IPSWITCH

WhatsUpGold

v.11

User Guide

IPSWITCH

CHAPTER 1 WhatsUp Gold Overview

CHAPTER 2 Installing and Configuring WhatsUp Gold

CHAPTER 3 Using Device Discovery

CHAPTER 4 Using the WhatsUp Gold Console

CHAPTER 5 Using the WhatsUp Gold Web Interface

CHAPTER 6 Managing Devices

CHAPTER 7 About Polling

CHAPTER 8 Using Actions

CHAPTER 9 Using Active Monitors

CHAPTER 10 Using Passive Monitors

CHAPTER 11 Using Performance Monitors

CHAPTER 12 Using Active Discovery

CHAPTER 13 Using Maps

CHAPTER 14 Using the Program Options

CHAPTER 15 Using Full Reports

CHAPTER 20 Using Ipswitch WhatsUp Gold v11 Premium Edition

CHAPTER 21 Troubleshooting

Index

Ipswitch WhatUpProfessional 2007 User Guide

CHAPTER 1

WhatsUp Gold Overview

In This Chapter

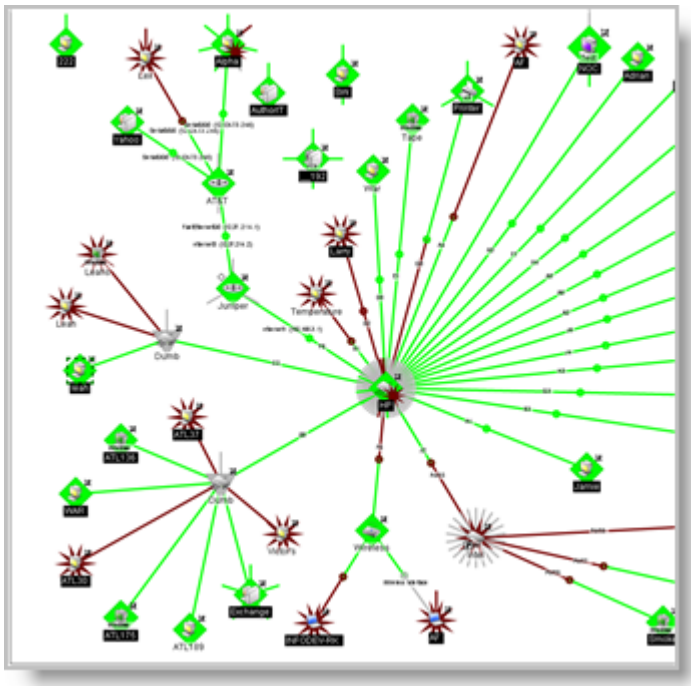
Welcome to Ipswitch WhatsUp Gold v11

Welcome to Ipswitch WhatsUp Gold v11, 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 discovery process searches for devices on your network and lets you decide which devices you want to monitor. You can view monitored devices as a list of devices or as a map.



Polling/Listening

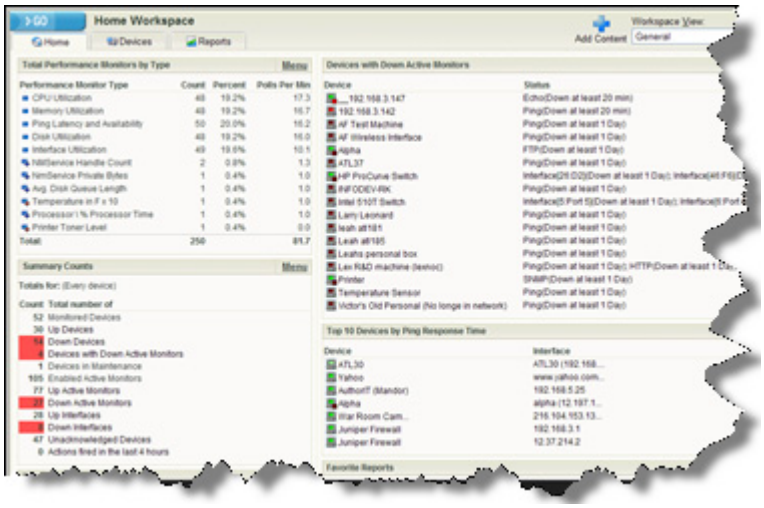
WhatsUp Gold actively polls devices to determine their status. You can use pre-configured monitors, or create your own, to poll services on a device, and to passively listen for messages sent across the network. Monitors can also report on device performance by checking and reporting on device resources, 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 speed problem resolution through options such as alerting via email or pager, or restarting a service.

Reporting and Workspaces

Reports provide 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. They provide crucial network data in one location, which allows for quick and easy access. WhatsUp Gold offers over 100 summary reports that can be use to customize Workspaces. Each user can have their own Workspace.



WhatsUp Gold Interfaces

WhatsUp Gold offers two types of interfaces, the Windows console interface and the web interface, which offer largely the same 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 the application and the database that drives it.

- Web interface

  The web interface provides access to WhatsUp Gold functionality, through HTTP or HTTPS, from a web browser. The newest release of WhatsUp Gold has a completely redesigned web interface, which includes improved navigation, enhanced feature set, and more robust reporting. Also new to the web interface are many features that in the past were only available on the WhatsUp Gold console.

  Some of the features now available in the web interface (previously only available on the console) are:

  - The Credentials Library
  - The complete Passive Monitor Library
  - A fully-functioning Device Properties screen
  - The Active Script Action and Monitor

About the Ipswitch WhatsUp Gold v11 Premium Edition

The Ipswitch WhatsUp Gold v11 Premium Edition is available for separate purchase. It provides all of the network monitoring capabilities of Ipswitch WhatsUp Gold v11 and extends the product to allow additional monitoring of applications and servers, including:

- Microsoft® Exchange™ and Microsoft SQL Server: lets 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 undergoes an unexpected rate of change.

For more information about the Premium Edition, and for purchase information, see the network management product pages (http://www.ipswitch.com/products/network-management.asp) on the Ipswitch Web site.

New in Ipswitch WhatsUp Gold v11

Ipswitch's release of Ipswitch WhatsUp Gold v11 includes the following new features and enhancements:

- An new web interface design that includes customizable workspaces and workspace reports.
- Added over 100 new workspace reports, which provide summaries of the data in status, performance and historical reports.
- Improved performance in rendering web interface pages.
- The ability to support IPv6 enabled devices.
- Improvements to the Bulk Field Change function.
- Enhanced Dependency capabilities that allow you to place Dependencies on devices' Active Monitors.
- Development measures to handle non-persistent SNMP instances for Performance Monitors.
- An Active Script Performance Monitor.
- Performance Counters in the engine.
- A database size information has been added to the console under **Tools > Database Utilities > Tools > Performance**. You can also view the database size indicator icon in the bottom right corner of WhatsUp Gold console application.
- You can now create multiple devices with the same address.
- SQL Server Active Monitor has been updated to support SQL 2005 Windows services.
- Map improvements:

  - Map icons no longer shift when a shared icon is deleted.
  - You can now click-and-drag multiple map icons.
  - Devices are added to maps in more obvious locations.
- Customer feature requests and defect fixes:
  - An issue has been corrected that could cause Interface Utilization to fill up the database rapidly.
  - Group Access Rights have been improved.
  - The capability to back-up the database on an upgrade has been added to the WhatsUp Gold install.
  - The capability to turn on the web interface has been added to the WhatsUp Gold install.
  - The capability to manually set an interface speed in data collection has been added.
  - You now can create device states that last as long as 7 days.
  - The removal of an extra zero (0) from the Interface Speed graph.
  - The removal of the requirement for users to acknowledge Passive Monitor State Changes.
  - Issue was corrected that prevented users from exporting reports or playing web alarms through SSL.

Finding more information

Following are information resources for Ipswitch WhatsUp Gold v11. This information may be periodically updated and available on the WhatsUp Gold support page (http://www.ipswitch.com/Support/whatsup_professional/index.asp).

- **Release Notes**. The release notes, located in the **Start > Programs > Ipswitch WhatsUp Gold v11 > 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.
- **Application Help for the console**. 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**. Contains dialog assistance, how-to's that explain how to use features, table of contents, index, and search. Click **?** to access the Help.
- **Getting Started Guide**. Provides an overview of Ipswitch WhatsUp Gold v11, information to help you get started using the application, the system requirements, and information about installing and upgrading. To view or download the Getting Started Guide, go to the Ipswitch Web site (http://www.ipswitch.com/WU11GSG).

- **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 go directly to the guide on the Ipswitch Web site http://www.ipswitch.com/WUG11Guide.
- **Translation Guide**. This guide describes how to use the translation features to create a localized version of the WhatsUp Gold web interface. To view or download the Translation Guide, go to the Ipswitch Web site http://www.ipswitch.com/WUG11Trans.
- **WhatsUp Gold Forum** (http://www.ipswitch.com/forums/messages.aspx?ForumID=14). Provides a resource for you to interact with other WhatsUp Gold users to share helpful information about the application.
- **The Ipswitch Knowledge Base** (http://support.ipswitch.com/kb/). Search the Ipswitch Knowledge Base of technical support and customer service information.

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 to suggest ways to make our products easier to use, fill out the product feedback form http://www.ipswitch.com/feedback.

CHAPTER 2

Installing and Configuring WhatsUp Gold

In This Chapter

Installation overview

Installing Ipswitch WhatsUp Gold v11 or WhatsUp Gold Premium Edition v11 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 v11 or WhatsUp Gold Premium Edition v11 for the first time, the installation program does the following with no actions required of you.

- Installs the database server, which is Microsoft Server 2000 Desktop Engine (MSDE 2000).

- Creates a WhatsUp database in the MSDE instance.
- Creates a system Data Source Name (DSN), which tells WhatsUp Gold where to find the WhatsUp database.
- Installs the Ipswitch WhatsUp Gold v11 or Ipswitch WhatsUp Gold v11 Premium Edition application.

Read the System Requirements (on page 8), then follow the steps in Installing or Upgrading (on page 10).

Upgrade Notes

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

- MSDE 2000 is installed on the computer on which you are installing WhatsUp Gold or WhatsUp Gold Premium Edition.
- 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 updgrade of the database.

Read the System Requirements (on page 8), then follow the steps in Installing or Upgrading (on page 10), and if necessary, configure the database manually as shown in Upgrading the Database Schema.

If you have an alternative database setup, after completing the WhatsUp Gold installation, you'll need to upgrade the WhatsUp database, as described in Upgrading a Non-Default Database Configuration (on page 23).

Custom Database

Though we recommend that you use the default database (MSDE 2000), 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 Alternative Database Setups (on page 17).

Ipswitch WhatsUp Gold v11 System requirements

Minimum software requirements

- Windows XP Professional SP2 or later; Windows 2000 SP4 Professional or Server; Windows 2003 Server
- Microsoft Internet Explorer 6.0 and later or Firefox 1.5x and later
- Microsoft Windows Scripting Host v5.6 or later. (Required for the WhatsUp web interface, and to run scripts for the active scripting capabilities within active monitors and actions.)

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, go to the Microsoft Scripting Site (http://www.microsoft.com/downloads/results.aspx?freetext=update&productID=478EA476-5552-479E-A200-2C33FFD43F24&sortCriteria=date&displaylang=en).

Important: To install and activate the e-commerce version of the application, you will need an active internet connection.

- Internet connectivity for activation and for running the web interface

Minimum hardware requirements

- Intel Pentium-compatible computers, 550 Mhz or higher (2 GHz or faster recommended)
- 256 MB memory (RAM) (1-2 GB RAM recommended)
- 256 MB of drive space (up to 3 GB additional for MSDE Database and 7200 RPM drive recommended)

Note: This is the requirement for installation. You will need more space for the database. An MSDE database can grow up to the 2 GB limit.

- CD-ROM drive
- Network Interface Card (NIC)
- To use pager, SMS, or beeper actions, a local modem and phone line is required (Ipswitch WhatsUp Gold v11 does not support modem pooling).
- Text to Speech Actions require a sound card configured to use SAPI v5.1, which comes with Windows 2003 and Windows XP operating systems. SAPI v5.1 can be downloaded from the Microsoft Speech site (http://www.microsoft.com/speech/download/sdk51/).

MSDE 2000 requirements

- MSDE has a 2 GB data limit, however up to an additional 1 GB may be used for temporary storage. Make sure you select a large capacity drive for data storage.
- File and Print Sharing must be enabled to run MSDE 2000.

To verify that file and print sharing are enabled:

1. Select **Start > Control Panel**.
2. On the Control Panel, select **Network Connections**.
3. From the menu bar, select **Advanced > Advanced Settings**.
4. On the **Adaptors and Bindings** tab, make sure the **File and Print Sharing** for Microsoft Networks option is selected.

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.
- MSDE 2000, Release A issues. Security policies may interfere with the installation of MSDE and Microsoft Data Access Components (MDAC). Some services may need to be stopped before installing Release A.

Installing or upgrading

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

To install or upgrade WhatsUp Gold:

1. Log in to an Administrator account.
2. Start the installation program:
   - If you purchased a WhatsUp 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.

   If you have an activation key, click **Activate** and follow the on-screen instructions to activate the product.

   If you do not have an activation key, the setup program installs a trial version of the software that expires in 30 days, if not activated. After completing the installation, each time you start the application, you will have an opportunity to purchase a key, as described in Activating the WhatsUp Application (on page 12) in the application Help.

   Click **Next** to continue.
4. Read the license agreement. Select the appropriate option, then click **Next**.
5. Select the default install directories for MSDE 2000, then click **Next** (For first-time installation only).

Note: If you want to customize your database setup, you need to first complete the installation, then manually configure your database as described in Alternative Database Setups (on page 17) in the application Help.

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.

Important: Make sure that you have a large capacity drive selected for data storage. Data files can grow up to the 2 GB MSDE limit.

6 Select the installation directory for the WhatsUp 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 Choose whether to backup your current WhatsUp Professional database. (For upgrade installation only.)

8 Choose how to handle existing Web and Report files. (For upgrade installation only.)

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 Choose whether to enable the web server during install and enter a port for this installation.

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. WhatsUp Gold 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 23) in the application Help.

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

If you choose to launch now, the next screen asks you to activate the application. For more information, see Activating the WhatsUp Application (on page 12) in the application Help.

After the activation screen, you are introduced to the Discover Devices (on page 29) wizard, which lets you set options on how to discover your network. If you choose to postpone these steps, click the **Cancel**.

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 (on page 261) 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.

Activating the WhatsUp application

If you have not activated the product, when you start WhatsUp Gold, a Welcome screen opens.

If you have a license key, click **Activate Now**. If you need a license key, click **Purchase one**. If you want to evaluate the application before purchasing, select **Activate Later**.

Online activation:

- Click **Internet**.
- Complete the steps for online activation.

Offline activation:

- Click **Offline**.
- Complete the steps for offline activation.

For more information about licensing, go to the Ipswitch customer support center (http://support.ipswitch.com/).

Migrating Data from previous versions of WhatsUp Gold

The Migrating from Version 7 or 8 of WhatsUp Gold (on page 239) chapter of this guide describes how to migrate data from WhatsUp Gold versions 7 and 8 to Ipswitch WhatsUp Gold v11 and WhatsUp Gold Premium Edition v11. You should complete the Ipswitch WhatsUp Gold v11 (or Premium Edition v11) installation before migrating your data.

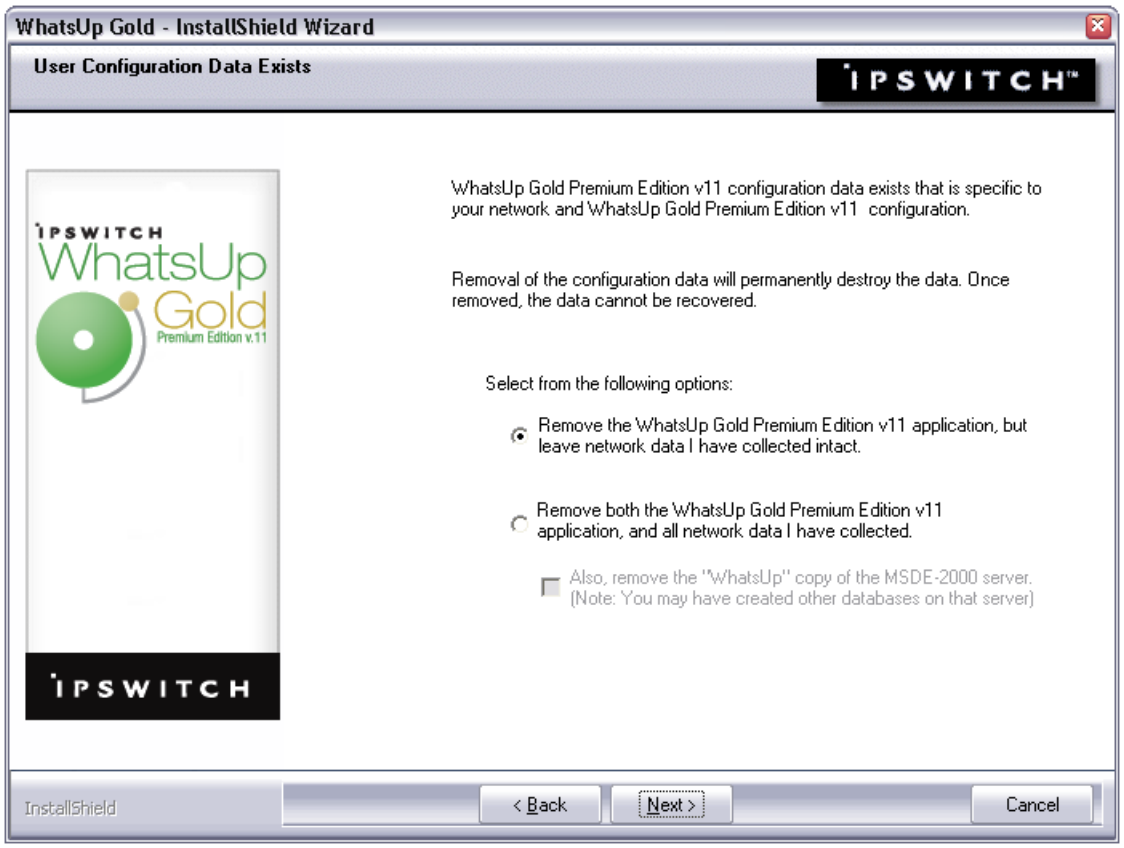
Uninstalling Ipswitch WhatsUp Gold v11

To uninstall Ipswitch WhatsUp Gold v11:

1. Select **Start > Settings > Control Panel**, then select **Add or Remove Programs**.
2. Select Ipswitch Ipswitch WhatsUp Gold v11.
3. Select **Remove**.

You can also run the Ipswitch WhatsUp Gold v11 executable, then select **Remove**.

The following dialog shows the uninstall options:



MSDE Database

The WhatsUp Gold installation program installs the MSDE 2000 database server and configures the WhatsUp database. As described on the MSDE Home page, *Microsoft SQL Server 2000 Desktop Engine (MSDE 2000)* is the free, redistributable version of SQL Server that's ideal for client applications that require an embedded database, and for Web sites serving up to 25 concurrent users.

For more information, see the Microsoft Web site (http://www.microsoft.com/sql/msde/).

You can find a copy of the MSDE 2000 installation program on:

- WhatsUp Gold CD-ROM
- Microsoft Developer Network (http://www.msdn.microsoft.com). Search on MSD to find information on MSDE and the latest downloads.

Note: Microsoft has issued a patch to MSDE 2000. Go to the Microsoft Web site (http://www.support.microsoft.com/?kbid=815495) for more information and for instructions on how to download this patch.

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 utilities, from the main menu in the WhatsUp Gold console, select **Tools > Database Utilities**.

Database backup and restore

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/MSDE 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$Whatsup service (or your customized SQL service.) The account must have write access to the mapped drive for the backup to be successful. To do this, go to **Administrative Tools > Services**, double click on MSSQL$WHATSUP and select the Log On tab on the Properties dialog.

