can use a packet capture tool to view these types of responses.

Using the Active Script Monitor

The Active Script Monitors let you write either VBScript or JScript code to perform a check on a device. If the script returns an error code, the monitor is considered down.



Note: Please be aware that Ipswitch does not support the scripts that you create, only the ability to use them in the Active Script Monitor.

- **Name.** The name of the monitor as it appears in the Active Monitor Library.
- **Description.** The description of the monitor as it appears in the Active Monitor Library.
- **Timeout.** The amount of time (in seconds) WhatsUp Gold should wait for a response to the poll.



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 you want to use to write this script (either VBScript or JScript).
- **Script text.** Write or insert your monitor code here.
- **Use in discovery.** Select this option to have the monitor appear in the Active Monitor list during discovery. From there, you can select the monitor to have WhatsUp Gold discover that monitor type in your devices.

This script monitor has a context object that you can use to poll for specific information about the device in context. For more information, see *Using the Active Script Monitor context object* (on page 174).

We have provided several code samples for you to create useful active script monitors for your devices. For more information, see *Examples: Active Script Monitor context code* (on page 177)

All script features in WhatsUp Gold utilize the SNMP API. For more information, see *Using the SNMP API* (on page 381).

Using the Active Script Monitor context object

The context object is available to the script programmer when scripts are executing. It delivers context aspects of the device that it is operating upon. All methods and properties are retrieved using the `Context` namespace.

We have provided several code samples for you to create useful Active Script Monitors for your devices.

Methods	Method description
<code>LogMessage (sText)</code>	<p>This method allows for a message to be written to the WhatsUp Gold debug log.</p> <p>Example:</p> <p>JScript:</p> <pre>Context.LogMessage("Checking Monitor name using Context.GetProperty() ");</pre> <p>VBScript:</p> <pre>Context.LogMessage "Checking Address using Context.GetProperty() "</pre>
<code>PutProperty (sPropertyName)</code>	<p>This method allows you to store a value in the INMSerialize object. This value is retained across polls.</p> <p>Example:</p> <p>JScript:</p> <pre>var nCount = parseInt(nNum) +1; Context.PutProperty("MyNumeric",nCount);</pre>
<code>SetResult (nCode, sText)</code>	<p>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.</p> <p>Important: Every script should have a result, otherwise it will report back positively.</p> <p>Example:</p> <p>JScript:</p> <pre>Context.SetResult(0, " Everything is OK"); //Success Context.SetResult(1, " Really big big error"); //Failure</pre> <p>VBScript:</p> <pre>Context.SetResult 1, " Really big big error"</pre>

Properties

Property	Description																																				
GetProperty (sPropertyName)	<p>This property offers access to many device specific aspects. You obtain access to these items using the names listed. These names are case sensitive.</p> <table border="1"> <thead> <tr> <th>Property</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>"ActiveMonitorTypeName"</td> <td>The active monitor display name</td> </tr> <tr> <td>"Address"</td> <td>The IP address of the device</td> </tr> <tr> <td>"DeviceID"</td> <td>The device ID</td> </tr> <tr> <td>"Mode"</td> <td>1 = doing discovery 2 = polling 3 = test</td> </tr> <tr> <td>"ActiveMonitorTypeID"</td> <td>The active monitor's type ID</td> </tr> <tr> <td>"CredSnmpV1:ReadCommunity"</td> <td>SNMP V1 Read community</td> </tr> <tr> <td>"CredSnmpV1:WriteCommunity"</td> <td>SNMP V1 Write community</td> </tr> <tr> <td>"CredSnmpV2:ReadCommunity"</td> <td>SNMP V2 Read community</td> </tr> <tr> <td>"CredSnmpV2:WriteCommunity"</td> <td>SNMP V2 Write community</td> </tr> <tr> <td>"CredSnmpV3:Username"</td> <td>SNMP V3 Username</td> </tr> <tr> <td>"CredSnmpV3:Context"</td> <td>SNMP V3 Context</td> </tr> <tr> <td>"CredSnmpV3:AuthPassword"</td> <td>SNMP V3 Authentication password</td> </tr> <tr> <td>"CredSnmpV3:AuthProtocol"</td> <td>SNMP V3 Authentication protocol</td> </tr> <tr> <td>"CredSnmpV3:EncryptPassword"</td> <td>SNMP V3 Encrypt password</td> </tr> <tr> <td>"CredSnmpV3:EncryptProtocol"</td> <td>SNMP V3 Encrypt protocol</td> </tr> <tr> <td>"CredWindows:DomainAndUserid"</td> <td>Windows NT Domain and User ID</td> </tr> <tr> <td>"CredWindows:Password"</td> <td>Windows NT Password</td> </tr> </tbody> </table>	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
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																																				
GetDB	This property returns an open connection to the WhatsUp Gold database.																																				

GetProperty Examples

JScript:

```
var sAddress = Context.GetProperty("Address");
var sReadCommunity = Context.GetProperty("CredSnmpV1:ReadCommunity");
var nDeviceID = Context.GetProperty("DeviceID");
```

JScript:

```
//Sending log message to the WhatsUp Event Viewer
Context.LogMessage ( "Checking Mode flag");

var nFlag = Context.GetProperty("Mode");

if (nFlag == 1)
{
    Context.LogMessage ("Doing a discovery");
}
else if (nFlag == 2)
{
    Context.LogMessage ("Doing a poll");
}
else if (nFlag == 3)
{
    Context.LogMessage ("Must be just a test.");
}
else
{
    Context.LogMessage ("Do not know the mode.");
}

//Set the result code of the check (0=Success, 1=Error)
Context.SetResult (0, "No error");
```

GetDB Examples

This example gets the Open connection and reads some values out of the WhatsUp Gold "Device" table using the deviceID context. Refer to the WhatsUp Gold Database Schema for more information about the WhatsUp Gold schema.

```
var oDb = Context.GetDB;
if (null == oDb)
{
    Context.SetResult( 1, " Problem creating the PRO DB object");
}
else
{
    var oRs = new ActiveXObject("ADODB.Recordset");
    // Get the device ID
    var nDeviceID = Context.GetProperty("DeviceID");
    var sSql = "SELECT * from Device WHERE nDeviceID = " + nDeviceID;
    oRs = oDb.Execute(sSql);
```

```
if ( !oRs.EOF )
{
  var sDisplay;
  sDisplay = "" + oRs("sDisplayName");
  Context.LogMessage("Display Name=" + sDisplay);
  sDisplay = "" + oRs("nWorstStateID");
  Context.LogMessage("WorstStateID=" + sDisplay);
  sDisplay = "" + oRs("sNote");
  Context.LogMessage("Note=" + sDisplay);
  sDisplay = "" + oRs("sStatus");
  Context.LogMessage("Status=" + sDisplay);
}
Context.SetResult( 0, " Ok");
}
```

Examples: Active Script Monitor context code

The following table lists several active script monitor context code examples that you can use to create useful active monitors for your devices. To use these examples, select the text of the context and then copy and paste the code into the **Script text** box of the Active Script Monitor dialog.



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

Sample Monitor 1

To return the results of the script to WhatsUp Gold.



Note: This affects the state of the device.

JScript:

```
Context.SetResult(0, "Everything is OK"); //Success
Context.SetResult(1, "Really big big error"); //Failure
```

VBScript:

```
Context.SetResult 1, "Really big big error"
```

Sample Monitor 2

To log a message to the WhatsUp Gold event viewer.



Note: In order to view Context.LogMessage entries, the **Debug On** option in the event viewer must be selected.

JScript:

```
Context.LogMessage("This is the message");
```

Sample Monitor 3

To access the Device ID.

JScript:

```
var nDeviceID = Context.GetProperty("DeviceID");
```

Sample Monitor 4

Accessing the IP address of the device.

JScript:

```
var sAddress = Context.GetProperty("Address");
```

Sample Monitor 5

To access the device credentials.



Note: All passwords are decrypted.

JScript:

```
var sV1ReadCommunity = Context.GetProperty("CredSnmpV1:ReadCommunity");  
var sV1WriteCommunity =  
Context.GetProperty("CredSnmpV1:WriteCommunity");  
var sV2ReadCommunity = Context.GetProperty("CredSnmpV2:ReadCommunity");  
var sV2WriteCommunity =  
Context.GetProperty("CredSnmpV2:WriteCommunity");  
var sV3UserName = Context.GetProperty("CredSnmpV3:Username");  
var sV3Context = Context.GetProperty("CredSnmpV3:Context");  
var sV3AuthPassword = Context.GetProperty("CredSnmpV3:AuthPassword");  
var nV3Authprotocol = Context.GetProperty("CredSnmpV3:AuthProtocol");  
var sV3EncryptPassword =  
Context.GetProperty("CredSnmpV3:EncryptPassword");  
var nV3EncryptProtocol =  
Context.GetProperty("CredSnmpV3:EncryptProtocol");
```

```
var sNTUsername = Context.GetProperty("CredWindows:DomainAndUserid");
var sNTPassword = Context.GetProperty("CredWindows:Password");
```

Sample Monitor 6

To access the WhatsUp Gold database.

This sample uses the device ID in context and accesses the 'Device' table.

JScript:

```
// Get the Open DB connection from the Context NameSpace
var oDb = Context.GetDB;
if (null == oDb)
{
Context.SetResult( 1, " Problem creating the PRO DB object");
}
else
{
// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");
// Retrieve all columns for this device.
var sSql = "SELECT * from Device WHERE nDeviceID = " + nDeviceID;
var oRs = oDb.Execute(sSql);
if ( !oRs.EOF )
{
// Display various columns in the debug log (Event Viewer).
var sDisplay;
sDisplay = "" + oRs("sDisplayName");
Context.LogMessage("Display Name=" + sDisplay);
sDisplay = "" + oRs("nWorstStateID");
Context.LogMessage("WorstStateID=" + sDisplay);
sDisplay = "" + oRs("sNote");
Context.LogMessage("Note=" + sDisplay);
sDisplay = "" + oRs("sStatus");
Context.LogMessage("Status=" + sDisplay);
}
Context.SetResult( 0, " Ok");
}
```

Sample Monitor 7

Using WMI, see who is currently logged on to a device.

You can set the monitor to be down if the logged on user is not the expected user. In this case, if no one is logged on, then the monitor is assumed up.

VBScript:

```
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.ActiveConnection = oDBconn
' oStateRS.CursorType =3 'adOpenStatic cursorType

      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
```

Sample Monitor 8

Use SNMP to monitor the total bandwidth utilization on an interface (in and out octets) by polling values of the interface MIB.

JScript:

```
// 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);
}
```

Sample Monitor 9

To monitor an SNMP agent running on a non standard port (the standard SNMP port is 161).

JScript:

```
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 );
    }
}
}
```

Sample Monitor 10

To access SNMP using WhatsUp PRO CoreAsp.dll Interface DLL.

This code sample uses WhatsUp PRO CoreAsp.dll and uses the Snmprqst interface.

JScript:

```
var oSnmprqst = new ActiveXObject("CoreAsp.Snmprqst");
// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");
//
// Function to get SNMP details
//
```

```
function getSnmpDetails()
{
var oResult = oSnmpRqst.Initialize(nDeviceID);
if(oResult.Failed)
{
return null;
}
var oReturnArray = new Array();
oReturnArray["sysDescr"] = SnmpGet("1.3.6.1.2.1.1.1.0"); // sysDescr
if(oReturnArray["sysDescr"] == null)
{
return null;
}
oReturnArray["objectID"] = SnmpGet("1.3.6.1.2.1.1.2.0"); // objectID
oReturnArray["sysUpTime"] = SnmpGet("1.3.6.1.2.1.1.3.0"); // sysUpTime
oReturnArray["sysContact"] = SnmpGet("1.3.6.1.2.1.1.4.0"); // sysContact
oReturnArray["sysName"] = SnmpGet("1.3.6.1.2.1.1.5.0"); // sysName
oReturnArray["sysLocation"] = SnmpGet("1.3.6.1.2.1.1.6.0"); //
sysLocation
return oReturnArray;
}
//
// Helper function to get specific OID
//
function SnmpGet(sOid)
{
var oResult = oSnmpRqst.Get(sOid);
if(oResult.Failed)
{
return null;
}
else
{
return oResult.GetPayload;
}
}
//
// Get the SNMP details for the device that we passed in via the
Context.
//
var oSNMPDetails = getSnmpDetails();
if(oSNMPDetails != null)
{
Context.LogMessage( "SNMP Details");
Context.LogMessage( " sysDescr=" + oSNMPDetails["sysDescr"]);
Context.LogMessage( " objectID=" + oSNMPDetails["objectID"]);
Context.LogMessage( " sysUpTime=" + oSNMPDetails["sysUpTime"]);
Context.LogMessage( " sysContact=" + oSNMPDetails["sysContact"]);
Context.LogMessage( " sysName=" + oSNMPDetails["sysName"]);
Context.LogMessage( " sysLocation=" + oSNMPDetails["sysLocation"]);
// Set success
Context.SetResult(0, "Device is SNMP enabled." );
}
```

```
}  
else  
{  
// Set an error  
Context.SetResult(1, "Device is not SNMP enabled.");  
}
```

Using premium 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:

- 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.
- 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.
- Email monitor lets you periodically verify that mail servers are not only up, but are receiving and delivering messages properly.

Monitoring a Microsoft Exchange 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 2000 or later versions, which can be on any machine in your network.

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 will be 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. In other words, you can detect a looming problem before it causes an application or service failure.

How to get started using the Exchange Monitor

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 parameters to monitor.
- 2 Determine which Exchange 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.

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. For example, a single monitor to check disk space, named ExchangeDisk, is reported in logs with this name. If ExchangeDisk is reported down, you know it's a disk space problem.

- 4 Configure an Exchange Monitor 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.

Configuring an Exchange Monitor

To configure an instance of the Exchange Monitor:

- 1 Go to the Active Monitor Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**.
 - or -
 - From the main menu bar of the console, select **Configure > Active Monitor Library**. The Active Monitor Library appears.



Tip: The Active Monitor Library is the starting point for creating any Active Monitor in WhatsUp Gold. This dialog shows all of the Active Monitors in your database.

- 2 Add an Exchange monitor:
 - a) Click **New**. The Select Active Monitor Type dialog appears.
 - b) Select **Exchange Monitor** from the list. The New Exchange Monitor Server dialog appears.
 - c) In the **Name** box, enter the name you want to use to identify this instance of the Exchange monitor. For example, if you are configuring a monitor to check disk space, you might enter ExchangeDisk.
 - d) In the **Description** box, enter any text information to further describe the monitor.
 - e) Select the thresholds to add to the monitor. For more information about specific thresholds, see *Exchange parameters* (on page 189).

- f) Select the services to monitor. For more information about specific services, see *Exchange services* (on page 190).
- g) Click **OK** to save the monitor in the Active Monitor Library.

3 Add the 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.

Select the 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 130).

If you select **Use in discovery**, WhatsUp Gold adds the monitor to the Active Monitors list. From that list, you can select to scan for that service on all applications found during discovery.

Exchange 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.

Exchange 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.

Example: Exchange Server monitor

To monitor what is happening with 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 Open the Active Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**. The Active Monitor Library appears.
- 2 Click **New**. The Select Active Monitor Type dialog appears.
- 3 Select Exchange Monitor and click **OK**. The New Exchange Server Monitor dialog appears.
 - a) In the **Name** box, enter `ExchangeSystemCheck` to identify that this monitor will do 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. You need to clear the selections for the other parameters and also for the other processes.
 - c) Select the **CPU** parameter, then click **Configure**. The CPU Threshold dialog opens. Enter an appropriate threshold and click **OK**.
 - d) Select the **Memory** parameter, then click **Configure**. The Memory Threshold dialog opens. Enter an appropriate threshold for the amount of free memory and click **OK**.
 - e) Select the **System** parameter, then click **Configure**. The System Threshold dialog opens. Enter an appropriate threshold and click **OK**.
 - f) Click **OK** to add the ExchangeSystemCheck monitor to the Active Monitor library.
- 4** 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.
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 130).
After you complete the wizard, the monitor immediately begins to monitor the Exchange server.

Monitoring Microsoft SQL Server

The SQL Server Monitor lets you monitor Microsoft® SQL Server. The SQL Server Monitor provides real-time information about the state and health of Microsoft SQL Server applications on your network.



Note: Microsoft SQL Monitor is available as part of WhatsUp Gold Premium Edition.

The SQL Server Monitor supports monitoring of Microsoft SQL Server 2000 or later versions, and MSDE 2000 or later versions, which can be on any machine in your network.

To create custom parameters to monitor, the SQL Server host must be WMI-enabled.

Why use it?

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, your users will be unable to get mail, transfer files, or use the web. It is a good idea to set up monitoring on these services so that you are the first to know if they fail. The SQL Server 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.

How to get started using SQL Server Monitor

- 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 will be reported down if any of the parameters or services in that monitor are down.

Configuring an SQL Server Monitor

To configure an instance of the SQL Server Monitor:



Important: You must activate WhatsUp Gold Premium Edition before configuring an SQL Server Monitor.

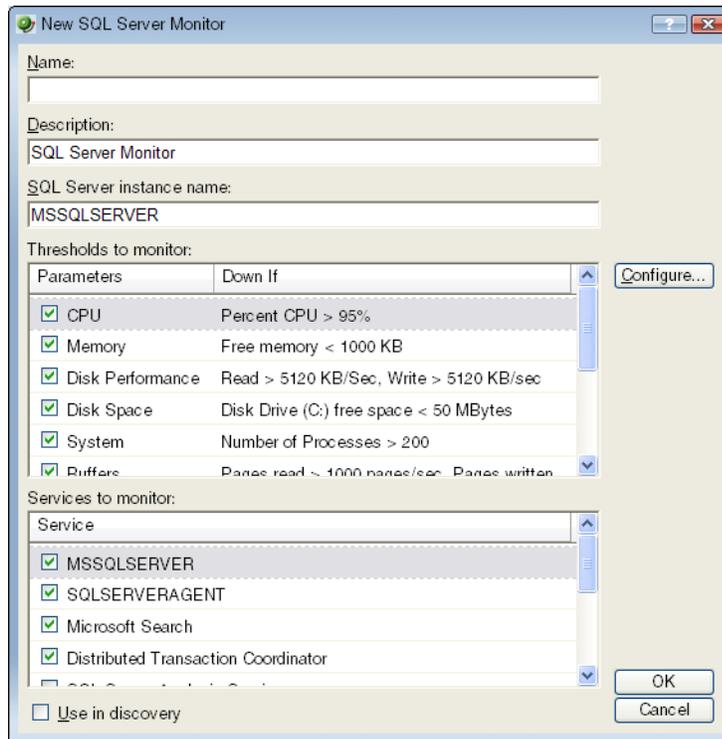
- 1 Open to the Active Monitor Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**.
- or -
 - From the main menu bar of the console, select **Configure > Active Monitor Library**. The Active Monitor Library appears.



Tip: The Active Monitor Library is the starting point for creating any Active Monitor in WhatsUp Gold. This dialog shows all of the Active Monitors in your database.

- 2 Add an SQL monitor:
 - a) Click **New**. The Select Active Monitor Type dialog appears.
 - b) Select SQL Service Monitor and click **OK**.

- c) The New SQL Service Monitor dialog appears.



- d) In the **Name** box, enter the name you want to use to identify this instance of the SQL Server monitor. For example, if you are configuring a monitor to check disk space, you might enter `SQLServerDisk`.
- e) In the **Description** box, enter any text information to further describe the monitor.
- f) In the **SQL Server Instance Name** box, enter the name of the database you want to monitor.
- g) Select the thresholds to add to the monitor. For more information about specific thresholds, see *SQL Server Parameters* (on page 194).
- h) Select the services to add to the monitor. For more information about specific services, see *SQL Server Services* (on page 194).
- i) Click **OK** to save the monitor in the Active Monitor Library.
- 3** Add the monitor to your SQL Server device.
- a) In your device list, find the device that represents the SQL Server. Right-click the device, then select **Properties**. Select **Active Monitors**.
- b) Click **Add**. The Active Monitor wizard appears.
- Select the 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 130).

If you select **Use in discovery**, WhatsUp Gold adds the monitor to the Active Monitors list. From that list, you can select to scan for that service on all applications found during discovery.

SQL Server Parameters

You can set thresholds on the following parameters:

Select this parameter:	If you want to:
CPU	Monitor 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:	If you want to:
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

To monitor user activity on an SQL Server, you can create a monitor called `SQLUser`, then select `Users` as the only parameter to monitor.

- 1 Open the Active Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**. The Active Monitor Library appears.
- 2 Click **New**. The Select Active Monitor Type dialog appears.
- 3 Select SQL Server Monitor and click **OK**. The New SQL Server Monitor dialog appears.
 - a) In the **Name** box, enter `SQLUser`.
 - b) In the **SQL Server Instance Name** box, enter the name of your database.
 - c) Make sure that **Users** is the only parameter that has a check in the box to the left of it. You will need to clear the selections for the other parameters and also for the processes.
 - d) Click the **Users** parameter to select it, then click **Configure**. The Users Threshold dialog opens. You should have in mind how many users or connections you want to consider as a threshold, and enter those values in the appropriate boxes on the dialog.
 - e) When finished, click **OK** to add the SQLUser monitor to the Active Monitor Library.
- 4 Add the SQLUser monitor to your SQL server device.
 - a) In the device list, select the device that represents the SQL server. Right-click the device, then select **Properties**. Select Active Monitors.
 - b) Click **Add**. The Active Monitor wizard appears.

Select the SQLUser monitor and continue with the wizard to add to configure actions for the monitor.

For more information on setting up an action, see *Configuring an action* (on page 130).

After you complete the wizard, the monitor immediately begins to monitor the SQL Server application.

Monitoring WMI-enabled applications

The WMI Monitor lets you monitor any WMI-enabled application. The WMI Monitor lets you create custom monitors to get real-time information about the state and health of applications and servers on your network. Most Windows applications and servers support WMI and provide their own set of real-time WMI data.



Note: WMI Monitor is part of the WhatsUp Gold Premium Edition, which extends monitoring capabilities.

To create custom monitors, the host on which the application or server is installed must be WMI-enabled. You can connect to a host and view the WMI parameters reported by the Windows applications and servers on that host.

Why use it?

WhatsUp Gold can monitor and report the status of the standard services associated with TCP/IP servers, such as SMTP, POP3, IMAP, FTP, HTTP. If any of these services fail, network users cannot send mail, transfer files, or use the web. It is a good idea to set up monitoring on these services so that you are the first to know if they fail. The WMI Monitor extends monitoring to parameters reported by Windows-based applications and servers, allowing you to get an early warning of a degradation in performance. For example, you can monitor system parameters on your Oracle® database server to see if performance is within an expected range, and if not, you can intervene before the Oracle server fails. In other words, you can detect a looming problem before it causes an application or service failure.

How to use WMI Monitors

This topic describes the overall process of 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 tell you when the monitor goes down or comes back up.



Note: The monitor will be reported down if any of the objects that you selected to monitor are down.

Configuring a WMI Monitor

To configure an instance of the WMI Monitor:

- 1 Open the Active Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select Active Monitor Library.

The Active Monitor Library is the starting point for creating any Active Monitor in WhatsUp Gold. This dialog shows all of the Active Monitors in your database.
- 2 Add a WMI Monitor:
 - a) Click **New**. The Select Active Monitor Type dialog appears.
 - b) Select **WMI Monitor** and click **OK**. The New WMI Monitor dialog appears.
- 3 Enter or select the appropriate information in the following fields.
 - **Name**. The name of the monitor as it appears in the Active Monitor Library.
 - **Description**. The description of the monitor as it appears in the Active Monitor Library.
 - **Performance counter/Instance**. Click the browse button next to this box to select a performance counter and instance for the monitor.
 - **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.
 - **Check values**. Enter the values for the check type selected above. For **Constant Value** and **Rate of Change**, select the state of the device when the check value is met.



Note: You can also click **Advanced** to access Advanced Monitor Properties.

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) Open the Active Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - a) On the **WhatsUp** section, select **Configure > Active Monitor Library**. The Active Monitor Library appears.
 - b) Click **New**. The Select Active Monitor Type dialog opens.
 - c) Select **WMI Monitor** and click **OK**. The Add WMI Monitor dialog appears.
 - d) In the **Name** box, enter "ErrorsLogon" to identify that this monitor checks for logon errors.
 - e) Click the **Browse (...)** button next to **Instance** to access the Performance Counters dialog.
 - f) Enter the computer name or IP address of the computer in which you want to connect.
 - g) Select a credential from a list of Windows credentials (pulled from the Credentials Library), then click **OK** to connect to the computer.
 - h) In the **Performance object** box, select Server.
 - i) In the **Server** folder, select the **ErrorsLogon** performance counter.

Take note of the Current value entry at the bottom of the dialog. This is the number of logon errors currently reported through WMI.

Click **OK** to add the Performance counter to the New WMI Monitor dialog.
 - j) In the **Check type** box, select **Rate of Change**.
 - k) 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.
 - l) In the **If the value is above the rate, then the monitor is** box, select **Down**.
 - m) 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 for the device, select the **Credentials** section.
 - b) In the Credentials Section, click the browse (...) button next to **Windows credentials** to access the Credentials Library.
 - c) Create a Windows credential using the administration login and password for the device you want to create the passive monitor for. When you have configured the credential, click **Close**.
 - d) On the Credentials page, select the new **Windows credential**, then click **OK**.
- 3 Add the **ErrorsLogon** monitor to the problem device.
 - a) In your device list, find the device. Double-click the device to display its properties, then select Active Monitors.

- b) Click **Add**. The Active Monitor wizard appears.
Select the ErrorsLogon monitor, and continue with the wizard to configure any actions for the monitor.
- c) For more information on setting up an action, see *Configuring an Action* (on page 130).

You may want to 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 may be able to block the IP or take the device off the network while the attack is addressed.

Monitoring Mail Servers

The Email Monitor lets you monitor that a mail server is available and functioning correctly. 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.

Configuring an Email Active Monitor

To configure an Email monitor:

- 1 Go to the Active Monitor Library:
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**. The Active Monitor Library appears.
 - or -
 - From the main menu of the console, select **Configure > Active Monitor Library**. The Active Monitor Library appears.
- 2 Add an Email Monitor:
 - a) Click **New**. The Select Active Monitor Type dialog appears.

- b) Select Email Monitor from the list, then click **OK**. The Add Email Monitor dialog appears.
- c) In **Name**, enter a title to identify this instance of the monitor.
- d) In **Description**, enter any additional information to further describe the monitor.
- e) In the **Outgoing mail** section of the dialog, in **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.
- f) In **Port**, enter the port on which the SMTP service is listening. The standard SMTP port is 25.
- g) In **Mail to**, enter the address to which the Email Monitor will send email.
- h) In **Mail from**, enter the address from which the Email Monitor was sent from.
- i) In the **Incoming mail** section of the dialog, in **Server**, enter the address of the server on which the POP3 or IMAP service is running.
- j) In **Account type**, select the protocol (POP3 or IMAP) you want the monitor to use to check for correct email delivery.
- k) In **Username**, enter the username of the email account in which the monitor will use to log in.
- l) In **Password**, enter the password for the email account in which the monitor will use to log in.
- m) Click **OK** to add the monitor to the Active Monitor Library.

If you want to configure advanced settings for this instance of the Email Monitor, click **Advanced**. From here, you can choose to use SMTP Authentication; set the port on which POP3 or IMAP is running; use encrypted connections for SMTP, IMAP, and POP3; and set timeouts for SMTP, IMAP, and POP3.

3 Add the monitor to your mail server.

- a) On the device list, find the device that represents the mail server. Right-click the device, then select **Properties**. Select **Active Monitors**.
- b) Click **Add**. The Active Monitor Wizard appears.

Select the 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 130).

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:

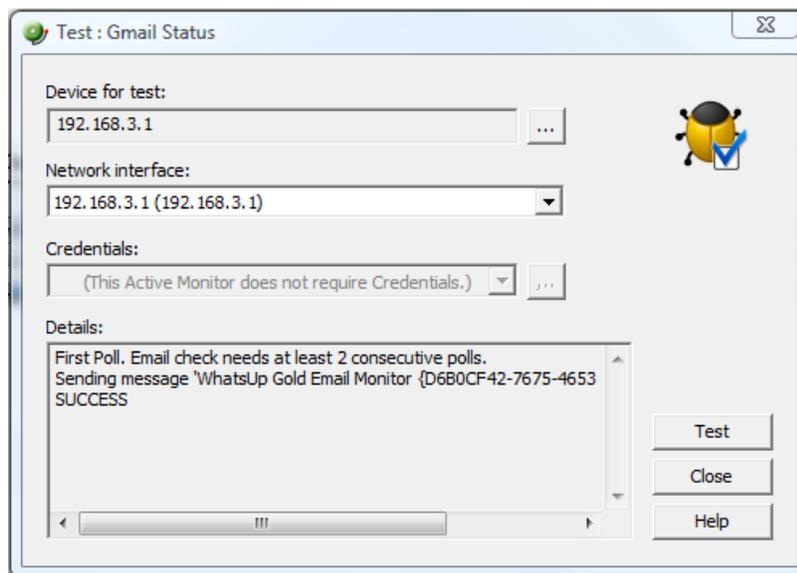
- 1 Open the Active Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Active Monitor Library**. The Active Monitor Library appears.

- 2 Click **New**. The Select Active Monitor Type dialog appears.
- 3 Select the Email Monitor, then click **OK**. The Add Email Monitor dialog appears.

The screenshot shows the 'Edit Email Monitor' dialog box. The 'Name' field is 'Gmail Status' and the 'Description' is 'Checks Gmail status'. Under 'Outgoing Mail', the SMTP server is 'smtp.gmail.com', the port is '587', the 'Mail to' is 'youraccount@gmail.com', and the 'Mail from' is 'youraccount@gmail.com'. Under 'Incoming Mail', the server is 'pop.gmail.com', the account type is 'POP3', the port is '995', the username is 'youraccount@gmail.com', and the password is masked with dots. The 'Advanced' button is visible on the right side of the dialog.

- 4 Enter or select the appropriate information in the dialog fields:
 - 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 Mail server.
 - h) Choose POP3 from the **Account type** list.
 - i) Enter 995 for the Port.
 - j) Again, enter your Gmail account in **Username**.
 - k) Enter the password for your Gmail account in **Password**.
- 5 Click **Advanced**. The Advance Monitor Properties dialog appears.
- 6 Enter or select the appropriate information in the dialog fields:
In the **Outgoing server advanced properties** section of the dialog:
 - a) Select **SMTP server requires authentication**.
 - b) Enter your Gmail account in **Username**.
 - c) Enter the password for your Gmail account in **Password**.

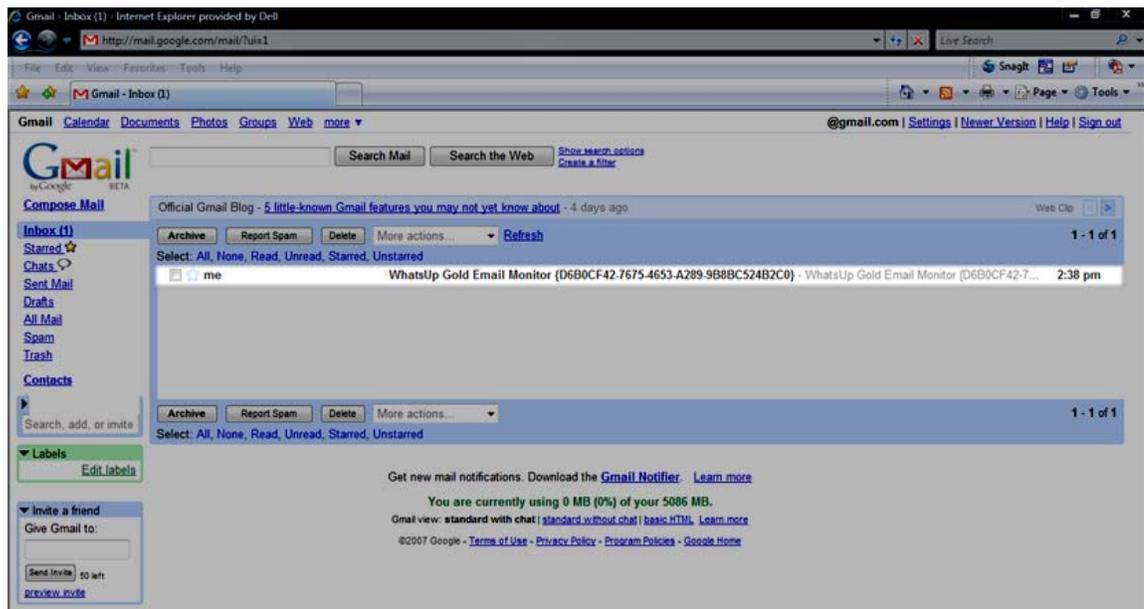
- d) Select **Use an encrypted connection (SSL/TLS)**.
 - e) Use the default **Timeout** of 5 seconds.
In the **Incoming server advanced properties** section of the dialog:
 - f) Select **Use an encrypted connection (SSL/TLS)**.
 - g) Ensure that **Use STARTTLS command** is not selected.
 - h) Use the 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.
- 7 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.

Using WhatsUp Gold v12

You can log in to the Gmail account used for the Gmail Status monitor and actually see the email sent by WhatsUp Gold via the Email Monitor.



Using Passive Monitors

In This Chapter

About Passive Monitors	205
Assigning passive monitors	206
Configuring Passive Monitor Listeners	207
About the Passive Monitor Library	209
Group and device passive monitor reports	210
Receiving SNMP Traps	210

About Passive Monitors

Unlike active monitors or performance monitors, which actively poll a device to check its status or to gather statistical data, passive monitors passively listen for events on devices.

Because it does not repeatedly poll devices and wait for a device to signal a problem, a passive monitor uses less resources than an active monitor both on the machine running WhatsUp Gold and on the network.

Passive monitors are also useful because some devices on a network may not provide a clear up or down status when queried. For example, a message may get logged to the system's Event log by another application (such as an antivirus application alerting when a virus is found). Since these messages/events can occur at any time, a Passive Monitor Listener "listens" for them, and notifies WhatsUp Gold when they occur.

However, the information that can be reported in a passive monitor event is not as customizable as it is with active monitors. In the case of a severe device failure, a device may enter a state where it is not able to successfully send a passive monitor event. A connectivity loss may prevent the WhatsUp system from receiving an event sent to it as well.

Passive monitors should be used to complement active monitors, but you should not rely solely on Passive Monitors to monitor a device or service.

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.

Assigning passive monitors

There are two steps in assigning a passive monitor to a device. The first is to configure the active monitor in the Passive Monitor Library, and the second is to add that Monitor to a device.

To configure (add/edit) a passive monitor manually:

- 1 Open the Passive Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Passive Monitor Library**.
- 2 Click **New** to configure a new Passive Monitor. The configuration dialog for the selected monitor type appears.

- or -

Select a monitor from the list, then click **Edit** to make changes to an existing configuration. The Edit dialog for the selected monitor appears.

- 3 After you make the necessary changes, click **OK** to add the monitor to the list or to save the changes you made to a monitor already on the list.

To assign a passive monitor to a device:



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 103).

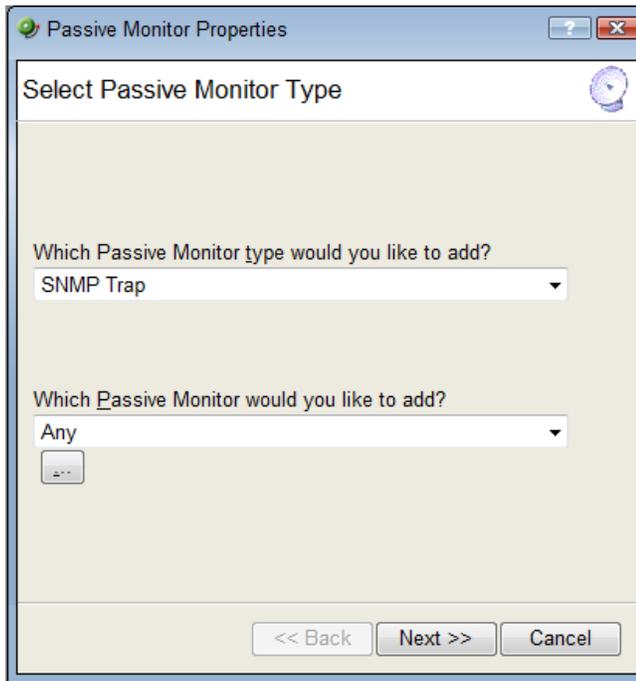
If you want to use multiple Windows Event Log passive monitors, you must assign a unique Windows Event Log passive monitor for each device.



Note: The upgrade process to WhatsUp Gold v12 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 103).

- 1 Right-click the device to which you want to assign a passive monitor, 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. Click:

Select an action from the Action Library

- or -

Create a new action

Follow the remaining Wizard dialog screens for the selection you made.

- 6 Click **Finish** to add the passive monitor to the device.

Configuring Passive Monitor Listeners

A Passive Monitor Listeners listens for an event to occur and then notifies WhatsUp Gold. This lets you get notification of an event when it occurs, rather than polling for all event types. The Passive Monitor Listener is solely responsible for how it monitors its events. This means that the server could listen for network traffic or application specific events.

WhatsUp Gold is installed with three Passive Monitor Listeners:

- **SNMP Passive Monitor (SNMP Trap)**. A trap is an unsolicited SNMP message (packet) sent from a device to indicate a change in status, such as a router indicating one of its interfaces went down or a printer indicating that it is out of paper.

- **Syslog Passive Monitor.** A Syslog monitor 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. A Syslog message consists of a priority and a text payload. The text message can contain anything you want permanently logged, such as a device failure, or a failed attempt to log in to the system. The only way to identify different types of syslog messages is to configure a regular expression in the Passive Monitor definition.
- **Windows Event Log Monitor.** This monitor can capture any Windows Event Log entry, such as a service start or stop, if there was a logon failure recorded, and other log entries.

Before you can configure passive monitors, you must configure listeners.

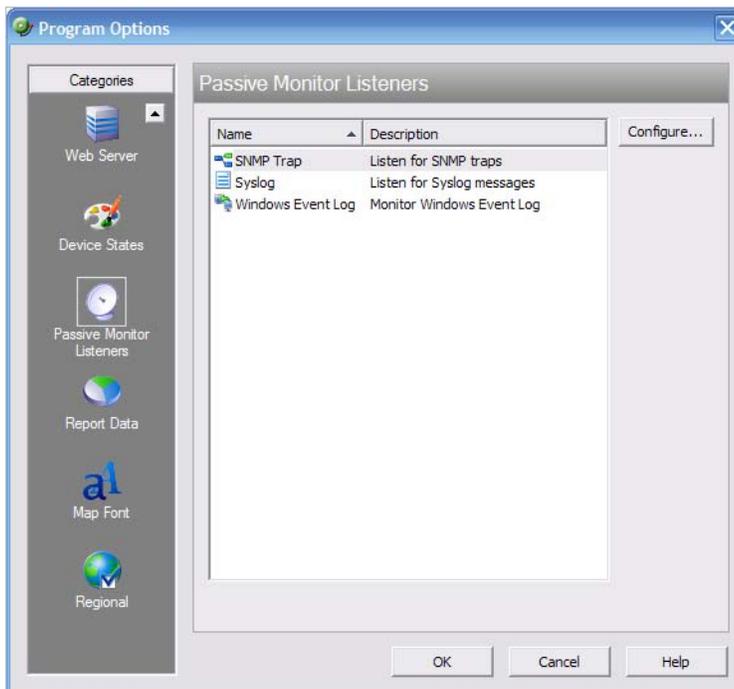
To configure a listener:

- 1 From the console, select **Configure > Program Options**. The Program Options dialog appears.



Note: If the Windows SNMP Trap Service (located in **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 Passive Monitor Listeners display in a list.



- 3 Select the listener you want to configure, then click **Configure**. The configuration dialog appears.
- 4 Select the appropriate settings based on the listener you are configuring. For more information about the Passive Monitor Listener options, refer to the Help.
- 5 Click **OK** to save changes.

About the Passive Monitor Library

The Passive Monitor Library dialog displays the Passive Monitor types that have been created for WhatsUp Gold. These types are specific configurations of SNMP traps, Windows Log Events, and Syslog Events. After the monitor types have been configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog.



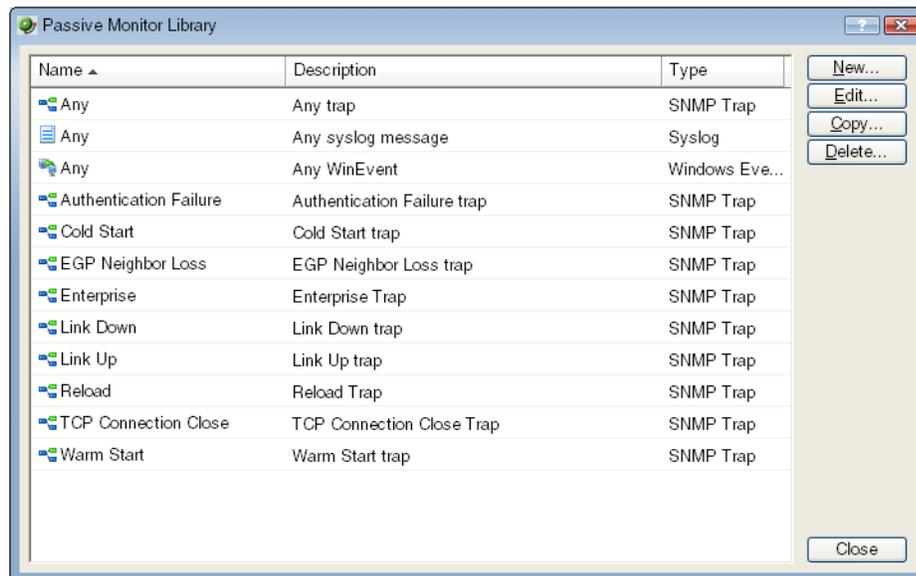
Note: If you are assigning a Windows Event Log passive monitor type to a device, make sure that the device has credentials assigned before creating a passive monitor for it. For more information, see *Using Credentials* (on page 103).

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 v12 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 103).

- 1 Go to the Passive Monitor Library.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Passive Monitor Library**.
- or -
- From the main menu bar of the console, select **Configure > Passive Monitor Library**.



- 2 Click **New** to create a new passive monitor type.
- 3 Select a monitor type in the list, then click **Edit** to change the settings.
- 4 Select a monitor type in the list, then click **Copy** to create a new monitor type based on the selected type.
- 5 Select a monitor type, then click **Delete** to remove it from the list.

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 web interface Reports tab. For more information, see *Using Full Reports* (on page 257).

- SNMP Trap Log
- Syslog Entries
- Windows Event Log
- Passive Monitor Error Log



Note: If you are missing traps or logs or receiving blank emails generated from an Action on a Passive Monitor, see the *Passive Monitor payload limitation* (on page 372).

Receiving SNMP Traps

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**.

You can also set up WhatsUp Gold to fire an Action when a trap is received for a device. For more information, see *Using the Trap Definition Import Tool* (on page 312).

To configure WhatsUp Gold to receive traps:

- 1 On the devices that will 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.
 - a) From the WhatsUp Gold console, select **Configure > Program Options**.
 - b) Select **Passive Monitor Listeners**.
 - c) Select **SNMP Trap**.
 - d) Click the **Configure** button.
 - e) Select the appropriate options.
 - **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 number. The changes are immediate, and you do not have to restart WhatsUp Gold for the changes to be in effect.
 - **Accept unsolicited SNMP traps.** If this is not selected, ONLY traps which are specifically added to devices as events are logged to the activity log and are able to trigger alerts. You may prefer to select this option so that ALL traps which occur are able to be detected and logged to the activity log. Note that regardless of this

filter setting, traps are logged to the SNMP Trap Log. By default there is no strict filtering of traps; this way you can see all traps from all sources, then make decisions about creating Actions based on specific traps you have seen. Later you may make the decision to filter out all traps except those you expect to see.

- **Forward traps.** Select this option to forward traps to IP addresses added to the **Forward traps to** list.
- **Forward unsolicited traps.** Select this option to forward all traps, including unsolicited traps.
- **Forward traps to.** Click **Add** to add an IP address and port to forward traps to. You can forward traps to multiple IP addresses.

f) Click **OK** to save changes.



Note: If the SNMP agent is installed on the WhatsUp Gold machine, this will also start an SNMP trap service. This can result in a port conflict, because both the SNMP trap service and the WhatsUp Gold SNMP trap handler listen on port 162. To fix this, turn off the SNMP trap service.

Using Performance Monitors

In This Chapter

Performance Monitor overview	213
About the Performance Monitor Library.....	214
Configuring and enabling Performance Monitors	215
Enabling SNMP on Windows devices.....	218
Adding monitors to the Performance Monitor Library.....	218
About performance reporting	223

Performance Monitor overview

Performance Monitors in WhatsUp Gold gather important information about the devices running on your network, then use that data to create reports trending the utilization and availability of different aspects of those devices. Through WhatsUp Gold, you can gather statistics on the following areas:

- CPU utilization
- Memory utilization
- Interface utilization (bandwidth)
- Ping availability
- Disk utilization

The system also lets you create custom Performance Monitors that you can use to monitor any performance counter made available through WMI or SNMP, as well as the use of JScript and VBScript.

Performance Monitors are configured in the *Performance Monitor Library* (on page 214), and added to individual devices through **Device Properties > Performance Monitors**. You can create global WMI, SNMP, and Active Script Monitors in the library, or create device-specific monitors in Device Properties.

About the Performance Monitor Library

The Performance Monitor Library dialog displays the Performance Monitors that have been created for WhatsUp Gold. Performance Monitors gather information about specific WMI and SNMP values from the network devices.

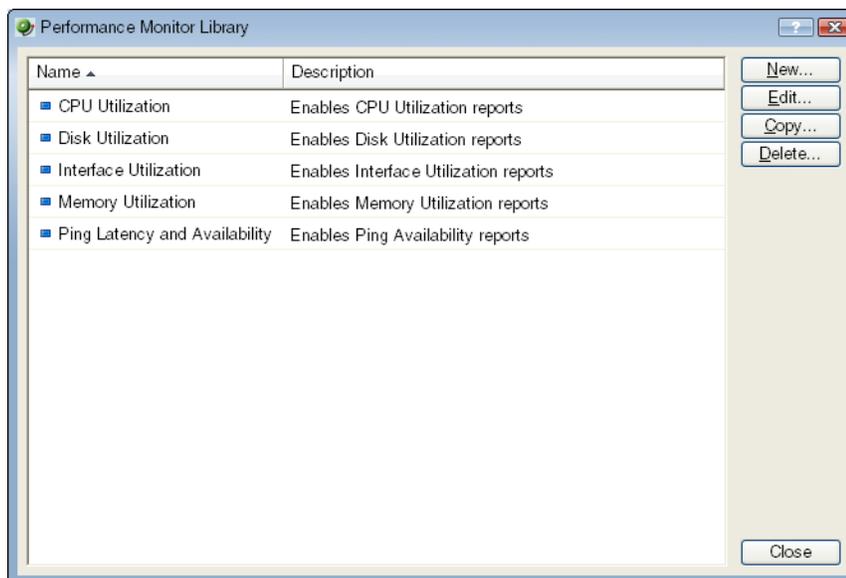


Note: Default monitors in the library cannot be edited or removed: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

Use the Performance Monitor Library to configure and manage Performance Monitors. When custom Performance Monitors are changed, the changes affect each instance of that particular monitor across the device groups.

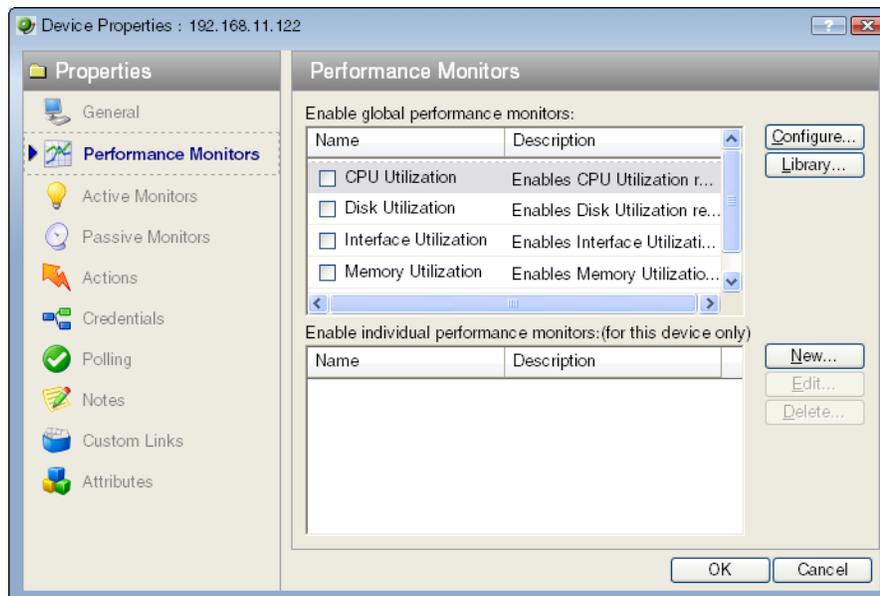
To access the Performance Monitor Library dialog:

- From the console main menu, select **Configure > Performance Monitor Library**.
- or -
- From the web interface, select **GO**. On the **WhatsUp** section, select **Configure > Performance Monitor Library**.



To configure Performance Monitors for the devices they are assigned to:

- 1 Right-click a device you want to configure. The shortcut menu appears.
- 2 Click **Properties**. The Device Properties dialog appears.

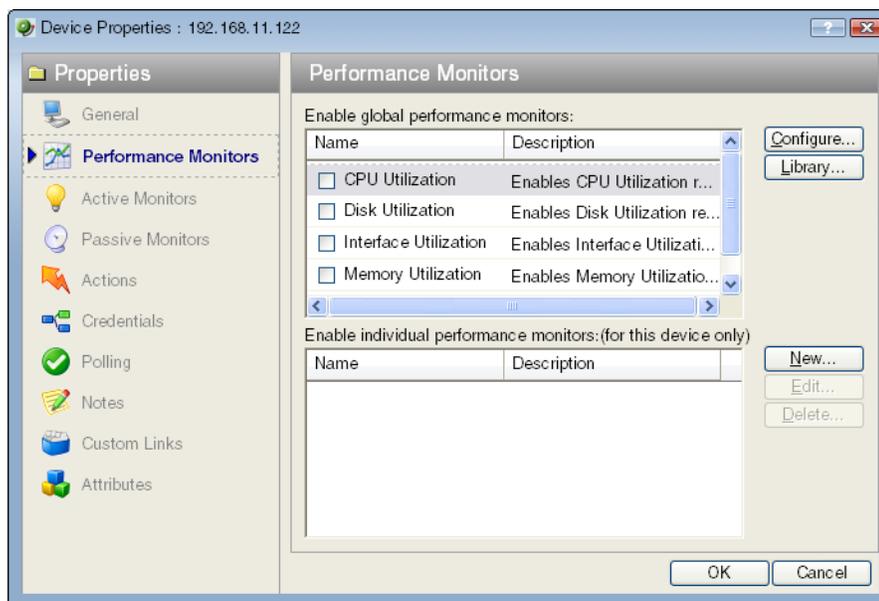


- Click **New** to configure a new monitor.
 - Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.
 - Select a performance monitor type, then click **Delete** to remove it from the list.
- 3 Click **OK** to save changes.

Configuring and enabling Performance Monitors

WhatsUp Gold is installed with five performance monitors that monitor specific types of data on your devices: CPU, Disk, Memory, and Interface Utilization; and Ping Latency and Availability. These monitors appear in the Performance Monitor Library.

To configure these monitors for use on specific devices, you must use either the **Device Properties > Performance Monitors** to configure for a single device, or **Bulk Field Change > Performance Monitors** to configure for multiple devices.



To enable a global performance monitor for a single device:

- 1 In Device View, select a device from the device list.
- 2 Right-click and choose **Properties** from the right-menu to view the device's Device Properties.
- 3 Click **Performance Monitors** to view the Performance Monitors dialog.

From the top section of the dialog, select the global performance monitor you would like to enable for the selected device.



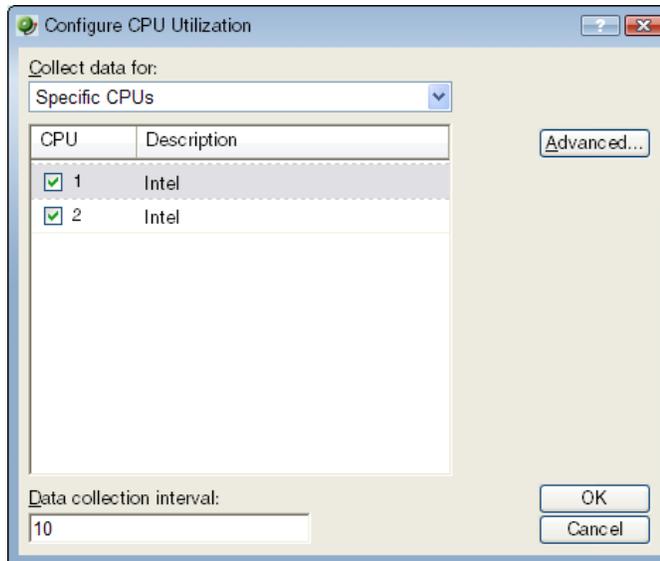
Important: To enable a CPU, disk, interface, or memory global Performance Monitor, you must first select and SNMP credential for the device from the SNMP credential page.

- 4 Click **OK** to save the changes.

To configure a global performance monitor:

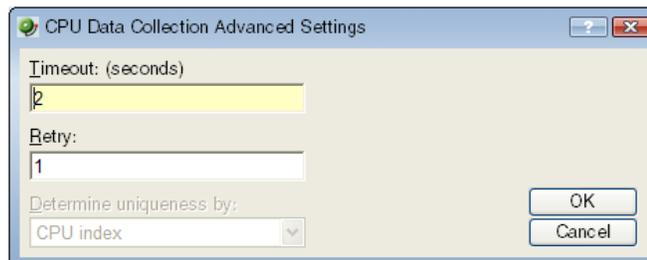
- 1 In Device View, select a device from the device list.
- 2 Right-click and choose **Properties** from the right-menu to view the device's Device Properties.
- 3 Click **Performance Monitors** to view the Performance Monitors dialog.
- 4 In the top section of the dialog, you can select a global performance monitor, then click **Configure**.

On the monitor configuration dialog, select the specific item you want to monitor by making a selection in the **Collect data for** drop-down list. Depending on the monitor, you can select to collect data for **All**, **Active**, **Specific**, or **Default** interfaces, memories, CPUs, or disks.



If you select **Specific**, the list is enabled and you can select or clear the selection for any of the items in the list. This is particularly useful with the Interface Utilization monitor where a device may have many interfaces.

- 5 Select the **Data collection interval**. This is the amount of time between performance polls.
- 6 Click **Advanced** to change connection settings on the device.



- 7 Click **OK** to save the changes.

To enable a global performance monitor for multiple devices, use the Bulk Field Change feature for performance monitors.

For information on the Active Script Performance Monitor, see *Adding custom performance monitors to the Performance Monitor Library* (on page 218).

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 Features* (on page 303).

To install SNMP Monitoring:

- 1 From the Windows Control Panel, click **Add or Remove Programs**.
- 2 Click **Add/Remove Windows Components**.
- 3 From the Components list, select **Management and Monitoring Tools**.
- 4 Click **Details** to view the list of Subcomponents.
- 5 Make sure Simple Network Management Protocol is selected.
- 6 Click **OK**.
- 7 Click **Next** to install the components.
- 8 After the install wizard is complete, click **Finish** to close the window.

To enable SNMP Monitoring:

- 1 In the Control Panel, click **Administrative Tools**.
- 2 Double-click **Services**. the Services console appears.
- 3 In the Services (Local) list, double-click **SNMP Service** to view the Properties.
- 4 On the **Agent** tab, enter the **Contact** name for the person responsible for the upkeep and administration of the computer, then enter the **Location** of the computer. These items are returned during some SNMP queries.
- 5 On the **Security** tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like WhatsUp to read information about the computer. This community string will be later used to create credentials for connecting to this device.
- 6 On the **General** tab, click **Start** to start the service (if necessary).
- 7 Click **OK** to close the dialog.

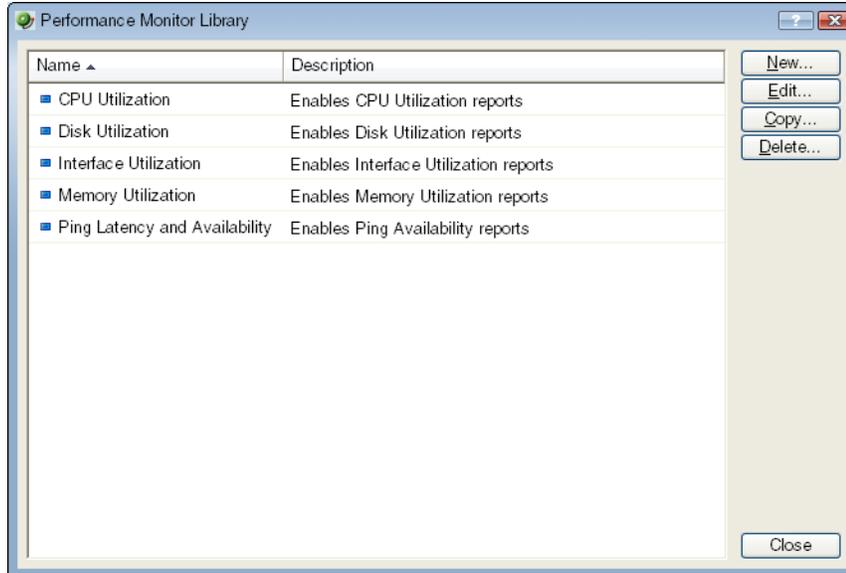
You can test the device by connecting to it through SNMP View.

Adding monitors to the Performance Monitor Library

Performance Monitors gather specific types of data on the devices to which they are assigned. System wide monitors are configured using the Performance Monitor Library, but you can also create specific SNMP and WMI monitors to be used on a per-device basis. The default performance monitors (CPU, memory, disk, and interface utilization; and ping latency and availability) cannot be edited or changed from their default settings. By creating custom performance monitors, you can adjust the settings to fit your specific monitoring needs.

To create custom performance monitors (for system wide use):

- 1 From the web interface, select **GO**.
- 2 On the **WhatsUp** section, select **Configure > Performance Monitor Library**. The Performance Monitor Library dialog appears.

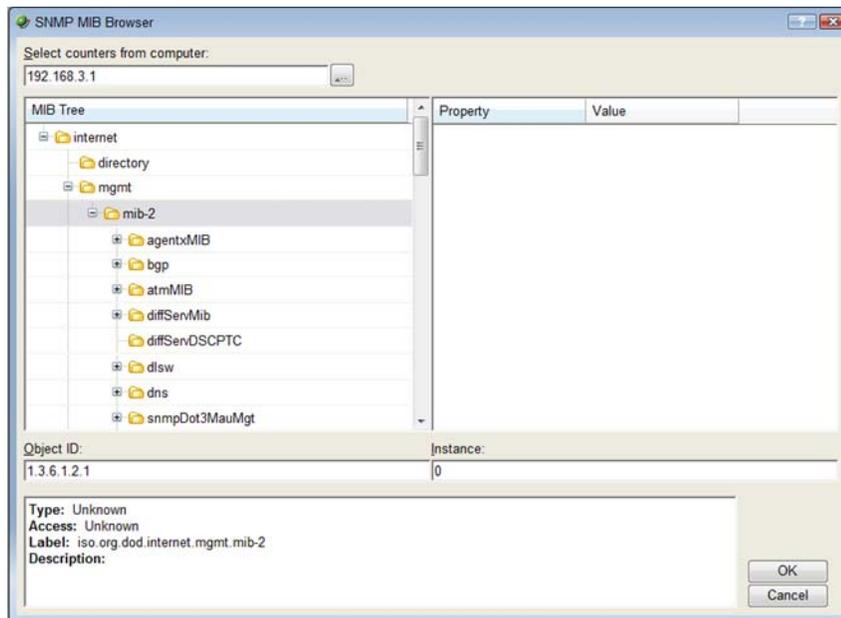


- 3 Click **New**.
- 4 Select the monitor type: SNMP Performance Monitor, WMI Performance Monitor, or Active Script Performance Monitor, then click **OK**.
- 5 Follow the instructions below for the type of monitor you choose.

To configure an SNMP monitor:

- 1 In the Add SNMP Performance Counter dialog, enter a **Name** and **Description** for the monitor as it will appear in the Performance Monitor Library. Either enter the Performance counter OID and Instance or click the browse (...) button next to the **Instance** box to go to the SNMP MIB Walker dialog.
- 2 In the MIB Browser dialog, enter the share name or IP address of the computer in which you want to connect.
- 3 Enter the SNMP credential used to connect to the device (or click the browse (...) button to access the Credentials Library to create a new credential).
- 4 If needed, adjust the **Timeout** and **Retries** count for the connection to the device.

- 5 Click **OK**. The SNMP MIB Walker appears.



- 6 Use the navigation tree in the left panel to select the specific MIB you want to monitor for the selected computer or device.
- 7 In the right pane, select the Property of that MIB you want to monitor. You can view more information about the property/value pair at the bottom of the dialog.
- 8 Click **OK** to add the OID to the **Performance counter** and **Instance** box in the Add SNMP Performance counter dialog.
- 9 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.

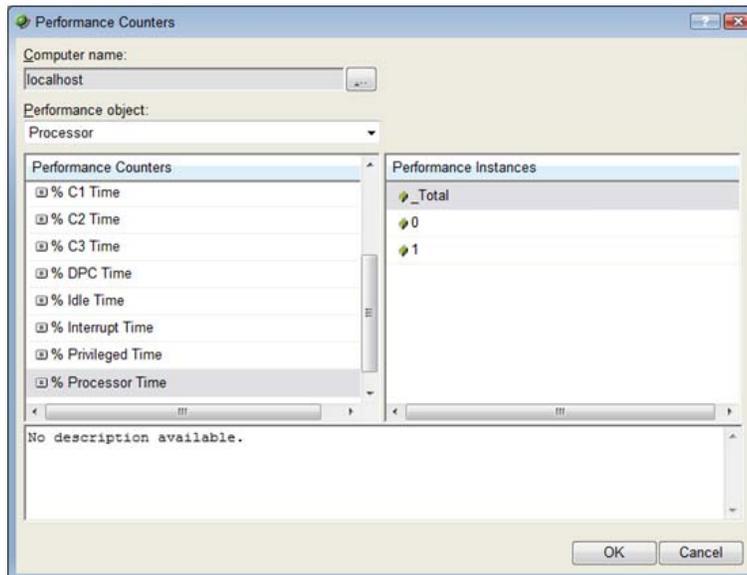


Note: After the monitor has been added to the library, make sure that you enable that monitor through **Device Properties > Performance Monitors** for that device or other devices.

To configure a WMI monitor:

- 1 On the Add WMI Performance Counter dialog, enter a **Name** and **Description** for the monitor, as it will appear in the Performance Monitor Library.
- 2 Click the browse (...) button next to **Instance**. The Performance Counters dialog appears.
- 3 Enter the computer name or IP address of the computer in which you want to connect.
- 4 Select a credential from a list of Windows credentials (pulled from the Credentials Library), then click **OK** to connect to the computer.

- 5 Use the **Performance counter** tree to navigate to the performance counter you want to monitor.



- 6 After you select the performance counter, select the specific instance you want to monitor.
- 7 Click **OK** to add the counter and instance to the Add Performance Counter dialog.
- 8 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.



Note: After the monitor has been added to the library, you can enable that monitor through **Device Properties > Performance Monitors** for that device or other devices.

To configure an SNMP active script performance monitor:

- 1 On the Add Active Script Performance Monitor dialog, enter a **Name** and **Description** for the monitor as it will appear in the Performance Monitor Library.
- 2 Enter a number for the timeout (in seconds).
- 3 Choose the type of script (JScript or VBScript) you will be using to write the monitor from the **Script type** list.
- 4 Add a new variable to the Reference Variables list by clicking **Add**.



Important: You can add up to 10 reference variables to the monitor.

- 5 On the Add reference variables dialog, enter a name and description for the variable.
- 6 Select the type of object (SNMP or WMI) from the **Object type** list.
- 7 If needed, adjust the **Timeout** and **Retries** count for connection to the device.
- 8 Click the browse (...) button next to **Instance**. The SNMP MIB Browser appears.
- 9 Enter the share name or IP address of the computer in which you are trying to connect.
- 10 Enter the SNMP credential used to connect to the device (or click the browse (...) button to access the Credentials Library to create a new credential).

- 11 If needed, adjust the **Timeout** and **Retries** count for the computer in which you are trying to connect.
- 12 Click **OK**. The SNMP MIB Walker appears.
- 13 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.
- 14 Click **OK** to add the OID to the **Performance counter** and **Instance box** in the Add new reference variable dialog.
- 15 Verify the configuration and click **OK** to add the variable to the **Reference variable** list on the Add active script performance monitor dialog.
- 16 Write or paste your monitor code in the **Script text** box.
- 17 Click **OK** to save changes and add the monitor to the Performance Monitor Library.

To configure a WMI active script performance monitor:

- 1 On the Add Active Script Performance Monitor dialog, enter a **Name** and **Description** for the monitor as it will appear in the Performance Monitor Library.
- 2 Enter a number for the timeout (in seconds).
- 3 Choose the type of script (JScript or VBScript) you will be using to write the monitor from the **Script type** list.
- 4 Add a new variable to the Reference Variables list by clicking **Add**.



Important: You can add up to 10 reference variables to the monitor.

- 5 On the Add reference variables dialog, enter a name and description for the variable.
- 6 Select the type of object (SNMP or WMI) from the **Object type** list.
- 7 Click the **Browse (...)** button next to the Instance box.
- 8 In the dialog that appears, enter the share name or IP address of the computer in which you want to connect.
- 9 Enter the domain and user login for the account on this computer. 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>.
- 10 Enter a password for the login used above and click **OK** to connect to the computer.
- 11 Use the Performance counter tree to navigate to the performance counter you want to monitor.
- 12 Once you select the performance counter, select the specific instance you want to monitor.
- 13 Click **OK** to add the variable to the **Reference variable** list on the Add active script performance monitor dialog.
- 14 Write or paste your monitor code in the **Script text** box.
- 15 Click **OK** to save changes and to add the monitor to the Performance Monitor Library.

About performance reporting

After you have configured a performance monitor, you can generate a performance report to see the results of the performance polling attempts. These reports can be used to troubleshoot your network problems.

More than 40 reports are installed with WhatsUp Gold. These reports can be viewed from the WhatsUp Gold web interface on the Reports tab.

The Reports tab contains all of the WhatsUp Gold Full reports. You can use the Reports Overview page and the Reports Category drop-down menu to navigate to reports according to their type and category.



All reports can be printed and many can also be exported into Microsoft Excel. Reports can also be saved as an .html file for later review. For more information on reports, see *Using Full Reports* (on page 257).

Performance Monitors gather specific types of data on the devices they are assigned to. System wide monitors are configured using the Performance Monitor Library, but you can also create specific SNMP and WMI monitors to be used on a per-device basis.

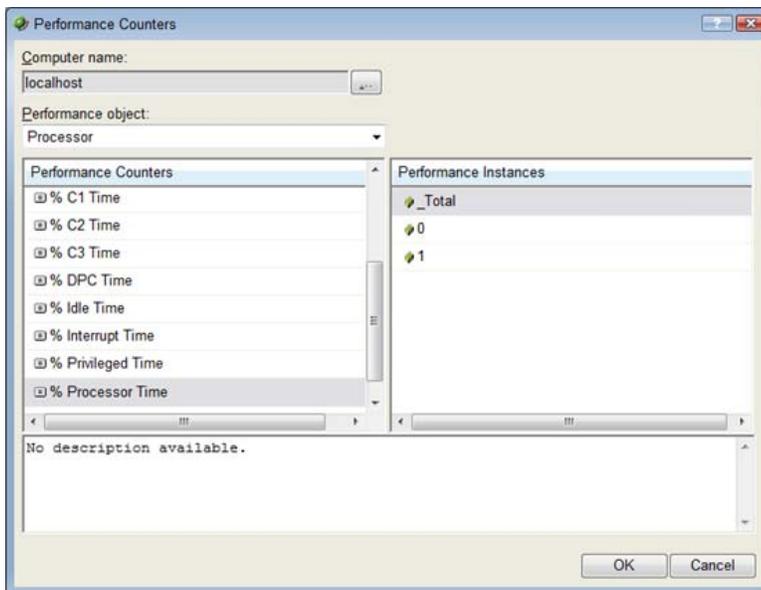
To create custom performance monitors for system-wide use:

- 1 From the web interface, select **GO**. On the **WhatsUp** section, select **Configure > Performance Monitor Library**.
- 2 In the Performance Monitor Library, click **New**.

- 3 Select the monitor type: SNMP or WMI.
- 4 Configure the monitor as follows for the type of monitor you are creating:

For WMI:

- 1 On the Add Performance Counter dialog, enter a name and description for the monitor.
- 2 Click the browse (...) button next to **Instance** to go to the Select Performance Counter dialog.
- 3 Click the browse (...) button next to **Select counters from computer**. The Select Computer dialog appears.
- 4 Enter the computer name or IP address of the computer in which you want to connect.
- 5 Select a credential from a list of Windows credentials (pulled from the Credentials Library), then click **OK** to connect to the computer.
- 6 Use the Performance counter tree to navigate to the performance counter you want to monitor.

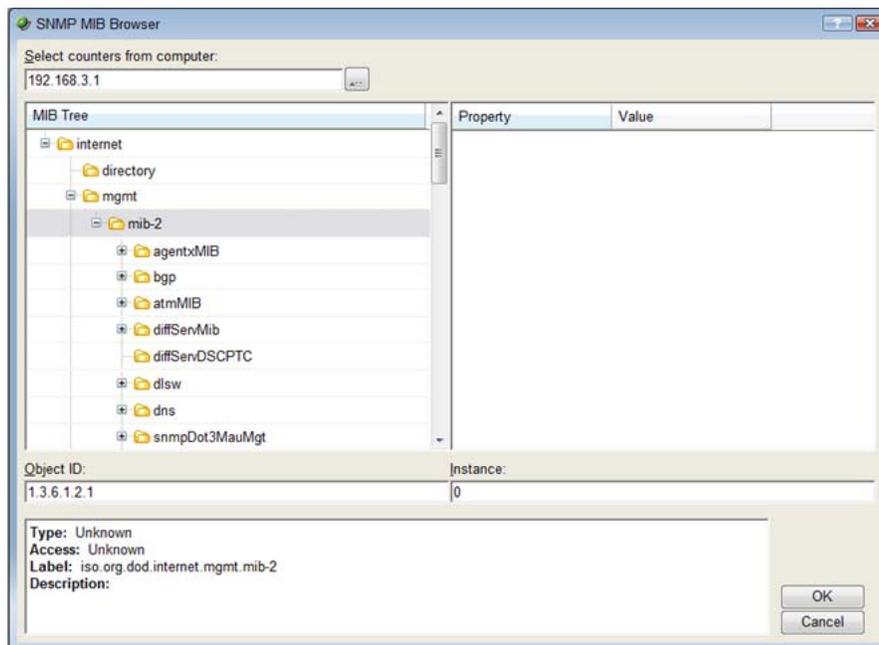


- 7 After you select the performance counter, select the specific instance you want to monitor.
- 8 Click **OK** to add the counter and instance to the Add Performance Counter dialog.
- 9 Verify the configuration and click **OK** to add the monitor to the library.

For SNMP:

- 1 On the Add SNMP Performance counter dialog, enter a name and description for the monitor.
- 2 Click the browse (...) button next to **Instance** to go to the Select Performance Counter dialog. You must enter a numerical value in the Instance field.
- 3 Enter the share name or IP address of the computer to which you want to connect.
- 4 Enter the SNMP credential used to connect to the device (or click the browse (...) button to access the Credentials Library to create a new credential).
- 5 If needed, adjust the **Timeout** and **Retries** count for the connection to the device.

- 6 Click **OK**. The SNMP MIB Browser appears.



- 7 Use the navigation tree in the left panel to select the specific MIB you want to monitor.
- 8 In the right pane, select the Property of that MIB you want to monitor. You can view more information about the property/value pair at the bottom of the dialog.
- 9 Click **OK** to add the OID to **Performance counter** and **Instance** in the Add SNMP Performance counter dialog.
- 10 Verify the configuration and click **OK** to add the monitor to the library.
- 11 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**.
- 12 On the WhatsUp Gold web interface, select a device and right-click. Select **Properties** from the right-menu.
- 13 On the Device Properties dialog, select Performance Monitors.
- 14 Click **New** next to the Individual performance monitors list.
- 15 Select the monitor type: SNMP or WMI.
- 16 Follow the directions above for creating either an SNMP or WMI monitor.
- 17 You can suspend or enable data collection on that monitor by selecting or clearing the checkbox next to the monitor name.
- 18 On the WhatsUp Gold web interface, select a device and right-click. Select **Properties** from the right-menu.
- 19 On the Device Properties dialog, select Performance Monitors.
- 20 Click **New** next to the Individual performance monitors list.
- 21 Select the monitor type: SNMP or WMI.
- 22 Follow the directions above for creating either an SNMP or WMI monitor.

You can suspend or enable data collection on that monitor by selecting or clearing the checkbox next to the monitor name.

Example: monitoring router bandwidth

Through the Performance Monitoring system, you have the ability to configure WhatsUp Gold to gather bandwidth usage on your SNMP enabled devices (routers, switches, etc.) and then track that usage through performance reports. Several Performance Monitors are installed with the application, but for bandwidth monitoring, the Interface Utilization monitor is the most useful (this will illustrate percent utilization and throughput).

The Interface Utilization monitor gathers statistics on the volume of bytes going through the active interfaces on the device. You can collect data on all interfaces, active interfaces, or just specific interfaces. This monitor is configured and enabled through **Device Properties > Performance Monitors**.



Note: Before you can configure the monitor, you must have SNMP enabled on the device, and the proper credentials configured in the Credentials Library for the device. 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 218).

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 Select **Properties** from the right-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 will fail (return to the Credentials Library to fix it). If the device is not SNMP-enabled, the scan will fail.

- 5 Select the interfaces you want to collect data for. From the **Collect data for** pull-down, select All, Active, or Specific. If you select Specific, select just the interfaces you want to monitor in the list below. By default, active interfaces will be measured.
- 6 (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.
- 7 On the Configure Interface Data Collection dialog, enter a time interval (in minutes) for how long you want the application to wait between polls. The default is 10 minutes. See, "Program Options - Report Data for more information on data collection and roll-up."
- 8 Click **OK** to save the Interface Utilization configuration.

Viewing the data

WhatsUp Gold will take 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.** For device-specific data, view the Interface Utilization report; or the Device Status report, which shows graphical statistics of all monitors configured on a device.
- **By Group.** Access the Group Interface Statistics report to view summarized statistics for all devices in the selected group that have interface statistics enabled.
- **System Wide.** Use the Top 10 report to view the top performers in terms of bandwidth utilization across your network. You can also view system-wide data by running the Group Interface Utilization report against the All Devices dynamic group.

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.

First, the scenario is described, then the steps taken by the network administrator to solve the problem are outlined.

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 goes to the Reports tab to select the Ping Response Time report.
- 2 From here, he checks the connection from the Atlanta WhatsUp Gold application to the Augusta primary server. The report shows an increased response time beginning at 11:45 a.m.



Note: This connection has been configured with the appropriate Performance Monitors and has been gathering data for weeks. 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 *Configuring performance monitors* (on page 215).

Monitoring Performance Data in Real Time

In This Chapter

About Real-Time Data features	229
Using InstantInfo popups	230
Using Network Tools to view real-time data	231
Using Split Second Graph Workspace Reports	233
Viewing Real-time Data in Full Reports	234

About Real-Time Data features



Note: These features are only available in WhatsUp Gold Premium Edition, WhatsUp Gold MSP Edition, and WhatsUp Gold Distributed Edition.

The historical performance data that WhatsUp Gold tracks helps you discover and analyze network usage trends that have already occurred; however, at times you need to view device usage data immediately, in real time.

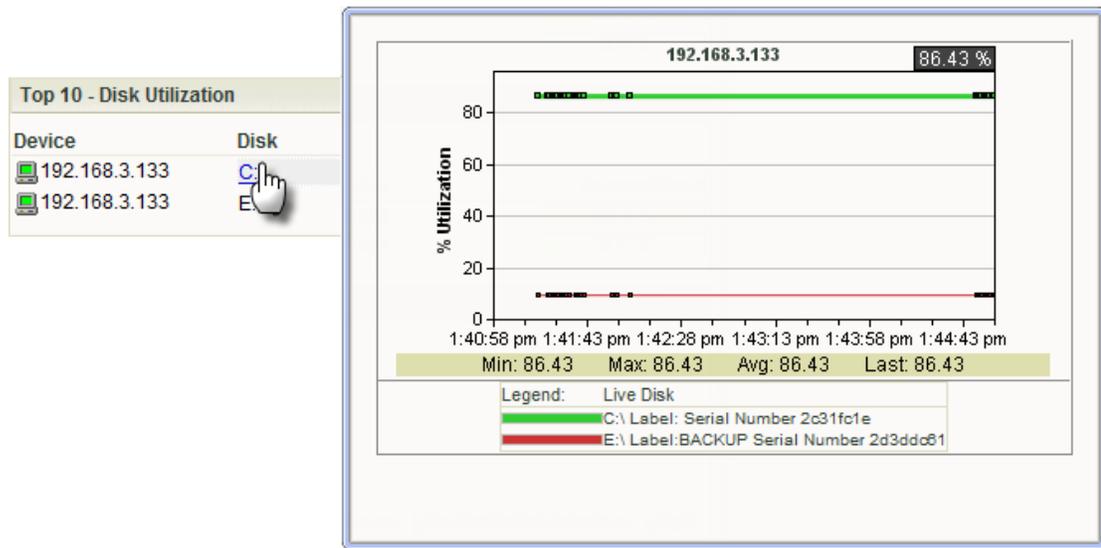
WhatsUp Gold includes several features that enable you to monitor performance data in real time.

- **InstantInfo popups.** Throughout workspaces and full reports, you can hover over some links (such as hard drive names or network interfaces) to see real-time data.
- **Web Task Manager and Web Performance Monitor.** These Web-based network tools extend the functionality of familiar Windows tools to every device you monitor in real time—even for devices that do not run Windows.
- **Split Second Graphs Workspace Reports.** These reports allow you to add real-time data into any workspace view.
- **Real-time data in Full Reports.** Many full reports now include a graph that updates with up-to-the-minute information. This real-time data is paired with historical data to give you a comprehensive report.

Using InstantInfo popups

InstantInfo popups provide easy access into real-time data that corresponds to the historical data viewed in performance workspace and full reports. The historical report data shows you device trends over the recent past hours, whereas InstantInfo popups provide dynamic graphs that show the latest device trends over the past minutes and seconds.

To determine if real-time data is available for a report, hover over each link in the report (in most cases, the InstantInfo popups are triggered by the link on the second column in the report). If more information is available for the link, a continuously updating graph of real-time data appears.



Important: InstantInfo popups require a minimum screen resolution of 1024 x 768 pixels, but is optimized for screen resolutions of 1280 x 1024 pixels and higher.

Disabling InstantInfo popups

By default, InstantInfo popups are available in both workspace and full reports, but you can disable them if you prefer.

To disable InstantInfo popups:

- 1 In the WhatsUp Gold web interface, click **GO**.
- 2 From the **WhatsUp** section of the **GO** menu, click **Configure > Preferences**. The User Preferences dialog appears.
- 3 Under **InstantInfo (popups)**, clear the checkboxes for the areas where you do not want popups to appear.
- 4 Click **OK** to save changes.