Note: 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 this feature:

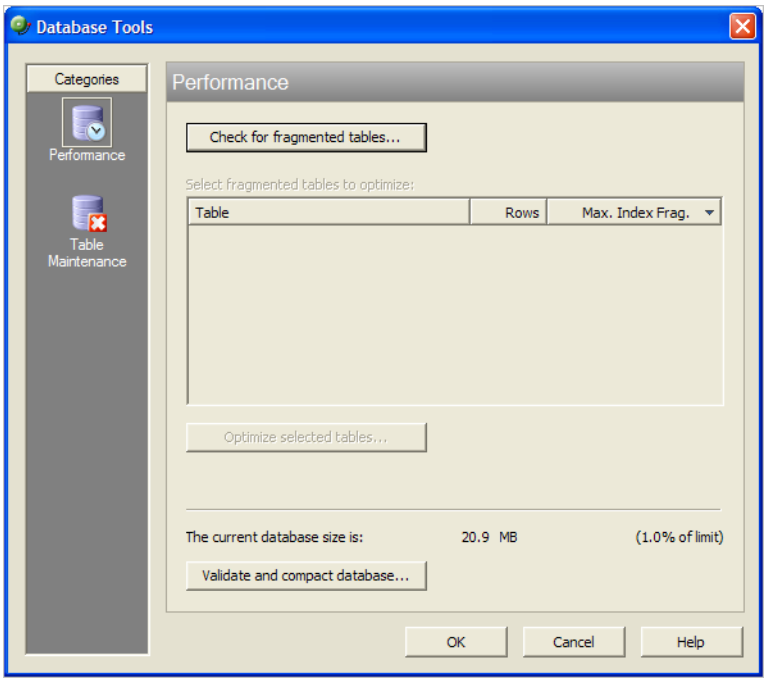
From the main menu in the WhatsUp Gold console, select **Tools > Database Utilities > Back up SQL Database** or **Tools > Database Utilities > Restore SQL Database**.

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

This is a database troubleshooting tool that 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 database 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 MSDE as the WhatsUp Gold database, this section also displays the percentage of the 2GB 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. More information can be found in Microsoft's "Books On-Line" for SQL Server (http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp).

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.) More information can be found in Microsoft's "Books On-Line" for SQL Server (http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp).

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. Select the tables you want to purge from the list.
- **Total Rows**. The total number of data rows in this table that is 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 kept longer than needed, according to your data roll-up settings.

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

Alternative database setups

We recommend using the default database, which is MSDE 2000, and letting the installation program set up the database for you. However, you can manually configure WhatsUp Gold to:

- Use Microsoft SQL Server instead of MSDE 2000

  MSDE 2000 is essentially a scaled down version of Microsoft SQL Server 2000. It can support up to 25 concurrent user connections and up to 2 GB of data. If you need to use more connections or more space, you can purchase Microsoft SQL Server to use with WhatsUp Gold.

- Run the database on a computer separate from the one on which you will install WhatsUp Gold.

  This can be either of the supported databases.

Either of these options requires manually configuring the database, so you need to know how to set up your particular database program.

Supported databases:

- MSDE 2000
- Microsoft SQL Server 2000

Caution: When you use an alternative database setup, you will need to run the database upgrade scripts when installing a new release of WhatsUp Gold. For information on running the upgrade scripts, see Upgrading the Database Schema (on page 23).

What you need to do:

1. First, complete the WhatsUp Gold installation.
2. Make sure the database server is installed on the appropriate computer.
3. Create a database called WhatsUp.
4. Create or the DSN that tells WhatsUp Gold where to find the custom database.

How you complete these three steps depends on which database server you will use and whether the database server is on the same computer as WhatsUp Gold or on a separate computer.

The following sections outline the steps required given different scenarios.

Using an Existing SQL Server on the same computer

This procedure steps you through creating a new WhatsUp database on an existing SQL Server installation that is on the same computer with WhatsUp Gold.

You must first complete the WhatsUp Gold installation, then configure Microsoft SQL Server 2000.

1. Move the database to the SQL Server instance.
   a) Back up the clean MSDE 2000 WhatsUp database.

      From the WhatsUp Gold console, select **Tools > Database Utilities > Back Up SQL Database**. Enter a name for the backup file, for example: `SP1cleanDB.dat`

      Or, from the command line, enter:

      ```
      osql -E -D whatsup -Q "backup database to
      disk='C:\WhatsUpcleanDB.dat'"
      ```

b) Restore the backup to your SQL Server. From the directory where the you saved the backup file, run:

```
osql -E -S <sql server name> -Q "restore database whatsup
from disk='<the .dat file> with Move 'whatsup_dat' to
'<location for the mdf file>', Move 'whatsup_log' to
'<location for the ldf file>'"
```

Substitute the <...> with your values:

<sql server name> = machine name\instance name
<the .dat file> = the backup file from the previous step (step a)
<location for the mdf file> = where you would like to keep the mdf file (data file used by the database)

<location for the ldf file> = where you would like to keep the ldf file (log file used by the database)

For example:

```
osql -E -S rra997\mySqlServerInstanceName -Q "restore
database whatsup from disk='D:\WhatsUpcleanDB.dat' with Move
'whatsup_dat' to 'D:\Program Files\Microsoft SQL
Server\MSSQL$mySqlServerInstanceName\Data', Move
'whatsup_log' to 'D:\Program Files\Microsoft SQL
Server\MSSQL$mySqlServerInstanceName\Data'"
```

2 Remove service dependencies. You need to remove the Ipswitch WhatsUp Engine service's dependence on MSSQL$WHATSUP, which is the MSDE instance created by the Ipswitch WhatsUp Gold v11 installation. To do this:

a) At the DOS prompt, navigate to the directory where Ipswitch WhatsUp Gold v11 is installed, and enter: `Nmservice /Service:`

Note: On some operating systems, you may have to reboot the machine before continuing.

b) At the DOS prompt, enter: `NmService /Service:<MS SQL Server Service Name>`

For example: `NmService /Service:MSSQL$mySqlServerInstanceName`

c) Go to **Control Panel > Administrative Tools > Services**, then start the Ipswitch WhatsUp Engine Service.

3 Configure the Data Source Name (DSN).

a) On the computer on which WhatsUp Gold was installed, click **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

b) Click the System DSN tab. Click Configure to modify the WhatsUp DSN. In the Server box, enter: `<machine name\sql server instance name>`

For example:

`computer123\mySqlServerInstanceName`

c) Click **Finish**.

4 Launch the application.

- Select **Start > Programs > Ipswitch WhatsUp Gold v11 > WhatsUp Gold**.

  - or -

- Select **Start > Programs > Ipswitch WhatsUp Gold v11 > WhatsUp Gold Task Tray Application**.

Using an Existing SQL Server on a remote computer

This procedure steps you through creating a new WhatsUp database on an existing SQL Server installation on a remote computer.

You must first complete the Ipswitch WhatsUp Gold v11 installation, then configure Microsoft SQL Server 2000.

1 Move the database to the SQL Server instance.

a) Backup the clean MSDE 2000 WhatsUp database.

From the WhatsUp Gold console, select **Tools > Database Utilities > Back Up SQL Database**. Enter a name for the backup file, for example:

```
WhatsUpcleanDB.dat
```

- or -

From the command line, enter:

```
osql -E -D whatsup -Q "backup database to
disk='C:\SP1cleanDB.dat'"
```

b) Restore the database.

2 Turn on TCP/IP.

a) On the computer on which WhatsUp Gold was installed, from Windows Explorer, select `C:\Program Files\Microsoft SQL Server\80\tools\bin\SVRNETCN.exe`

b) On the General tab, enable TCP/IP.

c) Stop and then restart the SQL Server.

3 On the WhatsUp Gold computer, create a System Data Source Name (DSN).

a) On the computer on which WhatsUp Gold was installed, click S**tart > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

b) Cick the System DSN tab. The recommended DSN Name used by WhatsUp Gold is: "WhatsUp"

c) Select SQL Server Authentication. You can specify sa (the default) as the LoginID, and its password as an alternative. You can use any LoginID and Password with rights to the WhatsUp database, which requires additional configuration on the remote SQL Server.

d) Make sure the **Change the default database to** option is selected, and that the default database is "WhatsUp".

e) In the final screen of the DSN wizard, click the **Test Data Source** button. Make sure the test is successful.

4 Run NMCONFIG.EXE. This program makes sure that WhatsUp Gold has the account information needed to log on to the database. The NMCONFIG dialog opens.

a) Enter the DSN name created in the previous step.

b) Enter a Username ("sa" is the default.)

c) Enter the Password for this Username (the one you specified in Step 5). The default password is: "wug_sa"

5 Remove service dependencies. You need to remove the Ipswitch WhatsUp Engine service's dependence on MSSQL$WHATSUP, which is the MSDE instance created by the WhatsUp Gold installation. To do this:

a) At the DOS prompt, navigate to the directory where Ipswitch WhatsUp Gold v11 is installed, and enter: Nmservice /Service:

Note: On some operating systems, you may have to reboot the machine before continuing.

b) At the DOS prompt, enter (for the second time:) NmService /Service:

c) Go to **Control Panel > Administrative Tools > Services**, then start the Ipswitch WhatsUp Engine Service.

6 Launch the application.

- Select **Start > Programs > Ipswitch WhatsUp Gold v11 > WhatsUp Gold**.

  - or -

- Select **Start > Programs > Ipswitch WhatsUp Gold v11 > WhatsUp Gold Task Tray Application**.

Installing a New SQL Server Instance on the same computer

This procedure steps through a new installation of SQL Server on the same computer on which you installed WhatsUp Gold.

1 Back up the clean MSDE 2000 WhatsUp database.

From the WhatsUp Gold console, select **Tools > Database Utilities > Back Up SQL Database**. Enter a name for the backup file, for example: SP1cleanDB.dat

- or -

From the command line, enter:

```
osql -E -D whatsup -Q "backup database to
disk='C:\WhatsUpcleanDB.dat'"
```

2 Uninstall MSDE at **Add/Remove Programs > Microsoft SQL Desktop Engine**. Then delete the whatsup.mdf and whatsup.ldf files in:

```
\Program Files\Microsoft SQL Server\MSSQL$WHATSUP\Data
```

3 Install the SQL server, and during install please specify the instance name: WhatsUp.

From the Services Control manager, start MSSQL$WHATSUP service - (**Control Panel > Administrative Tools > Services**).

4 Restore the backup to your SQL Server.

```
osql –E –S <sql server name> –Q "restore database whatsup
from disk='<the .dat file> with Move 'whatsup_dat' to
'<location for the mdf file>', Move 'whatsup_log' to
'<location for the ldf file>'"
```

Substitute the <...> with your values:

<sql server name> = machine name\instance name
<the .dat file> = the backup file from the previous step (step 1)
<location for the mdf file> = where you would like to keep the mdf file (data file used by the database)

<location for the ldf file> = where you would like to keep the ldf file (log file used by the database)

For example:

```
osql –E –S rra997\mySqlServerInstanceName –Q "restore
database whatsup from disk='D:\WhatsUpcleanDB.dat' with Move
'whatsup_dat' to 'D:\Program Files\Microsoft SQL
Server\MSSQL$mySqlServerInstanceName\Data', Move
whatsup_log' to 'D:\Program Files\Microsoft SQL
Server\MSSQL$mySqlServerInstanceName\Data'"
```

5 Configure the Data Source Name (DSN).

a) On the computer on which WhatsUp Gold was installed, click **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

b) Click the System DSN tab. Click **Configure** to modify the WhatsUp DSN. In the **Server** box, enter: <*sql server instance name*> For example: `whatsup`

c) Select **SQL Server Authentication**. You can specify **sa** (the default) as the LoginID, and its password as an alternative. You can use any LoginID and Password with rights to the WhatsUp database.

d) Click **Finish**.

6 Run NMCONFIG.EXE. This program makes sure that WhatsUp Gold has the account information needed to log on to the database. The NMCONFIG dialog opens.

a) Enter the DSN name (from Step 5).

b) Enter a Username ("sa" is the default.)

c) Enter the Password for this Username (the one you specified in Step 5). The default password is: "wug_sa"

`osql –E –S` <sql server name>

7 Launch the application.

- Select **Start > Programs > Ipswitch WhatsUp Gold v11 > WhatsUp Gold**.

  - or -

- Select **Start > Programs > Ipswitch WhatsUp Gold v11 > WhatsUp Gold Task Tray Application**.

Upgrading the database schema

Features in Ipswitch WhatsUp Gold v11 mandate an update of the original database schema. The WhatsUp Gold installation program updates the database, provided the database is in the default configuration. A default configuration is one that meets the following conditions:

- MSDE 2000 is installed on the computer on which you are installing WhatsUp Gold.
- The WhatsUp database instance exists in MSDE.
- A DSN named WhatsUP is configured to point to the WhatsUp database instance.

All other configurations are considered a non-default configuration. The WhatsUp Gold installation program will notify you if the database is in a non-default configuration.

You must first complete the WhatsUp Gold installation, then upgrade the database.

This section steps through how to upgrade an installation of WhatsUp Gold that is a non-default configuration.The procedures differ depending on whether the database server is on the same computer as WhatsUp Gold.

To upgrade the database from the WhatsUp Professional 2006 format to Ipswitch WhatsUp Gold v11 format, follow these steps:

1 If your WhatsUp database is not on the same computer as Ipswitch WhatsUp Gold v11, copy the *DB Scripts* directory and all sub-directories to the remote server.

  Make note of the fully qualified path to the *DB Scripts* directory, as it will be required in the steps that follow.

2 On the computer on which the database server is installed, from the command prompt window, go to the *Upgrade Script* sub-directory of the *DB Scripts* directory.

Important: Before running the scripts, close the WhatsUp Gold application; then, shut down the WhatsUp engine (right-click the WhatsUp icon in the task tray, then select **Close**.)

3 Run the upgrade scripts, by running the Visual Basic (VB) script which runs each script in sequence, or by running each script individually.

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

VB Script:

In the command prompt window, execute the following VB script:

```
cscript upgrade_db.vbs -E -S <sql server name> -d whatsup
```

where the argument, sql server name, specifies the machine name\database instance name.

Caution: osql arguments are case-sensitive (-d is not the same as -D)

For example:

```
cscript upgrade_db.vbs -E -S computer123\MySqlServerInstanceName
-d whatsup
```

The VB script executes the appropriate upgrade scripts, based on your existing WhatsUp Gold database schema file, by using information in the `Transform.ini` file.

To manually run the upgrade scripts:

The alternative to using the VB script is to manually execute the upgrade scripts on the SQL Server machine, as follows:

1 The Upgrade scripts are found in a sub-directory within the DB Scripts directory named Upgrade Scripts. Using Notepad or a similar text editor, open each file whose name starts with "upgrade_from_" and use the **Edit > Replace** function to replace every occurrence of the <DATAFILESPATH> placeholder with the path to the *DB Scripts* directory.

Note: Some of the upgrade scripts will have no placeholders; some will have more than one. No trailing slash should be used in the replacement string (For example, "upgrade_form_").

Save each updated file.

2 Run the scripts by using SQL Server Enterprise Manager (available on the SQL Server CD), or the osql command.

SQL Enterprise Manager:

Important: Open the SQL Server Enterprise Manager and select the server running the WhatsUp Gold database. From the Enterprise Manager, open the SQL Server Query Analyzer, and select the WhatsUp Gold database in the drop-down selector found in the toolbar.

Determine your current WhatsUp Pro database schema version by executing the following statement in the SQL Server Query Analyzer:

```
SELECT sValue FROM DatabaseProperty WHERE sName = 'Version'
```

The value returned should be a six digit number. Next, in Notepad, open the Transform.ini file (it is located in the Transforms folder) and locate, in the [VERSIONS] section, the "Version" entry that corresponds to that six-digit number. (For example,

102203 corresponds to Version 10.) Make a note of that number, which we'll refer to as the 'starting transform number'.

Next, look in the [SCRIPTS] sections, and make a note of all the "Transform" entries beginning with the one **after** your 'starting transform number'. In our 102203 example, that would be **10 + 1**, or **11**. These are the upgrade scripts that you need to run manually: in our example, that would be all the scripts starting with "Transform11" and ending with the highest number script.

Transform11=upgrade_from_102202_to_103001.sql

Transform12=upgrade_from_103001_to_103002.sql

Transform13=upgrade_from_103002_to_103003.sql

Transform*nn*=upgrade_from_*nnnnnn*_to_*nnnnnn*.sql (last script)

Using the SQL Server Query Analyzer, select **File > Open** and load each script, then press F5 to execute, in order.

Caution: Manually executing the incorrect scripts, or executing the correct scripts out of order, will cause database schema errors. Be sure you have a backup before attempting this manual execution.

Osql command:

Run the scripts in the order shown above using the osql command as follows:

```
osql -E -S <sql server name> -d whatsup
-1 <script name.sql> {-o errorlog.txt}
```

For example:

```
osql -E -S computer123\MySqlServerInstanceName -d whatsup
-1 upgrade_from_101206_to_102.sql -o errorlog.txt
```

Following successful execution of the scripts, your WhatsUp Gold database will be up-to-date and ready for use by Ipswitch WhatsUp Gold v11. All data previously collected should be present within the updated database.

3. To confirm that the database upgraded successfully, check the "Current Version" as you did in step 2, and confirm that it matches the version number in the last transform script.

4. Select **Control Panel > Administrative Tools > Services** and verify that the status of Ipswitch WhatsUp Engine service is Started. If it is not, start the service.

5. You can now launch `NMConsole.exe` or start the application via the program shortcuts.

Configuring the web interface to use IIS

Follow these steps to run the WhatsUp Gold web interface through an IIS (Internet Information Services) Web server.

1 Stop the following services and applications:

- Ipswitch WhatsUp Engine service
- Ipswitch Web service
- Task Tray application

Also make sure that you have the WhatsUp Gold console closed.

2 Allow MSDE to use SQL Server Authentication. Use Regedit.exe to set:

```
HKEY LOCAL MACHINE\Software\Microsoft\Microsoft SQL
Server\WHATSUP\MSSQLServer\LoginMode=0
```

3 Restart the MSSQL$WHATSUP service.

4 Specify a username and password for WhatsUp Gold to use when connecting to MSDE:

a) Go to **Control Panel > Administrative Tools > Data Sources** and select the **System DSN** tab.

b) Select the WhatsUp DSN and click **Configure**. The Configuration wizard appears.

c) Verify that the fields in the first dialog are correct and click **Next**.

d) On the second dialog, verify that the **With SQL Server authenitication using login ID and password entered by the user** option is selected. On this same dialog specify user=`sa` and password=`wug_sa` and click **Next**.

e) On the third dialog, ensure that the first option is selected and WhatsUp appears in the drop-down menu and click **Next**.

f) Continue to click **Next** until you come to the final dialog, and then click **Finish**.

5 Stop IIS.

6 Create a virtual directory in IIS named NmConsole which points to `<WhatsUp Gold install path>\HTML\NmConsole\`. Go to Windows **Control Panel** > **Administrative Tools** > **Internet Information Services**. Right-click on **Default Web Site** and choose **New > Virtual Directory**. We strongly recommend that you name this new directory NmConsole.

7 Enable Parent Paths for the default web site (to support use of the relative paths used to navigate in the WhatsUp web interface).

a) Go to **Control Panel > Administrative Tools > Internet Information Services**.

b) In the IIS Manager, expand Web sites, then right-click on the newly created NmConsole virtual directory and choose **Properties**.

c) On the Virtual Directory tab, click **Configuration**.

d) On the Options tab, select **Enable parent paths**. Click **OK**.

8 Set authentication for the virtual directory you set up in Step 6. To do this:

a) In IIS Manager, right-click the virtual directory and select **Properties**, then select the **Directory Security** tab.

b) In **Anonymous access and authentication control**, click **Edit**. Enable anonymous access and set the username and password to a local administrator. Click **OK**.

9 For IIS version 6:

In IIS Manager, select Web Service Extensions and allow Active Server Pages.

10 Restart IIS.

11 Set the internal web server to port 8080, or disable it. If you disable the WhatsUp web interface, ensure that the reports still load correctly.

12 Restart the services and applications you stopped in Step 1.

13 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/`

Important: A known issue with IIS: when adding a device through IIS, you will receive an "error scanning device" error. There are two ways to address this problem. Please refer to the KB article, WhatsUp Gold - "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, http://www.."

CHAPTER 3

Using Device Discovery

In This Chapter

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 WhatsUp Gold console.

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.

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 a step-by-step example of how to Discover devices, see Example: discovering devices (on page 31).