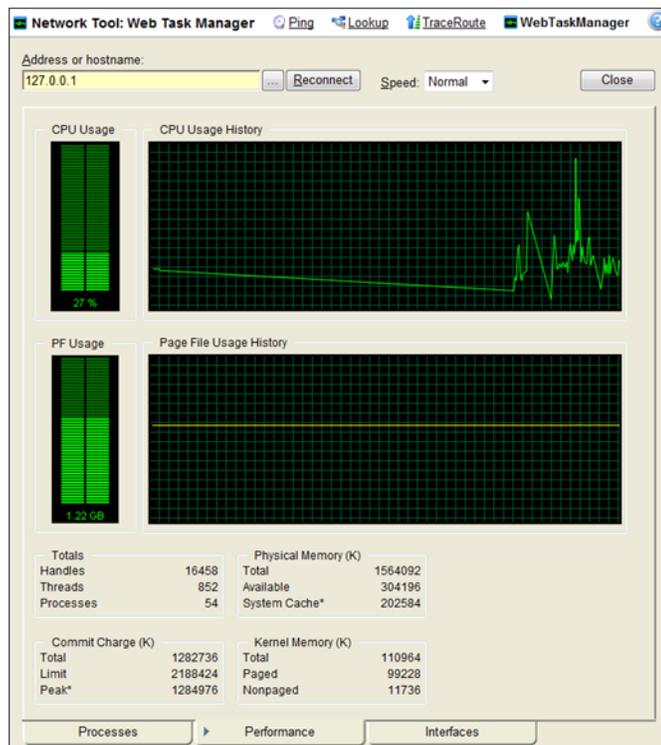
Using Network Tools to view real-time data

WhatsUp Gold includes two network tools you can use to view real-time data on network devices, the Web Task Manager and Web Performance Manager. These network tools provide the capability to view real-time device data directly from the WhatsUp Gold web interface.

About 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.** 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.** 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.

Using WhatsUp Gold v12

- **Interfaces.** 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 learn about how much data is transmitted and received via each interface.

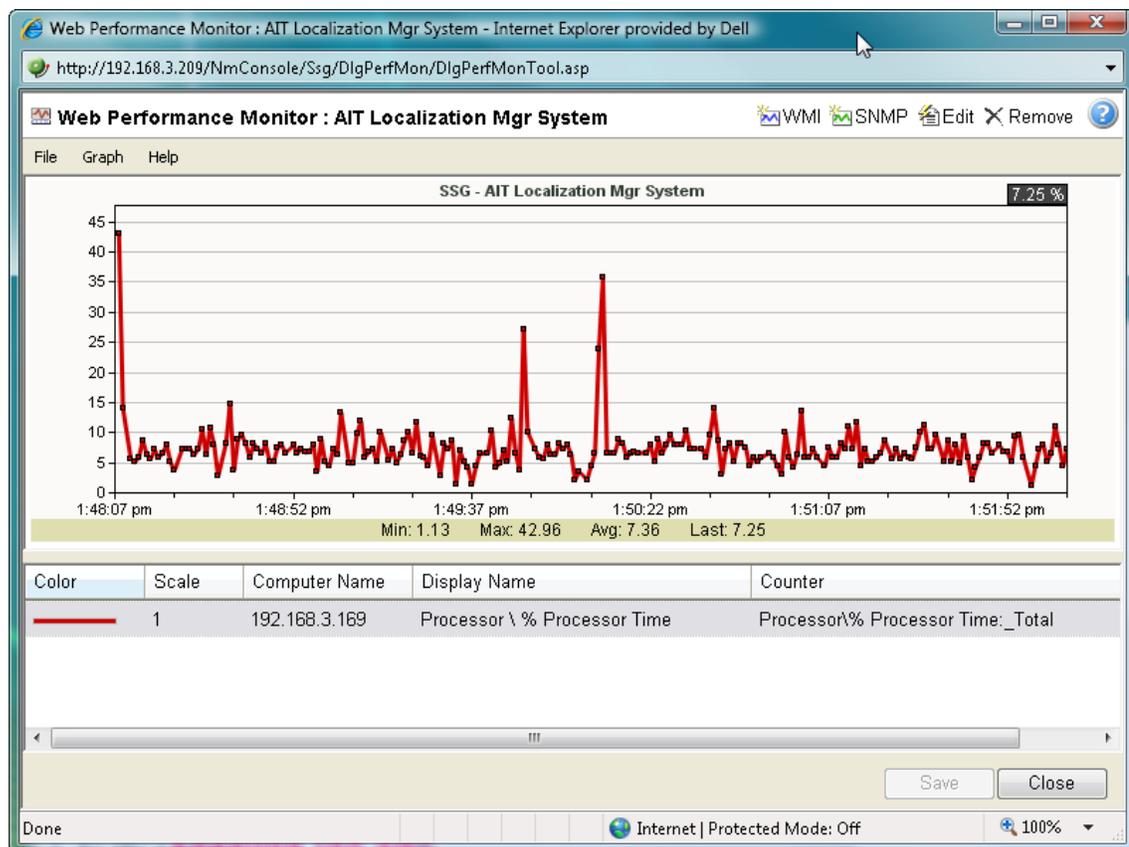
For more information on the Web Task Manager, see *Using the Web Task Manager* (on page 328).



Note: The Web Task Manager shows slightly different data on the Performance tab depending on the type of device being monitored. For Windows devices, the information matches the data that is available via the Windows Task Manager

About 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 workspace views using the Split Second Graph - Performance Monitor workspace 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 workspace report. You can use this workspace report to display any saved graph.

For more information, see *Using the Web Performance Monitor* (on page 325).

Using Split Second Graph Workspace Reports

With Split Second Graph Workspace Reports, you can embed the real-time data that is available from InstantInfo popups, the Web Task Manager, and the Web Performance Monitor into any workspace view.

For information on how to add a Workspace Report to a workspace view, see *Adding workspace reports to a workspace view* (on page 278).

Using the Performance Monitor workspace report

The Performance Monitor workspace report allows you to add a graph that you create in the Web Performance Monitor to a home workspace view.

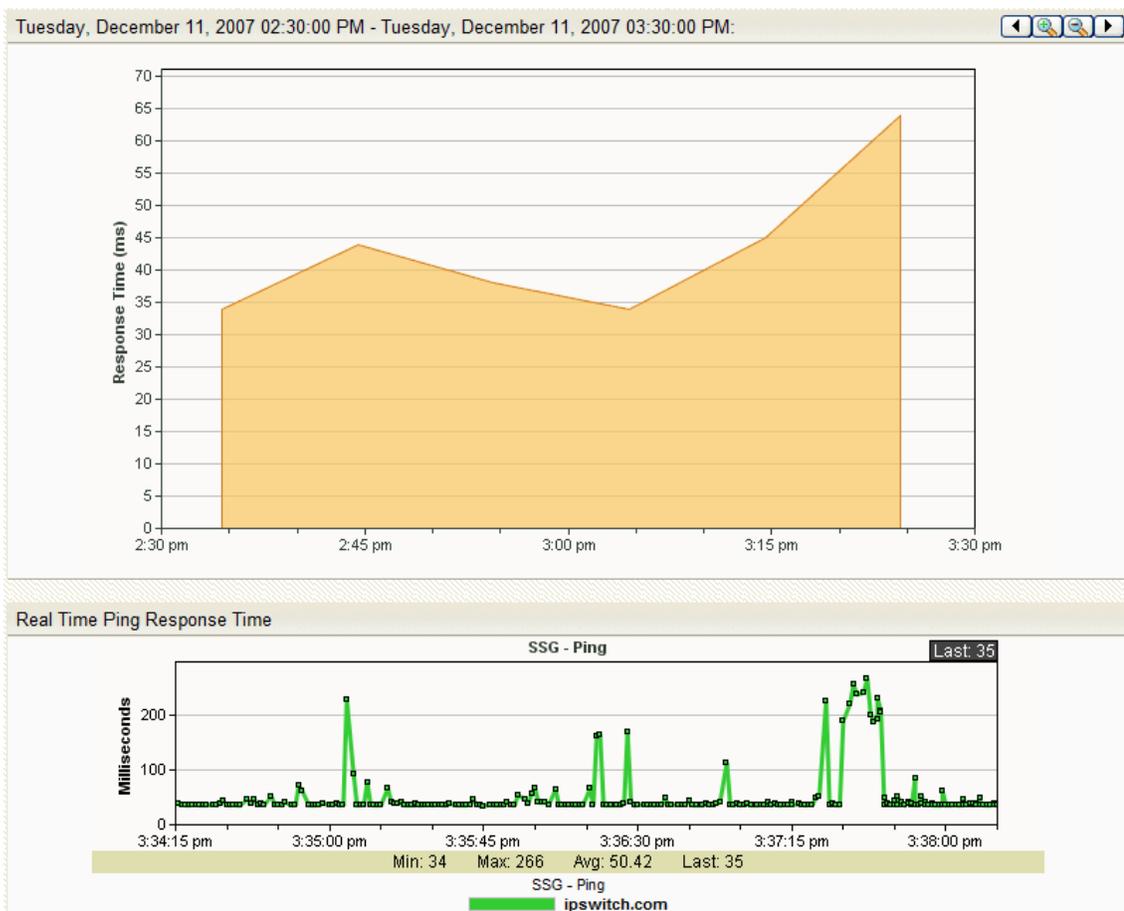
To use the Performance Monitor workspace report:

- 1 In Web Performance Monitor, create and save the graph you want to use in the Performance Monitor workspace report.
 - a) From the **WhatsUp** section of the **GO** menu, select **Tools > Web Performance Monitor**. The Web Performance Monitor appears.
 - b) From the **Graph** menu, add the **WMI** and **SMP** counters that you want to graph.
 - c) After the graph is configured to show the data you want to see in the Performance Monitor workspace report, select **File > Save Graph as**. The Save Graph dialog appears.
 - d) Enter a name for the graph, then click **OK**. Your graph is saved and ready to use in the Performance Monitor workspace report.
- 2 Add the Performance Monitor workspace report to a home workspace view.
 - a) From any home workspace view, click **Add Content**. The Add Content to View dialog appears.
 - b) Expand the **Split Second Graphs** section, select **Performance Monitor**, then click **OK**. The dialog closes and the home workspace view appears with the new Performance Monitor workspace report added.
 - c) On the new Performance Monitor workspace report, click **Menu > Configure**. The Configure Line Chart dialog appears.

- d) In **Graph name** list, select the graph you created. You can optionally configure any other options on this dialog to your preferences.
- e) Click **OK**. The dialog closes and the home workspace view appears with your custom Web Performance Monitor graph displayed in the Performance Monitor workspace report.

Viewing Real-time Data in Full Reports

For all full reports where real-time data is available, a second graph appears below the graph showing historical data. This second graph displays poll data for the report in real-time, updating every second.



Using Active Discovery

In This Chapter

About Active Discovery	237
Configuring Active Discovery	238
Enabling and disabling an Active Discovery task	240
Testing Active Discovery tasks.....	241

About Active Discovery

With Active Discovery, you can schedule WhatsUp Gold to scan your network for new monitors (active monitors and performance monitors) and devices on a regular basis. Newly discovered items are added to the Active Discovery Results report, and WhatsUp Gold notifies you that a new device was found, or a new monitor was found on an existing device. You can then review the report and select the items you want to add to your device list.

Active Discovery works with two types of device discovery:

- **SNMP SmartScan.** WhatsUp Gold discovers devices by reading SNMP information on your network. This scan type uses an SNMP enabled router to identify the devices in your network and also identifies subnetworks within your network.
- **IP Range Scan.** WhatsUp Gold scans a range of IP addresses and finds the devices that respond to a message sent via the Internet Control Message Protocol (ICMP).

If the scan finds results, an email is generated and sent to the address you provide during Active Discovery configuration. The email contains links to the reports that are populated by the scan:

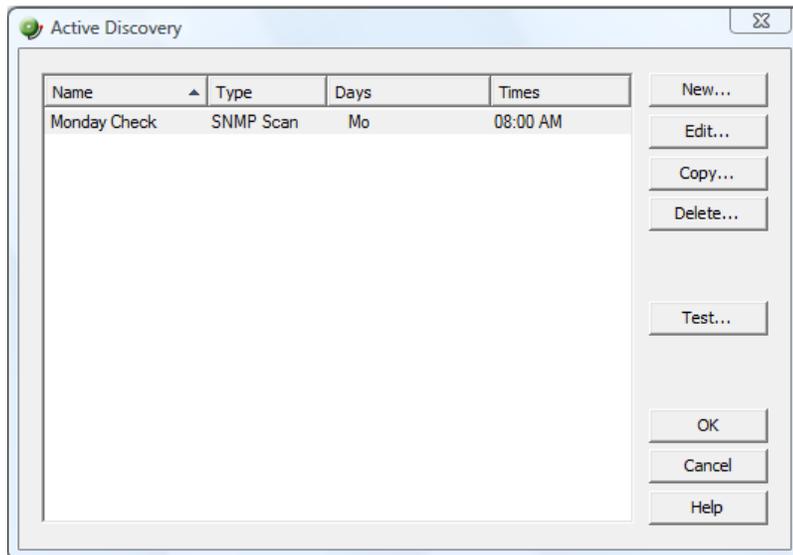
- Active Discovery Log shows the success or failure of the Active Discovery task, and any devices and/or Monitors found during that scan.
- Active Discovery Results shows all new items found in the latest scan, or all unprocessed items from previous scans. Through this report, you can add devices to the device list and new monitors (Active Monitors and Performance Monitors) to the device monitors.

If an email notification is not specified (in the wizard), these reports are also available in the System report list, on the Reports tab.

Configuring Active Discovery

To configure an Active Discovery Task:

- 1 From the console main menu, select **Configure > Active Discovery**. The Active Discovery dialog appears.



- 2 Click **New** to add a new task, or select an existing task and click **Edit**.
- 3 If you are adding a new task, follow the wizard to create the task.
- or -
If you are editing a task, you must click the sections you want to make changes to.
- 4 After the wizard is complete or your change edits are complete, the task is processed according to the schedule you set for the task.

For more information on how to test your new task, see *Testing Active Discovery tasks* (on page 241).

Scanning for new services on existing devices

If you want to scan the devices currently in your databases for new services, make sure that you select the **Scan for new services on existing devices** option.

Clear the **Scan for new services on existing devices** option to keep your existing devices from being scanned.

Example: configuring Active Discovery

In this example, we set up an Active Discovery task to scan our Atlanta network every morning and send an email update to the network administrator.

To configure an Active Discovery task:

- 1 From the WhatsUp Gold console, select **Configure > Active Discovery**. The Active Discovery dialog appears.

- 2 Click **New** to add a new Task.

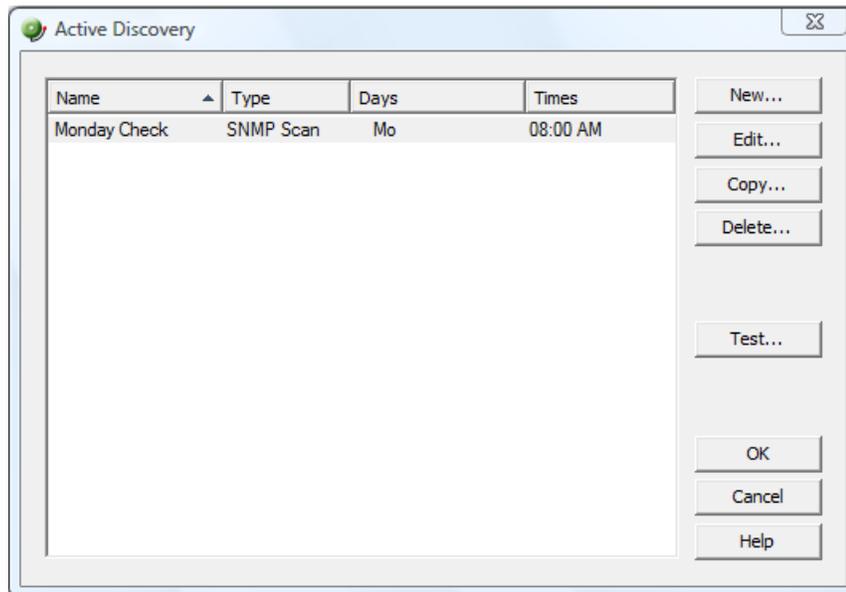
We completed the Add Active Discovery Task wizard example as follows:

Wizard screen	Settings
General	Task Name: Atlanta Network Sweep Description: Daily scan of Atl net Scan for new services on existing devices (selected)
Schedule	Enable Schedule (selected) Schedule Time: 8:00 AM Days: All days selected
Notification	Enable Email Notification (selected) Email address: netadmin@ipswitch.com Outgoing mail (SMTP) server: 192.2.200.10 Port: 25 From: whatsup@ipswitch.com
Scan Type	SNMP SmartScan (selected)
SNMP SmartScan Settings	SNMP enabled router: 192.168.2.1 SNMP read communities: public Windows credentials: none
Active/Performance Monitors	Select Active Monitors to be used in the scan process: FTP, HTTP SMTP, Ping Select Performance Monitors to be used in the scan process: CPU Utilization, Disk Utilization, Interface Utilization



Important: If you want to scan the devices currently in your databases for new services, make sure you select the **Scan for new services on existing devices** option. Clear the option to keep your existing devices from being scanned.

- 3 Click **OK** to complete the wizard. The new task is displayed in the Active Discovery dialog.



- 4 From the email, click the Active Discovery Results link to view the report.
- 5 Select the Discovery results (devices, services, or monitors found) you want to add to your device group, then click **Add**.

Enabling and disabling an Active Discovery task

To stop an Active Discovery task from being executed:

- 1 From the WhatsUp Gold console main menu, select **Configure > Active Discovery**. The Active Discovery dialog appears.
- 2 Select the task you want to stop, then click **Edit**.
- 3 Select the Schedule section.
- 4 Clear the **Enable Schedule** option to stop the task from being processed according to the schedule.
- 5 Click **OK** to return to the Active Discovery dialog.

Testing Active Discovery tasks

To test an active discovery task:

- 1 From the WhatsUp Gold console main menu, select **Configure > Active Discovery**. The Active Discovery dialog appears.
- 2 Select the task you want to test and click **Test**.
- 3 WhatsUp Gold scans the network based on the settings for that Task. After the task is complete, the Active Discovery Results dialog appears.
- 4 Review the dialog, then click **OK** to return to the Active Discovery dialog.



Note: The results of the Active Discovery test scan are not stored in the database and cannot be processed.

Using Maps

In This Chapter

Using the Map View	243
About the Map View	244
Using map display options	245
Using Arrange options	246
Organizing devices	247
Using device types	247
Using grid properties	247
Grouping objects	248
Using the lock position	248
Mapping fonts	248
Organizing devices	248
Using link lines	249

Using the Map View

Map View shows a graphical representation of the devices in a group. Map View can be used to:

- Organize devices into user-specified groups, for example, all HTTP servers.
- Customize individual device icons such as workstations, containers, routers, and bridges.
- Indicate relationships among devices by using annotation objects such as rectangles, ellipses, text, and "attached" or "free" lines to. Annotation objects let you organize your map to best represent your network. Attached lines show a connection between devices and move with the device.
- Show status of network link lines.

Map View is accessed on the Devices tab under **View > Map View**.

About the Map View

Map View shows a graphical representation of your devices. As in Device View, each device's icon provides information about its device type and status. Map View can also show the status of network interfaces (by using link lines) and provide visual indications of polling dependencies.



Current device state is shown by the color and shape of a device icon.

- Device ASA is a workstation that is currently up.
- Device HRA is a workstation that is currently in maintenance mode.
- Device JMA is an FTP server that is currently down.
- Device PDA has missed a poll, but has not yet missed enough polls to be considered down.
- Devices ASA, HRA, RRA, JMA, and PDA are "Up" dependent on Router 1, as shown by the green arrows pointing to the Router 1 device. These devices get polled only if Router 1 is Up.



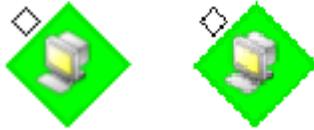
In addition, device icons can show complex states. For example, the icon to the left shows a device that is accessible but has a monitor that is reporting as down.

You can also use Map View to:

- Indicate relationships among devices by using annotation objects.
- Change the layout of devices and annotations.

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. Once the device has been acknowledged, the icon returns to the above appearance.



For more information, see *Using Map View* (on page 243).

Map Limitations

By default, WhatsUp Gold will not display a map 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 Go to `HKEY_LOCAL_MACHINE\Software\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 display options

Display options let you change the visual representation of a map, and add annotations that help you monitor dependencies and active monitors. Right-click on the Map View, then select from the following Display options.

- **Device Icons.** By default the map will show an icon for each device. If you only want to show a dot, or node, to represent each device, then clear this selection.

- **Polling Dependency Arrows.** If you have set up a device so that it gets polled only if a second device is down or up (a dependency), then by default you will see an arrow that shows this dependency. For example, if polling of device A is dependent on the state of device B, the arrow will point from device A to device B.
- **Unconnected Links.** Select this option to make the map display short lines for links that are not connected anywhere. If this is cleared, only connected links are displayed. This could be a network interface that is not connected to another device. It could also be any active monitor (such as HTTP, or SMTP), in which case, the short line will show green when up and red when down.
- **Snap to Grid.** Select this option to display a grid and automatically align objects along your grid when they come within a certain distance of it.
- **Clip Device Names.** Select this option if you want to shorten the device display names. The display names will be terminated at the first space or period in the name. If the display name is a dotted decimal IP address, **Clip Device Names** shows only the last digits of the IP address.
- **Wrap Device Names.** Select this option to wrap long display names. The display names will be wrapped at every space or period in the name.

Using Arrange options

Use the Arrange options to position device icons and annotations (such as lines, rectangles, text) on a map.

For example, you can automatically arrange device icons:

- 1 In the toolbar, click the **Select (arrow)** tool, then click in the Map view and drag the cursor to draw a box around the icons you want to select.
- 2 Then select **Arrange > Arrange All Device Icons**. This feature arranges all device icons on the current map in equally spaced rows starting in the top left corner.

Other ways to arrange map objects include:

- **Order.** You can arrange which annotations are moved to the foreground or background.
- **Align.** You can arrange icons or annotations so they share a common edge or centerline.
- **Distribute.** You can arrange icons or annotations so they are spaced evenly along a line. You can arrange icons in a radial format, in rows, or by links.
- **Grouping.** You can group selected annotations so that they can be arranged or moved as a unit.
- **Flip.** You can transpose the location of two selected annotations.

Organizing devices

In the console, the Map View has a number of options you can use to organize your view of devices. Arrange options are available from the Arrange menu on the main menu bar and right-click menu. Display options are available from the View menu on the main menu bar and the right-click menu.

Try the different functions on the Arrange menu until you are satisfied with the device layout.

For example, to clean-up a map, after completing discovery, you can try the following display options:

- 1 Select the device group, then click the **Map View** tab.
- 2 Right-click in the Map View, then select **Display > Clip Device Names**. This removes the domain part of the device name and shows only the host name.
- 3 Select all devices in the view by clicking and dragging a selection box around all devices. Then, from the Arrange menu, select **Distribute > Device Icons in Rows**.

If you have a large set of devices or want to represent a topology specific to your network, you can also use the graphics annotations (such as lines, text, circles) and attached lines to create custom map views.

Lock position can be useful in positioning objects on the map.

Using device types

The Device pool provides "Device Types" for ten standard device types; and some custom host types. It also displays any galleries that have been created. When you click one of these devices, it becomes the active tool. To add the device to the map, select and drag it to the map.

Using grid properties

Set these properties from the WhatsUp Gold console Map view toolbar.

To view the toolbar:

- Select **View > Toolbars > Grid**.
 - **Snap to the grid**. Select this option to display a grid and automatically align objects along your grid when they come within a certain distance of it.
 - **Increase the number of gridlines**. This allows you to display more gridlines, letting you place items closer together when using **Snap to the grid**.
 - **Decrease the number of gridlines**. This lowers the number of gridlines on your map view, spacing them further apart when using **Snap to the grid**.

Grouping objects

The Group function lets you change the layout of multiple map annotations in the Map view.

- **Group.** Allows multiple objects to be *grouped* together as a single object, which will make all of the objects react to drawing transformations as one.
- **Ungroup.** Undoes the *group* effect so that all the objects that were originally grouped are now separated objects once again. All transformations done when the object was grouped are kept when the object is ungrouped.



Note: You can also use these features together. For example: You could take 4 different objects and group them together to form 1 object. Then you could take the grouped object and flip it horizontally or vertically.

Using the lock position

To lock objects on the map:

- Right-click and select **Lock Position** from the menu.
Lock Position keeps an object from moving as you move other items around, or when adding devices to the map. If you want to change an object position on the map, remove the "lock position" selection. It is helpful to lock images or text you place in the background to protect them from changes.

Mapping fonts

You can specify the font used for device display names.

To change the font used in maps:

- 1 Click **Change Font** to open the standard Windows font selection dialog box.
- 2 Select the font properties you want to use and click **OK**.
- 3 The Sample Label (AaBbYyZz) shows the new font selection.

Organizing devices

Map View has a number of options you can use to organize your view of devices. Arrange options are available from the Arrange menu on the main menu bar and right-click menu. Display options are available from the View menu on the main menu bar and the right-click menu.

Try the different functions on the Arrange menu until you are satisfied with the topology.

If you have a large set of devices or want to represent a topology specific to your network, you can also use the graphics tools to create custom map views.

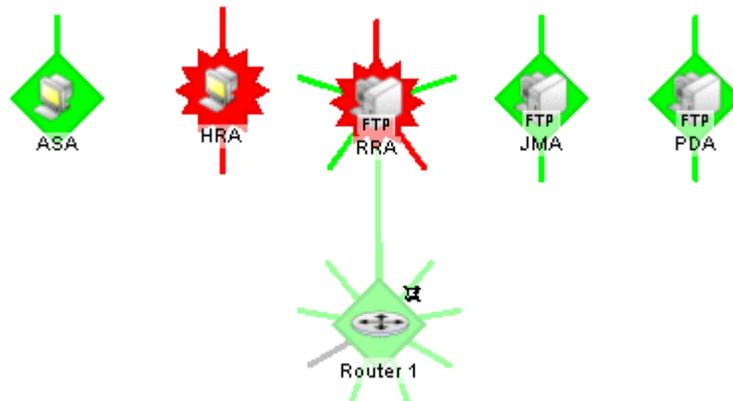
For example, to clean-up a map, after completing discovery, you can try the following display options:

- 1 Select the device group, and click the **Map View** tab.
- 2 Right-click in the Map View and select **Display > Clip Device Names**. This removes the domain part of the device name and shows only the host name.
- 3 Select all devices in the view by clicking and dragging a selection box around all devices. Then, from the Arrange menu, select **Distribute > Device Icons in Rows**.

Using link lines

You can use Link lines to get a graphical view of the network link (the Interface service) between two devices. Link lines can also show the status of any service which has an Active Monitor on the device.

The following example shows a map with link lines displayed.



There are three ways to set up the connecting link lines:

- 1 **Manually**, in the Map View select a device, then right-click the **Link > Link to** option on the context menu. (Click **Link > Disconnect link** to remove the link between devices)
 - a) Select a monitor for which you want to display a link line, then click **OK**. The link line cursor appears.
 - b) Drag the cursor to another device and click to create a link.
- 2 **Automatically**, during device discovery when using SNMP SmartScan (Click **File > Discover Devices > SNMP SmartScan**)



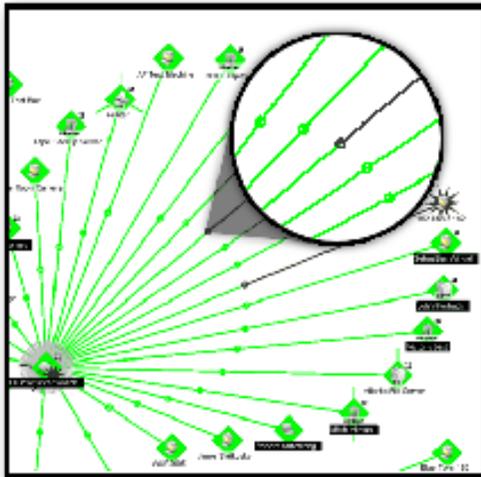
Note: The Interface service must be included in the scan.

- 3 **Automatically**, when you right-click a device, then click **Properties > Active Monitors > Discover**.



Note: When you use one of the automatic discover options, particularly when discovering interfaces on a router or switch, you need to enter the SNMP community string in the appropriate scan dialog. This lets the scan identify all the interfaces on the device. If scanning a specific device (from the **Device Properties > Active Monitors** dialog), with the device selected, right-click **Properties**, then select **Credentials**. In the **SNMP v1/v2/v3 credentials** box, select the **Public Read Community**. Click **Active Monitors**, then click **Discover**.

When creating links manually, you are always creating a connected link. If there was an unconnected link for the service, it will be replaced by the connected link. Both connect and disconnect skips the dialog if there is only one active monitor on the device because it assumes you meant that monitor.



In the graphic above, there are two link lines connected by a dot in the center of the line between the two devices. This shows that the devices are linked both directions. This is done by repeating the process above from the second device, back to the first. Now, when one of the links goes down, you can see on which side the problem occurs.

Using attached lines

Attached lines show an arbitrary connection between devices. When you move two devices that are connected by attach lines, the attach lines also move. Attach lines are visual representations assigned by the user, and not a reflection of a true connection between the two devices. The true connection between the two devices is done with Link lines.

To draw an attached line:

- 1 In the Map View, right-click a device. The right-click menu appears.
- 2 Click **Attach > Attach to**. A line displays next to the cursor.

- 3 Click the device icon you want to attach to. WhatsUp Gold draws an attached line between the two devices.



Note: Each device can attach to up to five other devices.

Connecting links

Connecting links represent a service, for example an interface, that connects two devices. They are drawn as lines from one device to another. If two devices have mutual links, the single line can consist of more than one color (if one object is up and the other is down). The center-point of the line back to the up object is green, while the other half of the line going to the down object is red. In essence, the color of the line represents the state of the service on the host that the color touches.

Example

If the red part of the line touches "System A" and the green part of the line touches "System B", then we know that some service on "System A" is the problem.

About unconnected links

Unconnected links represent a service that is not connected to some other host, for instance an unused interface on a router. They are drawn as short lines extending out from the host. The first unconnected interface is drawn straight up ("12 noon") and the rest are evenly distributed around the host in a clockwise fashion. You can choose to display or not display the unconnected links.

As these unconnected links show any service for which the device has an active monitor, you can use this feature to show a visual status of the services. For example, though the device is up (green), you may see that one of the unconnected links is down (red) and will know to check the services on the device.

Showing unconnected links

Unconnected links must be shown for all or none of the devices in a map.

To show unconnected links for all devices:

- 1 Right-click in Map View to display the pop-up menu.
- 2 Then, select **Display > Unconnected Links**.

Repeat these steps to disable Unconnected Links.

The **Unconnected Links** option makes the map display short lines for links that are not connected anywhere. If this is cleared, only connected links are displayed. This could be a network interface that is not connected to another device. It could also be any active monitor (such as HTTP, or SMTP), in which case, the short line will show green when up and red when down.

Creating connected link lines

There are three ways to set up the connecting link lines:

- 1 **Manually**, in the Map View select a device, then right-click the **Link > Link to** option on the context menu. (Click **Link > Disconnect link** to remove the link between devices)
 - a) Select a monitor for which you want to display a link line, then click **OK**. The link line cursor appears.
 - b) Drag the cursor to another device and click to create a link.
- 2 **Automatically**, during device discovery when using SNMP SmartScan (Click **File > Discover Devices > SNMP SmartScan**)



Note: The Interface service must be included in the scan.

- 3 **Automatically**, when you right-click a device, then click **Properties > Active Monitors > Discover**.



Note: When you use one of the automatic discover options, particularly when discovering interfaces on a router or switch, you need to enter the SNMP community string in the appropriate scan dialog. This lets the scan identify all the interfaces on the device. If scanning a specific device (from the **Device Properties > Active Monitors** dialog), with the device selected, right-click **Properties**, then select **Credentials**. In the **SNMP v1/v2/v3 credentials** box, select the **Public Read Community**. Click **Active Monitors**, then click **Discover**.



When creating links manually, you are always creating a connected link. If there was an unconnected link for the service, it will be replaced by the connected link. Both connect and disconnect skips the dialog if there is only one active monitor on the device because it assumes you meant that monitor.

Using the Program Options

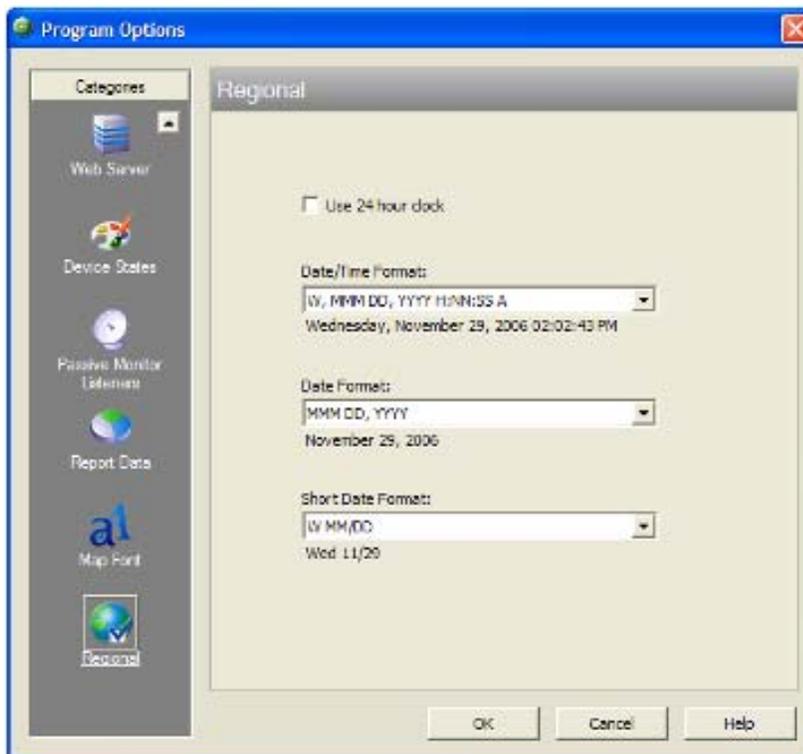
In This Chapter

Changing the date and time format.....	253
Changing how long report data is stored.....	254
Changing the device state colors or icons	255
Changing clock/regional preferences.....	256

Changing the date and time format

To change the date and time format:

- 1 From the WhatsUp Gold main menu, select **Configure > Program Options**.
- 2 Select the **Regional** section.



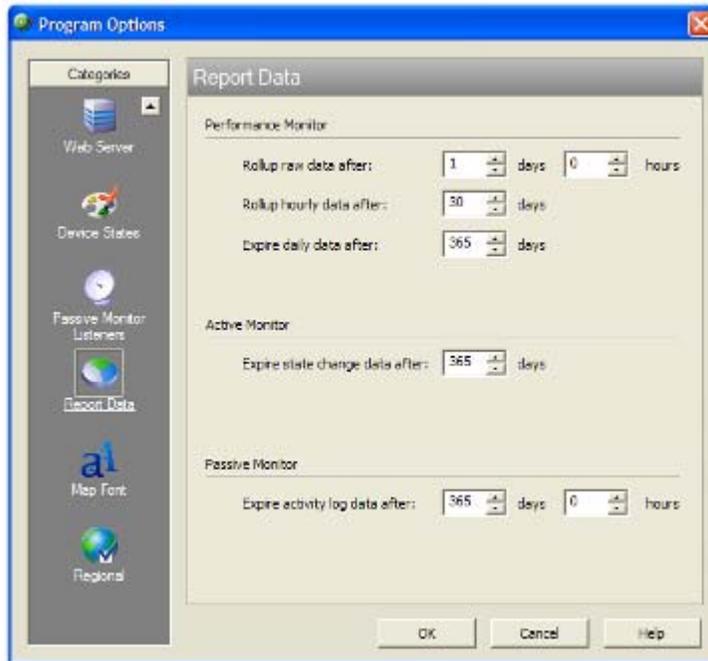
- 3 For each of the three date formats, select the one that best suits your needs.
- 4 Click **OK**.

These formats can be seen in use on several of the reports available on the Reports view.

Changing how long report data is stored

Ping Active Monitor data is stored in the WhatsUp Gold database to populate the Performance reports available in the application.

- 1 From the main menu, select **Configure > Program Options**.
- 2 In Program Options, select **Report Data**.



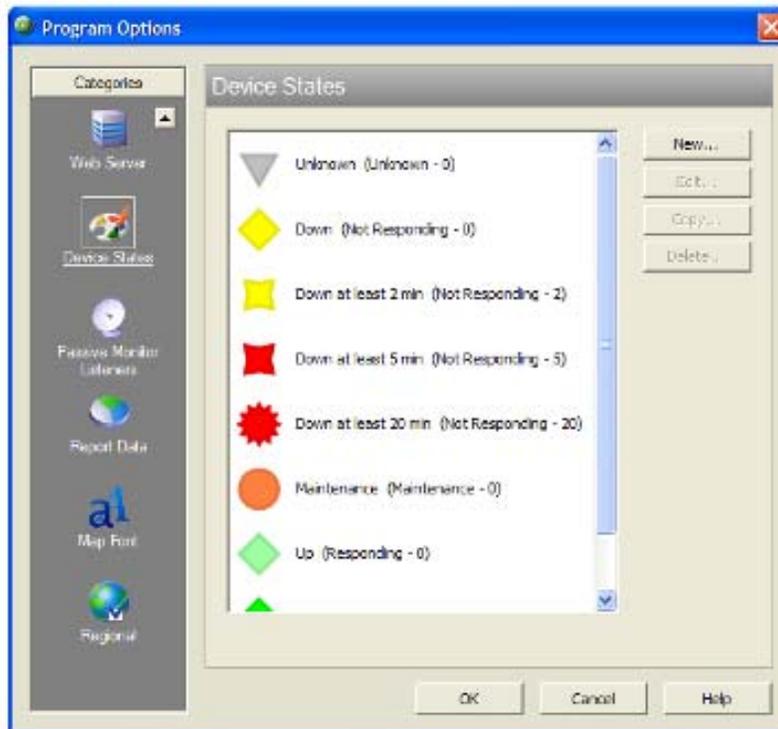
- 3 On the Report Data section, you can change the settings for raw data, hourly data, and daily data.
- 4 Click **OK** to save the changes.

You can see how many rows in the database that the data takes up by viewing the numbers under the time settings.

Changing the device state colors or icons

To change the device state colors or icons:

- 1 From the main menu, select **Configure > Program Options**.
- 2 In Program Options, select **Device States**.



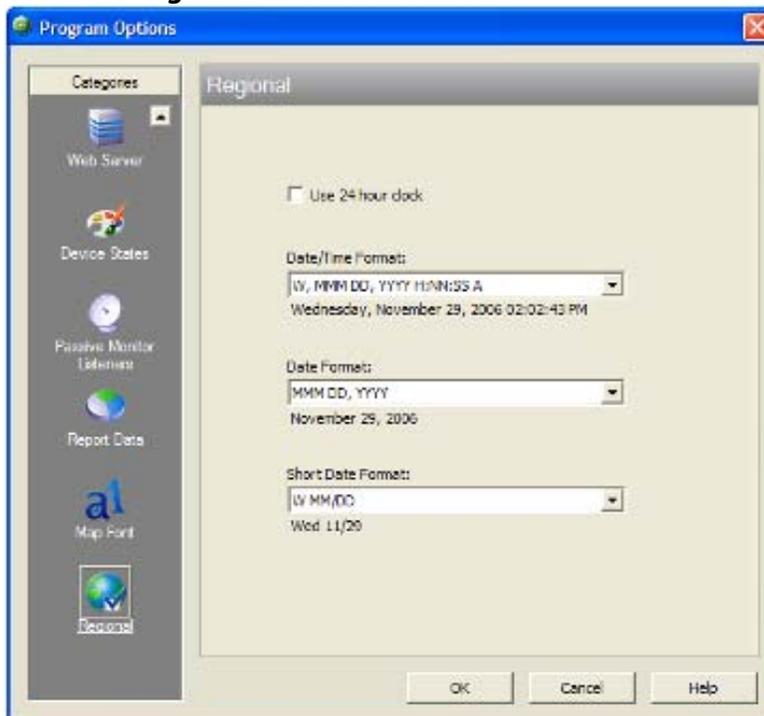
- 3 To change an existing icon or state, select the entry from the list and click **Edit**.
- 4 Adjust the shape and color of the icon using the settings in the **Device State Editor**.
- 5 Click **OK** to save changes.