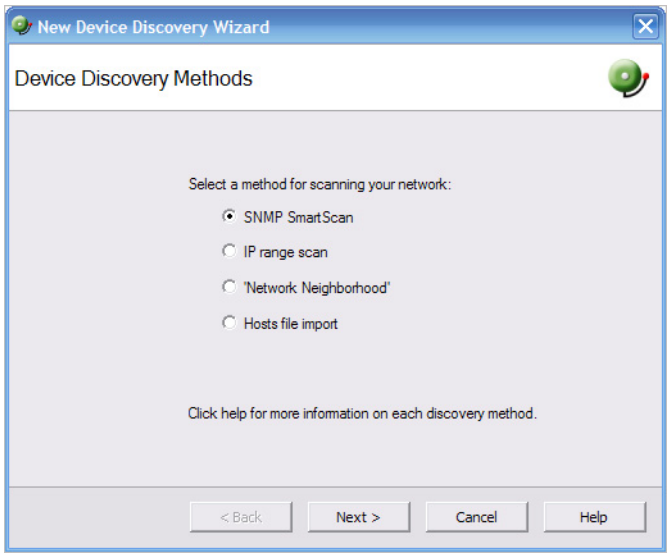
Using Device Discovery

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:

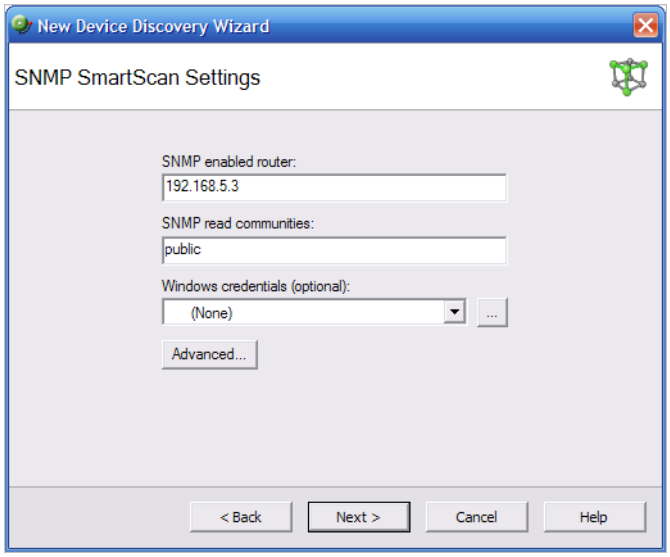
- Know the IP address of the SNMP-enabled router whose network you want to discover.
- Know the Read Community name assigned to the devices on the network.

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 opens.

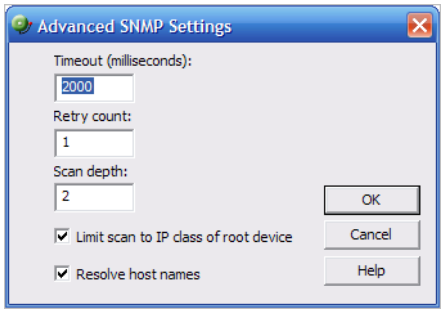


3 In the **SNMP enabled router** box, enter the IP address of the SNMP enabled router you want to use for this scan.

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.

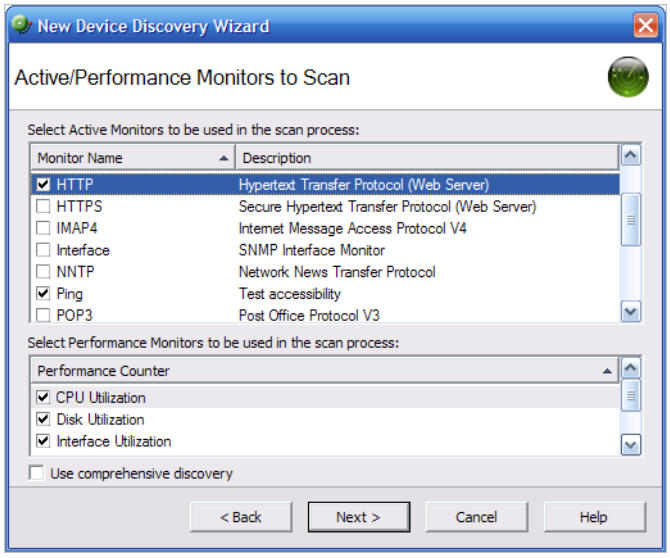
Optionally, select the Windows credential that you want to use during discovery. These credentials are configured in the Credentials Library, and store Windows authentication information (username and password) for those devices that require a logon for discovery or monitoring. Click the Browse (**...**) 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. Let's select Ping and HTTP as our Active Monitors and Disk Utilization as our Performance Monitor 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 over, the **Devices to Monitor** window opens, listing all of the devices just discovered. 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 opens. For more information about Action Policies, see the About Action Policies (on page 118) section.

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. For more information about Device Views, see About the Device View (on page 43).

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, 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 > Devices > New Device**.

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.

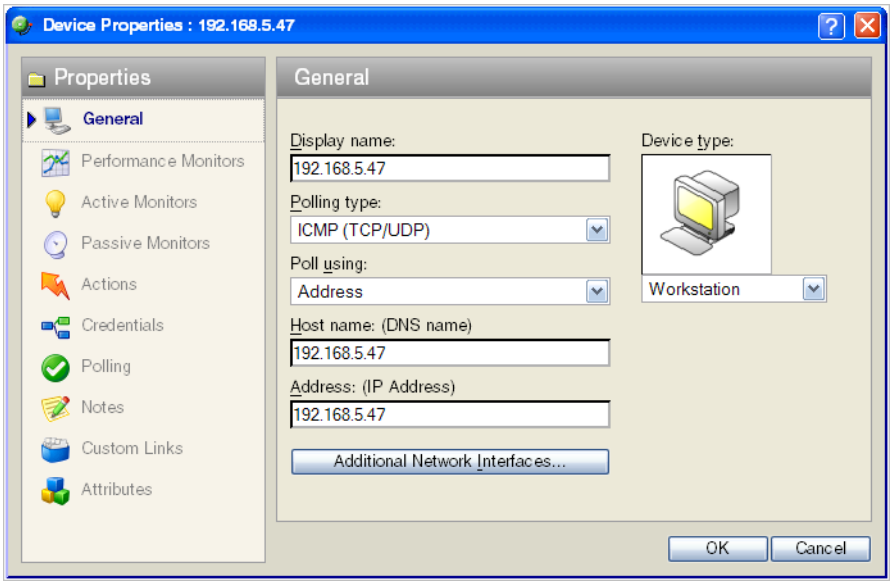
3. Enter the IP address or host name for the device into the box.

   Optionally, click **Advanced**, to set any of the Active Monitor scan, Performance Monitor scan, and other options. For more information, see the Help.

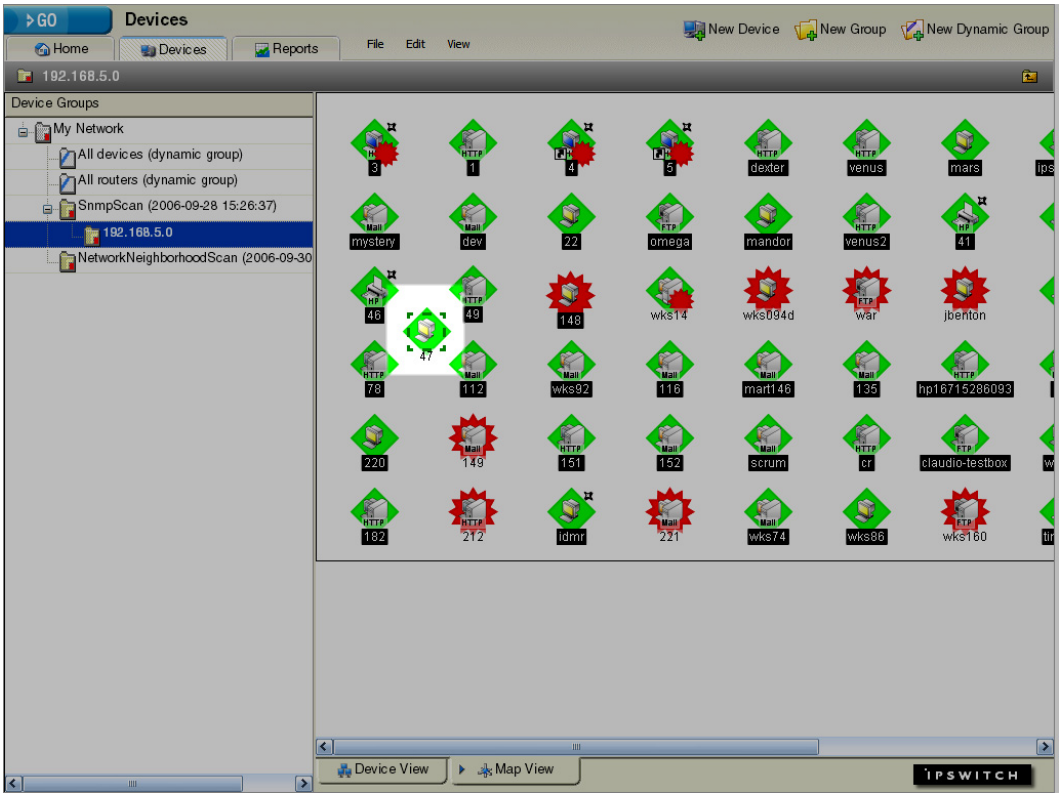
   Optionally, select **Add device immediately without scanning** to add a device without scanning for the device. This immediately adds a "bare-bones" device, generically categorized as a workstation.

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

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.



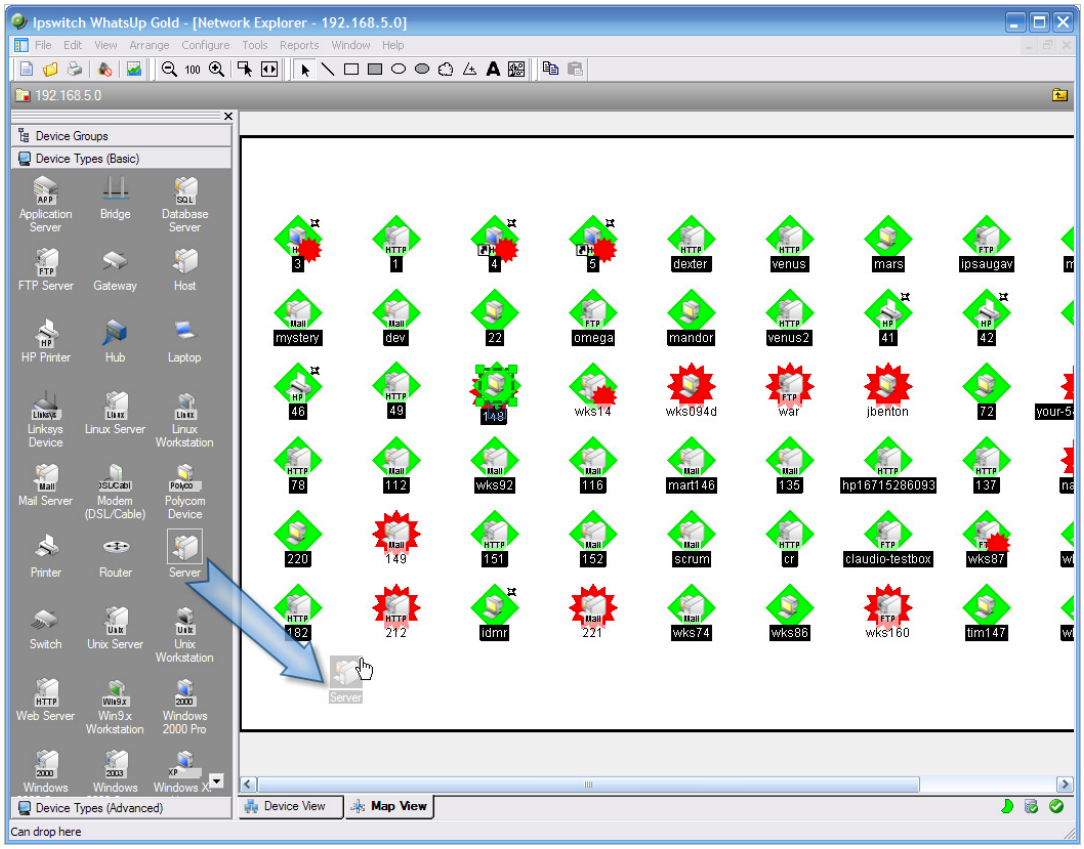
For more information about the Device Properties dialog, see Learning about the Device Properties (on page 62).

Example: clicking and dragging a device to a device group

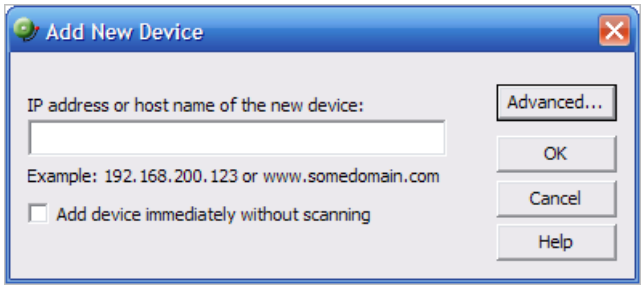
To click and drag a device to a device group:

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 The remaining steps are the same as those used in steps 3-5 of the Example: manually adding a device to a device group (on page 34).

Using Active Discovery

You can also 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 175).

CHAPTER 4

Using the WhatsUp Gold Console

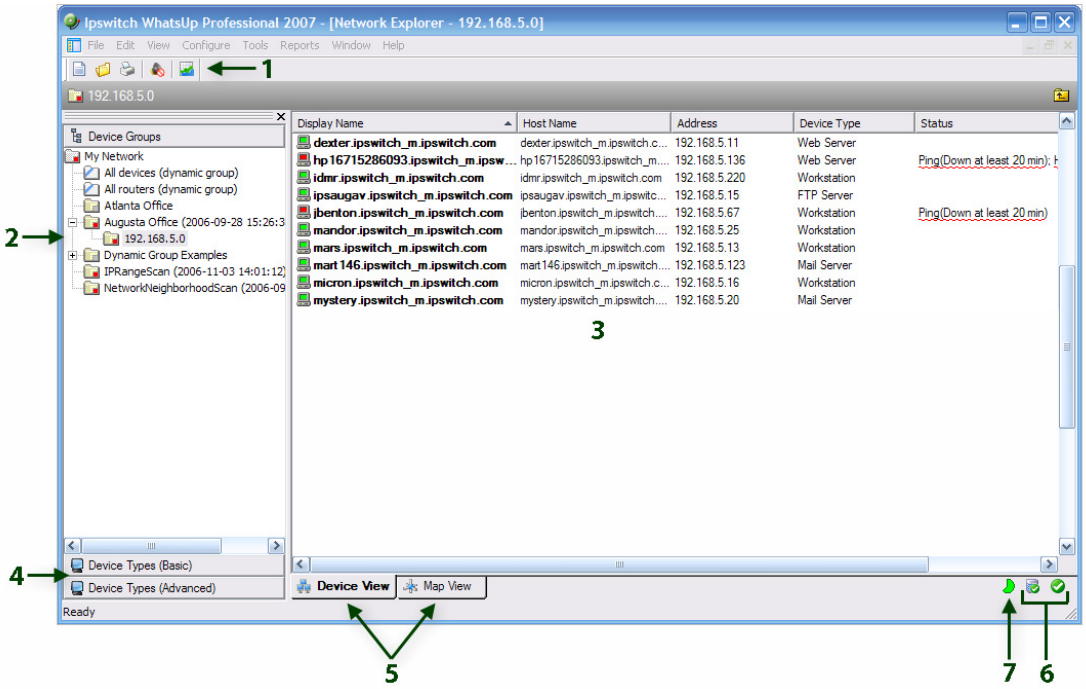
In This Chapter

About the WhatsUp Gold console

The WhatsUp Gold console is the primary interface to the configuration and management of the application and the database that drives it. This chapter describes the different parts of the console, how to navigate the interface, and what you need to know to get started using it.

Console overview

The following is a breakdown of the main features found on the WhatsUp Gold console.



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.

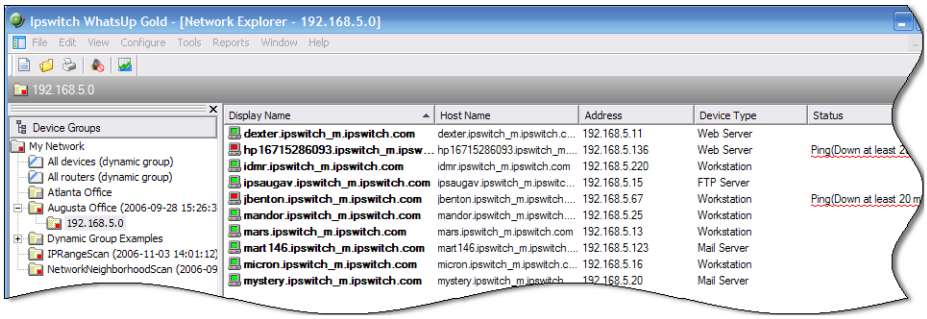
Poll engine is connected | Poll engine is not connected | Polling is enabled | Polling is disabled

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.

About the Device View

With a similar look and feel to Windows Explorer, WhatsUp Gold's 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) Device is currently in maintenance mode.
	Device group contains at least one device that is considered down.
	Device group is empty, or devices have not been polled due to a dependency on another device.
	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 Device Overview (on page 61).

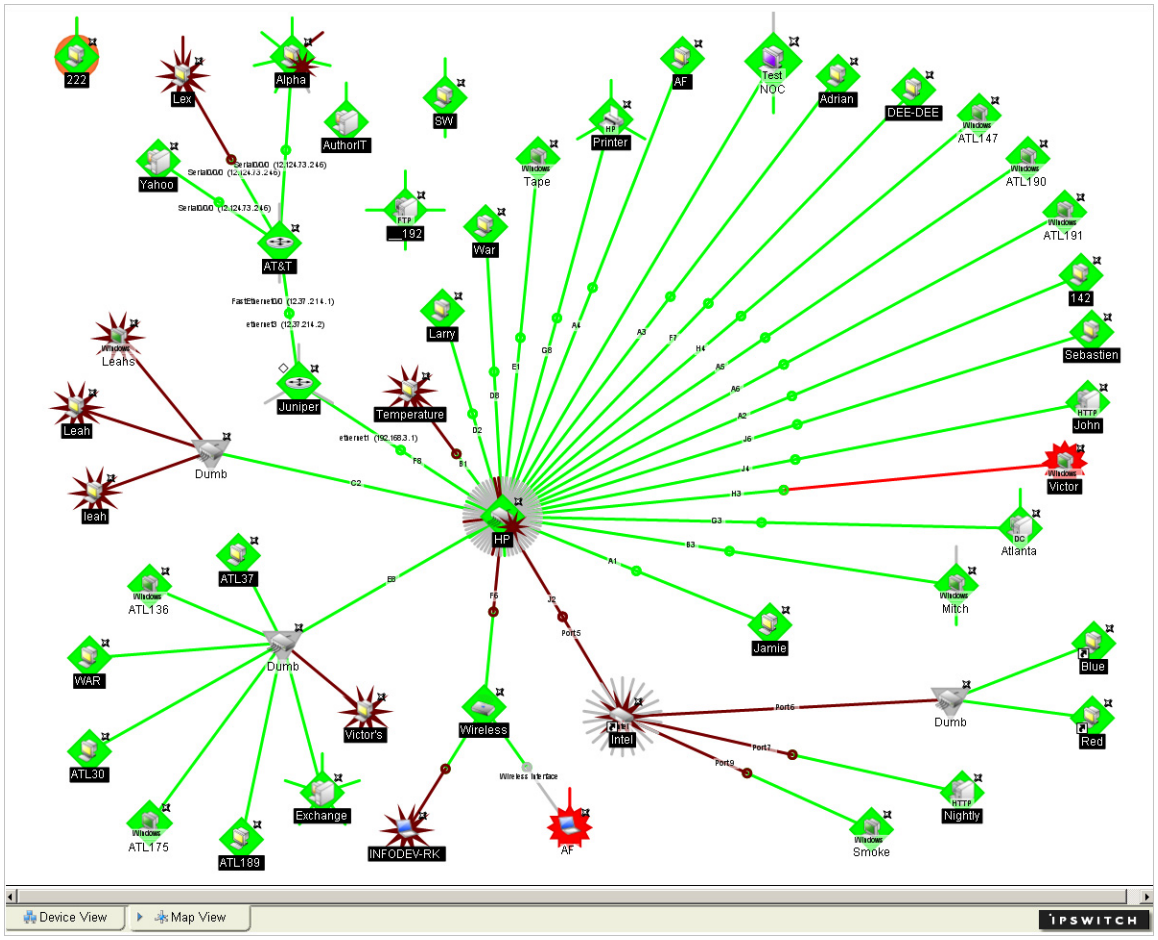
Organizing Devices and Device Groups

In the Device View, 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: Devices that are shared between two or more groups share common device properties. Therefore, you only have to change the settings on one device entry instead of remembering where each device is stored. This also means that each device is only polled once, no matter how many times it appears in your device group tree.

About the Map View

Through the Map View of WhatsUp Gold, you can create graphical representations of your network, organized by any means that suits your needs. Devices can be placed on as many maps as needed, without the devices being polled multiple times. In short, there is an enormous amount of flexibility in the way you can use the Map View feature.