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.

Changing clock/regional preferences

To use a 24-hour clock instead of the default 12-hour clock:

- 1 From the WhatsUp Gold main menu, select **Configure > Program Options**.
- 2 Select the **Regional** section.



- 3 Select the **Use 24 hour clock** option.
- 4 Click **OK**.

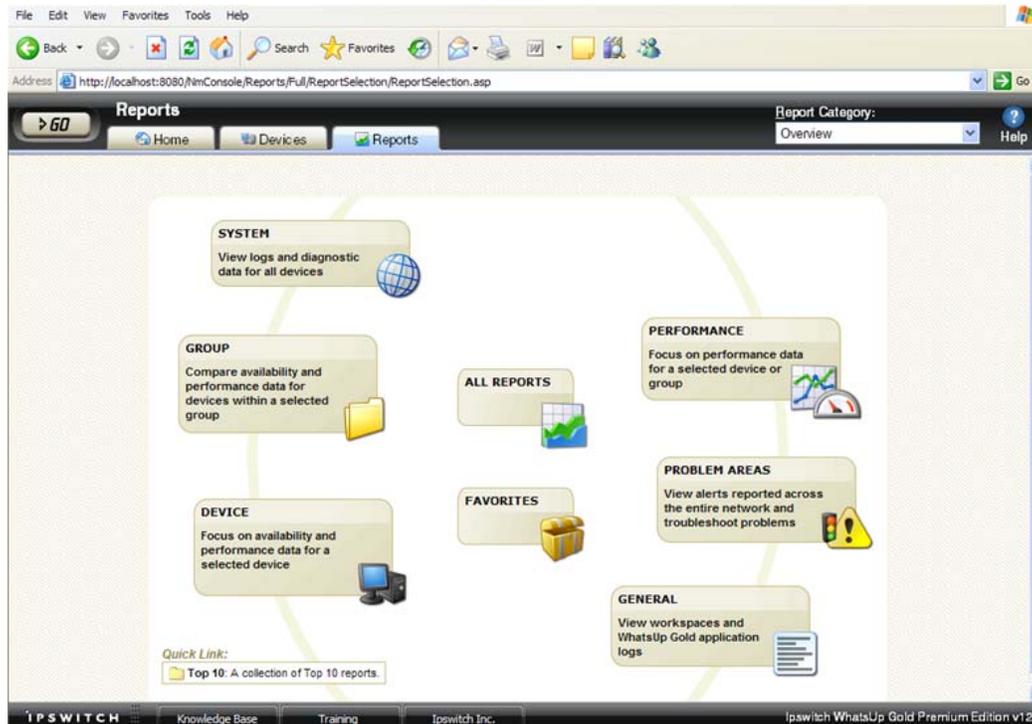
Using Full Reports

In This Chapter

- Learning about full reports257
- List of full reports260
- About report refresh intervals263
- Printing, exporting, and saving full reports264
- Report column sizing and sorting265
- Changing the report date range265
- Adding report to your list of favorites.....266
- Using Recurring Reports267

Learning about full reports

Full reports are used to troubleshoot and monitor performance and historical data that has been collected during the operation of the application.



From the WhatsUp Gold console, you can access full reports by clicking the Reports  button on the console toolbar.

Report categories

Reports in WhatsUp Gold are broken down by the scope and the type of information displayed within each report.

There are three categories for full reports based on the scope of information displayed:

- **System.** These reports display system-wide information. System reports do not focus on a particular device nor a specific device group. For example, the General Error Log and the Web User Activity Log are system reports.
- **Group.** These reports display information relating to a specific device group. For example, the Group State Change Timeline and the Group Actions Applied reports are group reports.
- **Device.** These reports display information relating to a specific device. For example, the Device Status Report is a device report.

There are three categories for full reports based on the type of information displayed:

- **Performance.** These 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. For example, the Device Custom Performance Monitors and the Group Memory Utilization reports are performance reports.



Note: By default, performance data is not collected for the monitors assigned to the devices in your database. To begin collecting performance data for a device, right-click on a device on the Devices tab and select **Properties** from the context menu. In the Device Properties dialog, select **Performance Monitors** and choose the monitors you want to apply to the selected device.

- **Problem Areas.** These are troubleshooting reports that allow you to investigate network issues. For example, the Group Active Monitor Outage and the Passive Monitor Error Log are problem area reports.
- **General.** These reports display information on your WhatsUp Gold settings and diagnostics, as well as device-specific and user-configured details. For example, the Home, Top 10, and Device Status workspaces/full reports are general reports.

Advantages of full Reports

- Larger than workspace reports, full reports give you a larger data view, which can be useful in pin-pointing the time an event occurred or viewing multiple graphed items. Many workspace reports link to full reports, so that you can view 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.

- A list in the upper-right corner of a full report screen allows you to navigate to other reports in the same category. When you use this list to navigate to another report, the date range selected in the report you are navigating away from is transferred to any report you view subsequently.
- Much of the data in full reports can be exported to Microsoft Excel or to a formatted text file.

About System Reports

System reports display system-wide information. System reports do not focus on a particular device nor a specific device group, but rather all devices that fall under a certain category. For example, when choosing to view the General Error Log, all errors that occurred on your network are listed, regardless to which group a device belongs.

When viewing a system report, take note of the features made available to you to enhance your report viewing experience:



The report **Date/Time Picker** located in the middle of the page allows you to easily change the time period for the report you are viewing.

The **More System Reports** drop-down menu allows you to easily jump to other system reports, or to bring up the report picker to select from all full reports.

To the right of the More System Reports drop-down are the report icons:

- **Export.** Allows you to export a report into text or Microsoft Excel.
- **Favorites.** Allows you to add a report to your list of Favorites.
- **Help.** Brings up the WhatsUp Gold help system.

About Group Reports

Group reports display information relating to a specific device group. For example, when choosing to view the Group Actions Applied report, you must choose to which group the report applies and will view only Actions applied in that specific group.

When viewing a group report, take note of the features made available to you to enhance your report viewing experience:



Along with the Date/Time Picker and the report icons also available to you when viewing system reports, there are two other features unique to group reports.

- The **More Group Reports** drop-down menu allows you to easily jump to other group reports, or to bring up the report picker to select from all full reports.
- The **All Devices** button, located to the right of the Reports tab, brings up the Device Group Picker dialog. From this dialog you can choose a group for the report you are viewing.

About Device Reports

Device reports display information relating to a specific device. For example, when choosing to view the CPU Utilization report for a specific device, only CPU utilization information is listed for the specific device you choose for the report.

When viewing a device report, take note of the features made available to you to enhance your report viewing experience:



Along with the Date/Time Picker and the report icons also available to you when viewing system and group reports, there are a few other features unique to device reports.

- The **More Device Reports** drop-down menu allows you to easily jump to other device reports, or to bring up the report picker to select from all full reports.
- The **Device Picker** button located directly to the right of the Reports tab allows you to change the device-in-context for the report you are viewing.
- The **Device Properties** button to the right of the Device Picker button brings up the Device Properties for the device-in-context.
- The **Chart Properties** button allows you to change the graph properties. These property configurations are user-specific.

List of full reports

The following is a list of all reports that are available in Ipswitch WhatsUp Gold v12.

System reports	Type	Description
Action Log	Problem Area	A record of all Actions that WhatsUp attempts to fire.
Active Discovery Log	General	A record of all Active Discovery task results.
Activity Log	General	A history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the selected time period.
General Error Log	Problem Area	A record of error messages generated by WhatsUp.

System reports	Type	Description
Passive Monitor Error Log	Problem Area	A record of Passive Monitor errors reported by WhatsUp.
Performance Monitor Error Log	Problem Area	A record of Performance Monitor errors reported by WhatsUp.
Recurring Action Log	General	Results of Recurring Action executions.
Recurring Report Log	General	Results of Recurring Report executions.
Remote Site Log	Problem Area	A record of messages generated by Remote Server connection attempts. Available in WhatsUp Gold MSP and WhatsUp Gold Distributed editions.
Remote Site Status	Problem Area	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	Problem Area	A history of SNMP traps that have occurred during the selected time period. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.
State Change Acknowledgement	Problem Area	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 which require acknowledgement and then acknowledge them.
Syslog Entries	Problem Area	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	General	Shows the history of user activity on the system.
Windows Event Log	Problem Area	Shows Windows events logged for all devices 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.

Group reports	Type	Description
Actions Applied	General	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	Problem Area	Compare the amount of time the Active Monitors on your devices have been available.
Active Monitor Outage	Problem Area	Compare the amount of time the Active Monitors on your devices have been down.

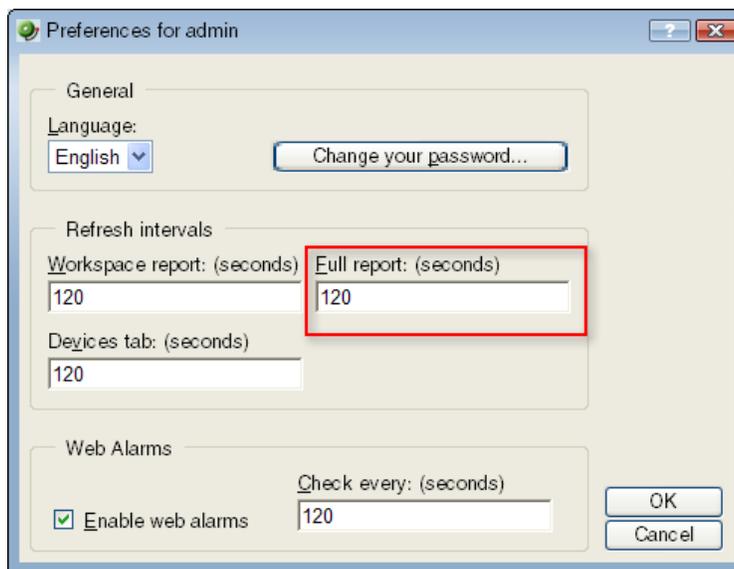
Group reports	Type	Description
CPU Utilization	Performance	CPU utilization statistics for devices by group.
Disk Utilization	Performance	Disk space utilization statistics for devices by group.
Health	Problem Area	The current status of monitored devices in the selected group, along with each Monitor configured to those devices.
Interface Utilization	Performance	Interface traffic and utilization for devices by group.
Memory Utilization	Performance	Memory utilization statistics for devices by group.
Ping Availability	Performance	Ping availability statistics for devices by group.
Ping Response Time	Performance	Ping response times for devices by group.
Quarterly Availability Summary	General	Shows the availability summary for a group.
State Change Timeline	Problem Area	A timeline of when each Monitor on a device in the selected group changed from one state to another during the selected time period.
State Summary	General	A summary of device states organized by device group.

Device reports	Type	Description
Active Monitor Availability	Problem Area	Find out when the Active Monitors on your device have been accessible.
CPU Utilization	Performance	CPU utilization statistics for a device.
Custom Performance Monitors	Performance	View information on your devices collected by Performance Monitors.
Device Status	General	A detailed look at a specific device.
Disk Utilization	Performance	Disk space and utilization statistics for a device.
Health	Problem Area	Displays the current status (a snapshot) of the selected device and all Monitors on that device. 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	Performance	Interface traffic and utilization statistics.
Memory Utilization	Performance	Memory utilization statistics for a device.
Performance Monitor Error Log	Problem Area	A record of Performance Monitor errors for an individual device.
Ping Availability	Performance	Availability statistics for a device.
Ping Response Time	Performance	Ping response times for an individual device.

Device reports	Type	Description
SNMP Trap Log	Problem Area	A history of SNMP traps that have occurred for the selected device during the selected time period. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.
State Change Timeline	Problem Area	This report shows a timeline of when each Monitor on the selected device changed from one state to another during the selected time period.
Syslog Entries	Problem Area	This report shows syslog events logged for the selected device 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.
Windows Event Log	Problem Area	This report shows Windows events logged for the 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.

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 at the time the change is made.

To change the report refresh interval:

- 1 Open the User Preferences dialog.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > Preferences**.
- 2 Enter a new time (in seconds) for the report refresh interval in the **Full report** field.
- 3 Click **OK** to save changes.

Printing, exporting, and saving full reports

All full reports can be printed and many can be exported into text or Microsoft Excel. In some cases, exported reports show more detailed data than that of the data displayed in the report in Report View. For example, an exported report may contain more data columns, or a floating data point with higher precision. For either the print or export functions to work, Client Side JavaScript must be enabled. Full reports can also be saved for later review.

To print a full report:

While viewing the full report you wish to print:

- 1 Right-click anywhere inside the report window.
 - 2 From the right-menu, select **Print**.
 - 3 On the Print dialog, click **Print**.
- or -
- Select **File > Print**.
- 4 On the Print dialog, click **Print**.

To export a full report to text:

While viewing the full report you wish to export:

- 1 On the Report Toolbar, click the **Export** button.
- 2 On the Export Report dialog, select **Export to Text**.
- 3 Clear or select the following options: **Include report title**, **Include column names** to either include or remove the report title or column names from the exported file.
- 4 Choose a **Column delimiter** from the drop-down menu.
- 5 Choose a **Text qualifier** from the drop-down menu.
- 6 Click **OK** to export the report to text.

To export a full report to Microsoft Excel:

While viewing the full report you wish to export:

- 1 On the Report Toolbar, click the **Export** button.
- 2 On the Export Report dialog, select **Export to Excel**.
- 3 Clear or select the following options: **Include report title**, **Include column names** to either include or remove the report title or column names from the exported file.
- 4 Click **OK** to export the report to Excel.

To save a full report:

While viewing the full report you wish to save:

- 1 Select **File > Save As**.
- 2 In the Save Web Page dialog, browse to the location you wish to save your file from the **Save in** box.
- 3 Give the file a title in the **File name** box.
- 4 Choose the type of file you wish to save the report as from the **Save as type** box.
- 5 Click **Save**.

Report column sizing and sorting

All full report columns can be resized. You can 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 again each time the report is viewed.

Most full 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 column's sort direction is indicated with an upward, or downward pointing arrow.



As in column sizing, column sorting settings are saved and are used again each time the report is viewed.

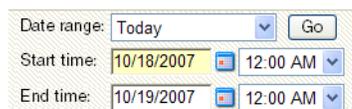
Both column sizing and sorting are maintained on a per user basis, and only for the report in which the column changes are made.

Changing the report date range

Date/Time picker

Most full reports have a date range selection tool (date/time picker) that you can use to change the range of data you are viewing in the report. This tool is useful in controlling the amount of information that you are viewing on a report.

You can select both start and end times for the report.



You can select from the following date ranges:

- Today
- Yesterday
- Last week
- Last month
- Week to date
- Month to date
- Last 4 hours
- Last 8 hours
- Last 3 days
- Last 7 days
- Last 30 days
- Custom

The date and time format for full reports matches the format specified in **Program Options > Regional**.

Zoom tool

The Zoom toolbar allows you to zoom the current date range in or out by selecting the zoom in our zoom out icons. The arrows on the toolbar control moving the selected date range forward and backward one calendar day.



Clicking outside the chart

Another way to move the report date backward and forward is to click in the space outside of the chart report. Clicking the space to the right of the chart will move the selected date forward, while clicking to the left will move the selected date backward.

Adding report to your list of favorites

As you're viewing reports, you may find that you tend to visit certain reports more than others. WhatsUp Gold allows you to save these reports to your list of favorites so that you can easily navigate to them.

To add a report to your list of favorites:

- 1 Select a report to view from the WhatsUp Gold Reports tab.
- 2 Click the **Favorites** button located in the upper right side of the report page.

To remove a report from your list of favorites:

- 1 Navigate to your list of favorites from the Report Overview page.
- 2 Click the **Remove** button next to the report(s) you wish to remove from your list of favorites.

Using Recurring Reports

Recurring reports let you send a "snapshot" of selected WhatsUp Gold Workspace Report or Full Report to email addresses at regularly scheduled intervals. This feature provides a way to easily receive reports or send them to other team members who need reports at specified intervals.

Recurring reports can be sent either in the body of the email message generated or as an attached Archived Web Page (.mht) file.

Configuring Recurring Reports

To create a new Recurring Report:



Important: Recurring reports for workspace reports that include Split Second Graphs display a user rights error. Currently, Split Second Graphs are not supported in recurring reports.



Note: Recurring reports are sent in a fixed format that cannot be modified. They may not appear as expected, depending on your email client and your email preferences. If this is the case, you can send the reports as attachments.



Note: Recurring reports of workspace reports can only be sent as attachments.

- 1 From the WhatsUp Gold console, select **Configure > Recurring Reports**.
- 2 On the Recurring Reports dialog, click **New** to create a new report.
- 3 On the General dialog, enter a title for the report in the **Report name** box.
- 4 Enter the full URL path to the report.

You can find this path by selecting a report in the web interface. The URL shown in the address bar is the URL you need to enter in the **URL box**. You can use "localhost" - or - the configured IP address for the WhatsUp computer in the report URL.

- 5 Click **Next**.
- 6 On the Schedule dialog, select the date and time on which to send the report.
- 7 Click **Next**.
- 8 On the E-mail dialog, enter the Email (SMTP) information for the Email address to which you are sending the report.
 - **E-mail address.** Enter an email address for where you would like the report sent.
 - **Outgoing mail (SMTP) server.** Enter the SMTP server for your network.
 - **Port.** Enter the port number for the mail server.
 - **From.** Enter an email address for whom is sending the report. The default address is from WhatsUp Gold.

- **Subject.** Enter a subject for the report email.
 - **Send reports as attachments.** Select this option to have reports sent as attachments, rather than inline text within the original email. Workspace reports can only be sent as attachments.
- 9 Click **Finish** to add the report.

To edit an existing Recurring Report:

- 1 From the From the WhatsUp Gold console, select **Configure > Recurring Reports**.
- 2 On the Recurring Reports dialog, select an existing Recurring Report and click **Edit**.
- 3 Follow through the Recurring Report dialogs as you would for creating a new Recurring Report.

Testing Recurring Reports

To test a recurring report before the scheduled time and date:

- 1 From the console, select **Configure > Recurring Reports**.
- 2 On the Recurring Reports dialog, select a report and click **Test**.
- 3 After the test is complete, a pop-up message tells you whether the test was successful.

Understanding and Using Workspaces

In This Chapter

Learning about workspaces	269
About types of workspaces.....	270
Managing Workspace Views	275
Navigating through workspace views	278
About workspace content.....	278
Adding workspace reports to a workspace view	278

Learning about workspaces

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

Workspaces in WhatsUp Gold are designed to be user-specific, and are configurable to include workspace reports specific to users' needs. Workspaces contain multiple *views* that let you organize various workspace reports by the type of information they display. When you begin customizing your workspace views, you should consider the types of information you need to view most often, the devices in which you need to pay closest attention, and what level of detail you want to monitor through a particular workspace view. You should also take into consideration the type of workspace, and the types of workspace reports you can add to a particular workspace type.

Home and Device Status workspaces

Home workspaces can display both Home- and Device-level workspace reports. You can place any workspace report on a Home workspace; mixing and matching summary, group, and device-specific data.

Changes that you make to a workspace view only affect your user account. If you decide to completely change all of the workspace views under your account, your user account will be the only account affected by these changes. For more information, see *Managing workspace views* (on page 275).

Device Status workspaces are limited to display only Device-level workspace reports. Only workspace reports specific to a single device can be placed on a device workspace. When you change the device-in-context, the reports displayed show data corresponding to the newly selected device. For more information, see *Adding workspace reports to a workspace view* (on page 278).

About types of workspaces

The WhatsUp web interface has three types of workspaces:

- *Home* (on page 270)
- *Device Status* (on page 271)
- *Top 10* (on page 273)

Each of the workspace types supports multiple user-defined views and up to 15 small reports known as workspace reports can be displayed within each view. These workspace reports show content ranging from Current Interface and CPU utilization to Syslog messages. It's up to you to decide which content is most important.

About the Home Workspace

Home Workspace

The WhatsUp Gold *Home Workspace* is the first screen that you see after you log in to the web interface. Referred to as "Home," this universal workspace is designed to house the network information that you need most visible.



The Home Workspace can display both Home- and Device-level workspace reports. You can place any workspace report on a Home workspace; mixing and matching summary, group, and device-specific data.

The content of this Workspace varies for each user. Changes that you make to a workspace view only affect your user account. This Workspace should contain the information about your network that is most important to you. This Workspace 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 job.

The Home Workspace also includes three starter views:

- General
- Problem Areas 1
- Problem Areas 2

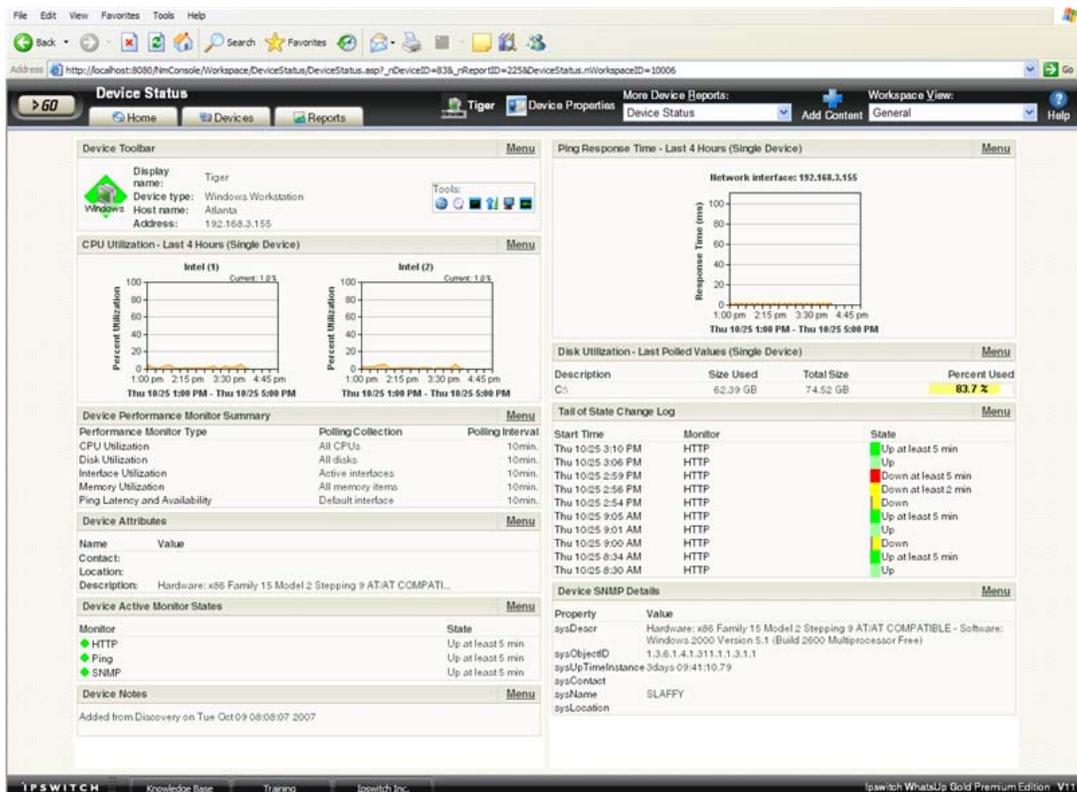
Each workspace view includes several default workspace reports that you can decide to keep, alter, or remove. You can also add other workspace reports to these views. For more information, see *Adding workspace reports to your Home Workspace* (on page 278).

You can create your own workspace views for the Home workspace through the *Manage Workspace Views* (on page 275) dialog.

About the Device Status workspace

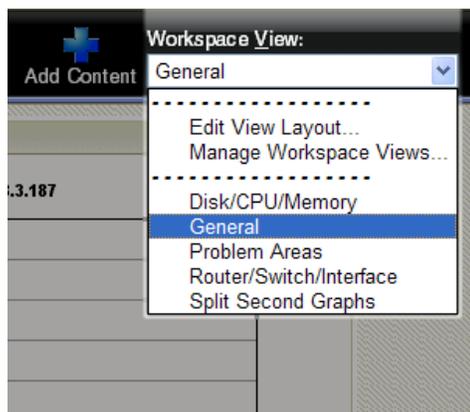
Device Status workspace

The Device Status Workspace is very similar to the Home Workspace, but the Device Status workspace is limited to display only Device-level workspace reports. Only workspace reports specific to a single device can be placed on a device workspace.



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

- Disk/CPU/Memory
- General
- Problem Areas
- Router/Switch/Interface

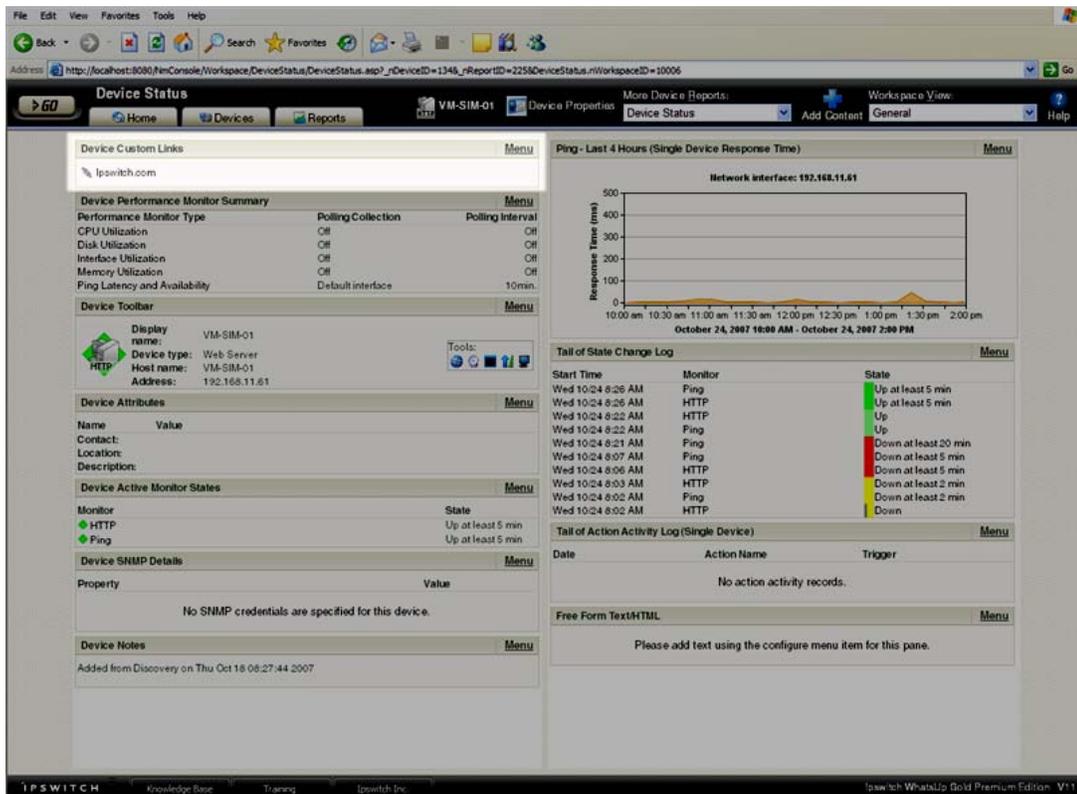


There are many different types of devices with a variety of features and services that can be monitored. The Workspace Views let you select a view that is most appropriate for the individual device. Each time the report is visited, it displays the last view that was selected for a device.

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

Using WhatsUp Gold v12

The device name and icon displays at the top of the Device Status report. You can click the device name, for example 192.168.5.151, to change the focus of the report to another device without leaving the report.



For more information, see *Adding workspace reports to a Device Status workspace* (on page 278).

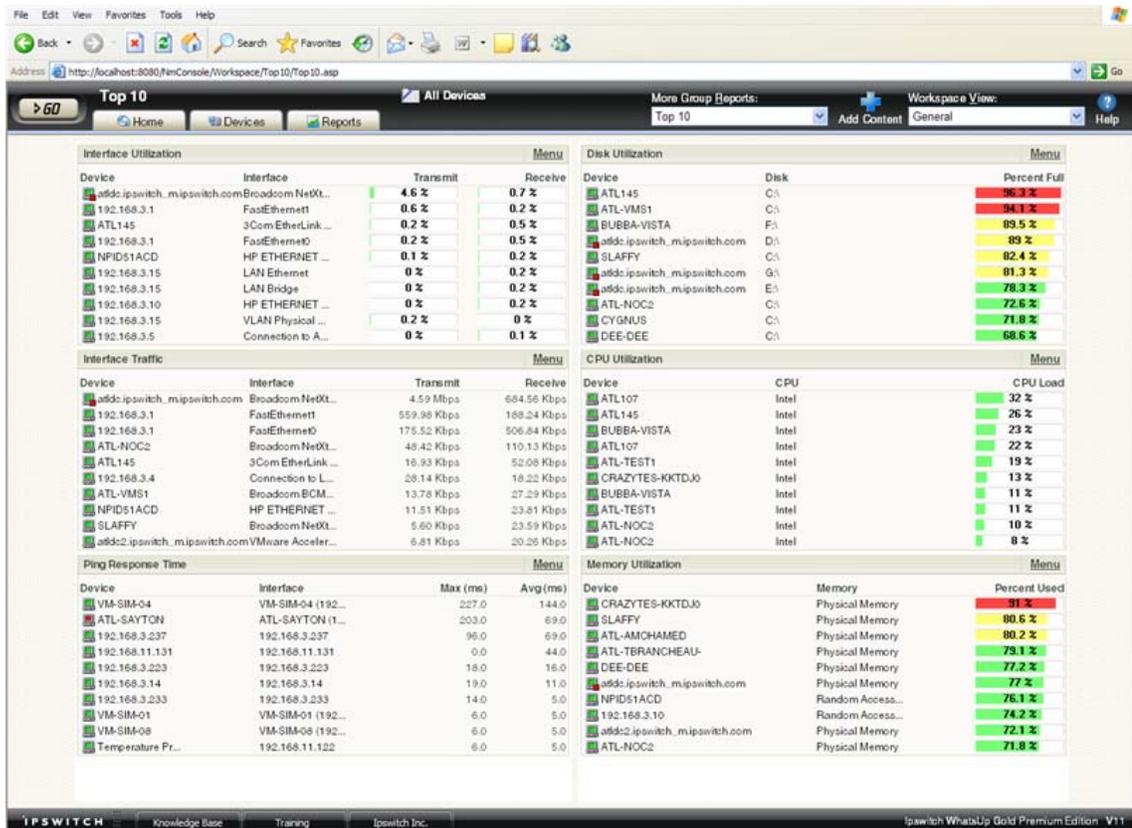
About the Top 10 workspace

The Top 10 workspace

The WhatsUp Gold Top 10 workspace displays the Top 10 full reports for your network devices. The role of the Top 10 Workspace is to show devices, at a glance, that may be potential problems and to provide information on the current health of your network devices. It is pre-configured to include workspace reports that display data on the top network devices by:

- Interface Utilization
- Interface Traffic
- Ping Response Time
- Disk Utilization
- CPU Utilization
- Memory Utilization

Using WhatsUp Gold v12



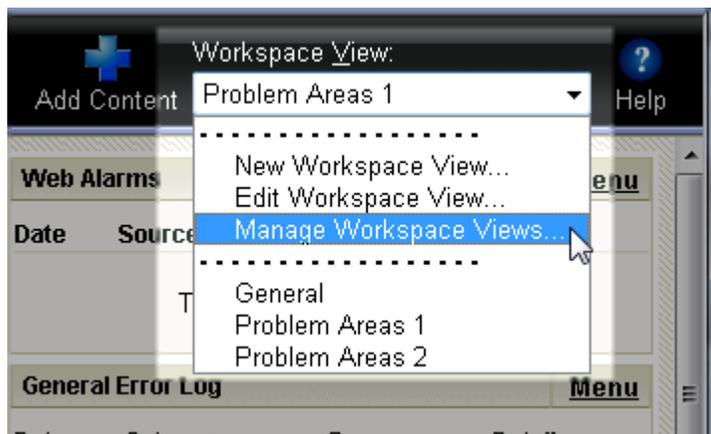
Unlike the Home and Device Status workspaces, the Top 10 workspace is designed with only the General workspace view. You can customize the general view in the same way you can other workspace views by removing the default workspace reports and/or adding other Top 10 and Threshold workspace reports. For more information, see *Adding workspace reports to your Home Workspace* (on page 278).

The Top 10 Workspace 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.

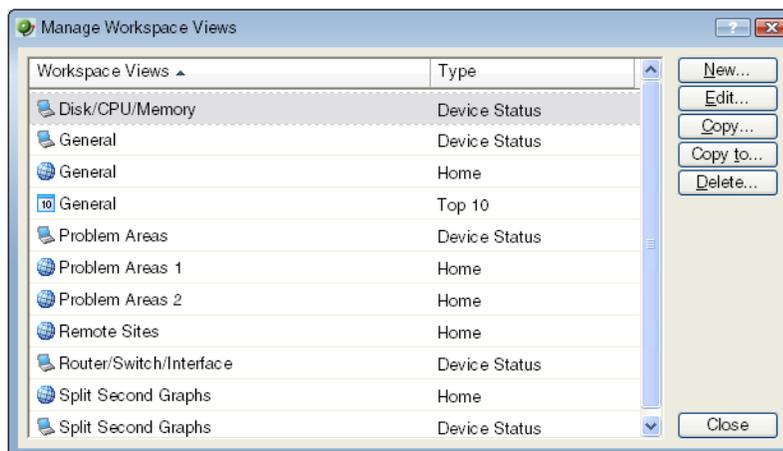
Managing Workspace Views

WhatsUp Gold comes with a few pre-configured workspace "views," including one for Default Remote Sites. You can create more of your own workspace views to use along with the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting. You can also edit, copy, copy to (another user), and delete these views as needed.

From the **Workspace View** list, select **Manage Workspace Views**.



In the Manage Workspace Views dialog, you can create new workspace views, and edit, copy, or delete an existing workspace view.

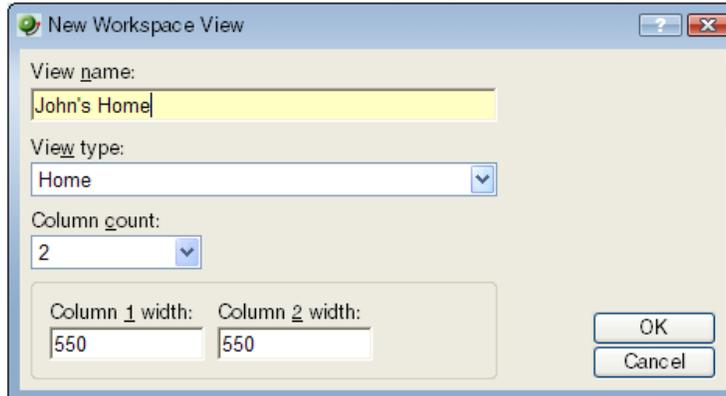


- Click **New** to configure a new workspace.
- Select an existing workspace view and click **Edit** to change the current configuration of a workspace.
- Double-click an existing workspace to change its configuration.
- Select a workspace view, then click **Copy** to make a copy of that workspace and add it to the list.

- Select a workspace view, then click **Copy to** to copy an existing workspace from here to another user's list of workspaces.
- Select a workspace monitor view, then click **Delete** to remove it from the list.

To create a new workspace view:

- 1 From the Manage Workspace Views dialog, select **New**. The New Workspace View dialog appears.



- 2 Enter the appropriate information in the following fields:
 - **View name.** Enter a name for the workspace view.
 - **View type.** Choose a type for the workspace view from the drop-down menu.
 - **Column count.** Enter a value for the number of columns you wish to have in the new workspace view. Keep in mind, the more columns you include, the smaller the data displayed inside a workspace.
 - Enter a value in pixels for each of the workspace columns.
- 3 Click **OK** to save changes.

To edit a workspace view:

- 1 From the Manage Workspace Views dialog, select **Edit**. The Edit Workspace View dialog appears.
- 2 Enter the appropriate information in the following fields:
 - **Workspace name.** The workspace title as it appears in the Workspace Library.
 - **Workspace type.** The workspace type as it appears in the Workspace Library (Home or Device).

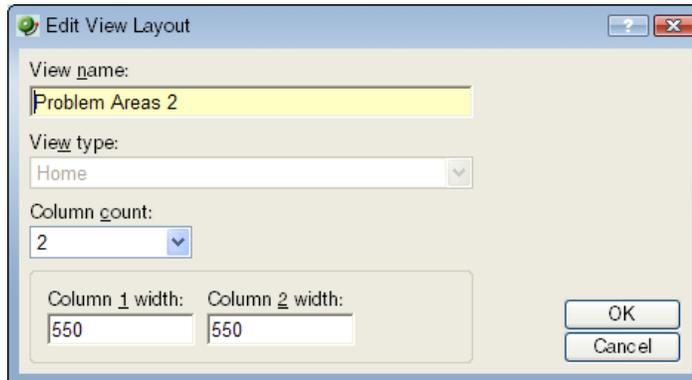


Note: Workspace view types cannot be changed after a view is created. For example, a Home workspace type cannot be changed later to a Device Status workspace type.

- **Column count.** The number of columns in the workspace.
 - **Column width.** The width of each column in the workspace in pixels.
- 3 Click **OK** to save changes.

To copy an existing workspace view:

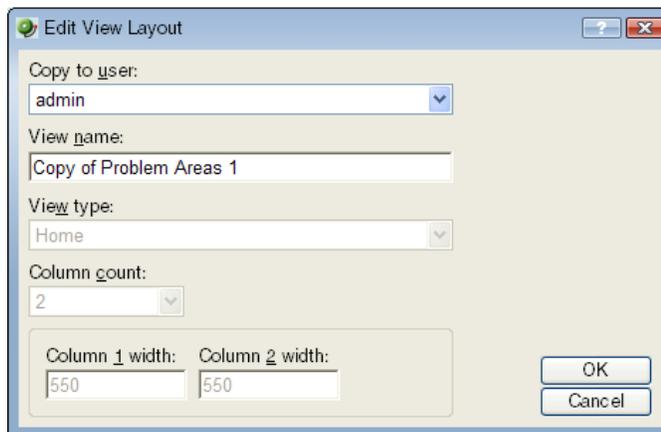
- 1 From the Manage Workspace Views dialog, select **Copy**. The Edit Workspace View dialog appears.



- 2 Enter the appropriate information in the following fields:
 - **Workspace name.** The workspace title as it appears in the Workspace Library.
 - **Column count.** The number of columns in the workspace.
 - **Column width.** The width of each column in the workspace in pixels.
- 3 Click **OK** to save changes.

To copy a workspace view to another WhatsUp Gold user:

- 1 From the From the Manage Workspace Views dialog, select **Copy to**. The Edit Workspace View dialog appears.



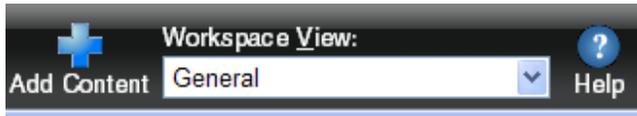
- 2 Enter the appropriate information into the following fields:
 - **Copy to user.** Select a user account from the drop-down menu in which to copy the workspace view.
 - **View name.** The name of the workspace view as it will appear in the Workspace Library.
- 3 Click **OK** to save.

To delete a workspace view:

- 1 From the From the Manage Workspace Views dialog, click **Delete**.
- 2 Click **OK** on the dialog that follows.

Navigating through workspace views

The main way to navigate from one workspace view to another is through the Workspace Toolbar. From here you can add content to a workspace, manage your workspace and workspace views, and access the WhatsUp Gold help system.