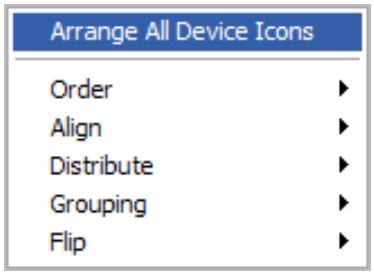


The map above was created after an SNMP Device Discovery Scan. It shows the relationship between the different subnetworks that are connected to each other via the network structures depicted here.

Organizing device layout and views

The WhatsUp Gold 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 toolbar.

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



For example:

To clean up a map after completing Discovery, try the following display options:

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.

Tip: See the WhatsUp Gold Help for more information about how to use specific features of the Map View, including grouping, grid lines and annotations, and other features.

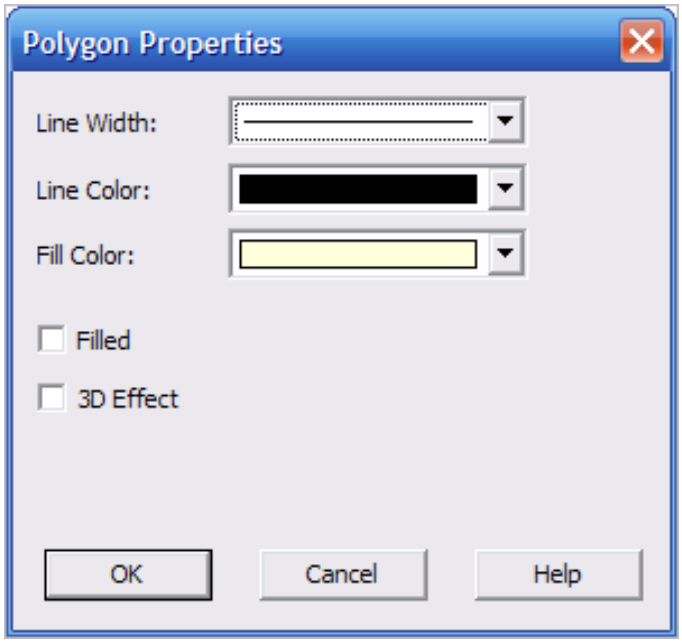
Adding annotations to a map

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 an 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.

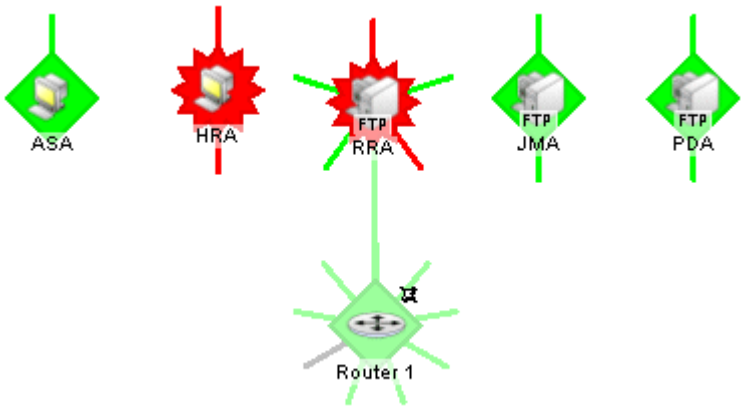
To change Annotation (Draw) tool properties, such as border width and color, select the annotation, then click **Properties** from the right-mouse menu.



Using link lines

In Map View, 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 (see "Connecting links" on page 187) to device RRA and this link is currently up. Also shown are eight unconnected links (on page 187), 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 can be rendered in one of three colors:

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

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 (on page 47), 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 attached lines

Attached lines show an arbitrary connection between devices and move with the device. These 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 (on page 47).

To draw an attached line:

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

Note: The root device can attach to up to five other devices.

CHAPTER 5

Using the WhatsUp Gold Web Interface

In This Chapter

About the WhatsUp Gold web interface

The newest release of WhatsUp Gold has a completely redesigned web interface designed with the intent of making it feel more like an actual application. The entire look and feel of the web interface has changed from previous releases and now includes a new way to navigate through the application. Also new to the web interface are many features that in the past were only available on the WhatsUp Gold console. The WhatsUp Gold web interface and console have never been as functionally compatible as they are the current release.

Features now available in the web interface (previously only available on the console):

- The Credentials Library
- The complete Passive Monitor Library
- A fully-functioning Device Properties screen
- The Active Script Action and Monitor

Accessing the web interface

You can connect to the WhatsUp Gold web interface from any 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:

Administrator

Username: `admin`

Password: `admin`

Guest

Username: `guest`

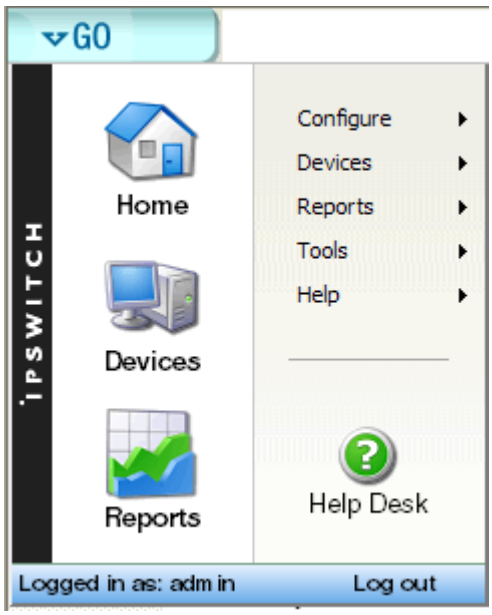
Password: `<password box left blank>`

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.**

For more information, see About Web Security (on page 57).

Navigating through the web interface

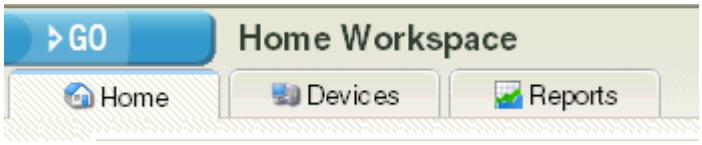
The main menu for the web interface is housed within the Go button, located in the upper-left corner of your browser. The **Go** menu is visible from anywhere within the web interface.



From 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.

The web interface is organized into three areas:

- Home
- Devices
- Reports



You can access each of these areas by:

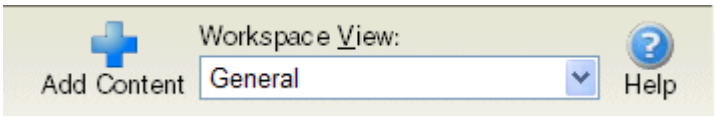
- Clicking on an icon from the **Go** menu.
- Selecting one of the web interface tabs.

The Home Workspace

The WhatsUp Gold Home Workspace is the first screen you see after logging in to the web interface. This is your personal, customizable Home Workspace. For more information on your Home Workspace, please see Customizing Workspace Views (on page 210).

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.

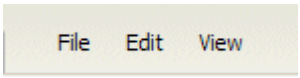


The Devices tab

The WhatsUp Gold Devices tab is where your monitored devices are displayed and managed. The Devices tab has two modes: Device View and Map View. You can add devices in either mode by using the Devices Toolbar located in the upper-right corner of your browser.

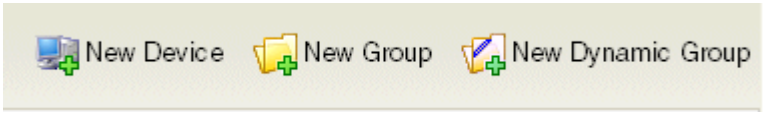
The Devices Menu bar

- **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.



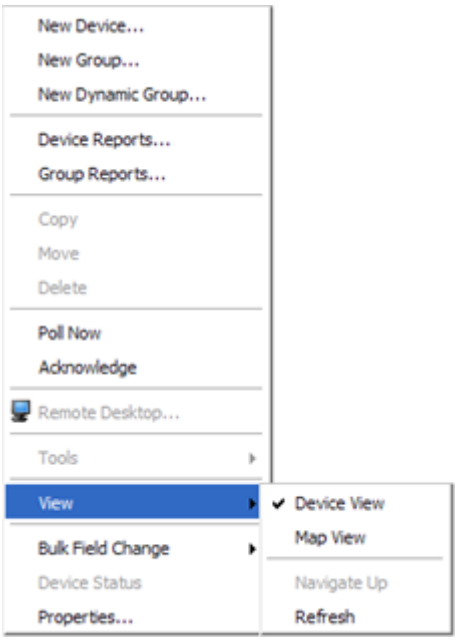
The Devices Toolbar

- **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.



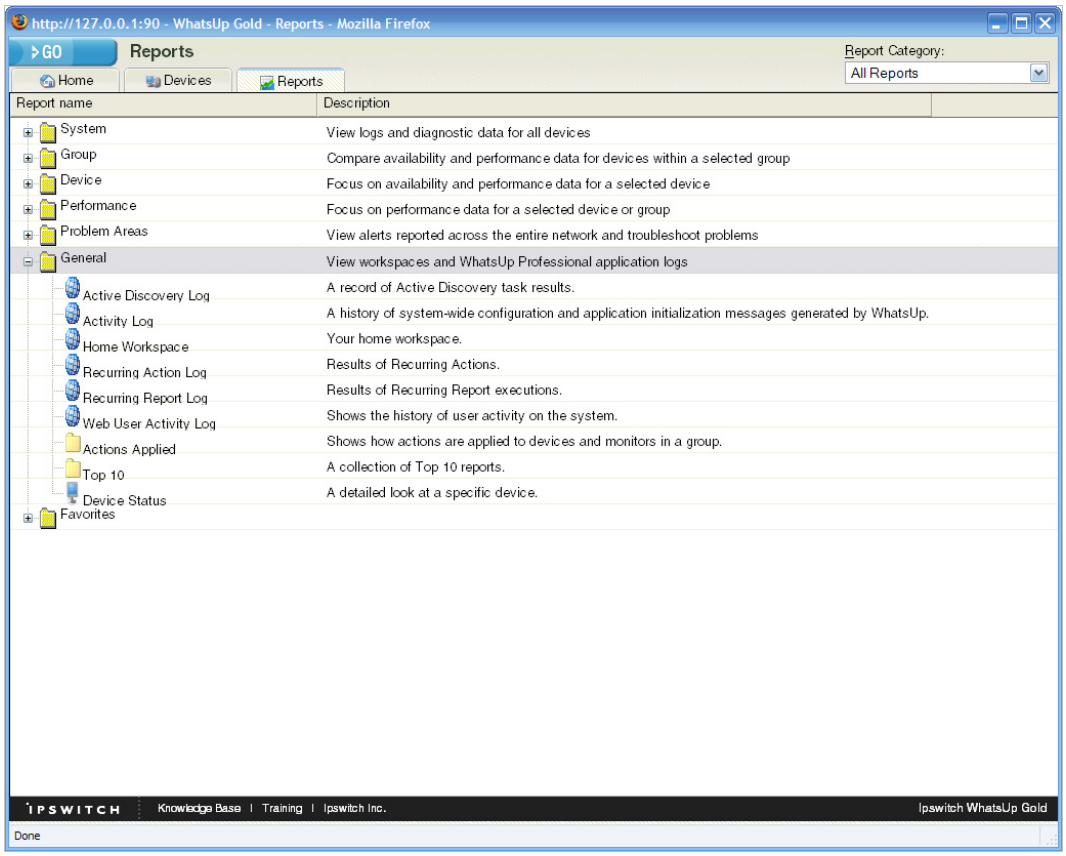
The Right-Mouse Menu

A similar right-mouse menu available in the WhatsUp Gold console is available on the web interface on the Devices tab. The right-mouse menu comes up when you right click in the Devices tab after selecting a device or set of devices.



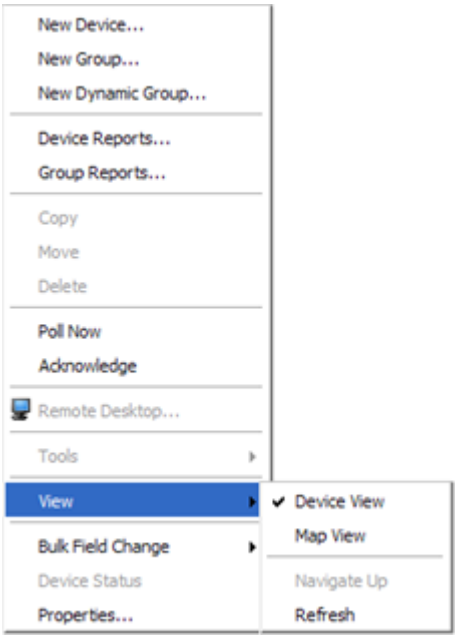
The Reports tab

The Reports tab contains all of the WhatsUp Gold Full Reports. The 2007 version has integrated a new Full Report Picker so that you can easily pick and choose reports to view.



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 web security

WhatsUp Gold is installed with the files needed to immediately begin connecting to the SSL web server using 128 bit encryption.

The files included with the install (root.pem and server.pem) are installed with every copy of WhatsUp Gold, therefore, your encrypted session may not be as secure as it could be.

These certificate files are installed for demonstration purposes only, and should be replaced with certificates that you generate and sign.

Furthermore, this sample certificate is issued with Ipswitch as the Common Name. This will always give a Domain Name Mismatch Security Error on every fresh browser session in your environment.

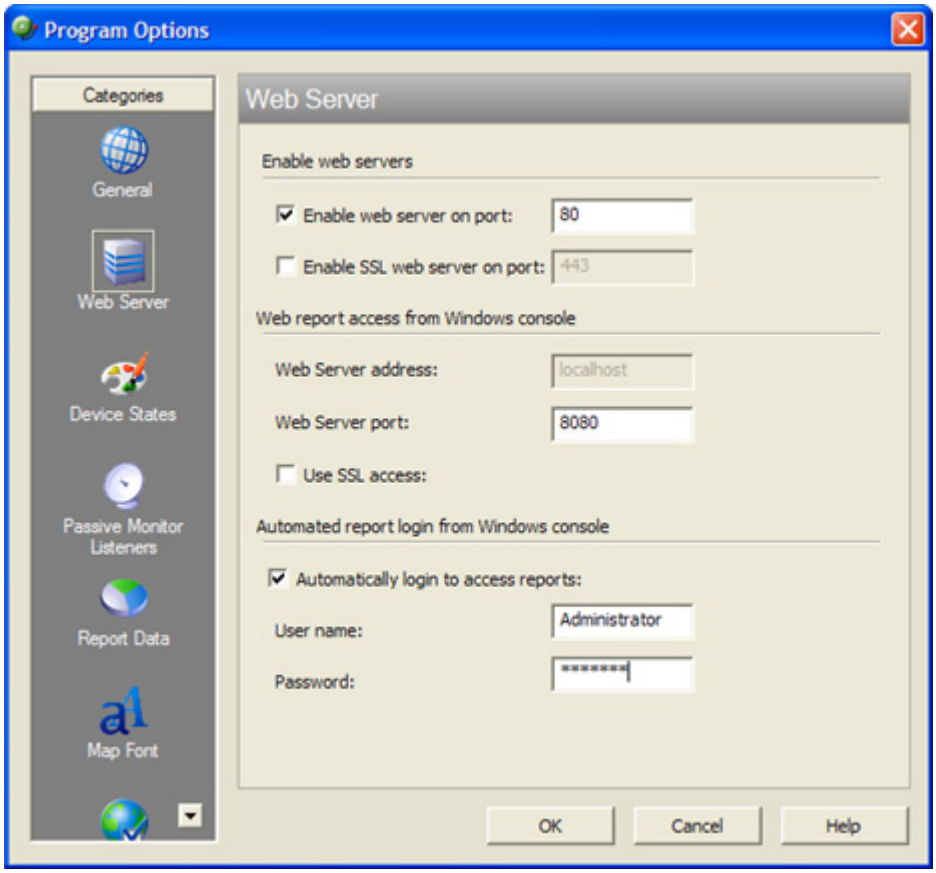
These sample files reside in the `WhatsUp Gold Install Directory>\data\SSL` directory and should be updated with your own files.

Stopping and starting the web server

To stop and restart the 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, then 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.

Configuring the web interface to use IIS

Follow these steps to run the WhatsUp Gold web interface through an IIS (Internet Information Services) Web server.

1 Stop the following services and applications:

- Ipswitch WhatsUp Engine service
- Ipswitch Web service
- Task Tray application

Also make sure that you have the WhatsUp Gold console closed.

2 Allow MSDE to use SQL Server Authentication. Use Regedit.exe to set:

```
HKEY LOCAL MACHINE\Software\Microsoft\Microsoft SQL
Server\WHATSUP\MSSQLServer\LoginMode=0
```

3. Restart the MSSQL$WHATSUP service.
4. Specify a username and password for WhatsUp Gold to use when connecting to MSDE:
   a) Go to **Control Panel > Administrative Tools > Data Sources** and select the **System DSN** tab.
   b) Select the WhatsUp DSN and click **Configure**. The Configuration wizard appears.
   c) Verify that the fields in the first dialog are correct and click **Next**.
   d) On the second dialog, verify that the **With SQL Server authenitication using login ID and password entered by the user** option is selected. On this same dialog specify user=`sa` and password=`wug_sa` and click **Next**.
   e) On the third dialog, ensure that the first option is selected and WhatsUp appears in the drop-down menu and click **Next**.
   f) Continue to click **Next** until you come to the final dialog, and then click **Finish**.
5. Stop IIS.
6. Create a virtual directory in IIS named NmConsole which points to `<WhatsUp Gold install path>\HTML\NmConsole\`. Go to Windows **Control Panel** > **Administrative Tools** > **Internet Information Services**. Right-click on **Default Web Site** and choose **New > Virtual Directory**. We strongly recommend that you name this new directory NmConsole.
7. Enable Parent Paths for the default web site (to support use of the relative paths used to navigate in the WhatsUp web interface).
   a) Go to **Control Panel > Administrative Tools > Internet Information Services**.
   b) In the IIS Manager, expand Web sites, then right-click on the newly created NmConsole virtual directory and choose **Properties**.
   c) On the Virtual Directory tab, click **Configuration**.
   d) On the Options tab, select **Enable parent paths**. Click **OK**.
8. Set authentication for the virtual directory you set up in Step 6. To do this:
   a) In IIS Manager, right-click the virtual directory and select **Properties**, then select the **Directory Security** tab.
   b) In **Anonymous access and authentication control**, click **Edit**. Enable anonymous access and set the username and password to a local administrator. Click **OK**.
9. For IIS version 6:

   In IIS Manager, select Web Service Extensions and allow Active Server Pages.
10. Restart IIS.
11. Set the internal web server to port 8080, or disable it. If you disable the WhatsUp web interface, ensure that the reports still load correctly.
12. Restart the services and applications you stopped in Step 1.

13 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/`

Important: A known issue with IIS: when adding a device through IIS, you will receive an "error scanning device" error. There are two ways to address this problem. Please refer to the KB article, WhatsUp Gold - “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.

CHAPTER 6

Managing Devices

In This Chapter

Device overview

In WhatsUp Gold, devices are virtual representations of resources (computers, servers, hubs, 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 the network connection. When those network resources cannot be reached by WhatsUp Gold, the device is considered down and an action can be configured to fire.

Device Services

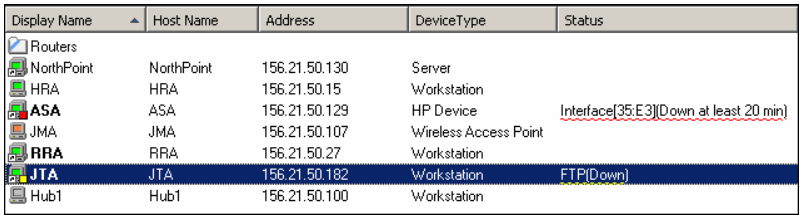
WhatsUp Gold associates Active Monitors with devices on your network. Active monitors query the network services installed on a device and then wait for a response. These monitors query the services running on a network resource, checking to make sure that the FTP server, web server, email server, etc., 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. If any one service on a device is down, then the device as a whole is considered down.

For a more information about service monitors, see Active Monitors Overview (on page 123).

About the Device View

This view provides an overview of each device in a selected group. Each device's icon provides information about its device type and status. In addition, the Status column indicates which specific service 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.

Following is an example of a device list.