The Workspace Toolbar

- **Add Content.** Use this button to add workspace reports to your workspace views.
- **Workspace View.** Use this drop-down menu to edit your workspace views and to switch between workspace views.
- **Help.** Use this button to view the WhatsUp Gold Help for the window you are currently viewing.

About workspace content

Workspace reports are smaller versions of the full reports. The workspace reports are displayed within WhatsUp Gold workspace views. For more information, see *Understanding and using workspaces* (on page 269).

To add, remove, and move workspace reports to a workspace view:

- To add a report, click **Add content** on the **Workspace Toolbar** to bring up the Workspace Report Picker. On the Add Content to View dialog, you can select multiple workspace reports, from multiple categories. A preview for the workspace report is displayed at the bottom of the dialog. For more information see, *Adding workspace reports to a Device Status workspace* (on page 278).
- To remove a report, go to the menu for that workspace report and select **Close**. Keep in mind, when you remove a report, any customizations you have made to it are lost.
- To move a workspace report, click on a report's title bar and drag it to a new space in the workspace view.

Adding workspace reports to a workspace view

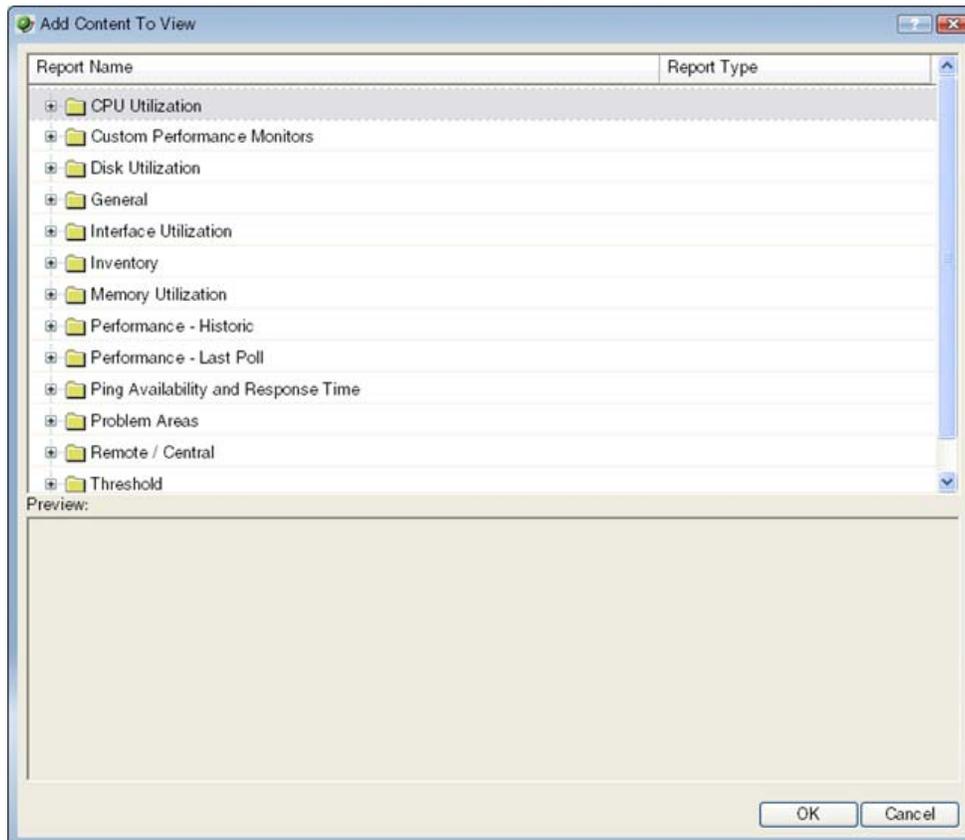
You can customize a workspace by adding additional reports to the workspace view. Click **Add Content** to add additional reports to the workspace view.



The reports that are available to add will vary, depending on the current workspace type. Home Workspace Views can display any available workspace report, while Device Status Workspace Views only present the reports that apply to a single device. There are a large number of available reports, so they have been categorized based on their function. The icon to the left of each report indicates the type of report listed. Report types include tabular, pie charts, line charts, gauges, and more. When you select a report in the list, a report preview shows in the Preview pane below the list.

To add a report to a workspace:

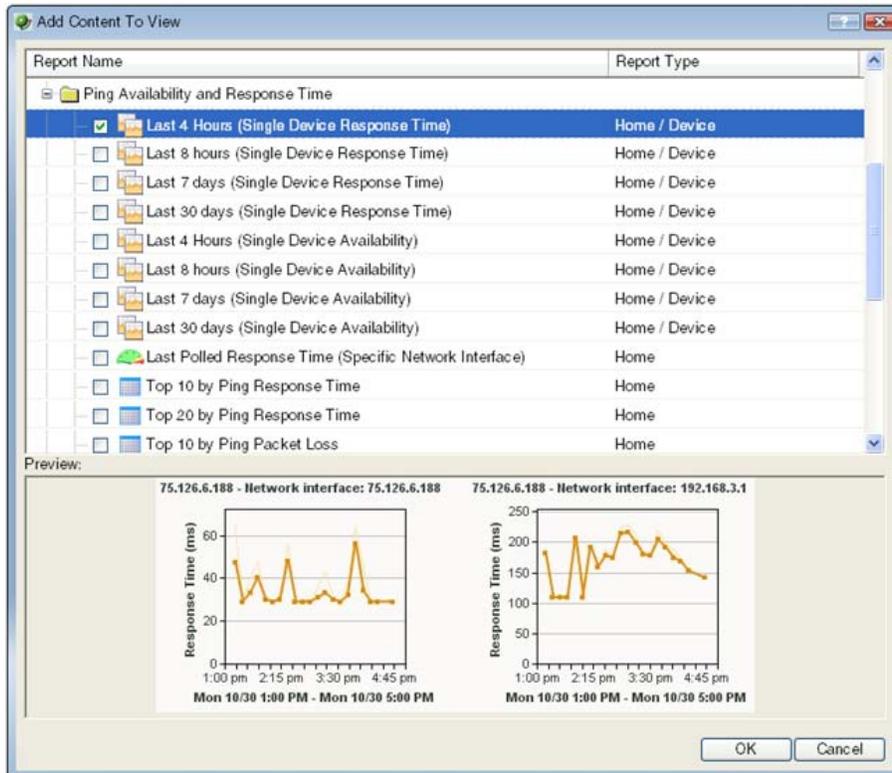
- 1 Open the workspace view to which you want to add content.
- 2 In the Workspace toolbar, click **Add Content**. The Add Content To View page appears.



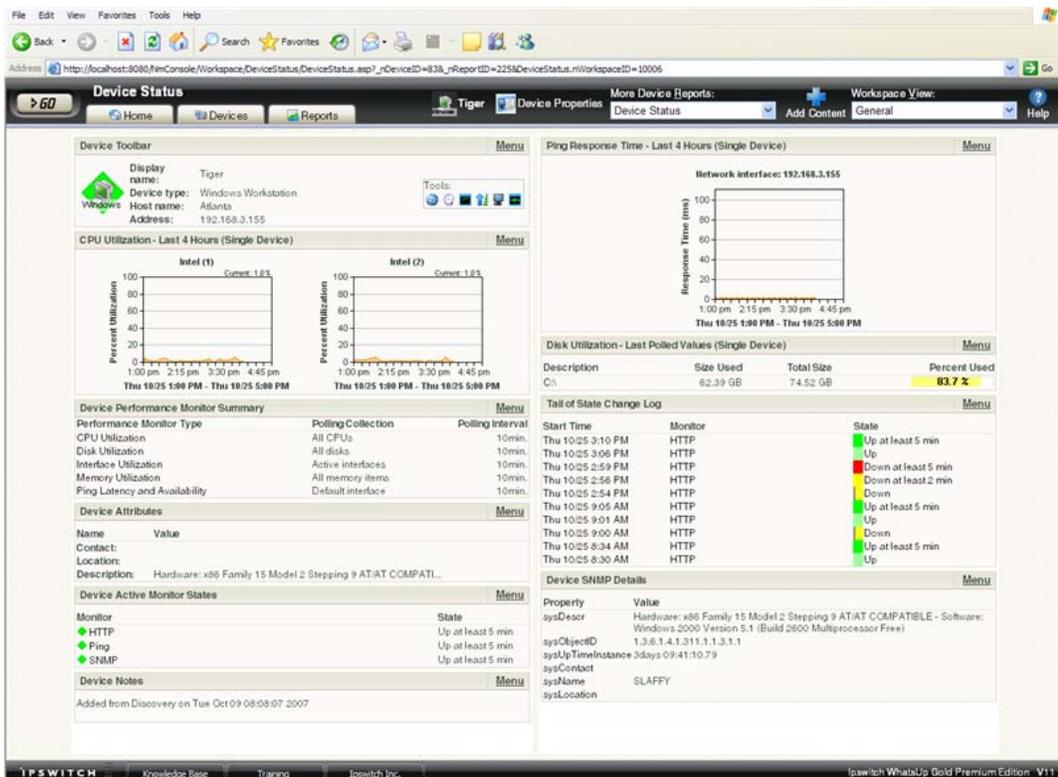
- 3 Click the button next to a report category folder, then click a report option box for each report(s) you want to add to the workspace. A preview image for each workspace report is displayed at the bottom of the dialog.

Using WhatsUp Gold v12

For example, click to expand the **Ping Availability and Response Time** category, select the **Last 4 Hours (Single Device Response Time)** option.



4 Click **OK** to save changes. The new report is added to the workspace view.



Using Workspace Reports

In This Chapter

Learning about workspace reports.....	283
List of workspace reports.....	285
About the workspace report menu	297
Configuring a workspace report	297
Moving Workspace Reports within a workspace view.....	299
Device Group Mini Status workspace report.....	300

Learning about workspace reports

WhatsUp Gold offers a collection of more than 100 configurable workspace reports for display in workspace views. 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 workspace view, making it possible to view multiple reports simultaneously.

Device and Home workspace reports

Like workspaces, workspace reports are also typed as either Device or Home:

- **Device** workspace reports are displayable in Device workspaces, such as the Device Status workspace.
- **Home** workspace reports are displayable in Home workspaces, such as the your default Home workspace.

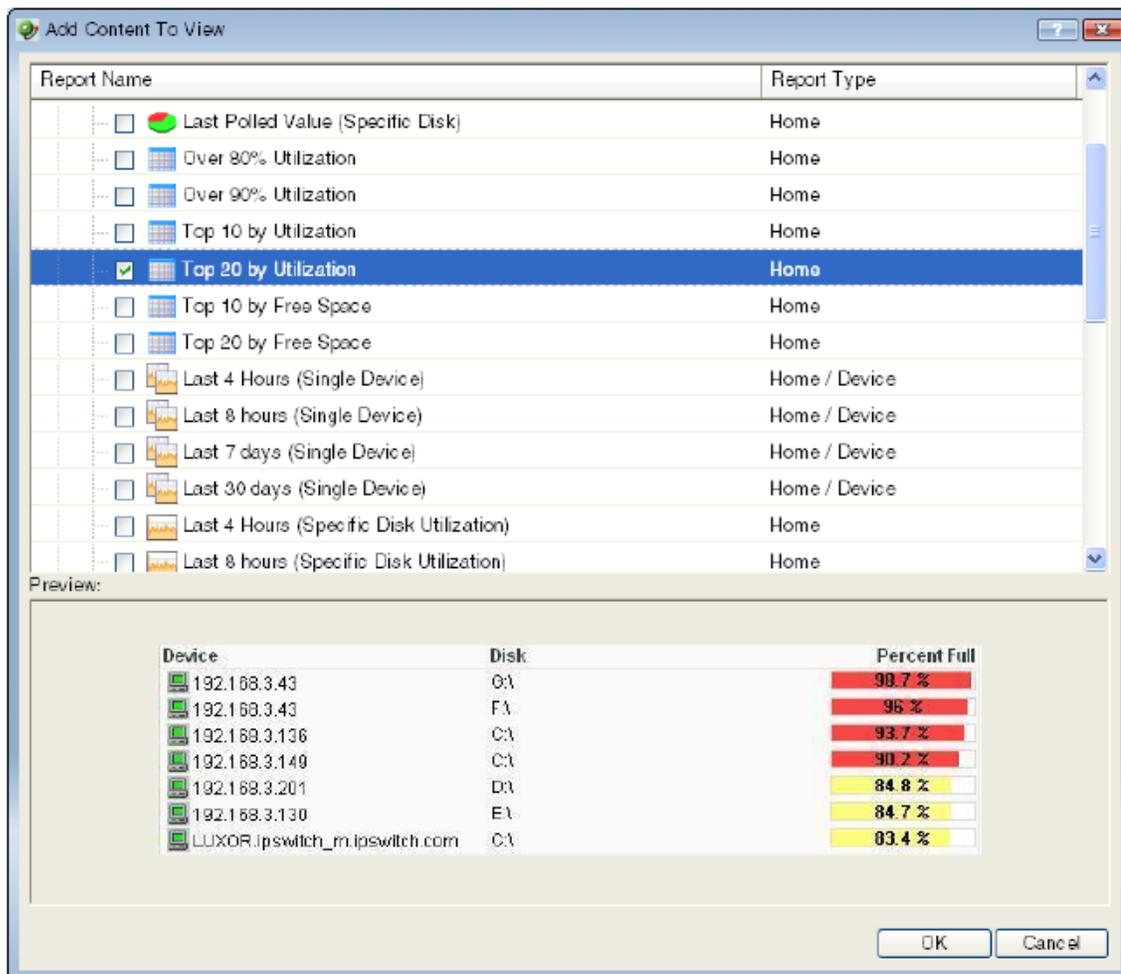
Workspace report categories

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

- **CPU Utilization.** These workspace reports display information pertaining to device and network CPU levels.
- **Custom Performance Monitors.** These workspace reports display information pertaining to your custom performance monitors.
- **Disk Utilization.** These workspace reports display information pertaining to device and network disk levels.
- **General.** These workspace reports display information on your WhatsUp Gold settings and diagnostics, as well as device-specific and user-configured details.

- **Interface Utilization.** These workspace reports display information pertaining to device and network interfaces.
- **Inventory.** These workspace reports provide a break-down of network devices and their settings, including Actions, monitors, and policies.
- **Memory Utilization.** These workspace reports display information pertaining to device and network memory levels.
- **Performance (Historic and Last Poll).** These workspace 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 workspace reports display information pertaining to device ping availability, response time, and packet loss.
- **Problem Areas.** These are trouble-shooting workspace reports that allow you to investigate network issues.
- **Remote/Central** (included in the WhatsUp Gold Distributed, and MSP Editions). These include a variety of workspace reports for the Remote Sites that you are monitoring with the WhatsUp Gold Central Site.
- **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 network tool and the Web Task Manager network tool in any workspace view.
- **Threshold.** These workspace reports display information on your network's CPU, disk, interface, and memory utilization, and ping function; at or above a specific threshold.
- **Top 10.** These workspace reports display the top devices on your network according to their CPU, disk, interface, and memory utilization, and ping function.

Workspace reports are listed multiple times on the workspace report picker. For example, the Disk Utilization workspace report is listed under the Disk Utilization, Threshold, Top 10, and Performance categories.



List of workspace reports

The following is a list of all workspace reports available in WhatsUp Gold.

CPU Utilization workspace 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.

CPU Utilization workspace reports	Type	Description
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 a specific CPU's utilization percentages for one device over the last 4 hours.
Last 8 hours (specific CPU)	Home	Details a specific CPU's utilization percentages for one device over the last 8 hours.
Last 7 days (specific CPU)	Home	Details a specific CPU's utilization percentages for one device over the last 7 days.
Last 30 days (specific CPU)	Home	Details a specific CPU's utilization percentages for one device of the last 30 days.

Custom Performance Monitor workspace reports	Type	Description
Last Polled Values (single device)	Home	Details information on a single device's custom performance monitor(s) 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 a device's custom performance monitors over the last 4 hours.
Last 8 hours (single device)	Device	Details a device's custom performance monitors over the last 8 hours.
Last 7 days (single device)	Device	Details a device's custom performance monitors over the last 7 days.

Custom Performance Monitor workspace reports	Type	Description
Last 30 days (single device)	Device	Details a device's custom performance monitors over the last 30 days.
Last 4 hours (specific monitor)	Home	Details a specific custom performance monitor over the last 4 hours.
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.

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

Using WhatsUp Gold v12

Last 30 days (specific disk utilization)	Home	Details a specific disk's utilization percentages for one device over the last 30 days.
Last 4 hours (specific disk free space)	Home	Details a specific disk's free space for one device over the last 4 hours.
Last 8 hours (specific disk free space)	Home	Details a specific disk's free space for one device over the last 8 hours.
Last 7 days (specific disk free space)	Home	Details a specific disk's free space for one device over the last 7 days.
Last 30 days (specific disk free space)	Home	Details a specific disk's free space for one device over the last 30 days.

General workspace reports	Type	Description
Device Notes	Device	Displays a device's notes configured in Device Properties > Notes .
Device Attributes	Device	Displays a device's attributes configured in Device Properties > Attributes .
Device SNMP Details	Device	Displays a device's SNMP details.
Device Toolbar	Device	Displays a device's details configured in Device Properties > General .
Device Custom Links	Device	Displays any custom links assigned to a device in Device Properties > Custom Links .
Device Dependencies	Device	Shows the state of a device and any devices that are up or down dependent on that device.
Device Active Monitor States	Device	Lists all of a device's Active Monitors and their current state.
Performance Monitor Summary	Device	Displays a polling summary for the device-in-context.
Map View	Home	Displays a smaller version of a network map.
Database Size	Home	Displays a graphical representation of the WhatsUp Gold database at the time of the last poll.
Custom Links	Home	Displays any custom links that you add to the workspace report.
Free Form Text/HTML	Home	Displays any free form text or HTML code that you add to the workspace report.
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.
Interface Details (specific interface)	Home	Displays SNMP information reported by a specific network interface.
User Orientation	Home	Displays information regarding the new the new web interface, workspaces, and workspace reports.
Favorite Reports	Home	Displays a list and link to any full report on your list of favorites.

Interface Utilization workspace 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.
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 a specific interface's utilization for one device over the last 4 hours.
Last 8 hours (specific interface utilization)	Home	Details a specific interface's utilization for one device over the last 8 hours.
Last 7 days (specific interface utilization)	Home	Details a specific interface's utilization for one device over the last 7 days.
Last 30 days (specific interface utilization)	Home	Details a specific interface's utilization for one device over the last 30 days.
Last 4 hours (specific traffic interface)	Home	Details a specific interface's traffic for one device over the last 4 hours.
Last 8 hours (specific traffic interface)	Home	Details a specific interface's traffic for one device over the last 8 hours.
Last 7 days (specific traffic interface)	Home	Details a specific interface's traffic for one device over the last 7 days.
Last 30 days (specific traffic interface)	Home	Details a specific interface's traffic for one device over the last 30 days.

Inventory workspace 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.
Active Discovery Results	Home	Once an Active Discovery is performed, the results are listed in this report.

Memory Utilization workspace reports	Type	Description
Last Polled Values (single device)	Device	Shows the memory utilization for all of device's memories 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 a specific memory's utilization for one device over the last 4 hours.
Last 8 hours (specific aspect)	Home	Details a specific memory's utilization for one device over the last 8 hours.
Last 7 days (specific aspect)	Home	Details a specific memory's utilization for one device over the last 7 days.

Using WhatsUp Gold v12

Last 30 days (specific aspect)	Home	Details a specific memory's utilization for one device over the last 30 days.
--------------------------------	------	---

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

Performance - Last Poll workspace reports	Type	Description
Custom Performance Monitor Values (single device)	Device	Shows the values for all of a device's custom Performance Monitors at the time of the last poll.
Interface Utilization (single device)	Device	Shows the interface utilization for all of a device's interfaces at the time of the last poll.
CPU Utilization (single device)	Device	Shows the CPU utilization for all of device's CPUs at the time of the last poll.
Memory Utilization (single device)	Device	Shows the memory utilization for all of a device's memories at the time of the last poll.
Disk Utilization (single device)	Device	Shows the disk utilization for all of a device's disks 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 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.

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

Using WhatsUp Gold v12

Last 7 days (single device)	Device	Shows the ping availability for all of a device's interfaces over the last 7 days.
Last 30 days (single device)	Device	Shows the ping availability for all of a device's interfaces 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 their current ping response time.
Top 20 by Ping Response Time	Home	Lists the top 20 devices based on their current ping response time.
Top 10 by Ping Packet Loss*	Home	Lists the top 10 devices based on their current ping packet loss.
Top 20 by Ping Packet Loss	Home	Lists the top 20 devices based on their 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 100msec	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%.

Problem Areas workspace reports	Type	Description
Devices with Down Active Monitors	Device	Displays a device's down Active Monitors.
All Down Interfaces	Device	Displays a device's down interfaces.
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.
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.
Devices that have fired an Action in the last X hours	Home	Displays devices that have fired an action over the selected time period.
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.
Map View	Home	Displays a smaller version of a network map.
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.

Remote/Central workspace 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.

Remote/Central workspace reports	Type	Description
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.
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.

Split Second Graph workspace 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 a SNMP enabled device.
CPU	Home Or Device	Displays real-time cpu utilization for all cpu's on an SNMP enabled device.
CPU gauge	Home or device	Displays real-time cpu utilization for all cpu's on an SNMP enabled device.
Ping	Home Or Device	Displays real-time ping response time for all network interfaces on device.
Ping gauge	Home or device	Displays real-time ping response time for all network interfaces on 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 a SNMP enabled device.

Split Second Graph workspace reports	Type	Description
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 Usage Bar Graph	Home or Device	Displays a bar graph of the memory usage of a WMI-enabled device in real time.

Threshold workspace 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.
Custom WMI/SNMP	Home	Displays the top devices based on their current custom WMI/SNMP thresholds.
Ping Availability	Home	Displays the top devices based on their current ping availability thresholds.

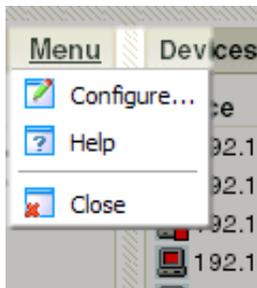
Top 10 workspace reports	Type	Description
Ping Response Time	Home	Displays the top devices based on their current ping response time.
Ping Packet Loss	Home	Displays the top devices based on their current ping packet loss.

Top 10 workspace reports	Type	Description
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 WMI/SNMP	Home	Displays the top devices based on their current custom WMI/SNMP.
Ping Availability	Home	Displays the top devices based on their current ping availability.

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

About the workspace report menu

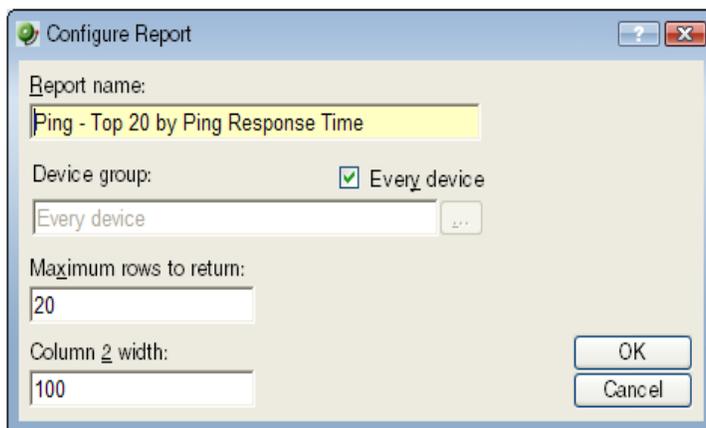
Each workspace report has a menu on the right side of its title bar. From the Workspace Report Menu, you can access help for a specific workspace report, go to the configuration dialog for a report, or close the report. Closing a report removes it from the workspace view. Keep in mind that after you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



Configuring a workspace report

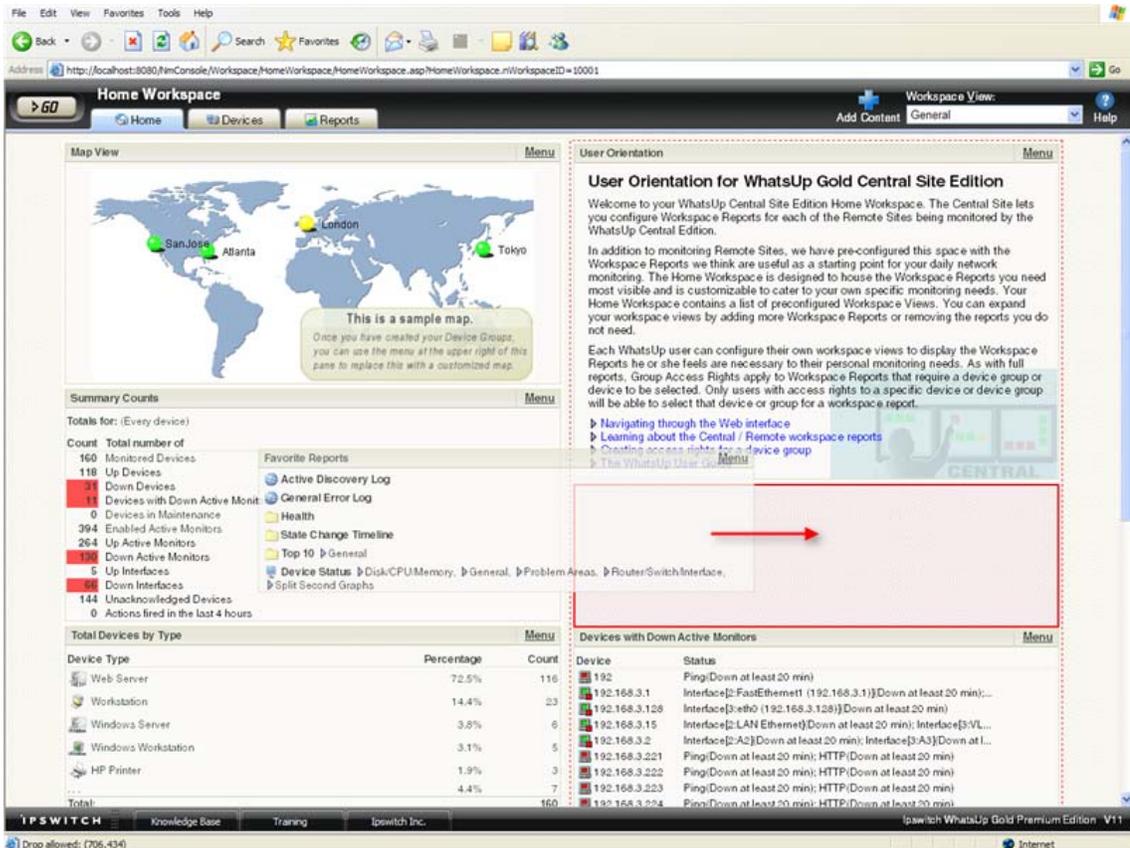
Workspace reports are designed to be customized to fit your specific needs. From a workspace report's menu, select  **Configure** to bring up the configuration dialog. On this dialog, you can:

- Change the report title
- Select a device or device group for the report
- Set the height and width of the report
- Specify the width of certain report columns



Moving Workspace Reports within a workspace view

WhatsUp Gold supports drag-and-drop within the web interface. You can move a workspace report from one column of a workspace view to another, or position a workspace report above or below another workspace report, by selecting it and dragging it to another area of the workspace view. These location changes are saved: workspace reports will appear in the location to which you moved them after logging out from the web interface or after moving between workspace views.



To move a workspace report:

- 1 Select the title bar of the report you want to move, then drag it to the desired location. A red box highlights the area that the report will be placed when the mouse button is released.
- 2 Release the mouse button to place the report in the new page location. If you want to cancel the move, while the report is selected, press the Esc key on your keyboard.

Device Group Mini Status workspace report

The Device Group Mini Status home workspace report lists all devices in a device group and displays their status by color, allowing you to quickly see the status of all devices in a group from across the room.

Device Group Mini Status					Menu
	◆ ether...	◆ ether...	◆ ether...	▼ ether...	
192.168.3.1	▼ vlan1				
	◆ HTTP	◆ Ping	◆ SNMP		
192.168.3.10	◆ HTTP	◆ Ping	◆ SNMP		
192.168.3.14	◆ HTTP	◆ Ping	◆ SNMP		
	◆ LAN ...	◆ LAN ...	◆ VLA...	▼ VLA...	
	▼ VLA...	▼ VLA...	▼ VLA...	▼ VLA...	
	▼ VLA...	▼ VLA...	▼ VLA...	▼ VLA...	
	▼ VLA...	▼ VLA...	▼ VLA...	▼ VLA...	
192.168.3.15	▼ VLA...	▼ LAN ...	▼ LAN ...	▼ LAN ...	
	▼ LAN ...	▼ LAN ...	▼ LAN ...	▼ LAN ...	
	▼ LAN ...	▼ LAN ...	▼ LAN ...	▼ LAN ...	
	▼ LAN ...	▼ LAN ...	▼ LAN ...	▼ LAN ...	
	◆ DNS	◆ HTTP	◆ Ping	◆ SNMP	
192.168.3.19	◆ Ping				
	◆ A1	◆ A2	◆ A3	◆ A4	
	◆ A5	◆ A6	◆ A7	◆ A8	
	▼ B1	▼ B2	▼ B3	▼ B4	
	◆ B5	◆ B6	◆ B7	◆ B8	
	◆ C1	◆ C2	◆ C3	◆ C4	
	▼ C5	▼ C6	▼ C7	▼ C8	
	▼ D1	▼ D2	▼ D3	▼ D4	
	▼ D5	◆ D6	▼ D7	◆ D8	
	◆ E1	▼ E2	▼ E3	▼ E4	
	▼ E5	▼ E6	▼ E7	◆ E8	

Displaying multiple mini status workspace reports within a workspace view grants you a quick look at more than one group on your network and can help monitor important or problem areas more efficiently. You also can display Active Monitors associated with the devices in a selected group, which is useful in pinpointing what services on your network are down.

To aid in maximizing your screen real estate, you have the ability to change the size and display style of the workspace report. Even if the font size is too small to read at first-glance, you can use the mouse-over hover text to find out the identity of a device. The static rows of the mini status workspace report also aid in device recognition, as devices remain in the same position regardless of their current state.

To configure the Device Group Mini Status workspace report:

- 1** On the workspace report menu, select **Configure**.
- 2** Enter the appropriate information in the following fields:
 - **Name.** Enter a title for the workspace report.
 - **Device group.** Select a device group by clicking the browse (...) button. To select every device on the network, regardless of their subgroup, select Every device.
 - **Every device.** Select this option to display every device in the system regardless of group. However, only devices that you have permissions to view will be displayed.
 - **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's 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.

Using SNMP Features

In This Chapter

SNMP overview	303
Monitoring an SNMP Service.....	304
About the SNMP Agent or Manager	304
About the SNMP Management Information Base (MIB).....	304
About SNMP Object Names and Identifiers	305
Using the SNMP MIB Manager	305
Using the SNMP MIB Manager to troubleshoot MIB files.....	306
About the SNMP operations.....	308
Using a custom name for SNMP device interfaces	309
About SNMP Security	312
Using the Trap Definition Import Tool.....	312

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`).

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 160).

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 NT 4.0, Windows 98, Windows 2000, Windows ME, Windows XP, Windows Server 2003, and Windows Vista 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 308) and *Enabling SNMP on Windows devices* (on page 218).

About the SNMP Management Information Base (MIB)

The 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 would be `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, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Configure > SNMP MIB Manager**. The SNMP MIB Manager dialog opens.
- 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.

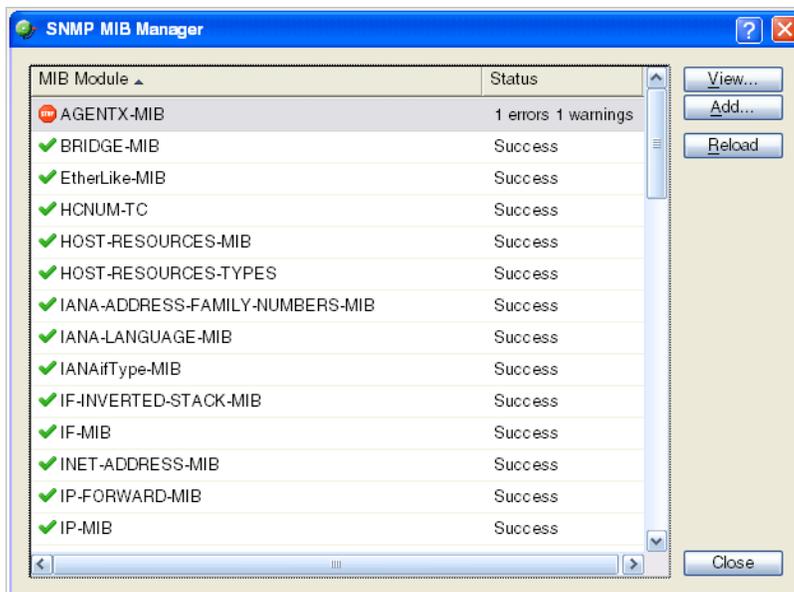


Note: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

- **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:

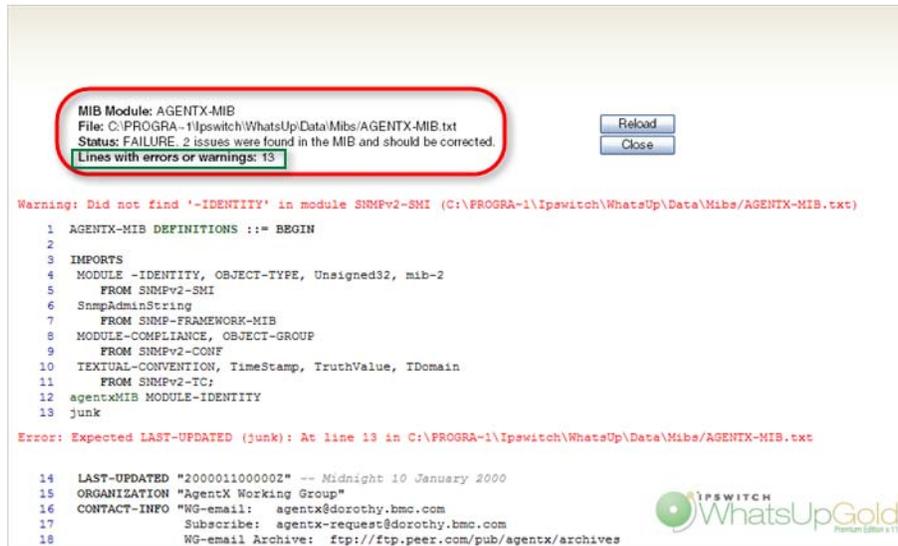
Cannot find module (IANA-RTPROTO-MIB).

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.



```
MIB Module: AGENTX-MIB
File: C:\PROGRAM-1\Ipswitch\WhatsUp\Data\Mibs\AGENTX-MIB.txt
Status: FAILURE. 2 issues were found in the MIB and should be corrected.
Lines with errors or warnings: 13

Warning: Did not find '-IDENTITY' in module SNMPv2-SMI (C:\PROGRAM-1\Ipswitch\WhatsUp\Data\Mibs\AGENTX-MIB.txt)

1 AGENTX-MIB DEFINITIONS ::= BEGIN
2
3 IMPORTS
4 MODULE -IDENTITY, OBJECT-TYPE, Unsigned32, mib-2
5 FROM SNMPv2-SMI
6 SnmpAdminString
7 FROM SNMP-FRAMEWORK-MIB
8 MODULE-COMPLIANCE, OBJECT-GROUP
9 FROM SNMPv2-CONF
10 TEXTUAL-CONVENTION, TimeStamp, TruthValue, TDomain
11 FROM SNMPv2-TC;
12 agentxMIB MODULE-IDENTITY
13 junk

Error: Expected LAST-UPDATED (junk): At line 13 in C:\PROGRAM-1\Ipswitch\WhatsUp\Data\Mibs\AGENTX-MIB.txt

14 LAST-UPDATED "200001100000Z" -- Midnight 10 January 2000
15 ORGANIZATION "AgentX Working Group"
16 CONTACT-INFO "WG-email: agentx@dorothy.bmc.com
17 Subscribe: agentx-request@dorothy.bmc.com
18 WG-email Archive: ftp://ftp.peer.com/pub/agentx/archives
```

- 2 Now that the Viewer has helped you identify the problems in the code, open a text editor and correct the code. The MIB files are located in `.. \Program Files\Ipswitch\WhatsUp\Data\Mibs`.
- 3 After you have made code changes, save the MIB file, then click **Reload** in the SNMP MIB Manager dialog.
- 4 Look for the MIB file, that you made changes to, in the list to determine 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 performance reports and other applicable workspace 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 workspace reports and split second graphs. If the device interface(s) already have performance monitors and/or active monitors set up, the new interface name displays in WhatsUp Gold accordingly.

Use the following example instructions for how to change a Cisco router interface name. If you have other devices, refer to the device documentation for instructions on how to change interface names.

To configure a device custom name for an SNMP interface on a Cisco router:

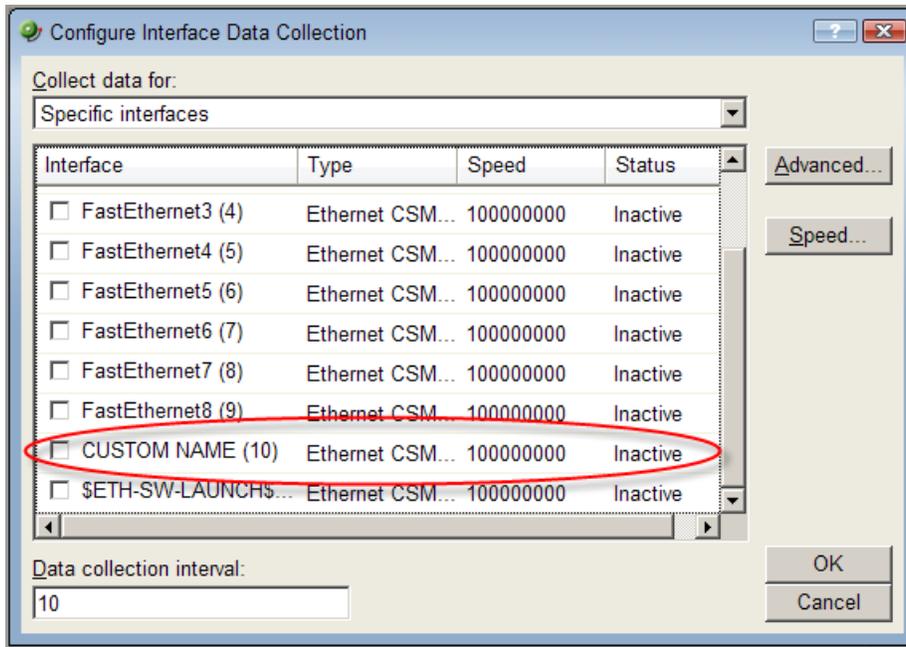
- Open the Cisco Command Line Interface (CLI) and enter the following commands:

```
Cisco1812# configure
Cisco1812(config)# interface FastEthernet 9
Cisco1812(config-if)# description CUSTOM NAME
Cisco1812(config-if)# ^Z
Cisco1812#
```

To add a Performance Monitor for a newly renamed device interface:

- 1 On the **Devices** tab, in **Device View** or **Map View**, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Performance Monitors dialog appears.

- 3 In the **Enable global performance monitors** section, click to select the **Interface Utilization** option, then click **Configure**. The Configure Interface Data Collection dialog appears.
- 4 In the **Collect data for** list, select **Specific Interfaces**. In this example, CUSTOM NAME is the interface name created for the Cisco router. Click to select **CUSTOM NAME**, then click **OK**.



- 5 Click **OK**, then click **Close** to close the Device Properties dialog.

To add an Active Monitor for a newly renamed device interface:

- 1 In the console application, 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 Active Monitors dialog appears.

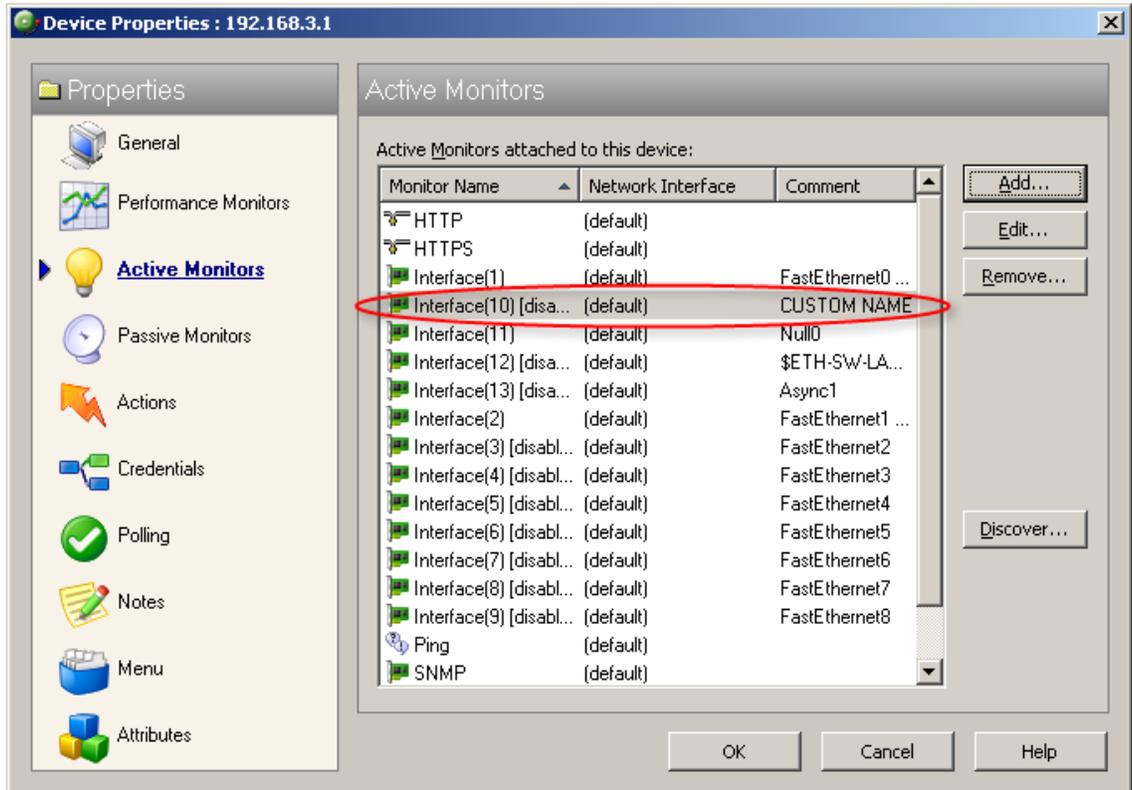


Important: If a device has active monitors set up prior to renaming the device's interface(s), then after renaming the device's interface(s), remove the old interface(s) from the Active Monitor dialog, then click **Discover** to refresh the device interface list. Use the console application for the discover process.

If a device has performance monitors set up prior to renaming the device's interface(s), the device interface names are automatically updated.

- 3 (Optional) If a device has active monitors set up for a device prior to renaming the device's interface(s), select the interface(s) that you renamed from the list of interfaces, then click **Remove**.

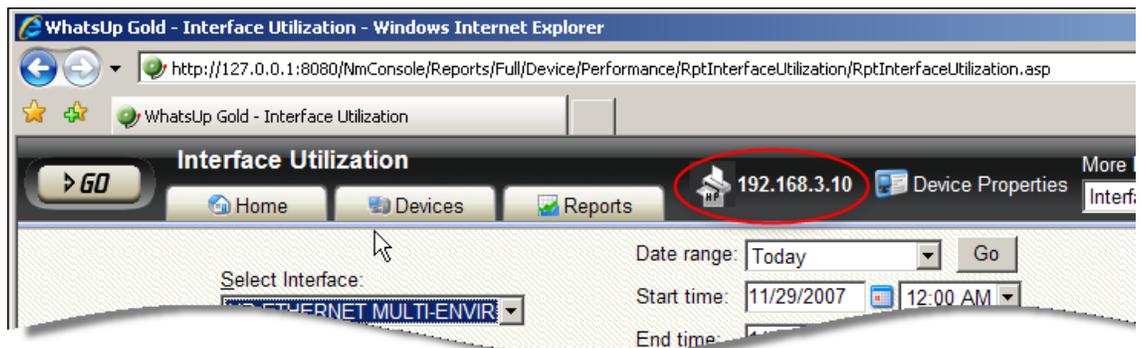
- (Optional) Click **Discover**. The interface list refreshes and populates with the new interface names in the Comment list.



- Click **OK**, then click **Close** to close the Device Properties dialog.

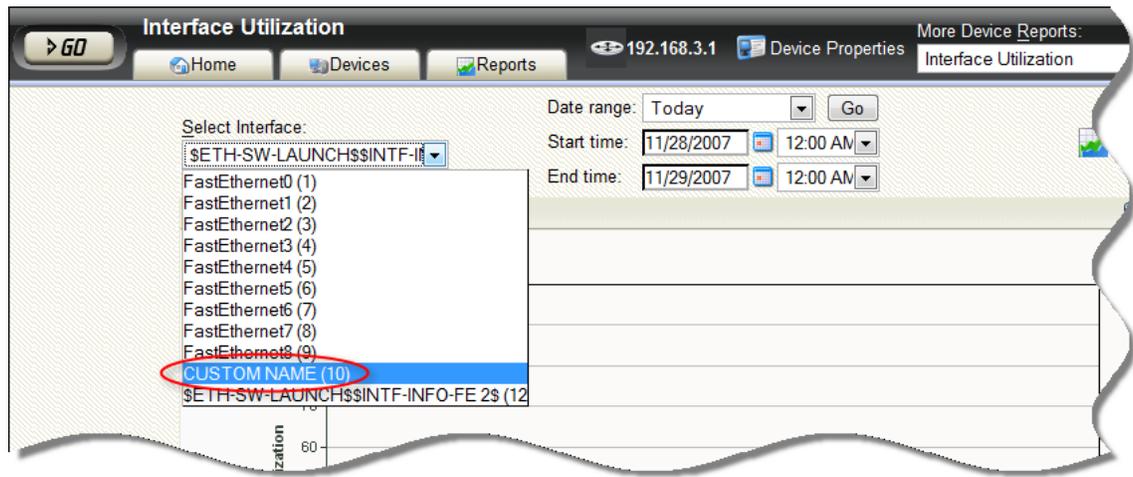
To select a newly renamed device interface for the Interface Utilization report:

- From the **WhatsUp** section of the **GO** menu, select **Reports > Performance**. The Performance Reports list appears.
- Under the Device category, click **Interface Utilization**. An Interface Utilization report appears.



- Click the device name/IP address (shown above) to select the device you want to view. The Select a Device dialog appears.
- Expand the network tree list to view the SNMPScan devices, then select the device for which you want to view the Interface Utilization report. The Interface Utilization report appears.

- 5 In the **Select Interface** list, select the newly named device interface. In this example, the interface is named CUSTOM NAME. View the interface utilization report.



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 (found on the web interface menu at **Go > 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 Field 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).

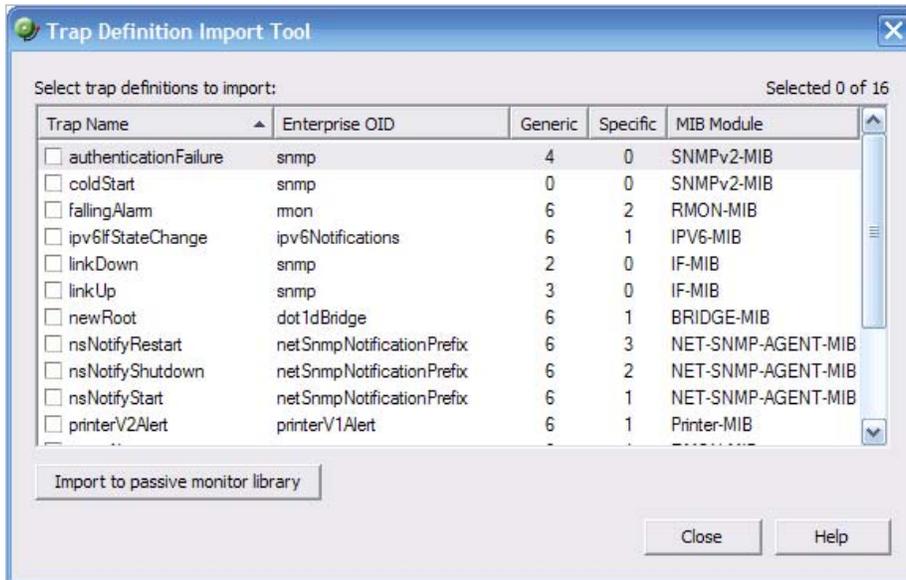
The SNMP Trap monitors that are listed are based on one of three things:

- **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 import SNMP trap definitions into the Passive Monitor Library:

- 1 In the WhatsUp Gold console, click **Tools > Trap Definition Import Tool**. The Trap Definition Import Tool dialog opens.



- 2 Click to select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog opens and provides a message about the import results. Traps that already exist in the database are not imported again.

Using Network Tools

In This Chapter

About Network Tools	315
Using the Ping tool	316
Using the Traceroute tool.....	317
Using the Lookup tool	318
Using the Telnet tool.....	319
Using the SNMP MIB Walker	319
Using the SNMP MIB Explorer	322
Using the MAC Address Tool.....	323
Using the Diagnostic Tool.....	325
Using the Web Performance Monitor	325
Using the Web Task Manager	328

About Network Tools

WhatsUp Gold includes several network tools. These troubleshooting tools allow you to take a closer look at the status of your network devices.

The following tools help you check the connectivity of networked devices:

- *Ping Tool* (on page 316)
- *Trace Route Tool* (on page 317)
- *Lookup Tool* (on page 318)
- *Telnet Tool* (on page 319)

The following tools help you identify information about MIB objects that network devices support:

- *SNMP MIB Walker Tool*
- *SNMP MIB File Explorer Tool* (on page 322)

The following tools help you identify problems with network devices so you can take corrective action to resolve issues:

- *MAC Address Tool* (on page 323)
- *Diagnostic Tool* (on page 325)

- *Web Performance Monitor* (on page 325)
- *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 GO menu.** To access the GO menu:
 - 1 From the web interface, select **GO**. The GO menu appears.
 - 2 On the **WhatsUp** section, select **Tools**. A list of all available tools appears.
- **Device List and Map View.** From either the Device List or Map View, right-click on a device and select **Tools**.
- **Device Toolbar Workspace Report.** To access network tools using the Device Toolbar workspace report:
 - 1 From either the Device List or Map View, double-click on a device. The device's Device Status workspace view appears.
 - 2 Locate the Device Toolbar workspace 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

This 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 appear in the bottom of the page after the request has been made.

- **RTT.** Round trip time; the amount of time it takes for the ping request to be returned from the remote device.
- **Destination.** The address specified in Address/Hostname.

- **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 in the following fields.
 - **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 is useful in finding out where on your network an 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 in the following fields.
 - **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 in the following fields.
 - **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:
 - **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.
 - **DNS.** 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.

- **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.
- 2 Click **Lookup** to run the tool.

Using the Telnet tool

Telnet is a simple service monitor that checks for a Telnet server on port 23. If no telnet service responds on this port, then the service is considered down.

To begin the service check, click the **Telnet** button. Refer to the Telnet application Help for more information.



Important: The Telnet protocol handler is disabled by default in Microsoft Internet Explorer 7. To re-enable it, see *Re-enabling the Telnet protocol handler* (on page 371).

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:

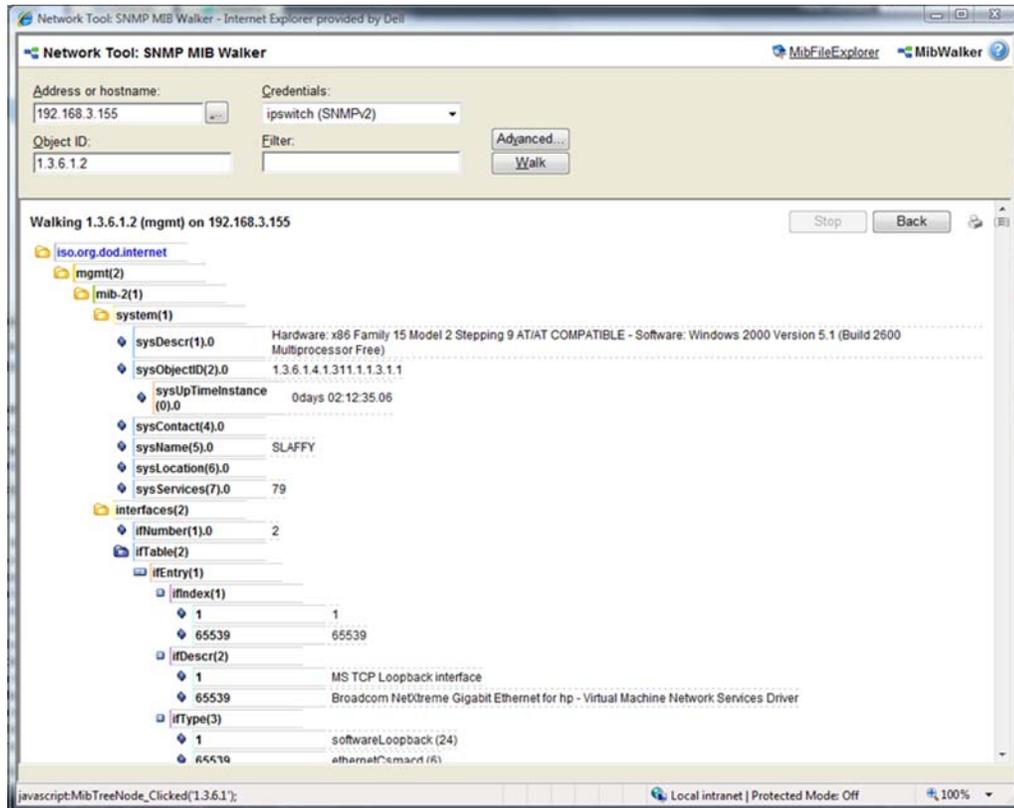
- 1 Enter or select the appropriate information in the following fields.
 - **Address or hostname.** Enter an IP address hostname for the device.
 - **Credentials.** Select the appropriate credentials for the device from the list. For more information, see *Using Credentials* (on page 103).
 - **Object 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*.

Using WhatsUp Gold v12

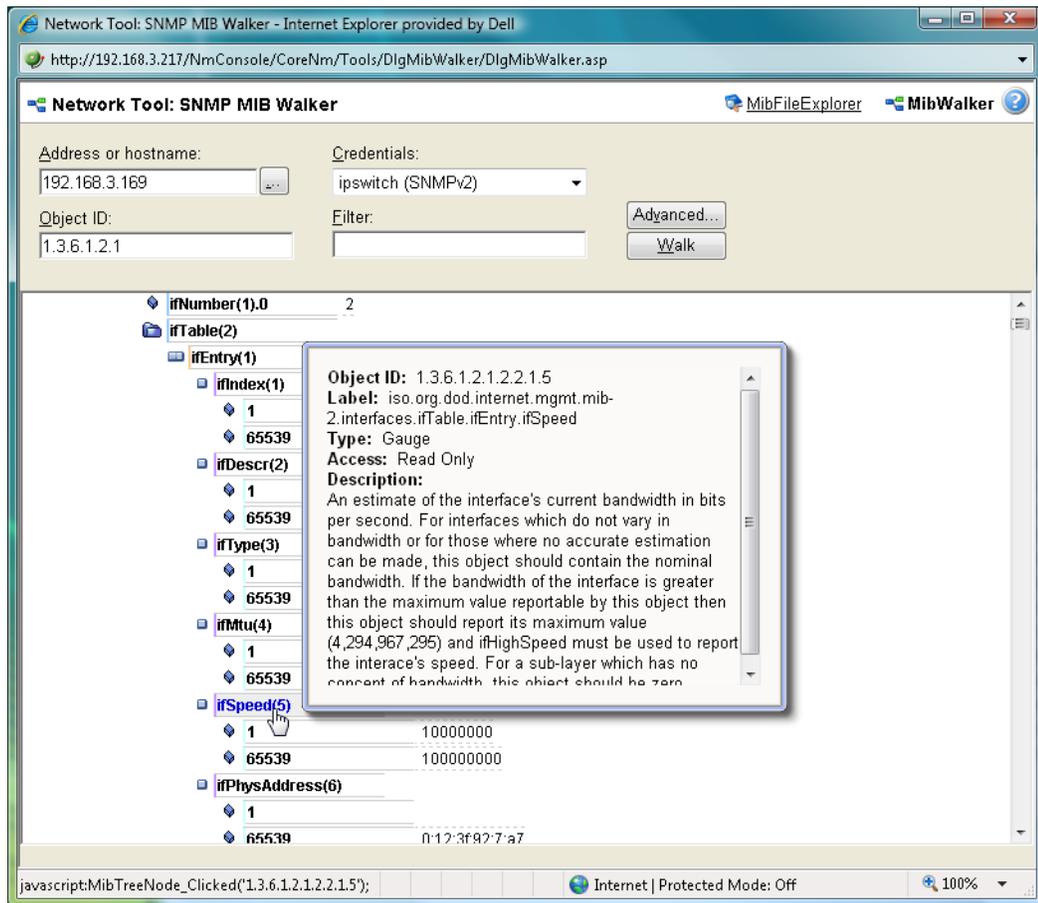
- Click the **Advanced** button to change the value for the search timeout and retries, output types (tree, list-numeric OIDs, list-labels), and the maximum number of lines displayed.
- 2 After you have entered all of the information, click **Walk** to perform the search. The SNMP MIB Walker returns a list of SNMP objects that are available on the selected device.



To cease 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 *Adding Custom Performance Monitors to Devices* (on page 218).

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 further to the left, the digits further to the right 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.

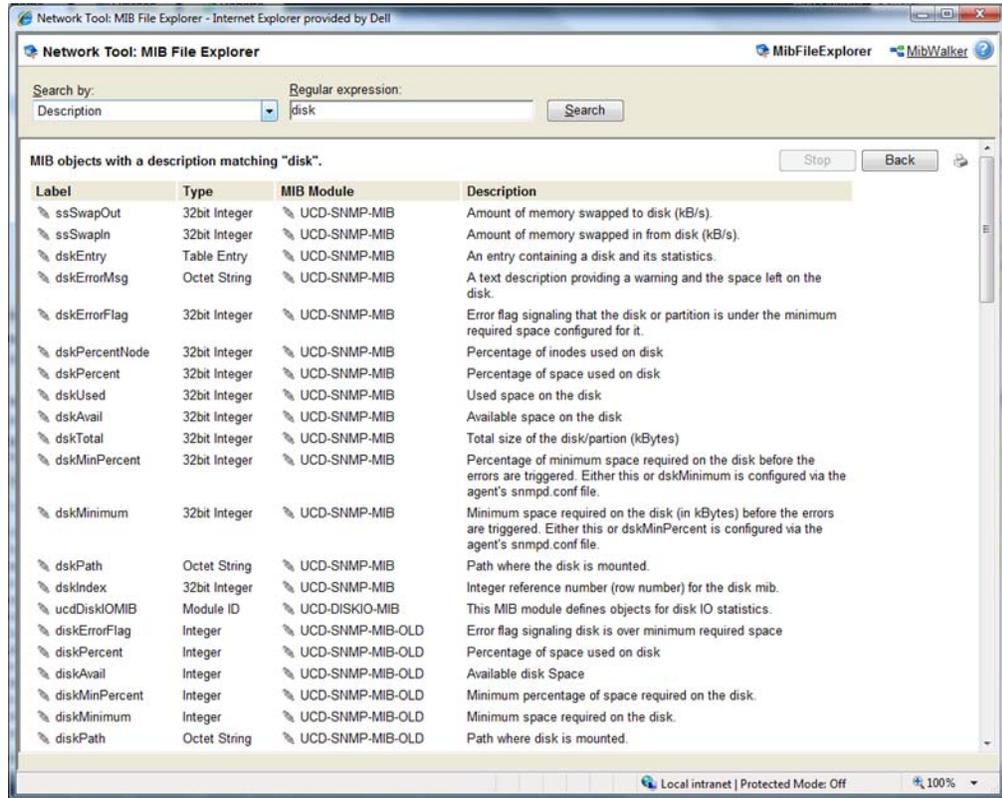
To search by object ID:

- Enter an object label or object ID in the **Object ID** field, 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** field. This is a regular expression, non-case-sensitive filter. For more information, see *Regular Expression Syntax* (on page 170). After entering the description in the field, 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 *Adding custom performance monitors to devices* (on page 218).



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 in the following fields.
 - **Local subnet.** Enter the subnet on which you would like to find MAC addresses.
 - **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 Diagnostic Tool

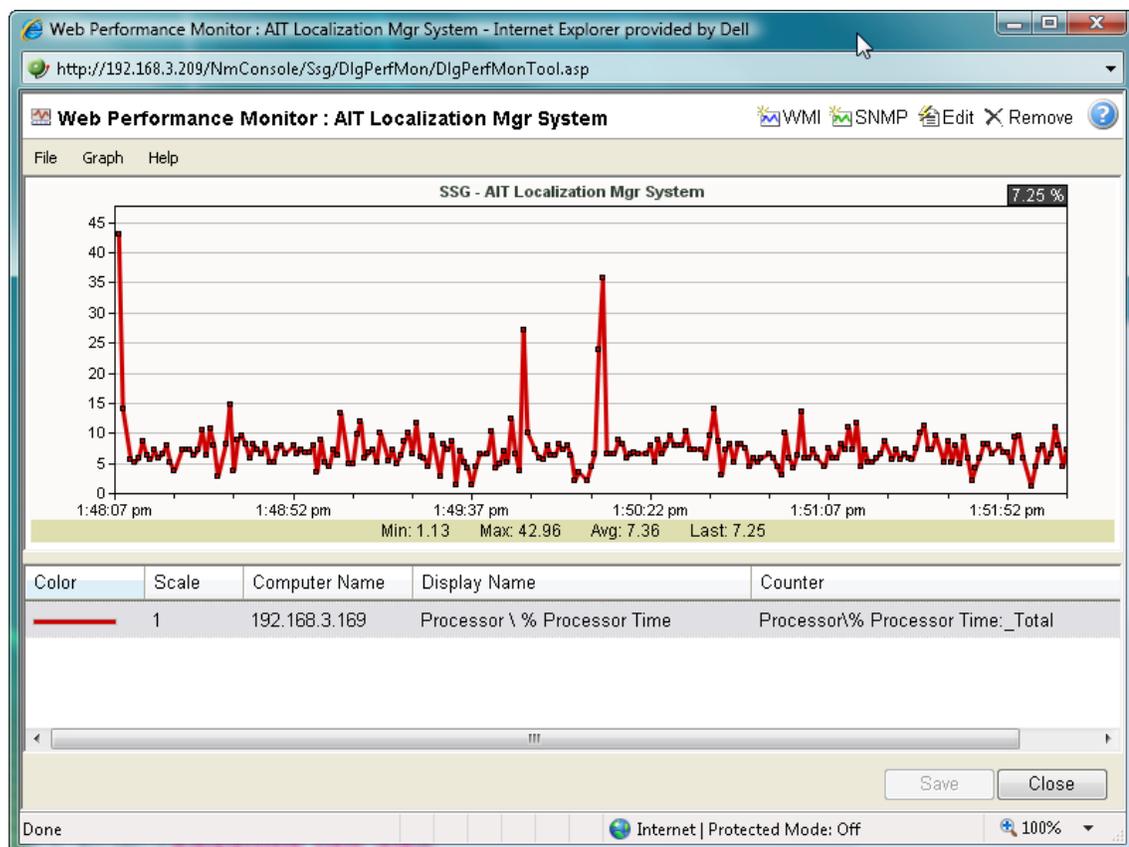
This tool diagnoses problems within your database by running a diagnostic scan.

To use the Diagnostic Tool:

- 1 To begin the scan, click the **Diagnostic** button.
- 2 After you have looked over and noted any problems, click **Close**.
- 3 To print the report, click the printer icon in the upper right corner of the window. If the tool finds any problems, instructions on how to resolve the problems appear onscreen.

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 workspace views using the Split Second Graph - Performance Monitor workspace 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 workspace report. You can use this workspace report to display any saved graph.

To add a WMI performance counter to the Web Performance Monitor:

- 1 Open the Web Performance Monitor.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Tools > Web Performance Monitor**. The Web Performance Monitor appears.

- 2 Click **Graph > Add WMI Performance Monitor**.

- or -

Click the WMI button in the top-right side of the dialog (see the Toolbar buttons table below). The Add WMI Performance Counter dialog appears.

- 3 Enter the appropriate information into the dialog fields.
- 4 Click **OK** to save changes.

To add a SNMP performance counter to the Web Performance Monitor:

- 1 Open the Web Performance Monitor.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Tools > Web Performance Monitor**. The Web Performance Monitor appears.

- 2 Select **Graph > Add SNMP Performance Monitor**.

- or -

Click the SNMP button in the top-right side of the dialog (see the Toolbar buttons table below).

The Add SNMP Performance Counter dialog appears.

- 3 Enter the appropriate information into the dialog fields.
- 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

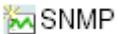
- **Graph > Add WMI Performance Counter.** This launches the Add WMI Performance Counter dialog.
- **Graph > Add SNMP Performance Counter.** This launches the Add SNMP Performance Counter dialog.
- **Graph > Edit Selected Counter.** This launches the appropriate dialog for editing the selected WMI or 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.

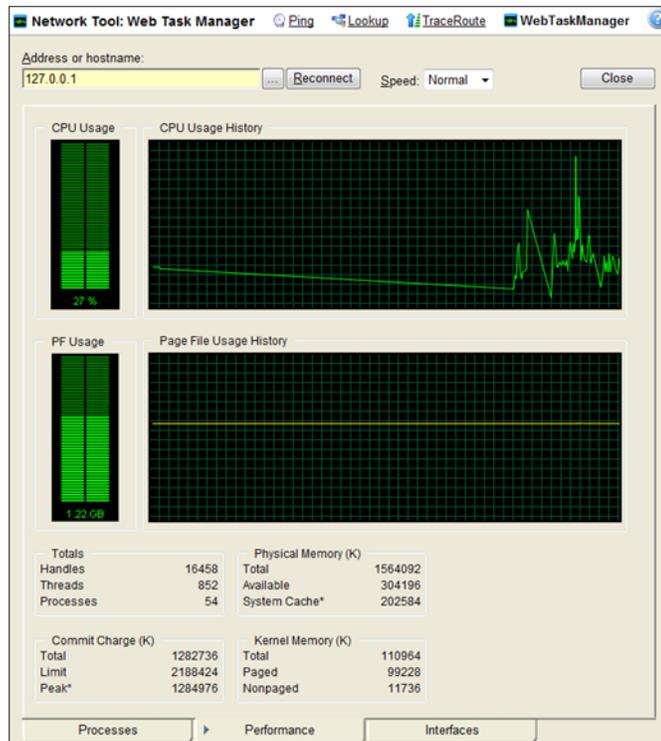
Button	Function
 WMI	Opens the Add WMI Performance Counter dialog.
 SNMP	Opens the Add SNMP Performance Counter dialog.
 Edit	Opens the appropriate dialog for editing the selected WMI or SNMP performance counter.
 Remove	Removes the selected graph item from the list and graph.
	Opens the help topic for the Web Performance Monitor

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 370).

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.** 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.** 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.** 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 learn about how much data is transmitted and received via each interface.



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 Open the Web Task Manager.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Tools > Web Task Manager**. The Web Task Manager appears.
- 2 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 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.

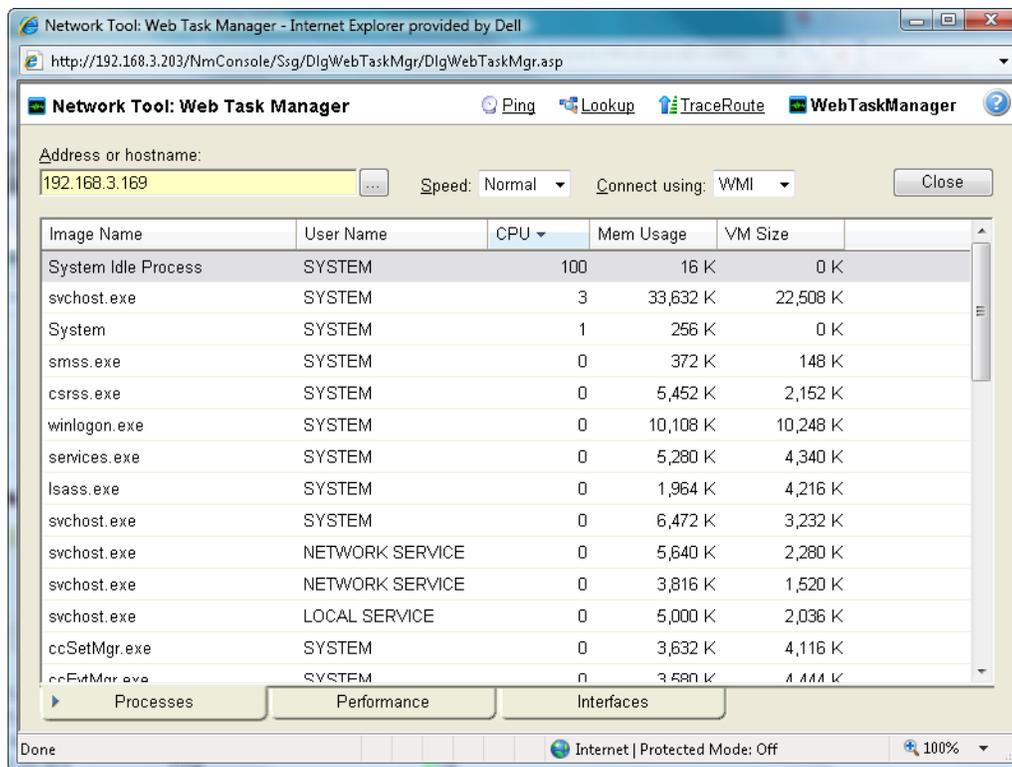
- 3 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).
- 4 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 370).

Using the Web Task Manager - Process tab

The 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 to view the processes running on WMI- or SNMP-enabled network devices.



Note: Microsoft Windows Server 2003 reports the **VM Size** column information in Kilobytes instead of Bytes. This is a known issue to be corrected in a future WhatsUp Gold release.



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 Open the Web Task Manager.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Tools > Web Task Manager**. The Web Task Manager appears.
- 2 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 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.

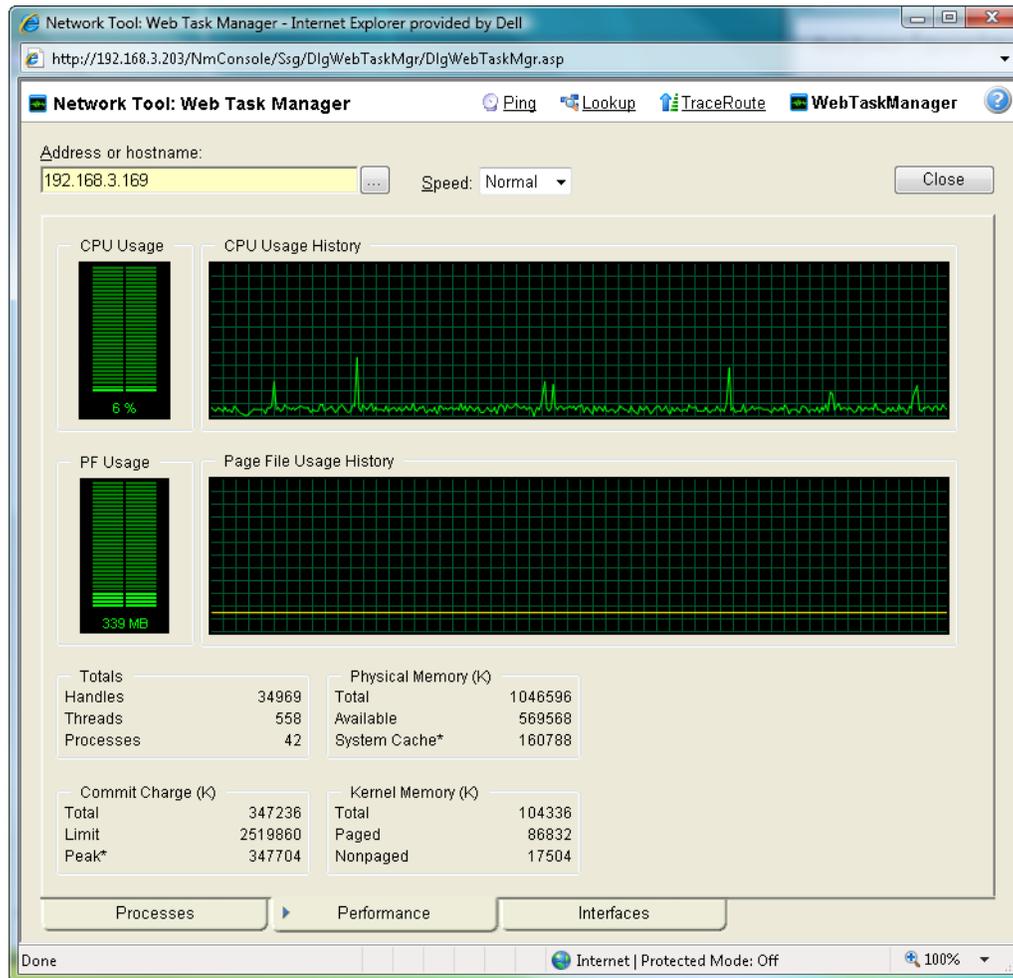
- 3** At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).
- 4** For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 370).



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 Open the Web Task Manager.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Tools > Web Task Manager**. The Web Task Manager appears.
- 2 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 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.

- 3 At the bottom of the Task Manager page, select the tab that you want to use (**Processes, Performance, or Interfaces**).
- 4 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 370).

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.

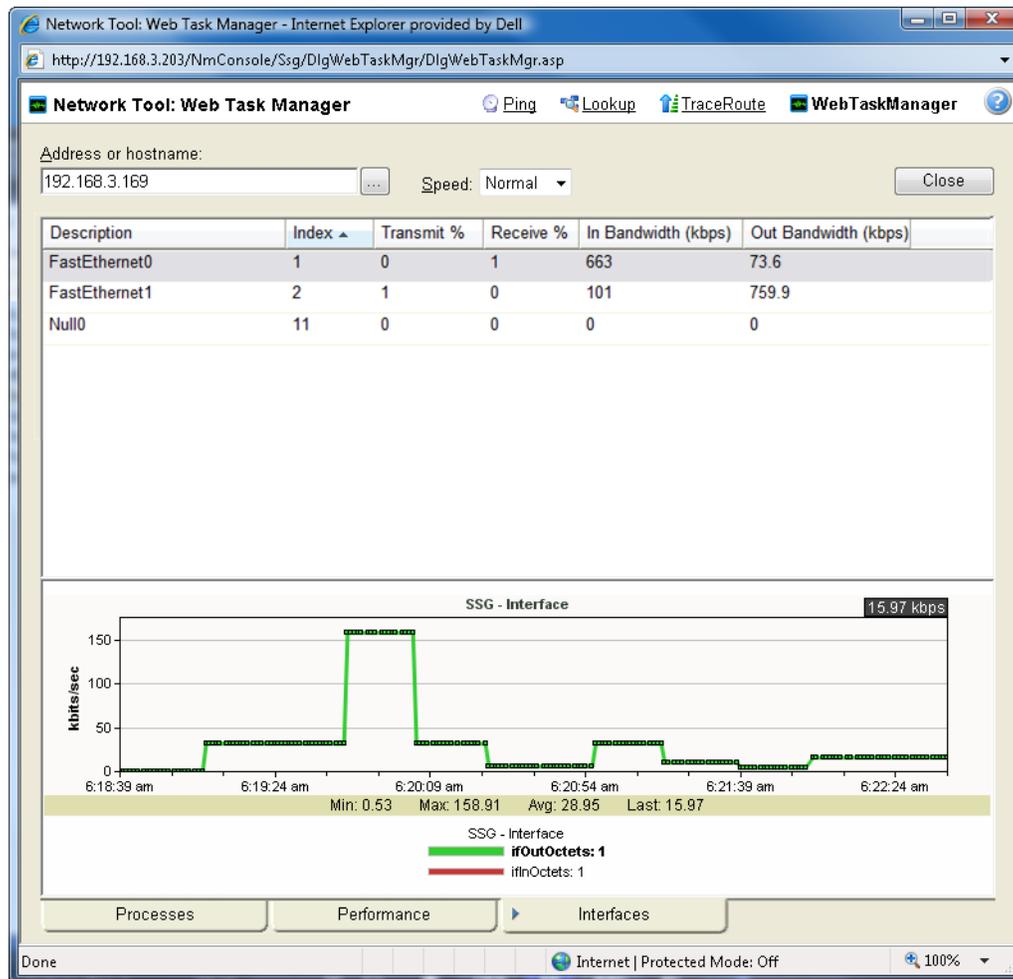
The following information are examples of the information that is provided when you connect to and view a SNMP enabled device. Note, this information varies by operating system:

- **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 370).

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 Open the Web Task Manager.
 - From the web interface, click **GO**. The GO menu appears.
 - On the **WhatsUp** section, select **Tools > Web Task Manager**. The Web Task Manager appears.
- 2 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 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.

- 3 At the bottom of the Task Manager page, select the tab that you want to use (**Processes, Performance, or Interfaces**).
- 4 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 370).

Using WhatsUp Gold Distributed and MSP Editions

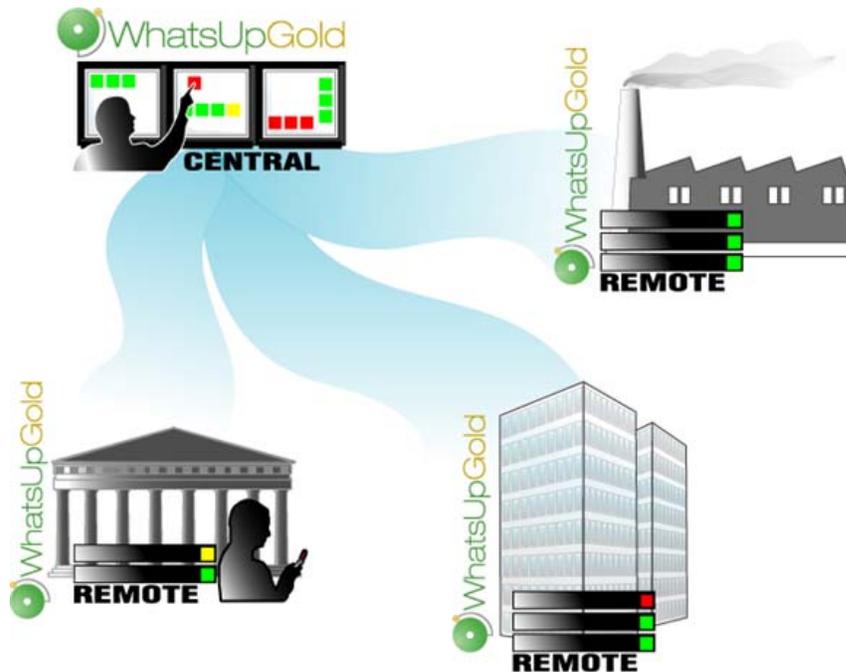
In This Chapter

About the WhatsUp Gold Distributed and MSP Edition.....	337
Installing Central and Remote Sites.....	338

About the WhatsUp Gold Distributed and MSP Edition

The WhatsUp Gold Distributed and MSP Edition extends the capabilities of a single WhatsUp product to let you monitor multiple remote networks (sites) from a central location. This solution includes a WhatsUp Gold Central installation and a WhatsUp Gold Remote installation.