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

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

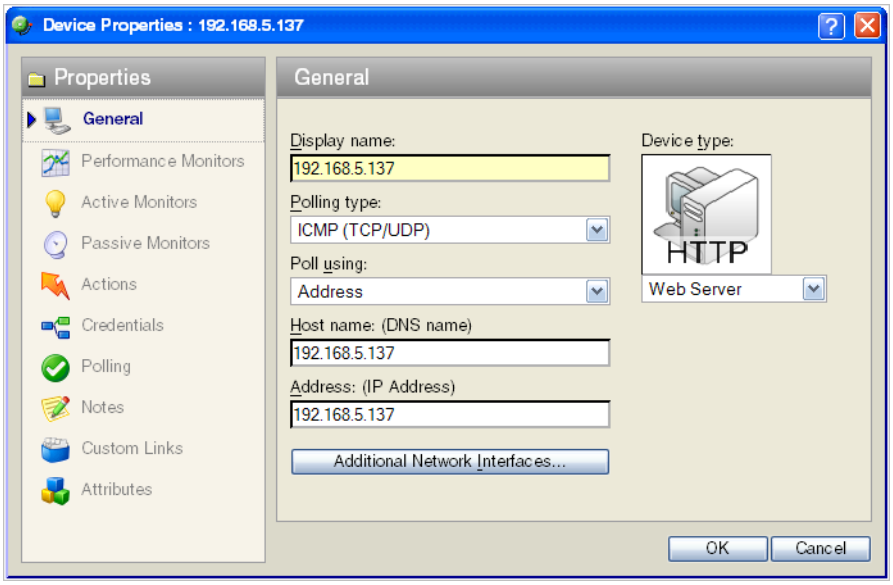
- Routers is a dynamic group.
- Device NorthPoint is a server that is currently up. The icon shows that this device is also in another device group.
- Device HRA is a workstation that is currently up.
- Device ASA is an HP Device (router) that is up, but one of the interfaces (E3) is not responding.
- Device JMA is a workstation 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.

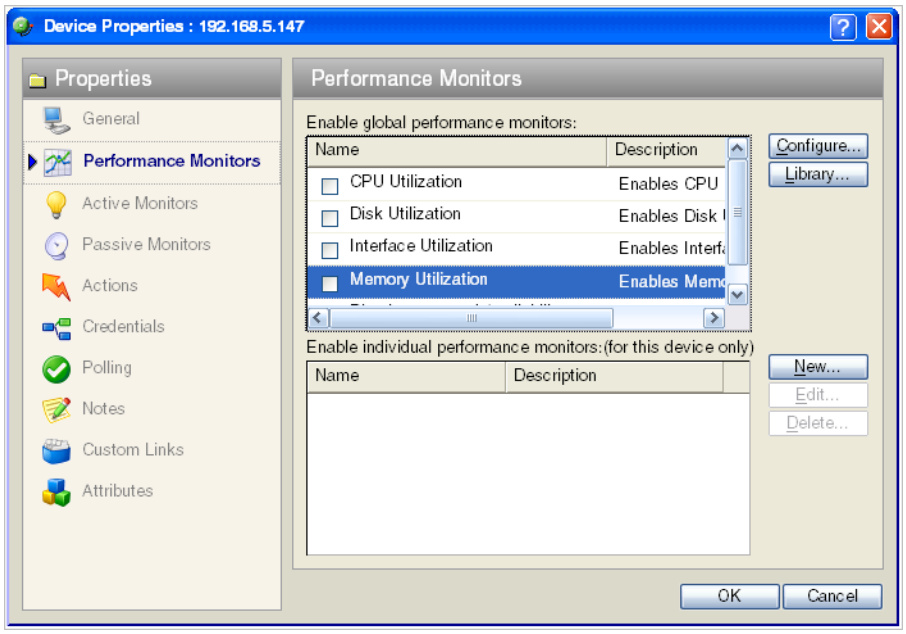
- **Poll using**. Select if you want WhatsUp Gold to use the IP address or the Host name (DNS) of the device for polling.
- **Host name (DNS)**. This should be the official network name of the device if the polling method is ICMP. The network name must be a name that can be resolved to an IP address. 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.

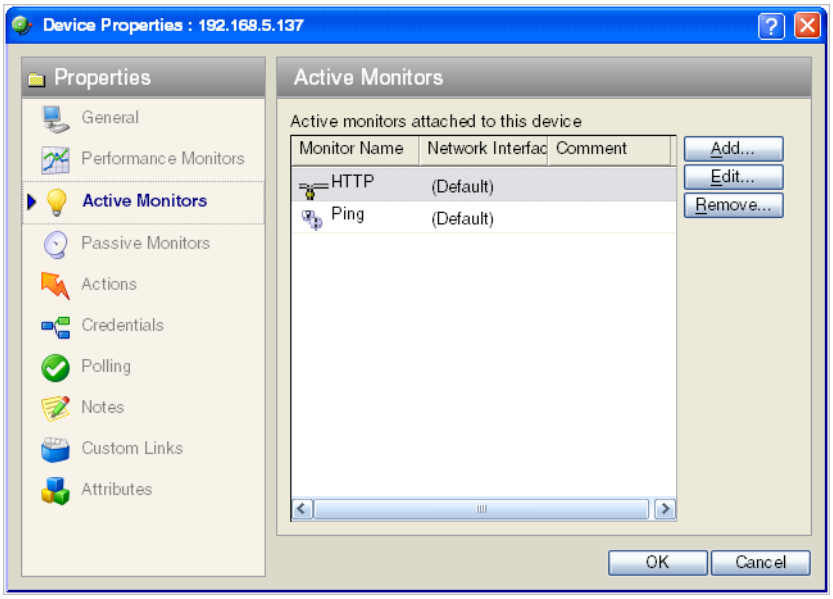
Note: For some performance monitors, the SNMP credential on the device must be configured. For WMI performance monitors, the NT credential is required.



For more information, see Performance Monitor Overview (on page 159).

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.

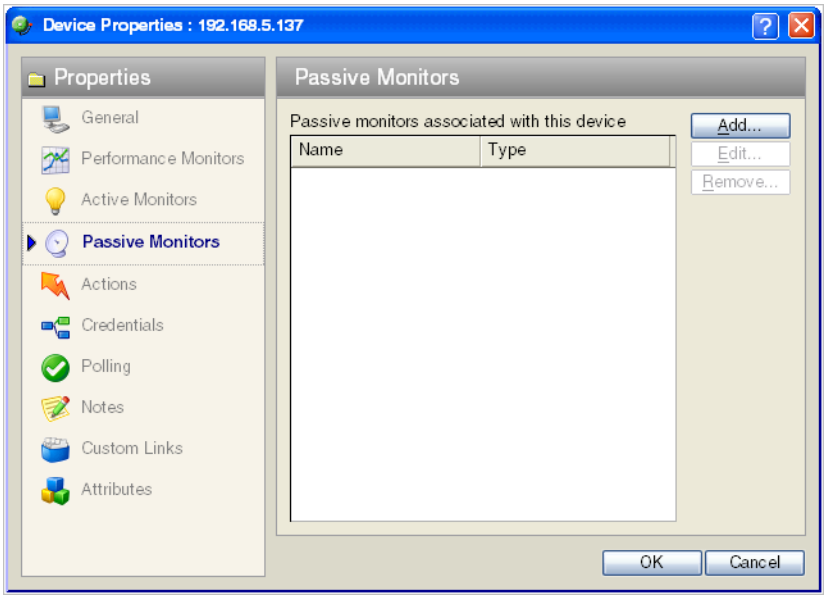


- Click **Add** to configure a new Active Monitor.
- Select an Active Monitor and click **Edit** to change the configuration.
- Select an Active Monitor and click **Remove** to remove the monitor from the device.
- On the WhatsUp Gold console, you can click **Discover** to have WhatsUp Gold scan the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

For more information, see Active Monitors Overview (on page 123).

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

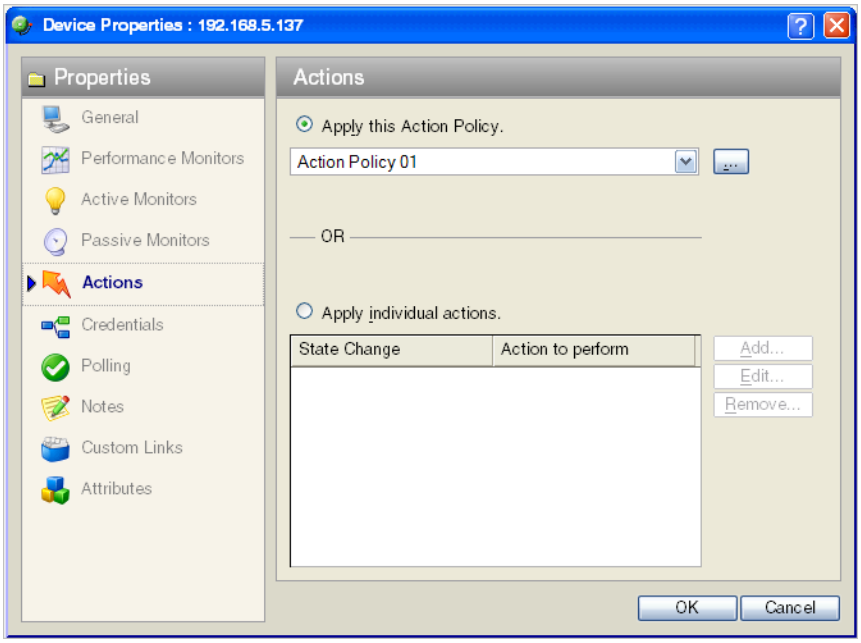
  - or -

  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 151).

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

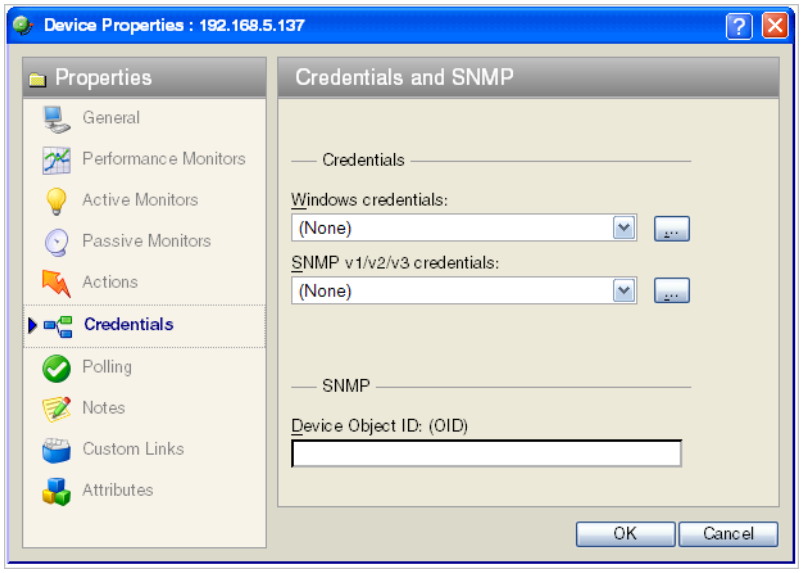
  - or -

  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 93).

About Device Property Credentials

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



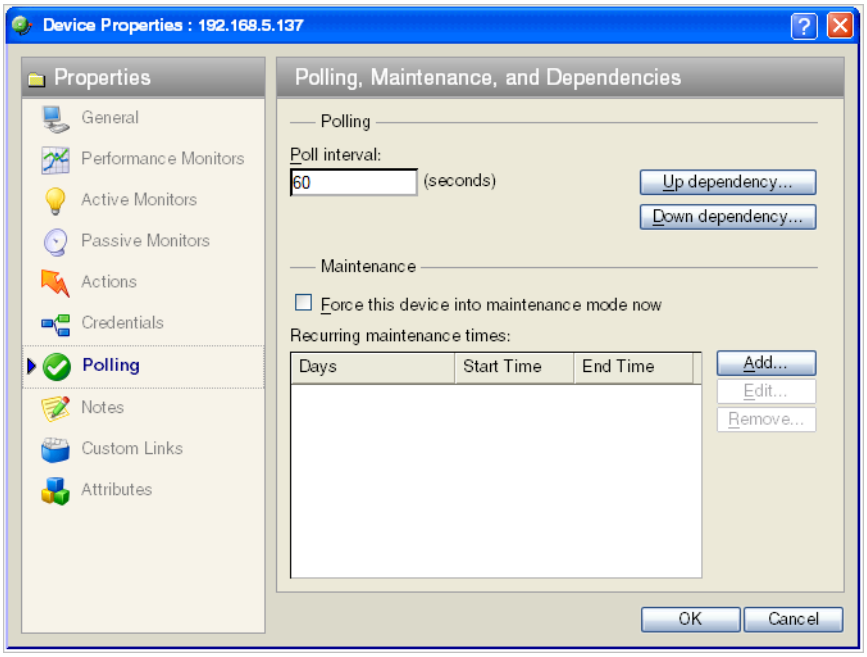
Devices that are SNMP manageable devices appear on the map view with an icon with a white star in the top right corner.

- **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**. 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.
- **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 85).

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.

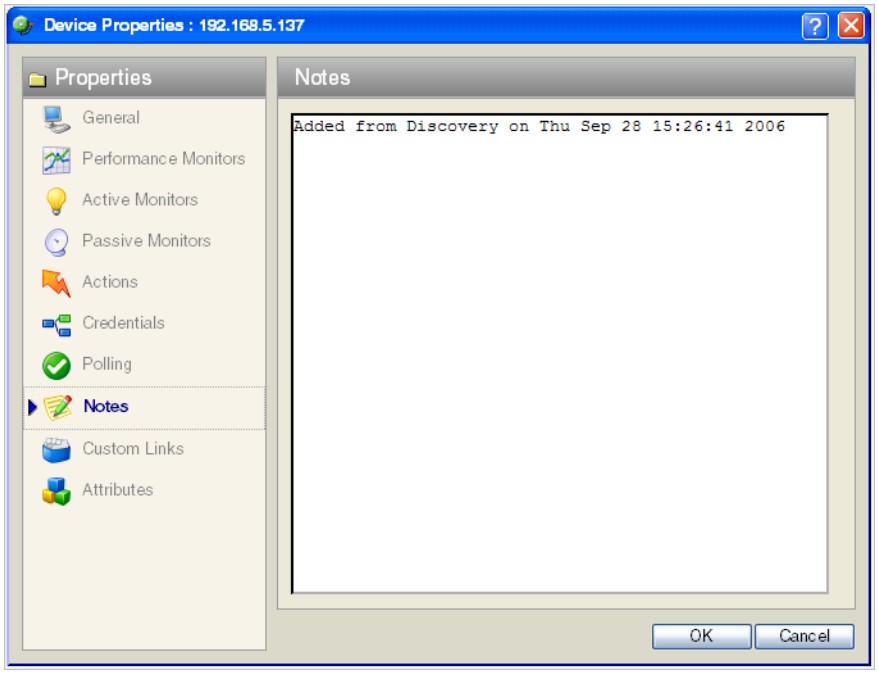
- **Force this device into maintenance mode now**. Select this option to put the selected device in maintenance mode. Clear the option to resume polling the device.
- **Recurring maintenance times**. This box displays all scheduled maintenance times for the device.
  - Click **Add** to schedule a new maintenance time for the device.
  - Select an entry, then click **Edit** to change a scheduled time.

- Select an entry, then click **Remove** to delete a scheduled time.

For more information, see Polling Overview (on page 87) and Dependencies Overview (on page 89).

About Device Property Notes

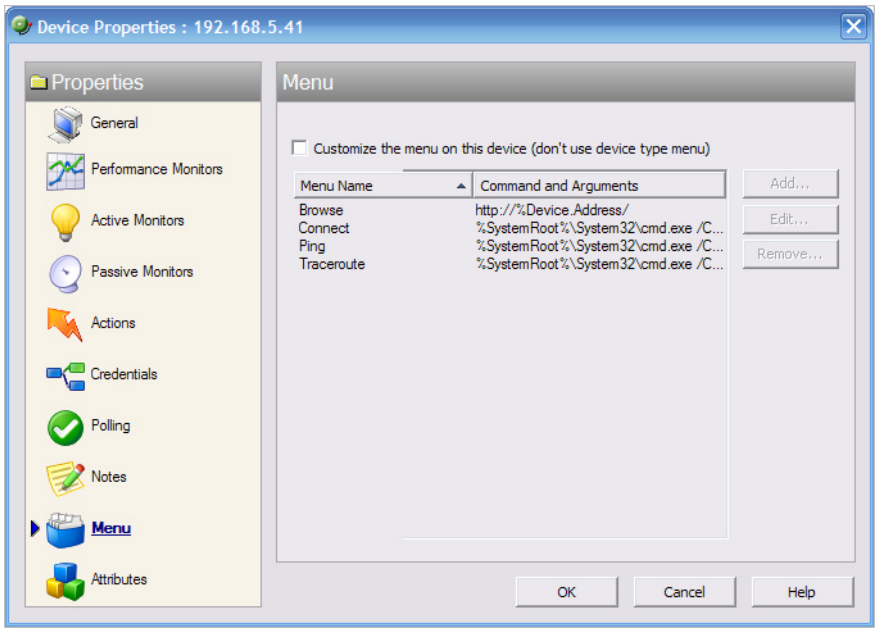
The Notes dialog provides an option to enter free-form messages to the device database.



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.

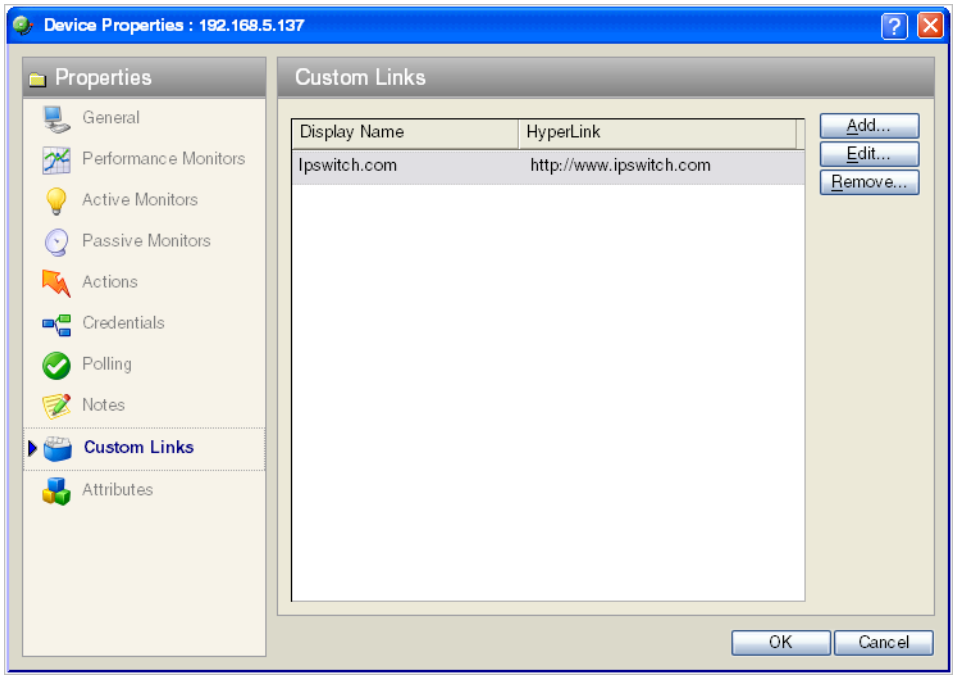


- **Customize the menu on this device (don't use device type menu)**. Select this option to create and/or modify a context menu for this device. This will override any separate context menu that has already been created for the device type of the device.
- **Menu list**. This box displays the commands that are currently configured for the device. After an item has been configured, it appears context (right-click) menu. When you click the menu item, the menu item is executed.
  - Click **Add** to add a new menu item.
  - Select an item, then click **Edit** to change the settings.
  - Select an item, then click **Remove** to remove it from the list.