The WhatsUp Gold Central Site installation coordinates data feeds from multiple WhatsUp Remote Site installations. The network data can then be viewed in reports that you select and customize on the Central Site. The Central and Remote installations, together, provide high visibility to the networks from one central location.



About the Distributed and MSP Edition reporting capabilities

The WhatsUp Gold Distributed and MSP Edition lets you set up and view reports associated with each monitored network. You set up centralized reports on the Central Site to gather key data from the Remote Sites. With the monitoring and reporting capabilities you can be confident that you will stay informed about the overall network health. In fact, if you lose the connection between the Central and Remote Sites, the information from the last network scan is still available on the Central Site. Each Remote Site continues to run an independent, full-featured version of WhatsUp, so it continues to gather network data, regardless of the connection status between the Remote and Central Sites.

All data communicated between the Central and Remote Sites is transferred over Secure Socket Layer (SSL) protocol to ensure that data is secure and confidential. The SSL communications between sites occur seamlessly, with no extra user setup required.

Installing Central and Remote Sites

Installation overview

The Ipswitch WhatsUp Gold Distributed and MSP Edition is comprised of the:

- **WhatsUp Gold Central Site** component installed on a network computer to collect data from and monitor all of the Remote Sites.
- **WhatsUp Gold Remote Site** component installed on a network computer at each remote location. Each remote site computer monitors the remote site network and reports the network status back to the Central Site.
- **Ipswitch Dashboard Screen Manager** application automatically installed with the WhatsUp Gold Central Site. After the Central and Remote Sites are set up, you can configure this application to cycle through a series of selected WhatsUp Gold web interface pages and other Web pages that you want to view on a regular basis. The Dashboard is ideal to set up across multiple monitors to view multiple networks or Remote Sites, increasing visibility to the information that is most important to you. For more information, see *Step 5: Using the Ipswitch Dashboard Screen Manager application* (on page 360).

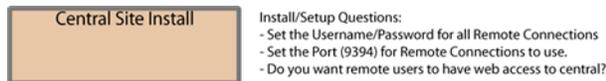
There are two installation programs for the Distributed and MSP Edition, one for the WhatsUp Gold Central Site and a second for the WhatsUp Gold Remote Site. The installation programs step you through the process of installing each part of the application.

Following are the overview steps required to install the Distributed and MSP Edition:

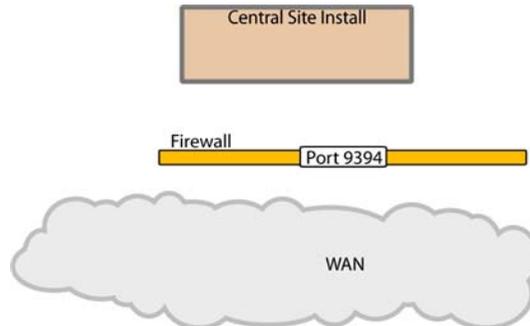
- 1 Install the Central Site application. For more information, see *Step 1: Installing the WhatsUp Gold Central Site* (on page 340).
 - (Recommended) Select whether to enable the WhatsUp Web server and select the Web server port.
 - Create a User Name and Password that the Remote Sites will use when connecting to the Central Site.

Using WhatsUp Gold v12

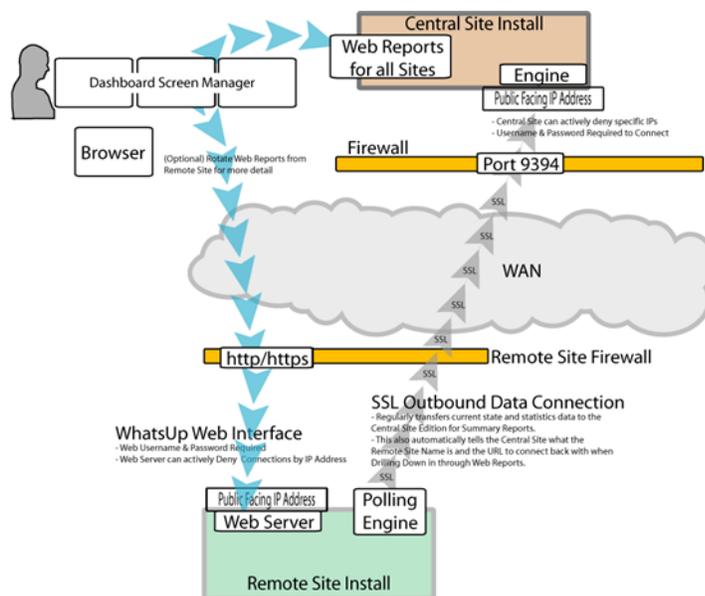
- Configure the TCP port that the Remote Sites will use to connect to the Central Site.



- Make sure the firewall ports are specified and open for the inbound connections (from the Remote Sites on Port 9394 TCP). For more information see, *Step 2: Configuring the firewall for Central and Remote Site connections* (on page 343).



- Install the Remote Site application at the remote locations. For more information, see *Step 3: Installing the WhatsUp Gold Remote Site* (on page 343).
 - Select whether to enable the WhatsUp Web server and select the Web server port.
 - Set up the Central Site IP Address and TCP Port that the Remote Site(s) will use to connect to the Central Site.
 - Set the User Name and Password that the Remote Site(s) will use to gain access to the Central Site.
 - Set up the Display Name for the Remote Site.
 - (Recommended) Enter the HTTP address that the Central Site will use to access this Remote Site's Web interface.
 - Run the network discovery to identify devices on the network and set up active and passive monitors.



- 4 Create Workspace Reports on the Central Site installation for each of the Remote Sites. For more information see, *Step 4: Using Reports for WhatsUp Gold Distributed and MSP Edition* (on page 346).
- 5 (Optional) Set up the Dashboard application on the Central Site. For more information, see *Step 5: Using the Ipswitch Dashboard Screen Manager application* (on page 360).

After the above steps are complete, the application is ready to monitor, and be further customized and expanded as required. Data will be communicated from the Remote Sites to the Central Site. The network data is rolled-up in the workspace reports and full reports that you set up. For more information, see *Step 4: Using Reports for WhatsUp Gold Distributed and MSP Edition* (on page 346). If you enabled access to the Remote Sites, you can drill-down from the Central Site reports to detailed historical data on the related Remote Site.

Step 1: Installing the WhatsUp Gold Central Site

The WhatsUp Gold Central Site serves as the monitoring system for important network activity data gathered by the Remote Sites. After the Remote and Central Sites are set up and reports are configured on the Central Site, the network status information from each Remote Site is communicated to the Central Site.

Following is the information that is configured during the Central Site installation:

- SQL Server 2005 Express (SSE) is installed on the Central Site computer.
- Select whether to enable the WhatsUp Web server and select the Web server port.
- Configure the TCP port that the Remote Sites will use to connect to the Central Site.
- Create a User Name and Password that the Remote Sites will use to gain access the Central Site.
- (Optional) Run the network discovery to identify devices on the network and set up Active and Passive Monitors.

To install the WhatsUp Gold Central Site:

The installation program is similar whether you are installing for the first time or upgrading from a previous WhatsUp installation. Steps that apply only to a first-time installation, or only to an upgrade, will be identified as such.

To install or upgrade the Distributed and MSP Edition:

- 1 Log in directly to Microsoft Windows using the Administrator account (or, if you do not have an account called Administrator, use an account that has full administrative privileges to the computer). Do not use Terminal Services or Remote Desktop to install WhatsUp Gold.



Note: When installing on Windows Vista, additional steps are necessary for the Task Tray application to work properly. For more information, see *Task Tray Application fails on Windows Vista* (on page 368).

- 2 Start the installation program:
 - If you purchased a WhatsUp Gold CD-ROM, insert the Central Site CD-ROM into the appropriate drive. If it does not run automatically, click **Start**, select **Run**, then enter the CD path followed by `AutoRun.exe`. For example: `D:\AutoRun.exe`
 - If you downloaded WhatsUp Gold from the WhatsUp Gold Web site, run the downloaded Central Site installation application.
- 3 Read the Welcome screen.

The Welcome screen recommends that you disable any running antivirus software, estimates how long it takes to install the application, and displays a button that, when clicked, displays the release notes.

Click **Next** to continue. The License Agreement dialog opens.
- 4 Read the license agreement. Select the appropriate option, then click **Next**.
- 5 **For first-time installation only:** Select the install directories for SQL Server 2005 Express Edition. The application and data files will be installed in default directories. If you want to change the locations, click the browse buttons to find and select a different directory.



Note: If you want to customize your database setup, you need to first complete the installation using Microsoft SQL Server 2005 Express. After installation completes, you can manually configure your database as described in *Using an alternative database setup* (on page 26).



Important: Make sure that you have a large capacity drive selected for data storage. Data files can grow up to 4 GB.

The application and data files will be installed in default directories. If you want to change the locations, click the browse buttons to find and select a different directory.

Click **Next**.



Note: The SQL Server 2005 Express Edition installation may take several minutes.

- 6 **For new installation only:** Select the installation directory for the WhatsUp Gold application files.

The default path is `C:\Program Files\Ipswitch\WhatsUp`. We recommend that you use the default path. Some users prefer to put application files on a partition separate from the operating system, which is usually installed on the C: drive, to isolate the application from an operating system crash.
- 7 **For upgrade installation only:** Choose whether to backup your current WhatsUp Gold database. We strongly suggest that you do this.

- 8 For upgrade installation only:** Choose how to handle existing Web and Report files.
If you have previously installed a version of WhatsUp, you may already have Web and Report files stored in your installation directory. You can choose to either delete them or back them up during the install.
- 9** If a sound card is installed and it has SAPI-compatible drivers, the install program asks whether you want to install Text to Speech capabilities. If you select **No**, you can always return and install Text to Speech at a later date.
- 10 For new install only:** Choose whether to enable the Web server during install and enter a port for this installation, then click **Next**. The default is Port 80.



Important: A Web server is required to view WhatsUp reports. If you do not enable a Web server during the installation, you need to enable the WhatsUp Web server or IIS Web server in order to view WhatsUp reports.



Note: This dialog will not be displayed during an upgrade if you have already enabled the WhatsUp Web server in a previous version of WhatsUp.

- 11** Enter the TCP port that the Remote Sites will use to connect to the Central Site (default port is 9394).
- 12** Enter a **User Name** and **Password** that the Remote Sites will use to access this Central Site, then click **Next**. The Ready to Install the Program dialog opens.



Note: Make note of this information. You will need the TCP port and User Name and Password information for each Remote Site installation.

- 13** Click **Install** to install the WhatsUp Gold application files. The installation program gives you the option to click **Back** and change options or click **Cancel** prior to completing the installation.



Important: When you use an alternative database setup, you will need to run the database upgrade scripts when installing a new release of WhatsUp Gold. The installation program will warn you if it detects a non-default database. For information on running the upgrade scripts, see *Upgrading the database schema* (on page 20).

- 14** Select whether you want to view the release notes and/or start the program, then click **Finish**.

After the application starts, you are introduced to the Discover Devices wizard, which lets you set options on how to discover your local network. If you want to postpone these steps, click **Cancel**. You can manually start the local Discover Devices wizard in the WhatsUp console application at a later time. Start the console application, then click **File > Discover Devices**.

Changing the Central Site configuration settings

The WhatsUp Gold Central Site installation program steps you through the configuration options for the Central Site. You can also update the configuration settings in the WhatsUp Console after installation.

To update the Central Site configuration:

- From the WhatsUp console, click **Configure > Program Options**, then click **Central Site Configuration**. For more information about the configuration settings, see the application Help.

Step 2: Configuring the firewall for Remote Site connections

Accessing the Central Site

The WhatsUp Gold Distributed and MSP Edition is designed to simplify firewall connections. Communications are outbound from each Remote Site back to the Central Site, so only one configuration is required for all Remote Sites to communicate back to the Central Site.

After you have set up the WhatsUp Gold Central Site, you need to determine what is required for the Remote Sites to connect across WANs, firewalls, routers, and other network security measures to communicate back to the Central Site. This information will be required as you install and configure each WhatsUp Gold Remote Site.

If you are not responsible for these network security configurations, contact the appropriate network administrator to help you identify the requirements to allow the connections in to the Central Site.

Accessing Remote Sites

Additionally, it is not required, but you can also configure the Remote Sites to be accessible via their Web interfaces. By doing so, users can drill-down from the Central Site to specific reports and data on a specific Remote Site. You can control access from the Central Site to the Remote Site by providing varying levels of user privileges to data on each Remote Site. For more information, see *Creating and modifying user accounts* (on page 70).

Step 3: Installing the WhatsUp Gold Remote Site

The WhatsUp Gold Remote Site monitors devices and network activity for each remote network site. After the Remote and Central Sites are set up and reports are configured on the Central Site, the network status information from each Remote Site is communicated to the Central Site.

Following is the information that is configured during the Remote Site installation:

- SQL Server 2005 Express (SSE) is installed on the Remote Site computer.
- Select whether to enable the WhatsUp Web server and select the Web server port.
- Set up the Central Site IP Address and TCP Port that the Remote Site(s) will use to connect to the Central Site.
- Set the User Name and Password that the Remote Site(s) will use to gain access the Central Site.
- Set up the Display Name for the Remote Site.
- (Recommended) Enter the HTTP address that the Central Site's browser will use to access this Remote Site's Web interface.

- Run the network discovery to identify devices on the network and set up Active and Passive Monitors.

To install the WhatsUp Gold Remote Site:

The installation program is similar whether you are installing for the first time or upgrading from a previous WhatsUp installation. Steps that apply only to a first-time installation, or only to an upgrade, will be identified as such.

To install or upgrade the Distributed and MSP Edition:

- 1 Log in directly to Microsoft Windows using the Administrator account (or, if you do not have an account called Administrator, use an account that has full administrative privileges to the computer). Do not use Terminal Services or Remote Desktop to install WhatsUp Gold.



Note: When installing on Windows Vista, additional steps are necessary for the Task Tray application to work properly. For more information, see *Task Tray Application fails on Windows Vista* (on page 368).

- 2 Start the installation program:
 - If you purchased a WhatsUp Gold CD-ROM, insert the Remote Site CD-ROM into the appropriate drive. If it does not run automatically, click **Start**, select **Run**, then enter the CD path followed by `AutoRun.exe`. For example: `D:\AutoRun.exe`
 - If you downloaded WhatsUp Gold from the WhatsUp Gold Web site, run the downloaded Remote Site installation application.
- 3 Read the Welcome screen.

The Welcome screen recommends that you disable any running antivirus software, estimates how long it takes to install the application, and displays a button that, when clicked, displays the release notes.

Click **Next** to continue. The License Agreement dialog opens.
- 4 Read the license agreement. Select the appropriate option, then click **Next**.
- 5 **For first-time installation only:** Select the install directories for SQL Server 2005 Express Edition. The application and data files will be installed in default directories. If you want to change the locations, click the browse buttons to find and select a different directory.



Note: If you want to customize your database setup, you need to first complete the installation using Microsoft SQL Server 2005 Express. After installation completes, you can manually configure your database as described in *Using an alternative database setup* (on page 26).



Important: Make sure that you have a large capacity drive selected for data storage. Data files can grow up to the 4 GB.

The application and data files will be installed in default directories. If you want to change the locations, click the browse buttons to find and select a different directory.

Click **Next**.



Note: The SQL Server 2005 Express Edition installation may take several minutes.

- 6 For new installation only:** Select the installation directory for the WhatsUp Gold application files.
The default path is C:\Program Files\Ipswitch\WhatsUp. We recommend that you use the default path. Some users prefer to put application files on a partition separate from the operating system, which is usually installed on the C: drive, to isolate the application from an operating system crash.
- 7 For upgrade installation only:** Choose whether to backup your current WhatsUp Gold database. We strongly suggest that you do this.
- 8 For upgrade installation only:** Choose how to handle existing Web and Report files.
If you have previously installed a version of WhatsUp, you may already have Web and Report files stored in your installation directory. You can choose to either delete them or back them up during the install.
- 9** If a sound card is installed and it has SAPI-compatible drivers, the install program asks whether you want to install Text to Speech capabilities. If you select **No**, you can always return and install Text to Speech at a later date.
- 10 For new install only:** Choose whether to enable the Web server during install and enter a port for this installation, then click **Next**.



Important: A Web server is required to view WhatsUp reports. If you do not enable a Web server during the installation, you need to enable the WhatsUp Web server or IIS Web server in order to view WhatsUp reports.



Note: This dialog will not be displayed during an upgrade if you have already enabled the WhatsUp Web server in a previous version of WhatsUp.

- 11** Enter the Central Site's **Address** <Central_Site_ip> (enter only the IP address without http://) and the **TCP Port** that the Central Site will use to listen for a connection from the Central Site (default port is 9394). After you have entered this information, you can click **Test** to test the connection to the Central Site.
- 12** Enter the **User Name** and **Password** that the Remote Site(s) will use to access this Central Site, then click **Next**. The Ready to Install the Program dialog opens.



Note: This is the User Name and Password that you set in the Central Site installation program.

- 13** Enter the Remote Site **Display Name**. This is the Remote Site name that the Central Site will use to identify this Remote Site (for example, Atlanta Office). The name will be particularly helpful to identify reports associated with each Remote Site. The default name is the computer name. Change it to better describe this Remote Site.
- 14** Enter the **HTTP Address** (recommended, but not required). This is the address that the Central Site's browser will use to access this Remote Site. This address allows users to

click links in the Central Site's Web interface to open browser connections directly to the Remote Site's Web interface (if the user has access permissions). Example:
`http://<Remote_Site_ip>:<Web server port>` or `http://192.168.200.123:8080`. Click **Next**.



Note: This IP address should be accessible in order to enable drill-downs into this Remote Site installation from the Central Site. If inbound Web connections are not possible, only status information will be available at the Central Site.

- 15** Click **Install** to install the WhatsUp Gold application files. The installation program gives you the option to click **Back** and change options or click **Cancel** prior to completing the installation.



Important: When you use an alternative database setup, you will need to run the database upgrade scripts when installing a new release of WhatsUp Gold. The installation program will warn you if it detects a non-default database. For information on running the upgrade scripts, see *Upgrading the database schema* (on page 20).

- 16** Select whether you want to view the release notes and/or start the program, then click **Finish**.

After the activation screen, you are introduced to the Discover Devices wizard, which lets you set options on how to discover your local network. Use this wizard if you plan to monitor the Central Site. If you only plan to use the Central Site to monitor Remote Sites, then you can click **Cancel**. If you want to postpone these steps, click **Cancel**. You can manually start the Discover Devices wizard in the WhatsUp console application at a later time. Start the console application, then click **File > Discover Devices**.

Changing the Remote Site configuration settings

The WhatsUp Gold Remote Site installation program steps you through the configuration options for the Remote Sites. You can also update the configuration settings in the WhatsUp Console.

To update the Remote Site configuration:

- 1** From the WhatsUp console, click **Configure > Program Options**.
- 2** Click **Remote Site Configuration**.

Step 4: Using Reports for WhatsUp Gold Distributed and MSP Edition

After the Central and Remote Site installations are complete and communicating with each other, you can determine the Remote Site reports to setup so you can view network health information for each site.

There are a number of new reports available for the WhatsUp Gold Distributed and MSP Edition. The two types of reports are:

- Workspace Reports
- Full Reports

Workspace Reports: learning about the Central/Remote Workspace Reports

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



The WhatsUp Gold Remote/Central workspace reports are similar to the workspace reports you may have used in other versions of WhatsUp Gold. The primary difference is the Remote/Central workspace reports let you set up workspace reports that watch Remote Site network status from your WhatsUp Gold Central Site. For more information, see *Learning about workspace reports* (on page 283).

Workspaces are designed to be user-specific, and are configurable to include workspace reports specific to users' needs. Workspaces contain multiple views that let you organize

various workspace reports by the type of information they display. When you begin customizing your workspace views, you should consider the types of information you need to view most often, the remote sites and devices in which you need to pay closest attention, and what level of detail you want to monitor through a particular workspace view.

There are several Central/Remote workspace reports included in a Remote Sites workspace view for the WhatsUp Gold Distributed and MSP Edition. They are available if you have completed a new installation of WhatsUp Gold application. If you are upgrading from a previous version of WhatsUp Gold, the Remote Sites reports are not added to the workspace view for existing users; however, you can create a new Workspace View and add the default Central/Remote workspace reports to it.

Following are the default Central/Remote workspace reports included in the Remote Sites workspace view:

Remote/Central Reports	Description
Remote Site List	Lists all configured Remote Sites. The report contains: Display Name Local device Last connect time Last refresh time
Device Status (Remote)	Provides a status summary of all monitored devices on a selected Remote Site. The report contains: Display name Devices up Devices down In maintenance Last refresh time
Monitor Status (Remote)	Provides a status summary of all monitors configured for the monitored devices on a Remote Site. The report contains: Display name Monitors up Monitors down Last refresh time
Remote Site Overview	Displays an information overview for a selected Remote Site. The report contains: Http address Last connect time Last refresh time # of devices # of monitors # of queries Display name Device type Host name Address

Summary Counts (Remote)	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
Tail of Action Activity Log (Remote)	Provides the tail (last 10 records) of the Action Log for a device group on a Remote Site. The report contains: Date Source Action Name Trigger
Tail of Remote Site Log	Provides the tail (last 10 records) of the Remote Site Log. The report contains: Date Type Message Remote Site
Active Monitor Status (Remote)	Lists all Active Monitors assigned to devices on the selected Remote Site
Threshold - Ping by Response Time Over 1 ms (Remote)	Displays ping response times by threshold for devices in a specific device group on a Remote Site. The report contains: Remote Site Last snapshot Device Interface Max (ms) Avg (ms)

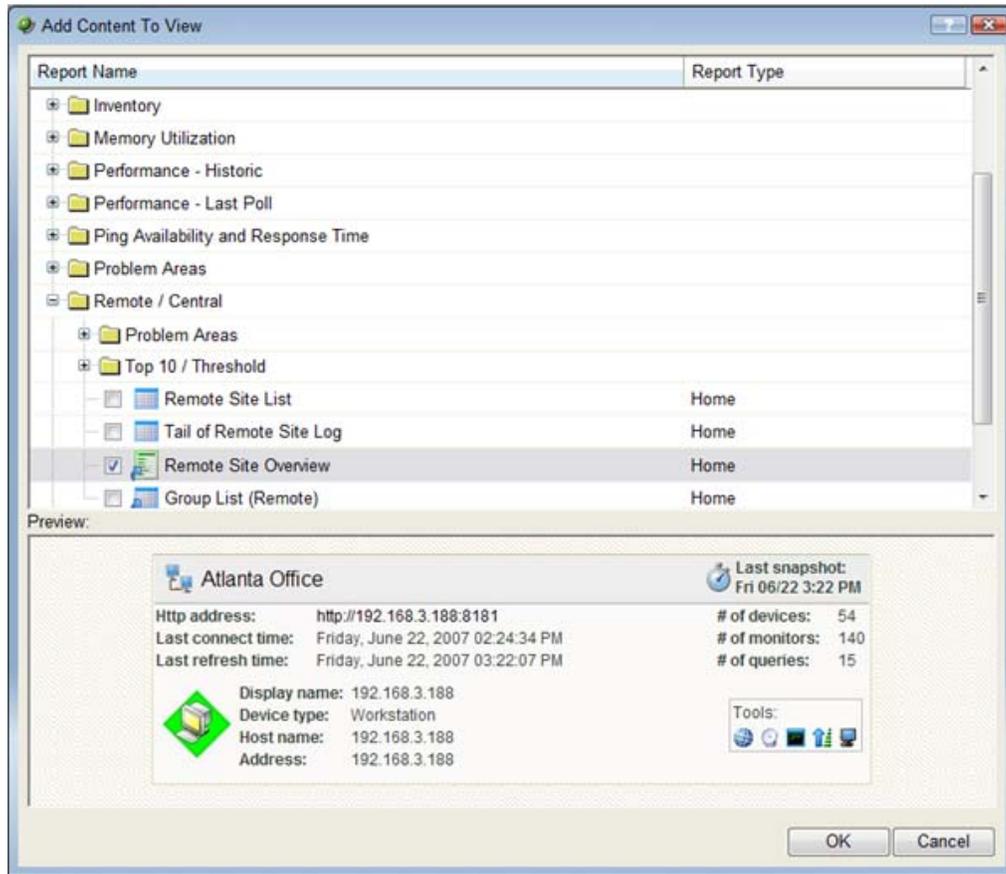
Adding Remote/Central workspace reports to your Home Workspace

You can add new Remote/Central workspace reports, including Top 10 reports, to the home workspace to customize workspace reports to best suit your needs. In the Workspace toolbar, click **Add Content**.



Using WhatsUp Gold v12

Use the Add Content To View dialog to add one or multiple Remote/Central workspace reports to a workspace.



Note: The Tail of Remote Site Log is the only workspace report only available from the Remote Site.

To add a workspace report:

- 1 Click the + button next to a report category folder, then click a report option box for each report you want to add to your workspace. A preview image for each workspace report is displayed at the bottom of the dialog.



Tip: The Central/Remote Reports shortcut icons   indicate that the report data originates from a Remote Site.

Using WhatsUp Gold v12

- 2 Click **OK** to save changes. The Home Workspace opens with the new workspace report added to the page. Also, notice the gray server icons when you first add a Remote Site workspace report. This indicates that you need to select a remote site for the workspace report.

Device	Status
192.168.3.72	Ping/Down at least 5 min)
JJ-Test	HTTP/Down at least 5 min)
QA/VistaUltmate	Ping/Down at least 5 min), HTTP/Down at least 5 min)

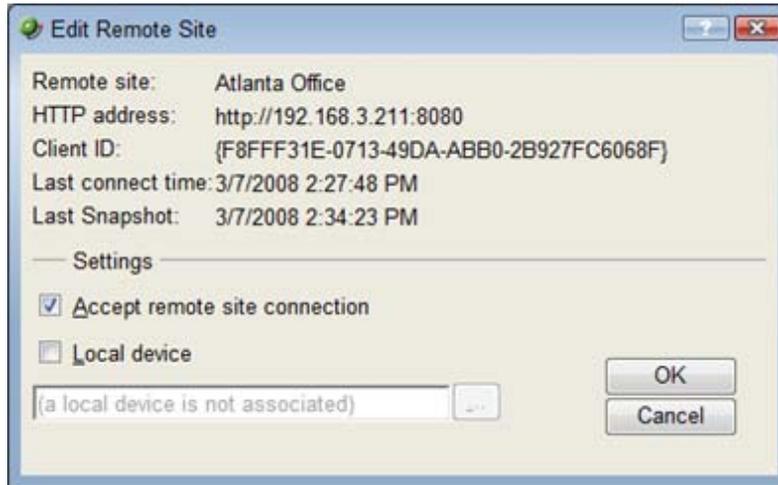
Device	Interface	Max (ms)	Avg (ms)
ATL-CINDYM	ATL-CINDYM (1...	166.0	56.0
ATL-WILLIAMS-2	ATL-WILLIAMS...	150.0	51.0
Sandbox-VistaB	Sandbox-VistaB...	74.0	33.0
192.168.3.5	192.168.3.5	40.0	32.0
192.168.3.10	192.168.3.10	41.0	29.0
ATL-JBENTON...	ATL-JBENTON...	14.0	4.0
192.168.3.2	192.168.3.2	8.0	4.0
ATL-WGREENB...	ATL-WGREENB...	8.0	3.0

- 3 In the new workspace report, click **Menu > Configure**.

The Configure Remote Report dialog opens.

- 4 Select the Remote Site you want to add to the Home Workspace, select other options available in the dialog (the options vary depending on the workspace report you selected), then click **OK**. The new workspace report displays in the Home Workspace. **(Additional options available only for the Remote Site Overview workspace report)**

- 5 After you select a Remote Site, the Local device box displays in the dialog. Click the Browse (...) button next to the Local device box. The Edit Remote Site dialog opens.

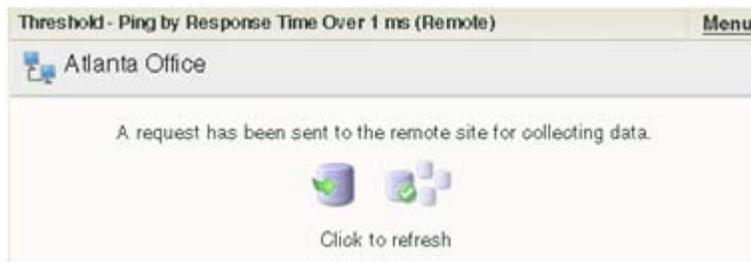


- 6 The **Accept remote site connection** option is selected by default. It allows users, with rights, the ability to select or deselect (from the Central Site) the option to accept connections from Remote Sites.

The primary reason to clear the check box option is if you need to disable the Central Site from accepting 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. You can use this option to disable the Central Site from accepting connections from this Remote Site until you resolve the problem.

Use the **Local device** checkbox to associate a device with the Remote Site. 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. Click the Browse (...) button, next to the Local device box, for a list of devices on the Remote Site. The Select a Device dialog opens.

- 7 Select a device that you want to associate with the Remote Site workspace report. This device will display in the workspace report. Click **OK**, then click **OK** to close the Edit Remote Site dialog. The Configure Remote Report dialog opens.
- 8 Click **OK** to save changes. The Home Workspace opens displaying the green collecting data icons. The icons indicate that the Remote Site has connected and is collecting data for the Central Site.



The Remote Site will update shortly or you can click the icons to force a refresh of the Remote Site data.

Using the Remote/Central workspace reports

While the Remote Site workspace reports work very much like workspace reports in WhatsUp Gold Standard and Premium Editions, there are a few items to note about the reports that help you identify them as Remote/Central workspace reports rather than local network workspace reports.

- The Remote Site workspace report header includes a network icon next to the Remote Site name to differentiate the Remote Sites from the local network devices (see 1).
- When you mouse over a Remote Site name, address, group name, status, etc., a shortcut icon  displays to indicate that you can click to drill through the information on the Remote Site (see 2). When you click the shortcut icon , a new web browser window opens for the selected Remote Site.



Important: Make sure that you select the option **Access Remote Reports** for each user that you want to provide access to the Remote Site reports. Also, make sure that you select the option **Configure Remote Sites** if you want a user to be able to access and change options in the Configure Remote Sites dialog (**Go > Configure > Configure Remote Sites**). For more information, see *Configuring user accounts* (on page 70).

- The Last snapshot information indicates the last date and time the Remote Site data was sent to the Central Site (see 3).
 - The date and time information turns blue if it has been longer than 5 minutes since the remote site last updated.
 - The date and time information turns red if it has been longer than 10 minutes since the remote site last updated.

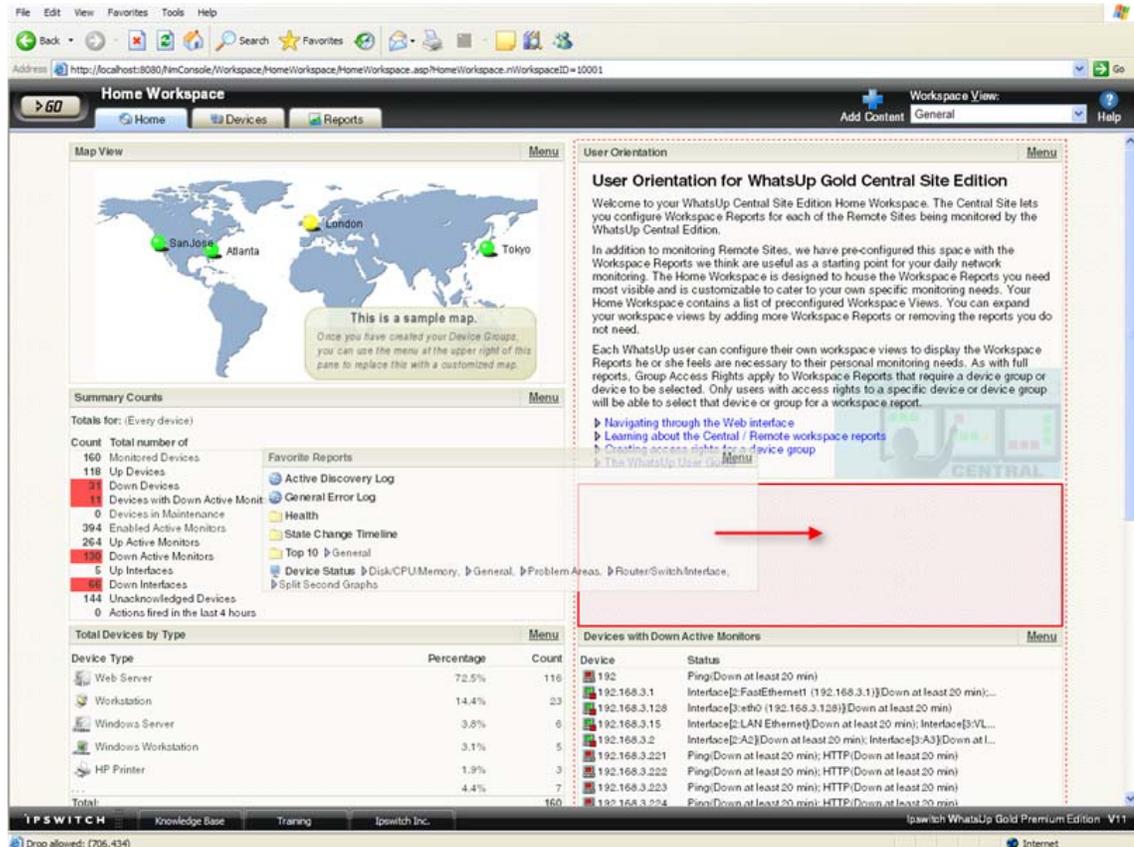
The screenshot displays the 'Home Workspace' interface with two panels: 'Atlanta Office' and 'Chicago Office'. Each panel shows 'Remote Site Overview' and 'Active Monitor States (Remote)'. Red circles 1, 2, and 3 highlight the network icon, the URL, and the 'Last snapshot' information respectively.

Remote Site	Http address	Last connect time	Last Snapshot	# of devices	# of monitors	# of queries
Atlanta Office	http://192.168.3.211:8080	Monday, March 10, 2008 09:24:55 AM	Monday, March 10, 2008 10:12:33 AM	131	521	14
Chicago Office	http://192.168.3.149:8088	Friday, March 07, 2008 04:06:31 PM	Monday, March 10, 2008 10:12:30 AM	91	91	13

Remote Site	Monitor type	Monitor state
Atlanta Office	All active monitor types	Down
Atlanta Office	192.168.3.2	D5, H4
Atlanta Office	ATL103	HTTP, Ping, SNMP
Atlanta Office	ATL212	HTTP, Ping
Atlanta Office	ATL-JWILLIAMS-2	HTTP
Atlanta Office	ATL-MZHANG2	HTTP
Atlanta Office	ATL-RKENNEDY.ipswitch_m.ipswitch.com	HTTP, Ping
Atlanta Office	ATL-TEST1	HTTP
Atlanta Office	ATL-WGREENBERG	HTTP
Atlanta Office	ATL-WGREENBERG	HTTP, Ping
Atlanta Office	ATL-WSANSBURY	Ping
Atlanta Office	CRAZYTES-KKTDJ0	Ping, SNMP
Atlanta Office	JJ-TEST	HTTP
Atlanta Office	MANDOR	WAN (PPP/SLIP) In...
Atlanta Office	QAVISTAULTIMATE	HTTP
Atlanta Office	SANDBOX-VISTAB	Ping, SNMP
Atlanta Office	VISTANUKER	HTTP, Ping, SNMP
Chicago Office	All active monitor types	Down
Chicago Office	192.168.3.115	Ping
Chicago Office	192.168.3.21	Ping
Chicago Office	192.168.3.250	Ping
Chicago Office	192.168.3.6	Ping
Chicago Office	2K-PROFESSIONAL	Ping
Chicago Office	2K-SERVER	Ping
Chicago Office	AJF	Ping
Chicago Office	ATL102	Ping
Chicago Office	ATL103	Ping
Chicago Office	ATL175	Ping
Chicago Office	ATL211	Ping
Chicago Office	ATLEXCH	Ping
Chicago Office	ATL-SAYTON-PC	Ping
Chicago Office	ATL-SKENWORTHY	Ping
Chicago Office	CRAZYTES-KKTDJ0	Ping
Chicago Office	GONZO	Ping

Moving and removing Remote/Central workspace reports

WhatsUp Gold supports drag-and-drop within the web interface. You can move a workspace report from one column of a workspace view to another, or position a workspace report above or below another workspace report, by selecting it and dragging it to another area of the workspace view. These location changes are saved: workspace reports will appear in the location to which you moved them after logging out from the web interface or after moving between workspace views.

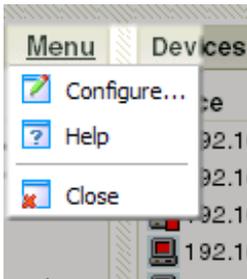


To move a workspace report:

- 1 Select the title bar of the report you want to move, then drag it to the desired location. A red box highlights the area that the report will be placed when the mouse button is released.
- 2 Release the mouse button to place the report in the new page location. If you want to cancel the move, while the report is selected, press the Esc key on your keyboard.

To remove a report:

In the Web interface, go to the menu for a specific workspace report and click **Close**.

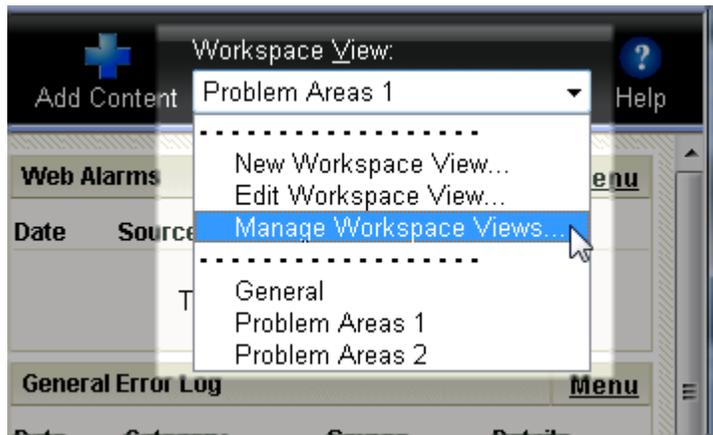


Keep in mind, when you remove a report, any customizations you have made to it are lost.

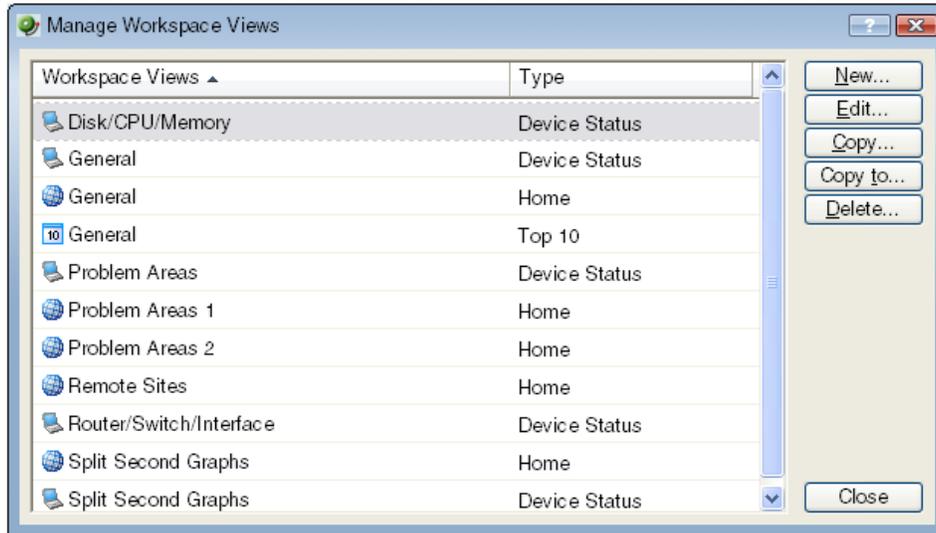
Managing Workspace Views

WhatsUp Gold comes with a few pre-configured workspace "views," including one for Default Remote Sites. You can create more of your own workspace views to use along with the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting. You can also edit, copy, copy to (another user), and delete these views as needed.