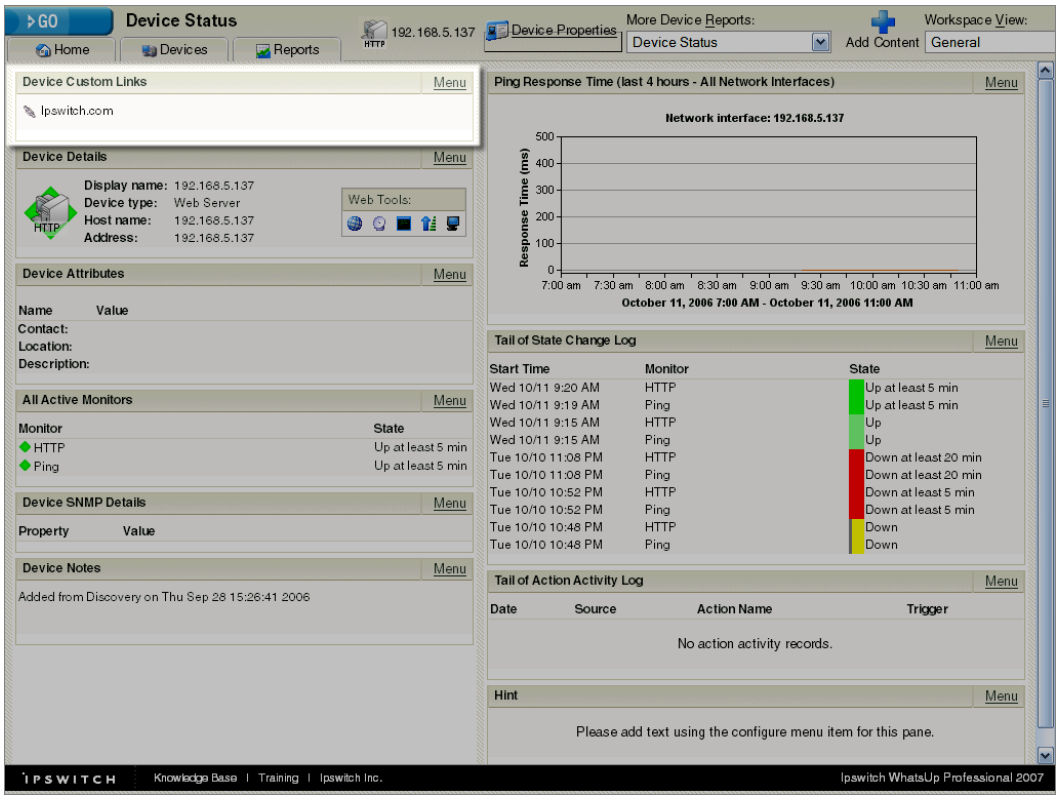
Important: Menu items configured in the console are not visible in the web interface. Custom links created in the web interface are not visible here in the console.

About Device Property Custom Links

In the WhatsUp Gold web interface, you can use this dialog to create a custom link for a device.



After a Custom Link has been configured and added to the Device Status workspace page, it appears in the Device Custom Links report on the Device Status page for the selected device. For more information, see Adding workspace reports to a Device Status workspace (on page 214).

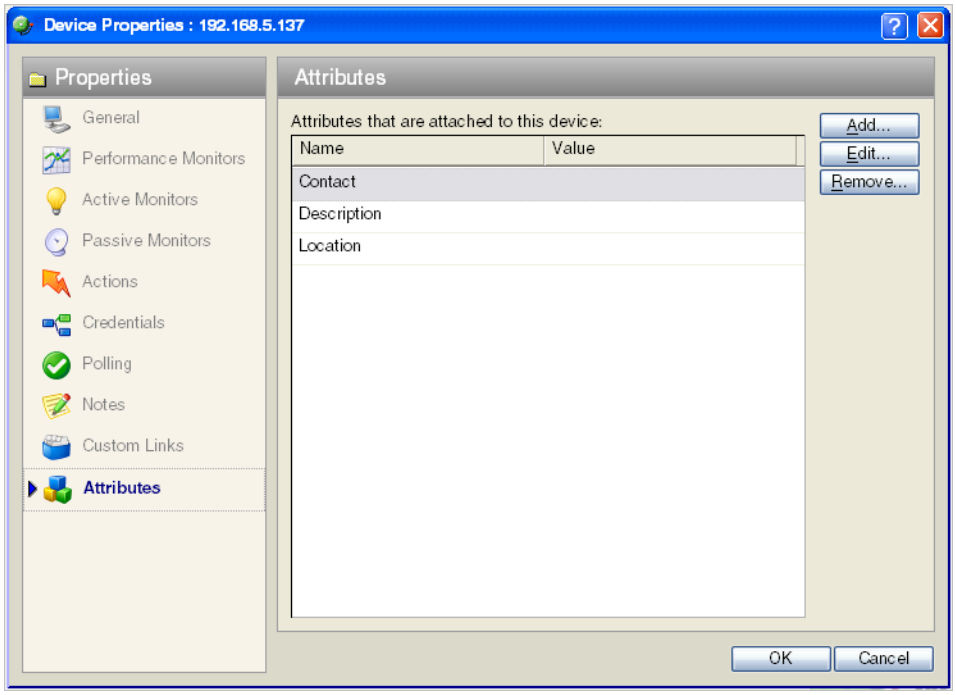


- Click **Add** to add a new custom link.
- Select a custom link in the list, then click **Edit** to change the settings.
- Select a custom link in the list, then click **Remove** to remove it from the list.

Important: Custom links created in the web interface are not visible in the console. Menu items configured in the console are not visible 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 attributes in the list are added by WhatsUp Gold when the device is added to the database, either by the Device Discovery wizard, or through another means.



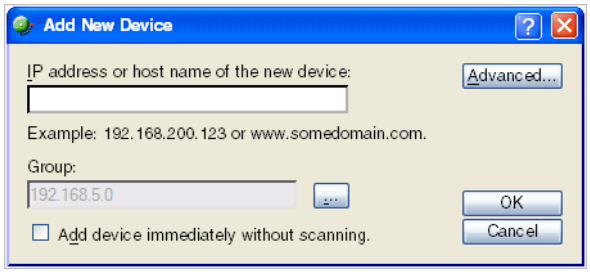
Adding a new device

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 29).
- 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.

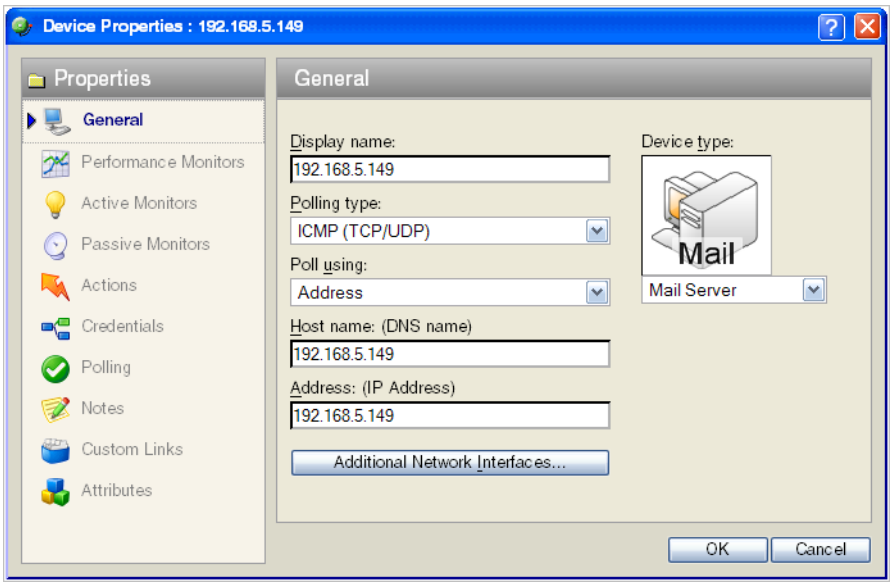
5 Click **OK** to save changes. The WhatsUp Gold attempts to resolve the IP address or hostname, then scans that device for Active Monitors. When the scan is complete, Device Properties dialog opens, allowing you to further configure the device as needed.

Adding additional network interfaces to a device

To configure a network interface:

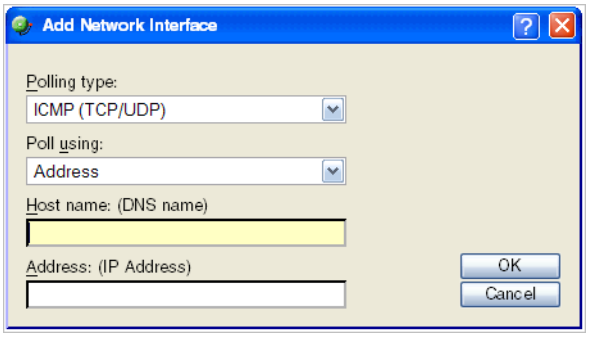
1 Right-click a device, then click **Properties**. The Device Properties dialog opens.

2 Click **General**. The General dialog opens.



3 Click **Additional Network Interfaces**. The Add Network Interfaces dialog opens.

4 Click **Add**. The Add Network Interfaces dialog opens.



5 Enter the network information for the new interface.

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

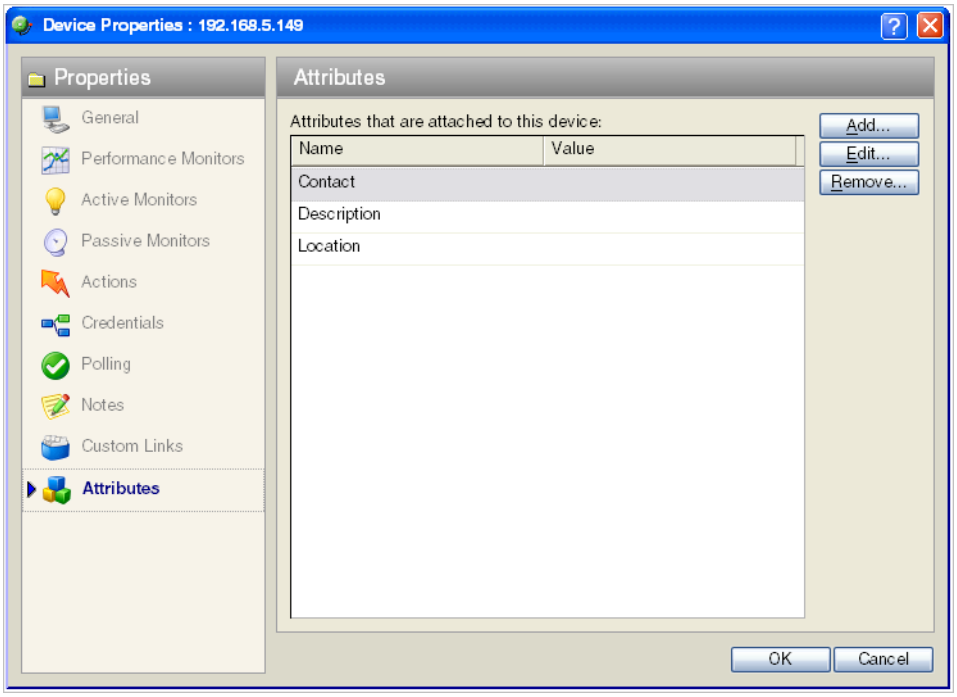
To change the default network interface on a device:

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 opens.
2. Click **Attributes**. The Attributes dialog opens.



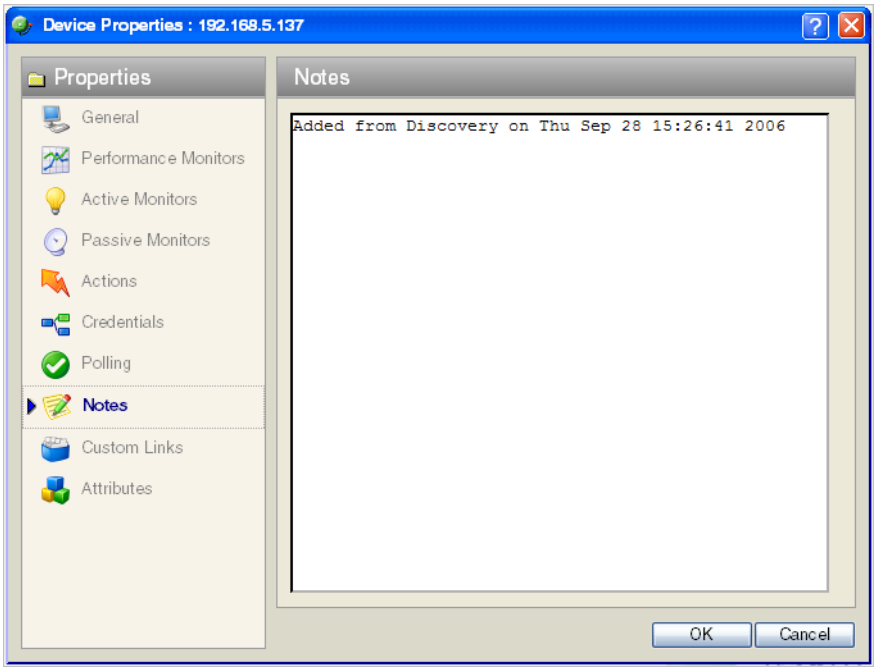
3. Use the following options:
   - Click **Add** to add a new device attribute. The Add Attribute dialog opens.
   - Select a device attribute in the list, then click **Edit** to change the settings.
   - Select a device attribute in the list, then click **Remove** to remove it from the list.
4. Enter 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 opens.

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. If viewing the notes on a shortcut, the date and time the device was added to the database is displayed.

  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

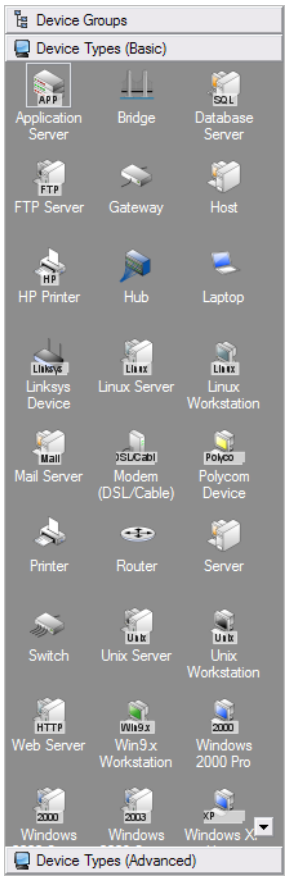
Changing the name of a device changes how it appears in the list views.

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 63).

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. In the context menu, click **Properties > General**.
2. In the **Device type** list, select a new device type.
3. Click **OK** to save changes.

Organizing Device Groups

Device groups are organizational folders that let you quickly find and diagnose problems with devices in your database. You can organize these folders in any way that makes sense to you, so feel free to experiment with different configurations.

Map View

The Map View is based on the device group folders, meaning that you will have a different map for each device group. If a folder contains a subfolder, you can double-click on the folder in the map view to display the map in the subfolder.

Discovery

During discovery, device groups are created for each subnetwork that is found on the network that was scanned. At the top level of the My Network tree, the entire scan is contained in a folder identifying the type of scan that was made and the date the scan was made. Devices that are already in the database are added to the new scan tree 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 state change.

Device State

Each folder in the My Network tree has a device state indicator on the folder icon. This indicator shows the worst state across all of the devices contained in that folder.

-  All monitors on all devices are up.
-  At least one monitor is down.

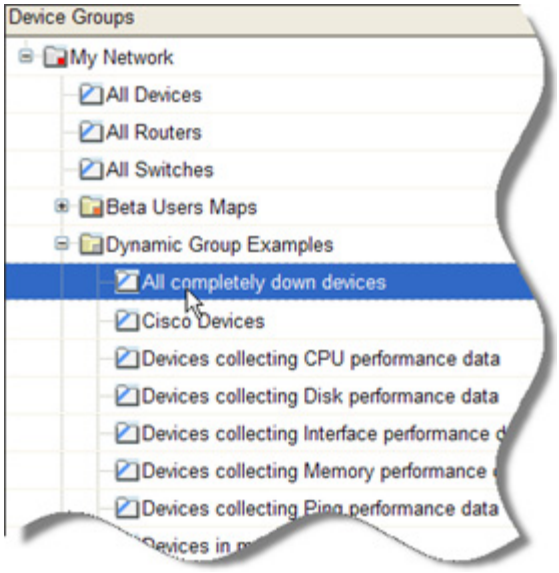
Renaming a Device Group

- In the console, right-click on the group in the My Network tree or Device View, then select **Rename**.
- In the web interface, right-click on the group in the My Network tree or Device View, click **Properties**, then change the name in the Group Name box.

Using 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 Dynamic Group dialog opens.
2. 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.
3. 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.ipswitch.com/Support/whatsup_professional/index.asp).

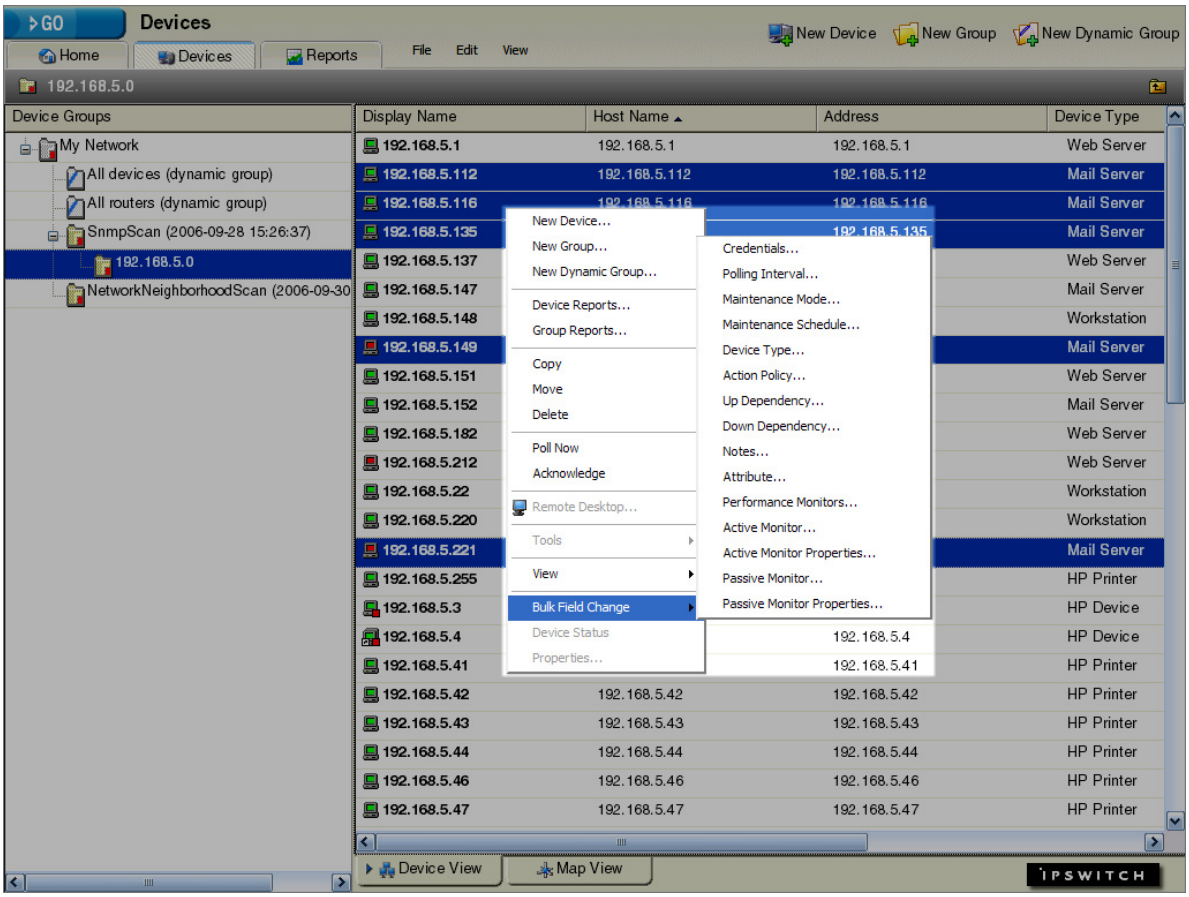
Editing multiple devices with Bulk Field Change

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 opens.

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.

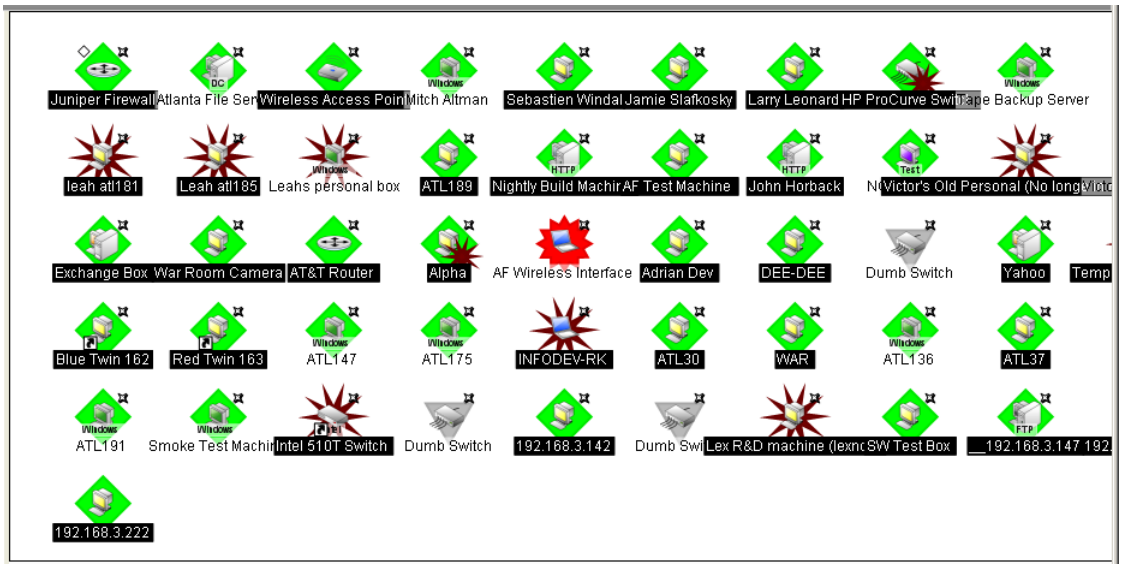
- Credentials
- Polling Interval
- Maintenance Mode
- Maintenance Schedule (web interface only)
- Device Type
- Action Policy
- Up Dependency
- Down Dependency
- Notes
- Attribute
- Performance Monitors
- Active Monitor
- Active Monitor Properties
- Passive Monitor (web interface only)
- Passive Monitor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

3 Enter the configuration information that you want set.

4 Click **OK** to save changes.

Using 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 the 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**.

Credentials Overview

The Credentials system stores login or community string information for Windows (WMI Active Monitors and WMI Performance Monitors) 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 at **Go > 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.

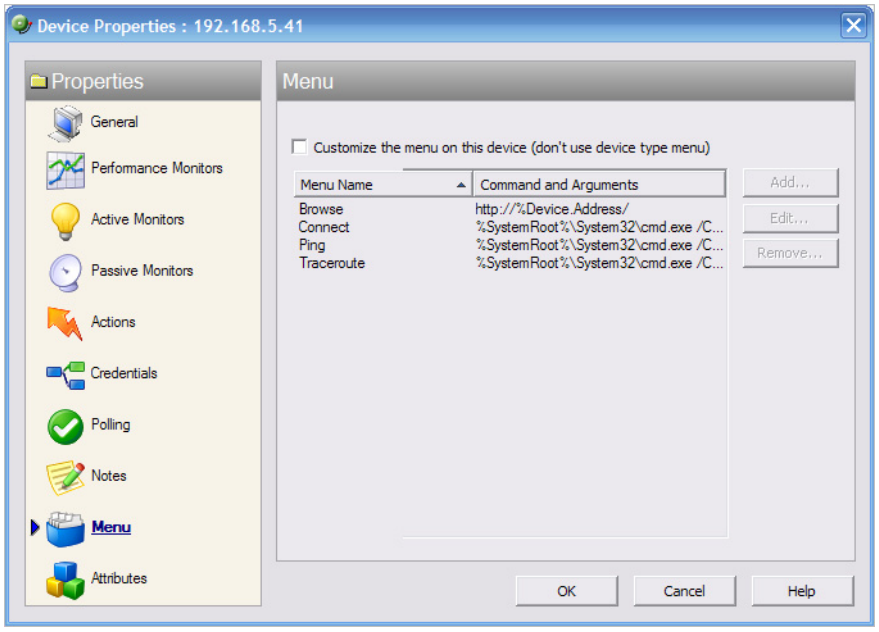
A device needs SNMP credentials applied to it before SNMP-based Active Monitors will work. Similarly, NT Service Checks must have Windows credentials applied.

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-mouse 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 opens.



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 opens.
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.

CHAPTER 7

About Polling

In This Chapter

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 the 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 be 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  .

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 or not.

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 dependant on the status of another device's active monitor(s) in your database.

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 describing that 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 describing that 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 that router's ping attempts are successful. Should the router's ping active monitor fail, the devices behind the router will be placed in the unknown state. Without the dependency, the devices behind the router would fire off actions when they become unreachable due to the router's failed ping attempts. With the dependency, only actions on the router will fire.

Setting Dependencies

There are two ways to set dependencies in WhatsUp Gold:

- Using Device Properties

  Double-click on a device in My Network view (**View > Device View**) to display Device Properties, and click the Polling Icon. Click either the Up **Dependencies...** or the **Down Dependencies...** button to bring up the Device Dependencies dialog and configure the up or down dependency.

- Using the Map View

  In My Network view, go to **View > Map View**. Right-click on a selected device and select **Set Dependencies** and either **Set Up Dependency on** or **Set Down Dependency on**. The cursor changes to the Set Dependency arrow. Click on any device in the current group to set the dependency. Selected **Display > Polling Dependency Arrows** to view the dependency between the two devices.

In the Map View, you are not able to set dependencies across groups. However, you can make shortcuts to the devices you want to set dependencies on in a group, and set the dependencies there.

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 is signified with a upward green arrow icon, while down dependencies is signified with a downward red arrow.

- Checking the first box on the dialog 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 are setting.
- To select a device for the dependency, click the **Browse (...)** button.
- Choose either **All active monitors** or **Specific active monitors** and check the active monitors you want to associate with the dependency.

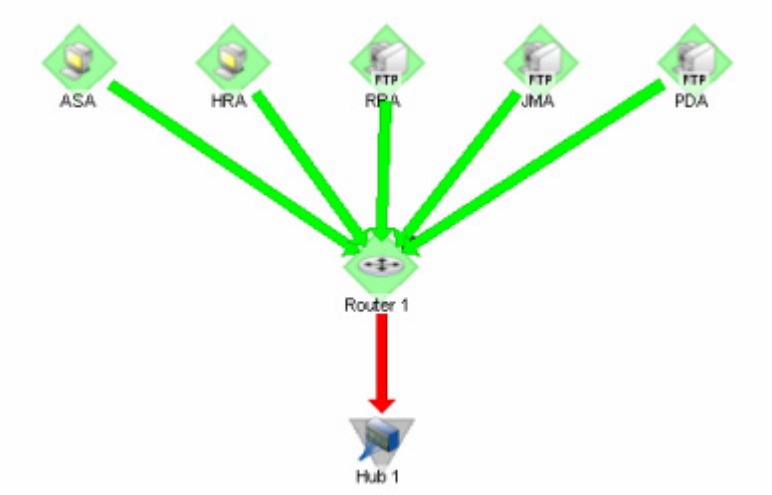
The statement at the bottom of the dialog is automatically generated for you to assist you in understanding the type of dependency you are creating.

An example statement would read:

"ATL145 is dependent on QATEST-WIN2K's FTP and HTP and Ping active monitors being up. (ATL145 is "behind" QATEST-WIN2K.)"

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 will have to refer to the Polling section of Device Properties to view the dependencies.



In the graphic 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 were to 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 WhatsUp Gold console (the system on which you installed WhatsUp Gold).

To add the IPX protocol:

1. Open the Network applet in the Windows Control Panel.
2. If you are using Windows NT, in the **Select Network Protocol** dialog box, select Microsoft, then select the IPX/SPX-compatible Protocol and follow the online instructions.

   - or -

   If you are using Microsoft Windows 2000 or XP, in the **Select Network Component** dialog box, select Microsoft, then select the IPX/SPX-compatible Component and follow the online instructions.

CHAPTER 8

Using Actions

In This Chapter

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 e-mail 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. Activate a beeper.
- Pager Action. Send a message to a pager.
- Program Action. Run another program (executable) to take some action.
- Email Action. Send an SMTP mail message.
- Winpop Action. Display a message in a pop-up window on a Windows NT system.

- SMS Action. Send a Short Message Service (SMS) notification to a pager or cell phone.
- Service Restart Action. Stop or restart a Windows NT system.
- Syslog Action. Send a message to a host that is running a Syslog server.
- Text to Speech Action. Send a text-to-speech notification to a speaker.
- Sound Action. Sound 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. Be aware that Ipswitch does not support the scripts that you create, only the ability to use them in the Script Action.
- Web Alarm. Sound an alarm by playing a sound file on the WhatsUp Gold web interface.

About Action strategies

When configuring actions for your devices and monitors, there are a few things you should take 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 (on page 89) 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 need to be 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 (on page 118) 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.

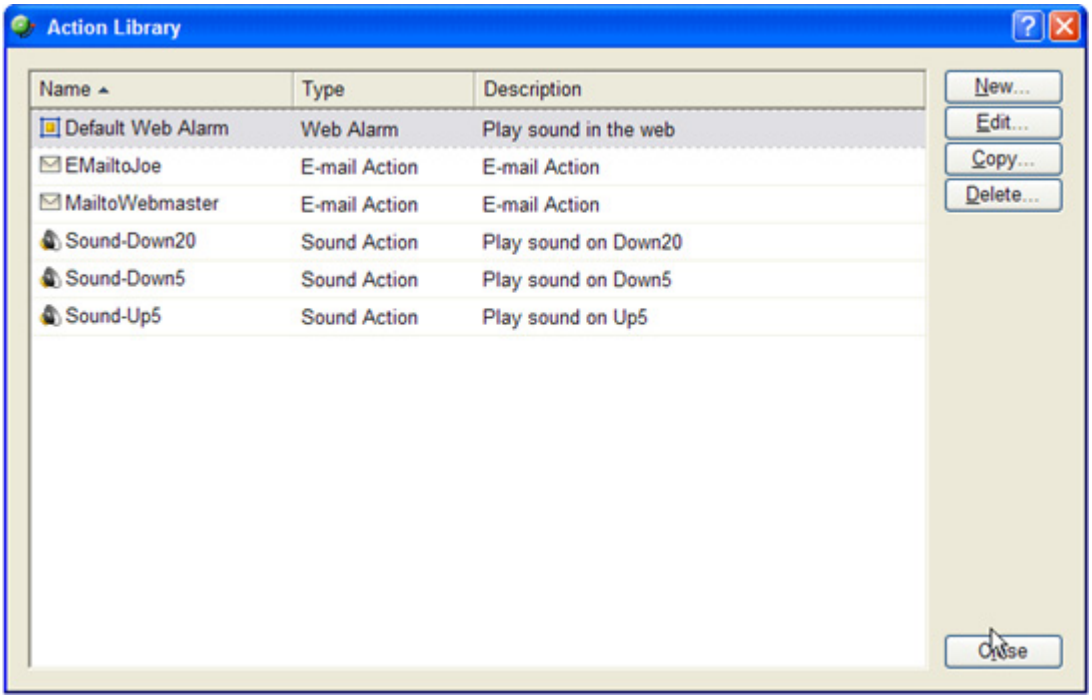
Unless the device is vital to the operations of the business or office, the state change color and shape should be enough to let you know what is going on with your monitored devices.

- 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.

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 associated 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
- SMTPMail
- Syslog
- Text to Speech
- WinPopup
- Web Alarms
- Action Script

- **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 and 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 removed 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 that the action is assigned to. 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.

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 has been 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 112)
- Assigning an Action to a Monitor (on page 112)
- Creating a Custom Action Policy (on page 118)

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

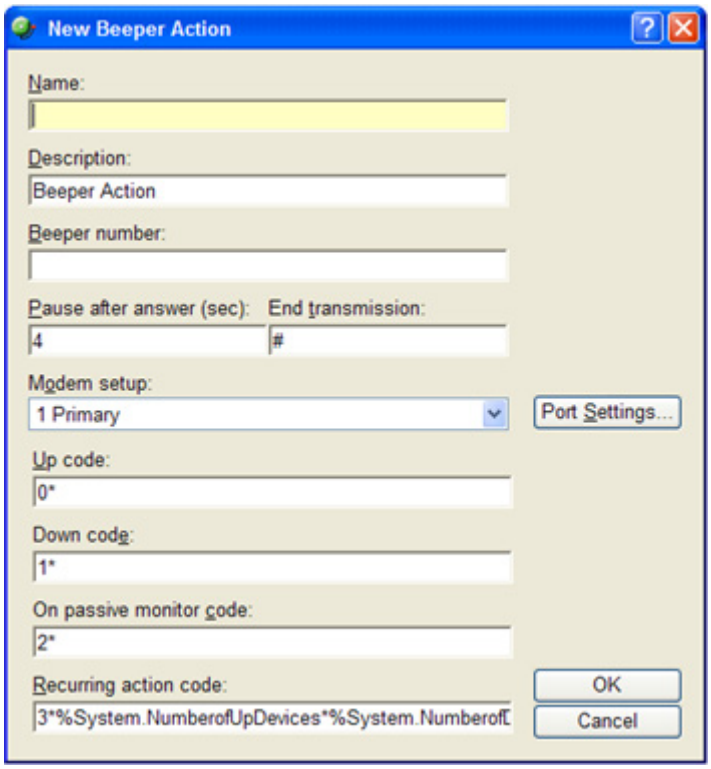
Creating a Beeper Action

1. Go to the Action Library:
   - In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

     - or -
   - From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.
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 opens.



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 the **Name** box.
- **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 (on page 115) 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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)

Assigning an Action to a Monitor (on page 112)

Creating a Pager Action

1. Go to the Action Library:
   - In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

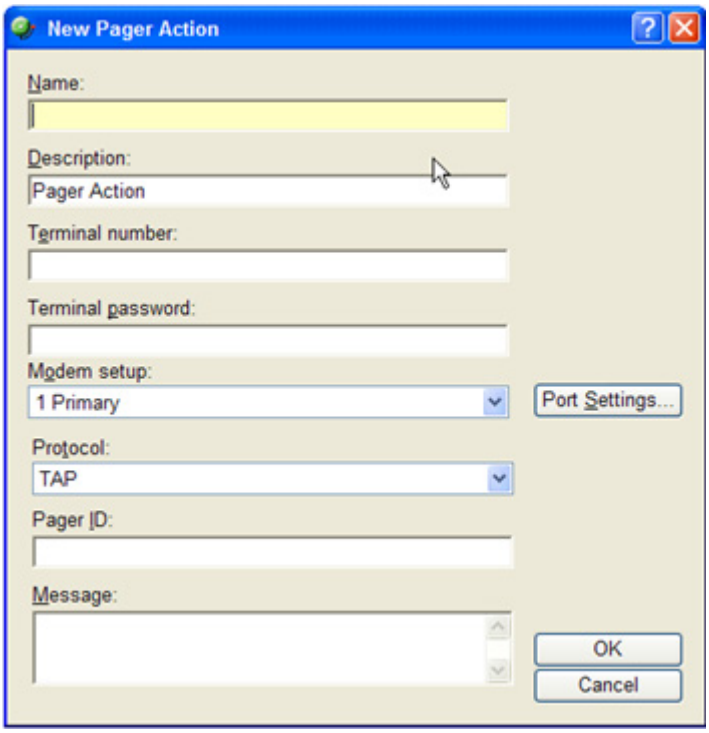
     - or -

   - From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.
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 opens.



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 (on page 115) 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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating an E-mail Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

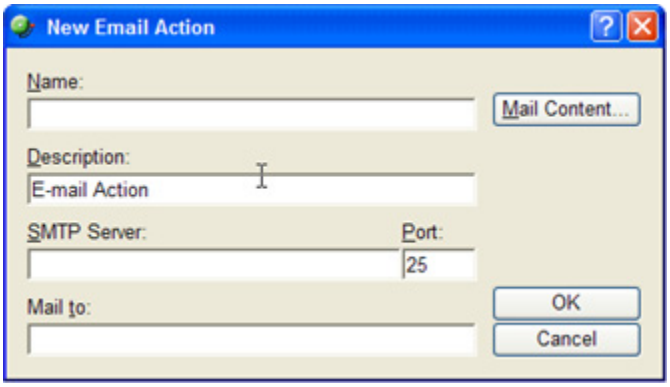
2 In the Action Library, do one of the following:

- Click **New**, then select **E-mail Action**.

  - or -

- Select an existing E-mail Action, then click **Edit**.

The action properties page opens.



3 Enter the e-mail 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 with the **Name** box.
- **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.
- **Mail To**. Enter the email addresses you want to send the alert to. Email addresses must be fully qualified. Two addresses may be entered, separated by commas (but no spaces). The address should not contain brackets, braces, quotes, or parentheses.

4 Click **Mail Content**. Enter the content of the e-mail alert.

- **From**. Enter the email address that will appear in the From field of the email that is sent by the E-Mail action.
- **Subject**. Enter a text message or edit the default message. You can use any of the percent variable codes. (on page 115)
- **Message body**. Enter a text message or edit the default message. You can use any of the percent variable codes. (on page 115)

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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating an SMS Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

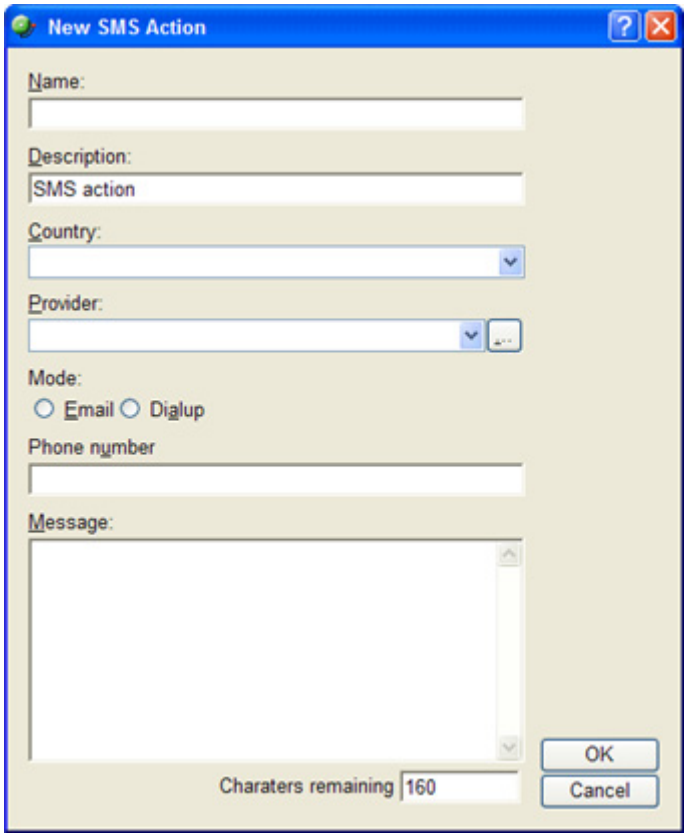
2 In the Action Library, do one of the following:

- Click **New**, then select **SMS Action**.

  - or -

- Select an existing SMS Action, then click **Edit**.

  The action properties page opens.



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 with the **Name** box.
- **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.
- **Message**. Enter a text message plus any desired percent variable codes (on page 115).

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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating a WinPopup Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

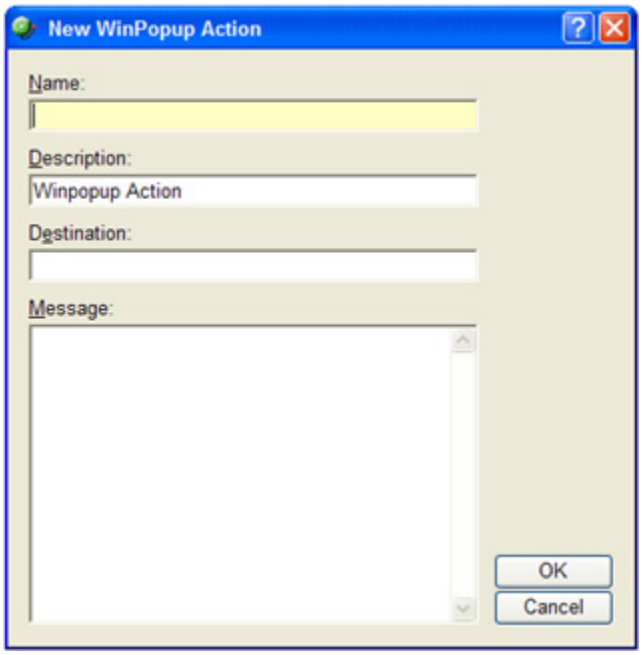
2 In the Action Library, do one of the following:

- Click **New**, then select **WinPopup Action**.

  - or -

- Select an existing WinPopup Action, then click **Edit**.

  The Action Properties page opens.



3 Set the appropriate options.

- **Name**. Enter an identifying name for this winpop action.
- **Description**. Enter a short description of the action. This is displayed in the Action Library along with the entry in with the **Name** box.

- **Destination**. Specify the Windows NT host or domain that you want to receive this notification.
- **Message**. Enter a text message using percent variables (on page 115) if needed.
- **Refresh**. Click this button to refresh the **Destination** list. This populates the list with all of the targets you can choose to send a winpop action to.

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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating a Syslog Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

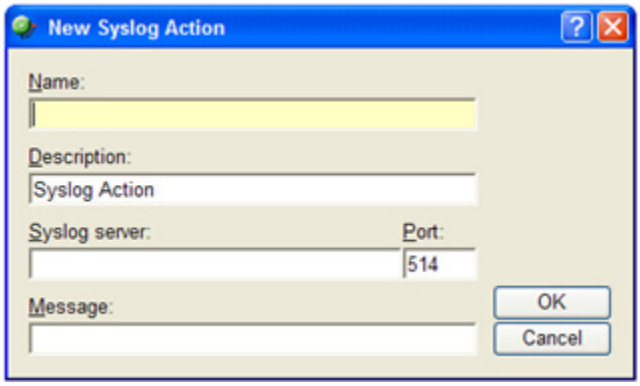
2 In the Action Library, do one of the following:

- Click **New**, then select **Syslog Action**.