From the **Workspace View** list, select **Manage Workspace Views**.



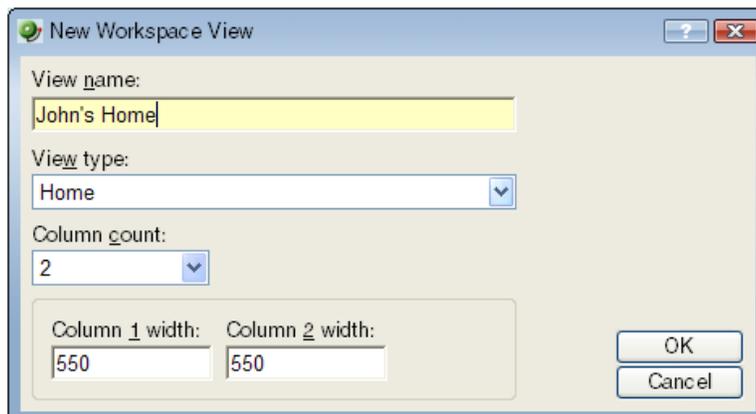
In the Manage Workspace Views dialog, you can create new workspace views, and edit, copy, or delete an existing workspace view.



- Click **New** to configure a new workspace.
- Select an existing workspace view and click **Edit** to change the current configuration of a workspace.
- Double-click an existing workspace to change its configuration.
- Select a workspace view, then click **Copy** to make a copy of that workspace and add it to the list.
- Select a workspace view, then click **Copy to** to copy an existing workspace from here to another user's list of workspaces.
- Select a workspace monitor view, then click **Delete** to remove it from the list.

To create a new workspace view:

- 1 From the Manage Workspace Views dialog, select **New**. The New Workspace View dialog appears.



- 2 Enter the appropriate information in the following fields:
 - **View name.** Enter a name for the workspace view.
 - **View type.** Choose a type for the workspace view from the drop-down menu.

- **Column count.** Enter a value for the number of columns you wish to have in the new workspace view. Keep in mind, the more columns you include, the smaller the data displayed inside a workspace.
 - Enter a value in pixels for each of the workspace columns.
- 3 Click **OK** to save changes.

To edit a workspace view:

- 1 From the Manage Workspace Views dialog, select **Edit**. The Edit Workspace View dialog appears.
- 2 Enter the appropriate information in the following fields:
 - **Workspace name.** The workspace title as it appears in the Workspace Library.
 - **Workspace type.** The workspace type as it appears in the Workspace Library (Home or Device).

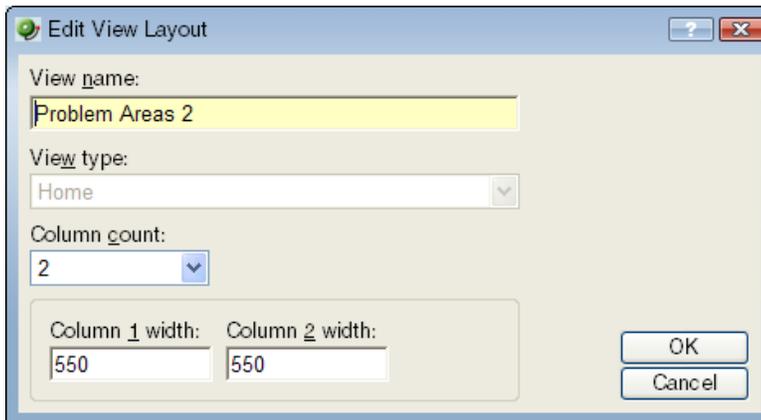


Note: Workspace view types cannot be changed after a view is created. For example, a Home workspace type cannot be changed later to a Device Status workspace type.

- **Column count.** The number of columns in the workspace.
 - **Column width.** The width of each column in the workspace in pixels.
- 3 Click **OK** to save changes.

To copy an existing workspace view:

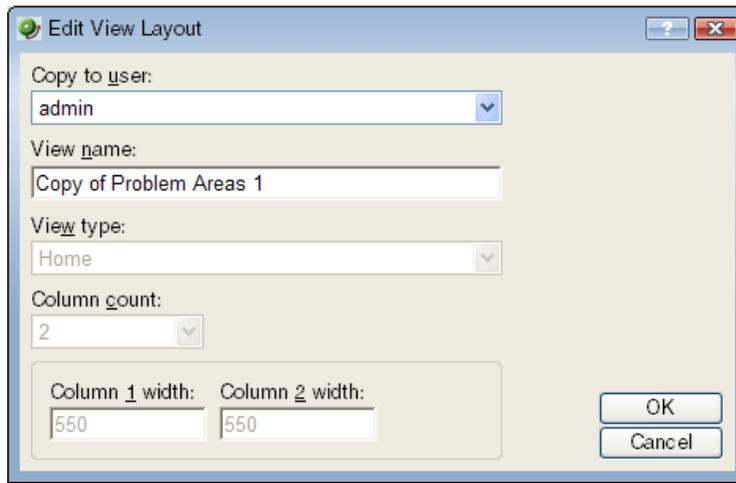
- 1 From the Manage Workspace Views dialog, select **Copy**. The Edit Workspace View dialog appears.



- 2 Enter the appropriate information in the following fields:
 - **Workspace name.** The workspace title as it appears in the Workspace Library.
 - **Column count.** The number of columns in the workspace.
 - **Column width.** The width of each column in the workspace in pixels.
- 3 Click **OK** to save changes.

To copy a workspace view to another WhatsUp Gold user:

- 1 From the From the Manage Workspace Views dialog, select **Copy to**. The Edit Workspace View dialog appears.



The screenshot shows the 'Edit View Layout' dialog box. The 'Copy to user:' field is set to 'admin'. The 'View name:' field contains 'Copy of Problem Areas 1'. The 'View type:' field is set to 'Home'. The 'Column count:' field is set to '2'. The 'Column 1 width:' and 'Column 2 width:' fields are both set to '550'. The 'OK' and 'Cancel' buttons are visible at the bottom right.

- 2 Enter the appropriate information into the following fields:
 - **Copy to user.** Select a user account from the drop-down menu in which to copy the workspace view.
 - **View name.** The name of the workspace view as it will appear in the Workspace Library.
- 3 Click **OK** to save.

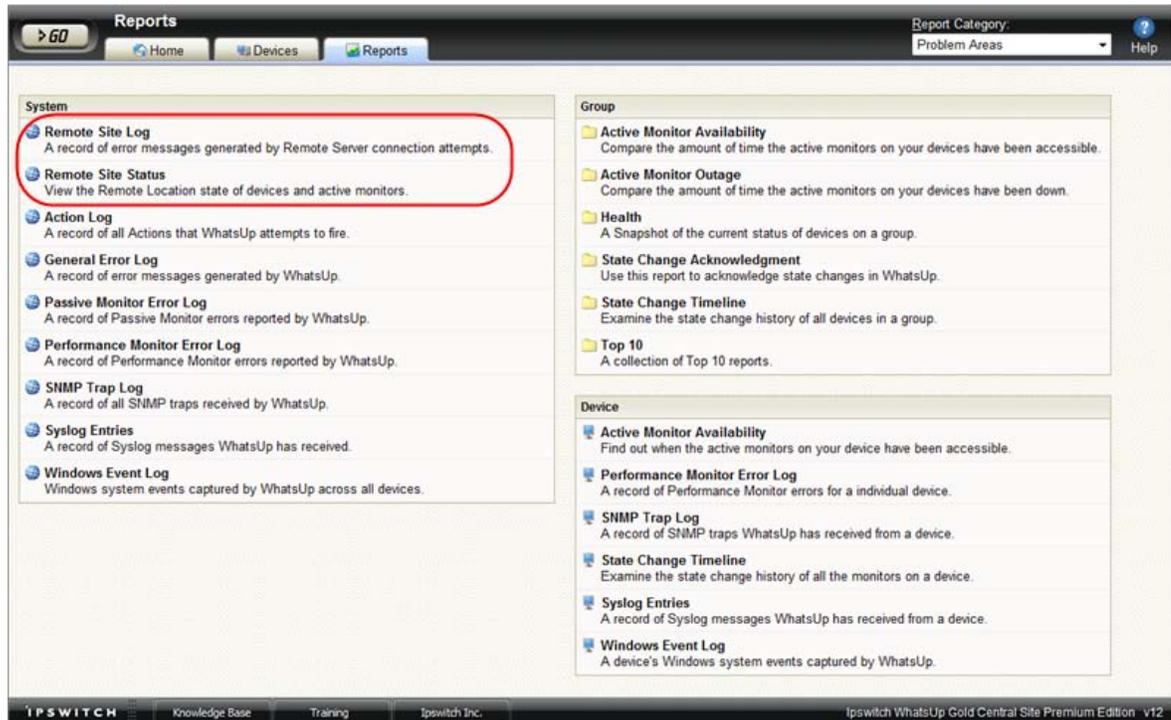
To delete a workspace view:

- 1 From the From the Manage Workspace Views dialog, click **Delete**.
- 2 Click **OK** on the dialog that follows.

Full Reports: learning about the Central/Remote Full Reports

The WhatsUp Gold Distributed and MSP Edition includes two full reports for Remote Sites, located on the Reports tab in the System category:

- Remote Site Log
- Remote Site Status



Advantages of full Reports

- Larger than the workspace reports, full reports give you a larger data view, which can be useful in pin-pointing the time something happened, or viewing multiple graphed items. Many workspace reports link to full reports, so that you can view this larger data view to troubleshoot.
- The date range on full reports can be zoomed in on, or zoomed out on, so that you can get a smaller or larger picture of what's going on with a particular aspect of the network.
- A list in the upper-right corner of a full report screen allows you to navigate to other reports in the same category. When you use this list to navigate to another report, the date range selected in the report you are navigating away from is transferred to any report you view subsequently.

Much of the data in full reports can be exported to Microsoft Excel or to a formatted text file.

Using the Remote Site full reports

The Remote Site Log provides a record of error messages generated by the Remote Site connection attempts.

The screenshot shows the 'Remote Site Log' interface. At the top, there are navigation buttons for 'Home', 'Devices', and 'Reports'. A search bar contains 'Remote Site Log'. Below this, there are filters for 'Date range: Last Week', 'Start time: 03/02/2008 12:00 AM', and 'End time: 03/09/2008 12:00 AM'. The main content is a table with the following data:

Date	Remote Site	Type	Message
Friday, March 07, 2008 04:10:15 PM	Atlanta Office	Information	Remote Host Disconnect: Socket read error
Friday, March 07, 2008 03:54:00 PM	[unknown]	Error	Authentication Failure (192.168.3.149): Login fail...
Friday, March 07, 2008 03:50:18 PM	[unknown]	Error	Authentication Failure (192.168.3.149): Login fail...
Friday, March 07, 2008 03:47:53 PM	[unknown]	Error	Authentication Failure (192.168.3.149): Login fail...
Friday, March 07, 2008 03:44:56 PM	[unknown]	Error	Authentication Failure (192.168.3.149): Login fail...
Friday, March 07, 2008 03:40:31 PM	[unknown]	Error	Authentication Failure (192.168.3.149): Login fail...
Friday, March 07, 2008 03:28:44 PM	[unknown]	Error	Authentication Failure (192.168.3.149): Login fail...
Friday, March 07, 2008 02:27:47 PM	Atlanta Office	Information	Remote Host Disconnect: An existing connectio...

Click a Remote Site name to open an instance of the Remote Site WhatsUp Gold Web interface. For more information about the Remote Site Log, see the application Help.

The Remote Site Status report provides overview information about the state of the devices and active monitors on the Remote Sites.

The screenshot shows the 'Remote Site Status' interface. It displays a summary table for 'March 10, 2008' with the following data:

Remote Site	Devices Up	Devices Down	Devices in Maintenance	Monitors Up	Monitors Down	Last Snapshot
Atlanta Office	115	8	0	370	26	Mon 03/10 10:00 AM
Chicago Office	62	29	0	62	29	Mon 03/10 9:59 AM

Click a number in one of the columns to drill-down to more detailed information about up and down devices and monitors and devices in maintenance.



Note: The Remote Site Status report is only available from the Central Site.

Step 5: Using the Ipswitch Dashboard Screen Manager application

After you have the Central and Remote Sites working, have customized your workspace reports and started viewing the Remote Site full reports, you can take advantage of the Ipswitch Dashboard Screen Manager capabilities. The Dashboard is installed on the Central Site by default. However, if you prefer to install the Dashboard on a system other than the Central site, you can locate the .exe installation file at `.. \Program Files\Ipswitch\WhatsUp\Dashboard.exe`.

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 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.



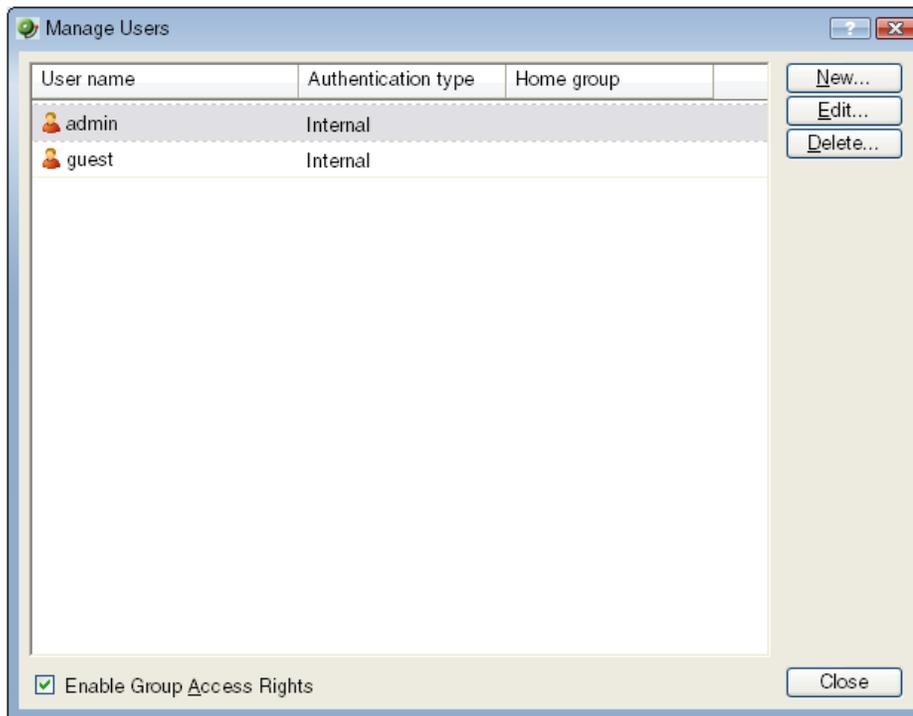
Note: If you want to display a password protected page for another Web application, you must supply a valid username and password for the page. For more information, see the Dashboard application Help.

For more information about installing and using the Dashboard Screen Manager, see *Using the Ipswitch Dashboard Screen Manager*, a document located on the *Ipswitch Network Monitoring Web site* (<http://www.whatsupgold.com/>).

To further enhance your network activity visibility, you may also want to set up a multi-monitor network display, for more information see *Setting up a WhatsUp Multi-Monitor Network Display*, a document located on the *Ipswitch Network Monitoring Web site* (<http://www.whatsupgold.com/>).

Creating and modifying user accounts

User accounts that are granted the **Manage User** right can create and edit user accounts.



To create a new or edit a WhatsUp Gold user account:

- 1 From the WhatsUp Gold web interface, select **GO**. The GO menu appears.
- 2 On the **WhatsUp** section of the **GO** menu, select **Configure > Manage Users**. The Manage Users dialog appears.

3 Click **New**. The Add User dialog appears.

- or -

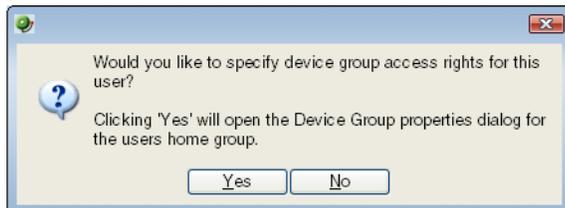
Select a user account and then click **Edit**. The Edit User dialog appears.

The screenshot shows the 'Add User' dialog box. The 'User name' field contains 'Mitch'. The 'Authentication type' is set to 'Internal' and the 'Language' is set to 'English'. The 'Internal password' and 'Confirm password' fields are masked with dots. The 'Home group' is set to 'My Network'. The 'User rights' section is expanded, showing a list of permissions with checkboxes. The 'General' section includes 'Change Your Password', 'Configure Workspaces', 'Manage IP Security', 'Manage Web Server', 'Translations', 'Manage Workspace Views', 'Manage Users', 'Configure LDAP Credentials', and 'Manage SNMP MIBs'. The 'Monitors / Actions' section includes 'Configure Active Monitors', 'Configure Performance Monitors', 'Configure Actions', 'Configure Passive Monitors', 'Configure Action Policies', and 'Manage Recurring Actions'. The 'Devices' section includes 'Manage Groups', 'Access Active Discovery Results', 'Manage Devices', and 'Configure Credentials'. The 'Reports' section includes 'Check all rights'. The 'OK' and 'Cancel' buttons are located at the bottom right of the dialog.

4 Enter the appropriate information.

- **User Name.** Enter the name of the user.
- **Authentication Type.** Select the method of authenticating the user.
 - **Internal.** Use the internal user database built in to WhatsUp Gold.
 - **LDAP.** Use an external LDAP database.
- **Language.** Select the language to display for the user.
- **Internal Password.** Enter a password for the user. This option is disabled if **Authentication Type** is set to LDAP.
- **Confirm Password.** Confirm the user's password. This option is disabled if **Authentication Type** is set to LDAP.
- **Home Group.** Select the device group that the user will see when they log into the WhatsUp Gold web interface. If they have the correct group access rights, they will be able to navigate out of this group.

- **User Rights.** Select the rights that correspond to the actions you want to allow the user to complete.
 - **Check all rights.** Select this option grant the user rights to perform all of the actions listed.
- 5 Click **OK** to save changes.
 - 6 If you have enabled Group Access Rights, you will be prompted if you would like to specify Group Access Rights for the new user account.



Select **Yes** to open the Device Group Properties dialog for the user's home group.

- or -

Select **No** to close the dialog and return to the Manage Users dialog.

Learning more about using the WhatsUp distributed solution

For additional information to help you get started using the WhatsUp Gold distributed solution, see *Using WhatsUp Gold to Gather and View Network Data* (on page 11).

Troubleshooting

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 Health Detail Report 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.

Database Performance Tool

The Database Performance Tool is used to monitor the size of your database, and to manage the index fragmentation percentage of the individual tables. Fragmented indexes can cause database operations to slow down considerably, in much the same way that disk fragmentation causes your computer to run slower.

Click **Check for fragmented tables** to begin. This may take a considerable amount of time (up to a few minutes), depending on how many records are in your database.

- **Select fragmented tables to optimize.** This list shows all database tables with greater than 10% index fragmentation, along with the total number of data rows in that table.
- **Optimize selected tables.** Select the tables in the list above to defragment those database tables. WhatsUp Gold automatically stops and restarts the WhatsUp Service. The status of the operation appears on the dialog, next to this button.
- **The current database size is.** This section of the dialog shows the total amount of space used by the database. If you are using SQL Server 2005 Express as the WhatsUp Gold database, this section also displays the percentage of the 4 GB file size limit currently in use.
- **Validate and compact database.** Click this button to execute commands that validate the database, index, and database links, and to compact the database. WhatsUp Gold automatically stops the WhatsUp Service 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.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp) on the Microsoft Web site..

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.

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, select **Remote Desktop**. If the connection is successful, the log in dialog opens. 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 restart the WhatsUp Gold engine:

- 1 Open the Windows **Control Panel**.
- 2 Select **Administrative Tools > Services**. The Services window appears.
- 3 Select **Ipswitch WhatsUp Engine**, 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 103). 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.msp#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 WMI monitors been reporting down services when in fact your services 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.

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. 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 WhatsUp Engine.

To restart the WhatsUp Engine:

- 1 Go to **Control Panel > Administrative Tools > Services**.
- 2 Select **Ipswitch WhatsUp Engine** from the list of services and select **Restart** from the left side of the dialog.

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 box opens.
- 2 In the Open box, enter: `Regedit`, then click **OK**. The Registry Editor opens.
- 3 Go to the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl

- 4 Under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl, create a new key named FEATURE_DISABLE_TELNET_PROTOCOL.
- 5 Add a DWORD value named iexplore.exe and set the value to 0 (decimal).
- 6 Close the Registry Editor and restart Microsoft Internet Explorer 7. 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. Due to this limitation, a payload may not show up in a trap or event log when expected, or actions that fire when no payload is present may cause WhatsUp Gold to send a blank email alert.

Restarting the WhatsUp Gold services from the command line

You can quickly restart the WhatsUp Gold polling engine and the Ipswitch Web Server using the NmServiceRestart.exe command line utility. This utility can be called directly from the command line or from batch scripts or scheduled tasks as part of your automated processes.

Usage

NmServiceRestart.exe [/s] [/p] [/w]

Parameter	Description
/s	Run in silent mode. When this option is included, the utility does not report any feedback.
/p	Restart the WhatsUp Gold polling engine only.
/w	Restart the Ipswitch Web Server only.



Note: If both /p and /w are specified, the utility restarts both services. If only one is specified, the utility restarts only the service that is specified.

Recommended SMS modems and troubleshooting tips

Ipswitch has tested and currently recommends the following SMS modems for use with the SMS Direct Action (not the SMS Action):

- *Motorola® RAZR V3* (<http://www.motorola.com>)
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/>), model: MTCBA-G-F2
- *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.
- *Falcom Samba 75* (<http://www.falcomusa.com>)

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.
- 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  
Plugins\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`

About the Dashboard Screen Manager

In This Chapter

Ipswitch Dashboard Screen Manager overview	375
How does the Dashboard Screen Manager work?	376
Installing the Dashboard Screen Manager	376
Configuring a Dashboard Screen Manager playlist	378

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 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 378).

For more information about configuring a multi-monitor network display, see *Setting up a WhatsUp Multi-Monitor Network Display*, located on the *WhatsUp Gold Web site* (<http://www.whatsupgold.com/>).

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 Select 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

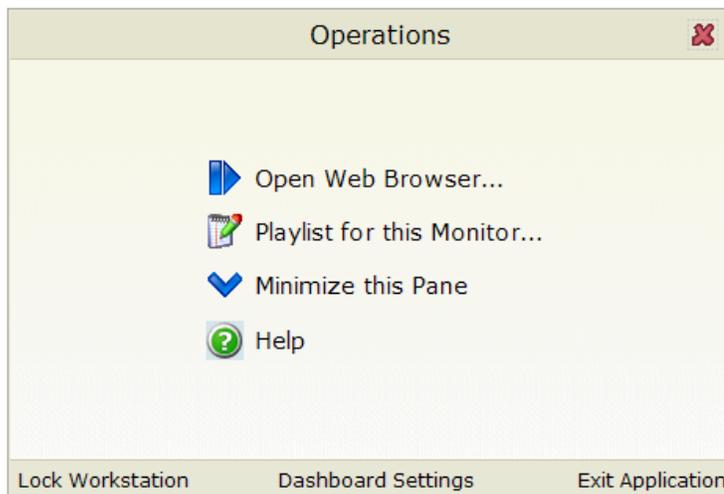
After successfully installing the Dashboard, you can access the application from your Windows Start Menu by selecting **Ipswitch Dashboard > Dashboard**.



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 378).



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.

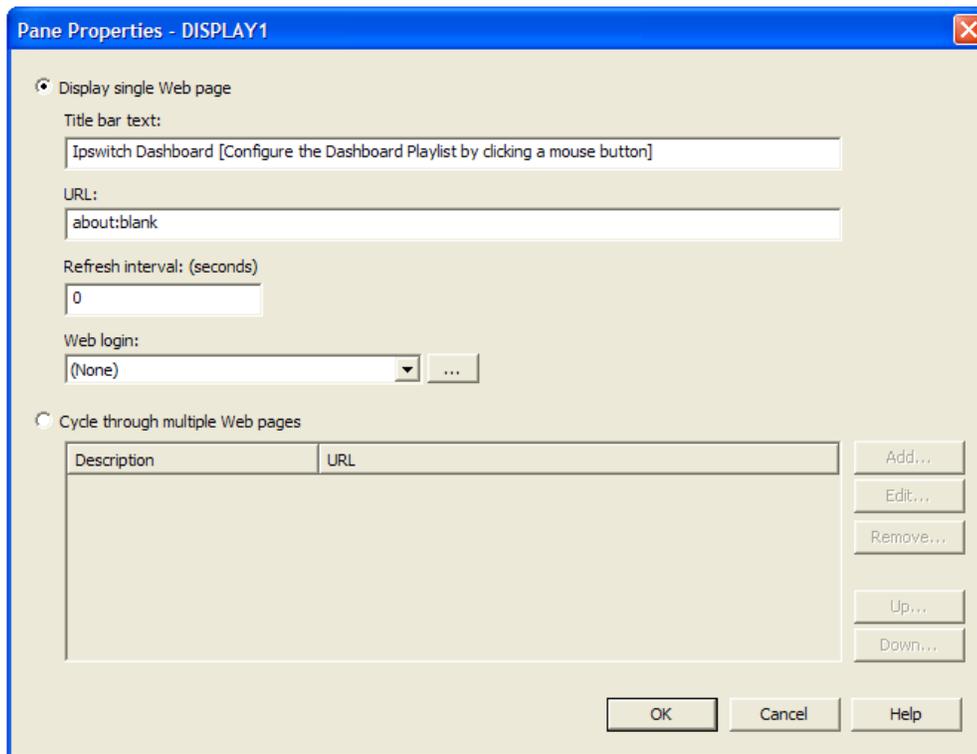
To configure a single Web page playlist:

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 fields:
 - **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 drop-down 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** field, appended to the Web page URL.

4 Click **OK** to save changes.



Important: The Web Login drop-down 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 you want to configure a playlist for, 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 fields:
 - **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 drop-down 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** field, 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.

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 OID's 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).

CoreAsp.SnmpRqst

This object is used to send SNMP requests to a remote device.

`Initialize` or `Initialize2` must be called prior to any other members.

CoreAsp.SnmpRqst uses a three step process:

- 1 Calls `Initialize` or `Initialize2` to initialize the object against a particular device.
- 2 Sets optional parameters such as timeout value, port, etc.
- 3 Performs any number of `Get`, `GetNext`, `GetMultiple` or `Set` operations against a device. Those operations return an `ComSnmpResponse` object that contains the status of the operation and the value either directly (use `Failed/GetValue/GetOid`) or as a list of SNMP variable binding returned as XML data (use `GetPayload`).

Method	Description	Returns
Initialize (nDeviceID)	<p>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.</p> <ul style="list-style-type: none"> ▪ <code>nDeviceID</code>. A positive integer corresponding to the device ID of a device configured in WhatsUp Gold. <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: <code>Context.GetProperty("DeviceID")</code></p>	ComResult object
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> <ul style="list-style-type: none"> ▪ <code>sDeviceAddress</code>. The address or hostname of the device to be queried. ▪ <code>nCredentialID</code>. A positive integer corresponding to the credential ID of a credential configured in WhatsUp Gold. 	ComResult object
SetTimeoutMs (nTimeoutInMilliSec)	<p>Sets the timeout value in milliseconds. If not specified, the timeout defaults to 2000 milliseconds.</p> <ul style="list-style-type: none"> ▪ <code>nTimeoutInMilliSec</code>. A positive integer representing the number of milliseconds after which unresolved requests should be terminated. 	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> <ul style="list-style-type: none"> ▪ <code>nNumberRetries</code>. A positive integer representing the number of times to retry timed out requests. <p>Tip: To send only one SNMP packet per request, set <code>nNumberRetries</code> to 0 (zero).</p>	ComResult object
SetPort (nPort)	<p>Sets the TCP/IP port to be used by <code>SnmpRqst</code>. If not specified, port 161 is used.</p> <ul style="list-style-type: none"> ▪ <code>nPort</code>. A positive integer between 1 and 65535 corresponding to the port to be used. 	ComResult object

Method	Description	Returns
Get (sOid)	Issues an SNMP Get command to retrieve the value of the specified object. <ul style="list-style-type: none"> ▪ sOid. A string containing a valid OID. 	ComSnmprResponse object
GetNext (sOid)	Issues an SNMP GetNext command to retrieve the value of the object that follows the specified object in lexicographic order. <ul style="list-style-type: none"> ▪ sOid. A string containing a valid OID. 	ComSnmprResponse object
GetMultiple (sListOfOids)	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. <ul style="list-style-type: none"> ▪ sListOfOids. A comma-separated list of valid OIDs. 	ComSnmprResponse object
Set (sOid, sType, sValue)	Issues an SNMP Set command to set an OID value on a device. <ul style="list-style-type: none"> ▪ sOid. A string containing a valid OID for the object for which you want to set the value. ▪ sType. A single character corresponding to the type of value to set. <ul style="list-style-type: none"> i = integer u = unsigned integer s = string x = hexadecimal string d = decimal string n = NULL object o = object ID t = timeticks a = IPv4 address b = bits ▪ sValue. A string containing the value to set. 	ComSnmprResponse object

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	<p>Returns XML data describing SNMP variable bindings (each containing OID, Type and Value).</p> <p>This XML data consists of a single <code>VarBindList</code> node which contains one or many <code>SnmpVarBind</code> nodes.</p> <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" /> </VarBindList></pre> <p>You can use the Microsoft XML DOM object to access this information. For more information, see the Read multiple objects in one request example.</p>
-------------------	--



Note: All the members of the `ComSnmpResponse` object are methods. They have no arguments and should be called without using parenthesis.

Example scripts using the SNMP API

These example scripts demonstrate the SNMP API in use. All of these examples are written in JScript.

▪ Initialize an SNMP object with error check from a device ID

The `SnmpRqst.Initialize` method returns a `ComResult` object that tells if the initialization succeeded or failed.

This script uses the `Failed` method to detect an error and logs an error message using `GetErrorMsg` if the initialization failed:

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
```

Alternatively, initialization using a device address and an SNMP credential ID:

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var sAddress = "192.168.3.1";
var nCredentialID = 1;
var oComResult = oSnmpRqst.Initialize2(sAddress, nCredentialID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
```

- **Send a standard Get and log the polled value**

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
var oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.2.1.0");

if (oSnmpResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
    Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ",
got " + oSnmpResponse.GetValue);
}
```

- **Send a Get using non-standard port and timeout**

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}

oComResult = oSnmpRqst.SetPort(1234);
oComResult = oSnmpRqst.SetTimeoutMs(5000); // 5 second timeout

var oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.2.1.0");

if (oSnmpResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
    Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ",
got " + oSnmpResponse.GetValue);
}
```

- **Walk the MIB using GetNext**

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
```

```
        Context.LogMessage(oComResult.GetErrorMsg);
    }

    var sOid = "1.3.6.1.2";

    //get the next 10 objects

    for (i=0; i<10; i++)
    {
        var oSnmprResponse = oSnmprRqst.GetNext(sOid);

        if (oSnmprResponse.Failed)
        {
            Context.LogMessage("Failure. Error=" +
oSnmprResponse.GetErrorMsg);
            break;
        }
        else
        {
            sOid = oSnmprResponse.GetOid;
            Context.LogMessage(sOid + "=" + oSnmprResponse.GetValue);
        }
    }
}
```

▪ Read multiple objects in one request

```
var oSnmprRqst = new ActiveXObject("CoreAsp.SnmprRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmprRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}

// Get three objects in one packet:
var oSnmprResponse =
oSnmprRqst.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 (oSnmprResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmprResponse.GetErrorMsg);
}
else
{
    var sXML = oSnmprResponse.GetPayload;

    var objXMLDocument = new ActiveXObject("Microsoft.XMLDOM");
    objXMLDocument.async = false;
    objXMLDocument.loadXML(sXML);

    var oVarBinds =
objXMLDocument.getElementsByTagName("SnmprVarBind");
}
```

```
        // 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

```
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);
}
```

Ipswitch WhatUp Gold User Guide

This manual, 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 manual 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. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

Index

A

Action Policy	
about.....	152
assigning to a monitor	161
assigning to device.....	147
creating	152
creating custom.....	152
editing.....	153
implicit.....	153
Actions	
about the Actions Library.....	127
assigning.....	130, 147, 161
blackout period	148
configuring.....	130
deleting	147
emailing	154
policies.....	152
strategies	126
testing.....	147
text to speech.....	141
Active Discovery	
about.....	237
configuring.....	238
enabling/disabling	240
using	53
Active Monitor	
about.....	157
Active Script.....	159
adding/editing.....	160
assigning Active Monitors.....	160
assigning an action.....	161
configuring.....	160
context code examples.....	177
deleting	163
DNS	159
email.....	159, 199
Exchange	159
library	158
NT Service.....	159
Ping.....	159
scripting	173, 174, 177
SNMP.....	159
SQL Server	159
TCPIP	159
Telnet	159
types.....	157
WMI.....	159
Alerts.....	18
task tray icon.....	18

API	
SNMP	381

B

backing up	
database	30
Blackout Period	
creating.....	148
browsing	
accessing web interface	63

C

Central site	
configuring	342
installing	340
reporting	
full reports.....	360, 378
workspace reports.....	347, 349, 353, 354, 359

Community String		
Credentials overview	103	
Console interface	55	
Context Code		
examples	177	
using Active Script Monitor context object	174	
Copyright.....	389	
Credentials		
overview.....	103	
D		
Data Collection		
using Performance Monitors.....	215	
database		
backing up and restoring	30	
performance tool	31	
table maintenance tool.....	32	
Dependencies		
about.....	117	
setting dependencies.....	119	
viewing dependencies.....	123	
Device Discovery		
about.....	237	
using.....	44	
using the wizard.....	43	
Device Groups		
group access rights	76, 77, 78	
organizing	105	
users' home groups.....	78	
Device Properties		
about.....	96, 97	
Device Types		
changing.....	100	
configuring.....	99	
Device View		
about.....	82	
organizing	57	
Devices		
about.....	81	
adding.....	48, 94	
adding additional network interfaces.....	94	
adding attributes	96	
adding notes.....	96	
adding with Device Discovery wizard.....	43	
assign action	147	
assign actions	161	
changing device IP address.....	97	
changing device name.....	97	
changing device type	100	
configuring groups.....	105	
creating	99	
discovering.....	43	
Discovery.....	1, 43, 44	
active.....	53, 237, 238, 240, 241	
Distributed Edition		
about	337	
configuring		
central.....	342	
remote	346	
installing	338	
central.....	340	
remote	343	
Drag and drop		
organizing devices	57	
Dynamic Groups		
examples	109	
using	107	
E		
Exchange Monitor		
configuring	188	
monitoring.....	187	
Expression Editor		
about	165	
G		
Grid Properties		
using	247	
H		
Hosts File Import scan.....	44	
I		
Importing		
Hosts file	44	
using the Trap Definition Import Tool.....	312	
installing		
Multi-Site Edition	338	
central.....	340	
remote	343	

interface		organizing.....	248
adding additional to a device.....	94	using attached lines.....	62
IP address		using device layout.....	247
changing.....	97	using device types.....	247
IP Range Scan.....	44	using grid properties.....	247
IPX devices		using map display options.....	245
adding support for.....	123	using Map View.....	243
M		using the lock position.....	248
MAC Address Tool.....	323	viewing dependencies.....	123
Maintenance mode		Mapping.....	243, 245
using maintenance mode.....	116	menus	
Map View		creating custom context.....	103
about.....	244	message	
annotating.....	60	WhatsUp Gold engine service.....	369
arranging.....	246	MIBs	
grouping objects.....	248	about.....	304
Links		MIB.....	319
about connecting.....	251	using SNMP MIB File Explorer.....	322
about unconnected.....	251	Microsoft Exchange	
creating connected link lines.....	252	parameters.....	189
showing unconnected.....	251	services.....	190
using link lines.....	61	Monitors	
		Active.....	157
		assigning Actions.....	161
		assigning Active Monitors.....	160
		deleting.....	163
		Passive.....	205
		Performance.....	213
		MSP Edition	
		about.....	337
		configuring	
		central.....	342
		remote.....	346
		installing.....	338
		central.....	340
		remote.....	343

N

network interface	
adding to a device	94
Network Neighborhood	44
network tools	
SNMP MIB File Explorer	322
SNMP MIB Walker	319
Telnet	319
using to view real-time data	231
Web Performance Monitor	232
Web Task Manager	231
Notes	
about	90
adding to a device	96

O

objects	
about SNMP names and identifiers	305
online help	8

P

Pager	
configuring actions	132
Passive Monitors	
about	205
about Device Properties	86
assigning an action	161
configuring	206
configuring listeners	207
using Passive Monitor Library	209
Performance Monitor	
about	213
about Device Properties	84
about reports	223
adding custom Performance Monitors to library	218
configuring/enabling	215
Performance Monitor Library	214
permissions	
group access rights	74, 76, 77, 78, 79
user rights	72
Polling	
about	115
about Device Properties	89
changing polling method	115
setting polling frequency	116
starting and stopping polling per-monitor	117
starting and stopping service	116
Program Actions	
about actions	125
creating	142

Program Options

changing Clock/Regional preferences	256
configuring Passive Monitor Listeners	207
setting date and time format	253
setting Device States colors and icons	255
setting Web Server options	33

R

real-time data	229
in Full Reports	234
InstantInfo popups	230
Split Second Graphs	233
Regular Expression syntax	170
remote desktop	
connecting	369
Remote site	
configuring	346
installing	343
reporting	
full reports	360, 378
workspace reports	347, 349, 353, 354, 359
Reports	
Central and Remote site reports	275, 347, 349, 353, 354
full reports	360, 378
workspace reports	347, 349, 353, 354, 359

configuring Recurring Reports	267
recurring.....	268
setting Report Data storage time	254
restoring	
database.....	30
rights	
group access.....	74, 76, 77, 78, 79
user	72
Rules and Scripts	
about Script Syntax	165
Script Syntax keywords... ..	166, 167, 168, 170, 172
using Expression Editor.....	165
S	
Schedule	
blackout period	148
maintenance.....	116
Scripts	
about Script Syntax	165
example disconnect string	170
example text string	172
Script Syntax keywords... ..	166, 167, 168, 170, 172
using Active Script Monitor context object	174
using Expression Editor.....	165
using Telnet to determine	173
Security	
about SNMP	312
web	34
Server	
starting and stopping polling.....	33
starting and stopping polling per-monitor	117
starting and stopping the web server.....	33
Services	
Exchange Server	190
monitoring for SNMP	304
SQL Server	194
SNMP	
about.....	303
about operations.....	308
about security	312
about the Agent or Manager	304
API381	
ComResult	384
ComSnmpResponse.....	384
example scripts.....	385
SnmpRqst.....	384
Credentials overview.....	103
enabling on Windows devices	218
MIB.....	319
monitoring service	304
Object Names and Identifiers.....	305
receiving SNMP Traps	210
SNMP Management Information Base	304
using SNMP MIB File Explorer.....	322
using the Trap Definition Import Tool.....	312
SNMP SmartScan	44
Split Second Graphs	
in the Web Performance Monitor	232
in the Web Task Manager	231
SSG workspace reports.....	233
SQL	
about SQL Server monitor	191
configuring a monitor.....	192
server parameters.....	194
Syslog	
creating an action.....	140
T	
table maintenance.....	32
task tray icon.....	18
Telnet	
using Telnet to determine	173
testing	
Actions	147
Active Discovery tasks.....	241
Text	
example text string	172
Traps	
receiving SNMP Traps	210
using the Trap Definition Import Tool.....	312
Troubleshooting	
network.....	367
U	
Upgrading	
activating.....	18
backing up and restoring.....	30
User accounts	
about	69
configuring	70
permissions.....	72
W	
Web interface	
accessing	63
Web Performance Monitor	
about	232
using	325

Web Server	
about WhatsUp Gold web security	34
starting and stopping the web server.....	33
Web Task Manager	
using	328
WMI	
monitoring WMI-enabled applications ..	196
Workspace.....	283