  - or -

- Select an existing Syslog Action, then click **Edit**.

  The action properties page opens.



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 with the Name box.
- **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 (on page 115). 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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating a Text-to-Speech Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

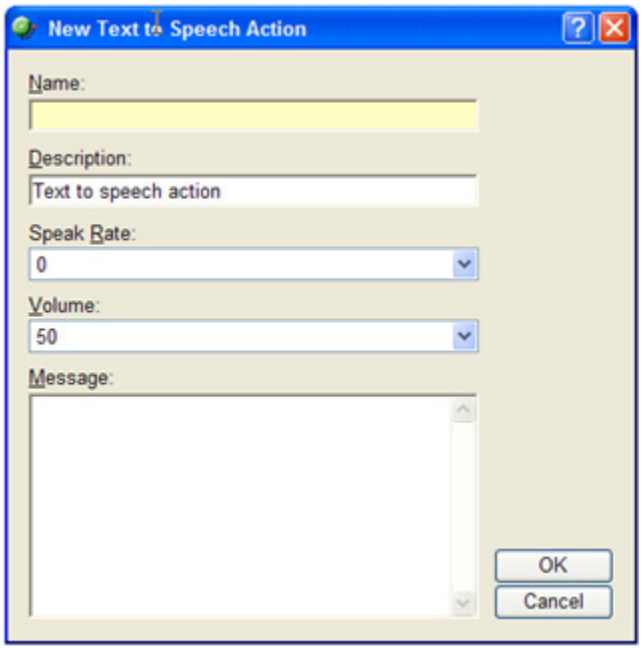
2 In the Action Library, do one of the following:

- Click **New**, then select **Text-to-Speech Action**.

  - or -

- Select an existing Text-to-Speech Action, then click **Edit**.

  The action properties page opens.



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 with the **Name** box.
- **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 (on page 115).

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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating a Program Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

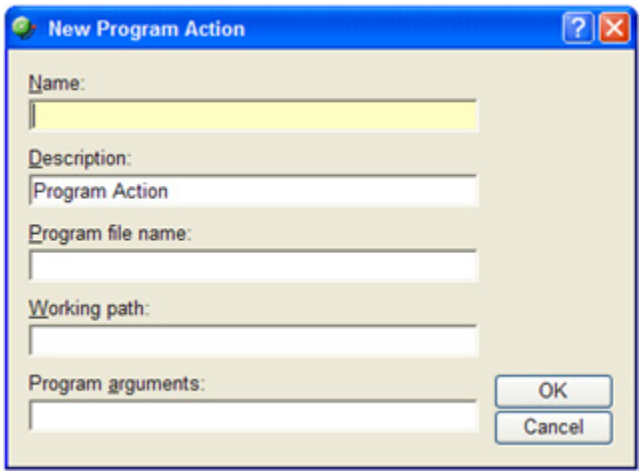
2 In the Action Library, do one of the following:

- Click **New**, then select **Program Action**.

  - or -

- Select an existing Program Action, then click **Edit**.

  The action properties page opens.



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 with the **Name** box.
- **Program filename**. Enter the executable name of the application you want to launch. Use the folder button to help you do this.
- **Working path**. Specify a directory where the working files for the application are stored. Use the folder button to help you do this. The working path is located on the server where WhatsUp is running.
- **Program arguments**. Enter any percent variables (on page 115) 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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating an Active Script Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

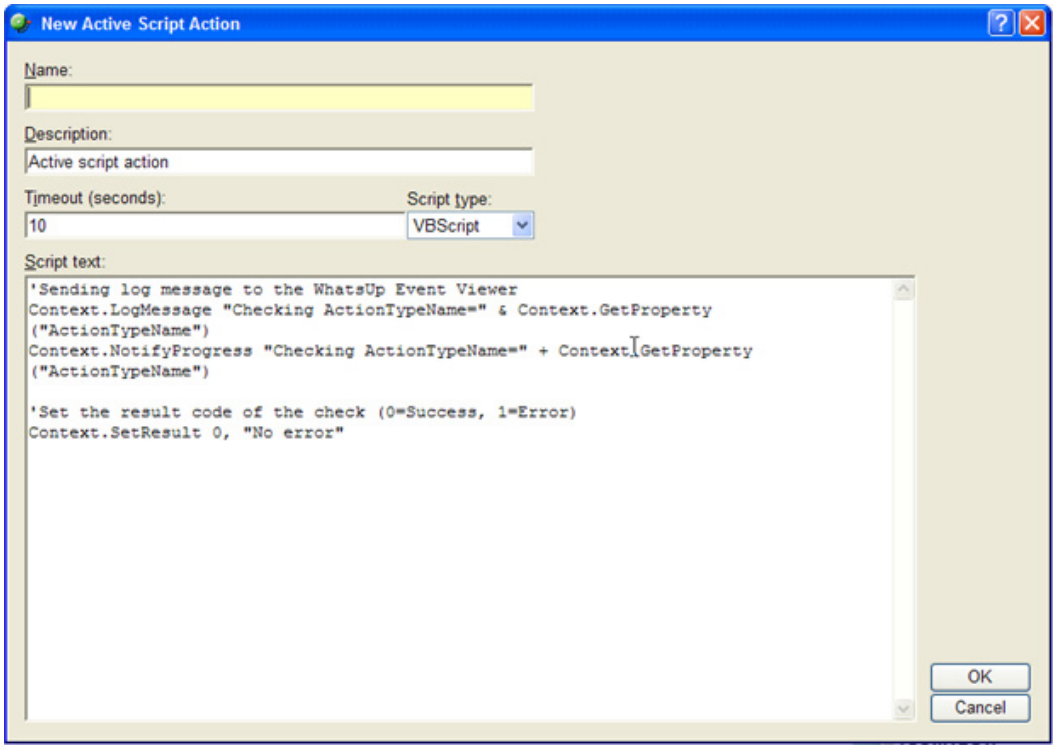
2 In the Action Library, do one of the following:

- Click **New**, then select **Active Script Action**.

  - or -

- Select an existing Active Script Action, then click **Edit**.

The action properties page opens.



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.** 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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

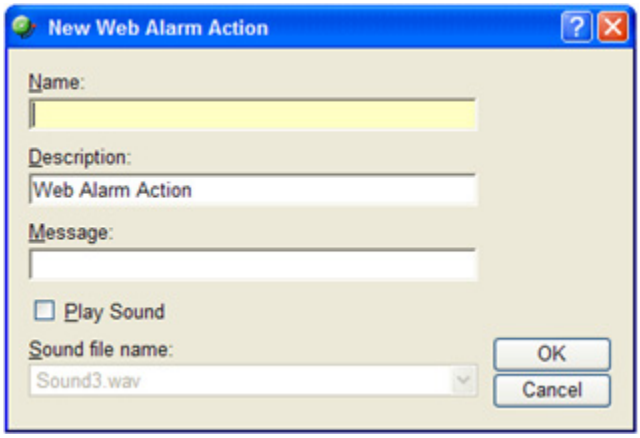
Creating a Web Alarm Action

1. Go to the Action Library:
   - In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

     - or -
   - From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.
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 opens.



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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

Creating a Service Restart Action

1 Go to the Action Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Action Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Action Library**.

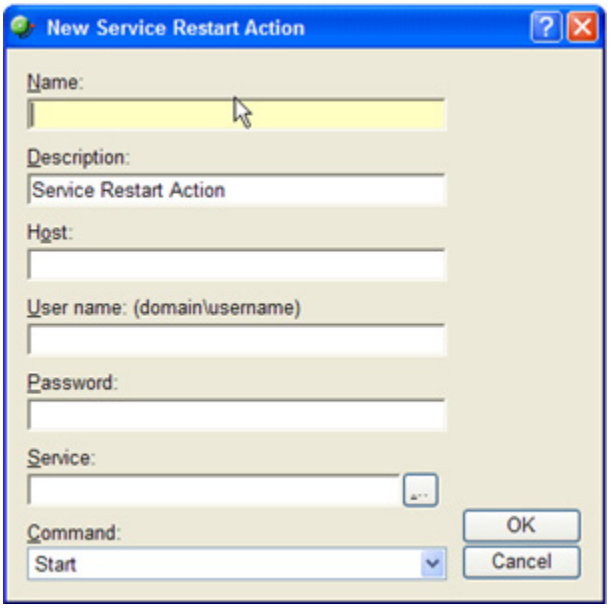
2 In the Action Library, do one of the following:

- Click **New**, then select **Service Restart Action**.

  - or -

- Select an existing Service Restart Action, then click **Edit**.

  The action properties page opens.



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 in the Name box**.**
- **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 v11 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, by using the procedure defined in:

- Assigning an Action to a Device (on page 112)
- Assigning an Action to a Monitor (on page 112)

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 opens.
2. Click **Actions**. The Actions dialog opens.
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 opens.
2. Click **Actions**. The Actions dialog opens.
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.

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 opens.

2 Click **Active Monitors**. The Active Monitors dialog opens.
3 Double-click the monitor you want to add actions to.
4 Go to the Actions properties:
   - In the web interface, in the Active Monitor Properties wizard, click **Next**.

     - or -

   - In 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 the Active Monitor is configured on, then click **Properties**. The Device Properties dialog opens.
2 Click **Active Monitors**. The Active Monitors dialog opens.
3 Double-click the monitor you want to add actions to.
4 Go to the Actions properties:
   - In the web interface, in the Active Monitor Properties wizard, click **Next**.

     - or -

   - In 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 Passive Monitor is configured on, then click **Properties**. The Device Properties dialog opens.
2 Click **Passive Monitors**.
3 Double-click the monitor you want to add actions to. The Passive Monitor Properties open.
4 Go to the Actions properties:
   - In the web interface, in the Passive Monitor Properties wizard, click **Next**.

     - or -

   - In the console, the Passive Monitor dialog opens.

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.

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.
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
%ActiveMonitor.Argument	SNMP instance number. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.Comment	The human readable name that coincides with the network switch This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.Name	The name of the active monitor that fired an action. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.NetworkInterfaceAddress	IP address for the network interface. This is only used when an action is associated directly with an active monitor, and not the device as a whole.
%ActiveMonitor.Payload	The payload returned by a WMI, Exchange, SQL, or SNMP active monitor. This is only used when an action is associated directly with an active monitor and not the devices as a whole.
%ActiveMonitor.State	The Current status of the monitor, such as "Down at least 5 min." This is only used when an action is associated directly with an active monitor, and not the device as a whole.

Device Variables	Description
%Device.ActiveMonitorDownNames	List of down services using the abbreviated name if available.
%Device.ActiveMonitorUpNames	Full service names of all UP monitored services on a device.
%Device.Address	IP address (from device properties).

%Device.Attribute.[Attribute Name]	Returns an attribute from the SNMP information available for the device, such as the Contact name. To specify the attribute, append the category name (listed below) to the end of the variable. For example: %Device.Attribute.Contact, returns the contact name. Default categories: · *****. Returns all attributes · **Info1**. Upgrade path from v8 · **Info2**. Upgrade path from v8 · **Contact**. Contact information from SNMP · **Location**. Location information from SNMP · **Description**. Description information from SNMP · Custom. If you have created a custom attribute you can use the name of that custom attribute in the percent variable. Example: %Device.Attribute.Phone %Device.Attribute.RackPosition To avoid an error, when placing %Device.Attribute in quotation marks, place a space between the last letter and the closing quotation mark. Example: "%Device.Attribute.Contact "; correct "%Device.Attribute.Contact"; incorrect
%Device.DatabaseID	Returns the database ID of a device.
%Device.DisplayName	Display Name (from General of device properties)
%Device.HostName	Host Name (from General of device properties)
%Device.Notes	Notes. (Notes are from the device properties Notes)
%Device.SNMPOid	SNMP Object identifier.
%Device.State	The state's description (such as "Down at least 2 min" or "Up at least 5 min")
%Device.Status	This shows the name of the active monitor, preceded by the device state id : 10|DNS
%Device.Type	Device Type (from General of device properties)

Passive Monitor Variables	Description
%PassiveMonitor.DisplayName	The name of the monitor as it appears in the Passive Monitor Library.
%PassiveMonitor.LoggedText	Detailed Event description. (SNMP traps - Returns the full SNMP trap text.) (Windows Log Entries - Returns information contained in the Windows Event Log entries.) (Syslog Entries - Returns the text contained in the Syslog message.)
%PassiveMonitor.Payload.*	Payload generated by a passive monitor.
%PassiveMonitor.Payload.EventType	The type of passive monitor (Syslog, Windows Event, or SNMP Trap)

System Variables	Description
%System.Date	The current system date. Configure the date format in Regional Options (from Program Options)
%System.DisplayNamesDownDevices	Display names of devices with down monitors
%System.DisplayNamesDownMonitors	Shows the name of a device and each monitor that is down on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping
%System.DisplayNamesUpDevices	Display names of up devices
%System.DisplayNamesUpMonitors	Shows the name of a device and each monitor that is up on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping
%System.InstallDir	Displays the directory on which WhatsUp Gold is installed
%System.NumberofDownDevices	Number of down devices on your network
%System.NumberOfDownMonitors	Shows the number of down monitors on your network
%System.NumberofUpDevices	Number of up devices on your network
%System.NumberOfUpMonitors	Shows the number of up monitors on your network
%System.Time	The current system time. The format is hh:mm:ss

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 118)
- Editing Action Policies (on page 119)
- Implicit Action Policy (on page 119)

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. From the menu bar, select **Configure > Action Policies**. The Action Policies dialog opens.
2. On the Action Policies dialog, click **New**.
3. In the New Action Policy dialog, enter a name in the **Policy name** box. 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 by using the procedure defined in:
   - Assigning an Action to a Device (on page 112)
   - Assigning an Action to a Monitor (on page 112)

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. From the main menu, select **Configure > Action Policies**. The Action Policies dialog opens.
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 and can be edited 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.

About 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. In the device list, the name of the device appears in bold, and in the map view, the device name appears on a black background.

After the device is in Acknowledgement mode, it will remain until you actively acknowledge it.

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 (on page 88).

To acknowledge a state change:

- Select the device or devices you want to acknowledge and right-click on a selected item. In the right-mouse menu, select **Acknowledge**.

  - or -

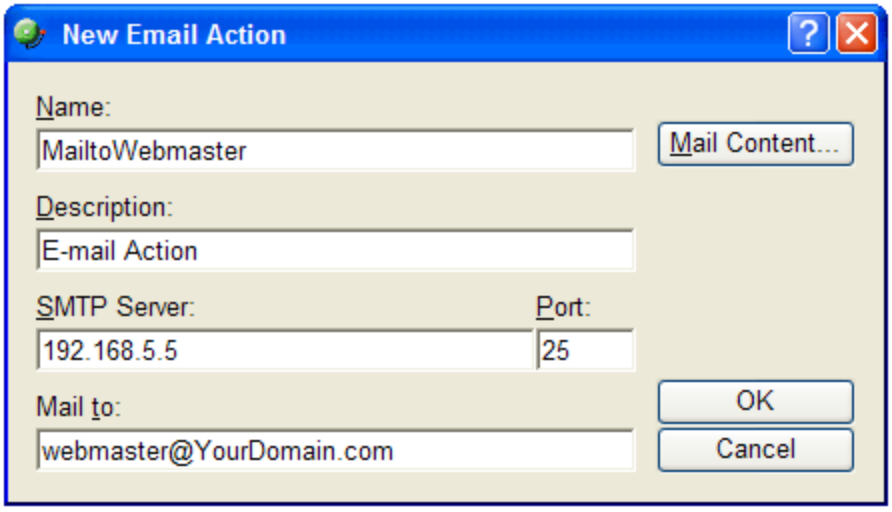
- Access the State Change Acknowledgement report and select the devices you want to acknowledge. After the devices are selected, click **Clear** to remove the devices from the report, thereby acknowledging the state change.

Example: getting an E-Mail Alert when the web server fails

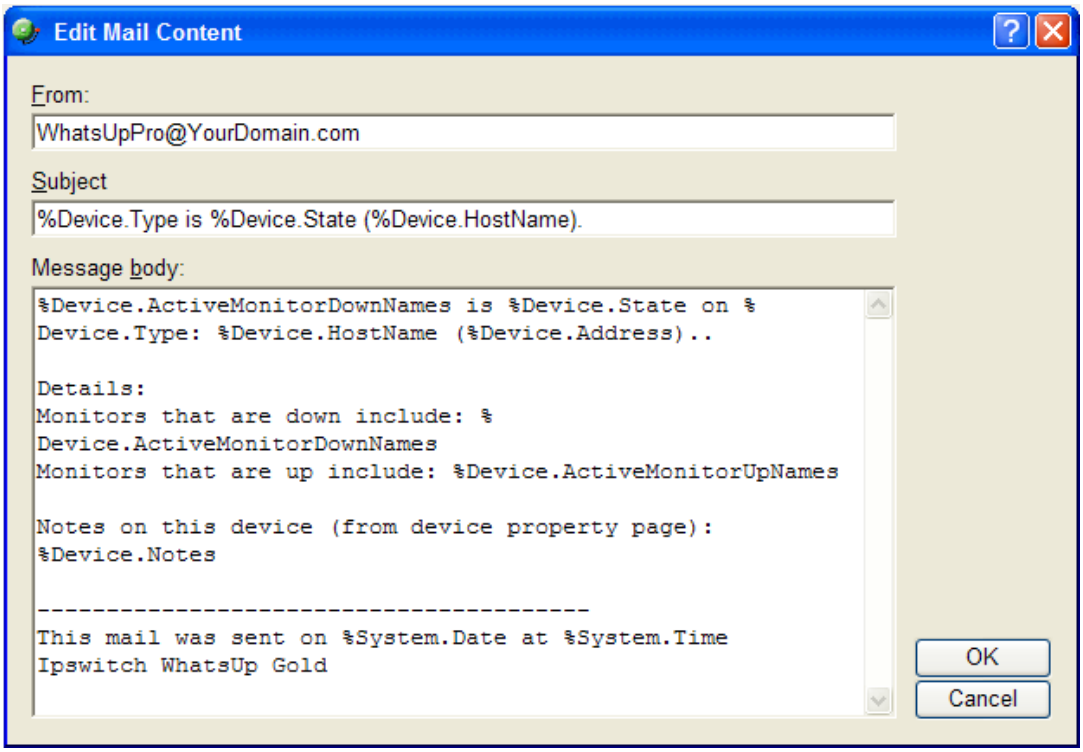
This example shows how to set up monitoring of your web server so that you get an email alert when the web server fails, or when web content is not available.

First, you need to set up the monitors for your web server. Then, create an email action and assign it to the monitors. Both tasks can be done within a wizard.

1. Open device properties for your web server device, then select the Active Monitor properties.
2. Click **Add**. The Active Monitor Properties wizard opens.
3. Use the wizard 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**.
   b) On the Set Polling Properties screen, click **Next**.
   c) On the Setup Actions for Monitor State Changes screen, select **Apply individual actions**, then click **Add**.
   d) On the Select or Create Action screen, select **Create a new action**, then click **Next**.
   e) On the Select Action Type screen, select **E-Mail Action**, then click **Next**.
   f) On the Select State Change screen, click **Finish**.
   g) On the New Email Action screen, then enter the information as shown:



h) Click Mail Content, then enter the information as shown:



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. Click **Finish**.

4 Use the same wizard to add the HTTP Content active monitor. This monitor checks that the web server returns some valid content in response to an HTTP request.

a) On the Select Active Monitor Type screen, select **HTTP Content**, then click **Next**.

b) On the Set Polling Properties screen, click **Next**.

c) On the Setup Actions for Monitor State Changes screen, select **Apply individual actions**, then click **Add**.

d) On the Select or Create Action screen, select **Select an action from the Action Library**, then click **Next**.

e) 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 screen.

f) Click **Finish**.

The two active monitors and resulting e-mail action are now enabled. When the web server is down for more than 2 minutes, HTTP active monitor will fail, triggering the e-mail action, which sends an e-mail message similar to the following:

If the web server could not return web content, the e-mail action would report:

along with any details or notes specified in the action.

CHAPTER 9

Using Active Monitors

In This Chapter

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:

- DNS Monitor
- NT Service Monitor
- Ping Monitor
- Active Script 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.

About Monitors and Actions

The Monitors and the Action systems work together in WhatsUp Gold to help you stay informed about what is happening on your network and the devices connected to your network. It is a cooperative relationship that can be configured to go well beyond the default setting included with the installation of the product. With some helpful examples and some creativity, a network administrator should be able to tailor the Monitors and Actions systems to watch over all of their important devices and troubleshoot problems that may arise.

Using Monitors and Actions

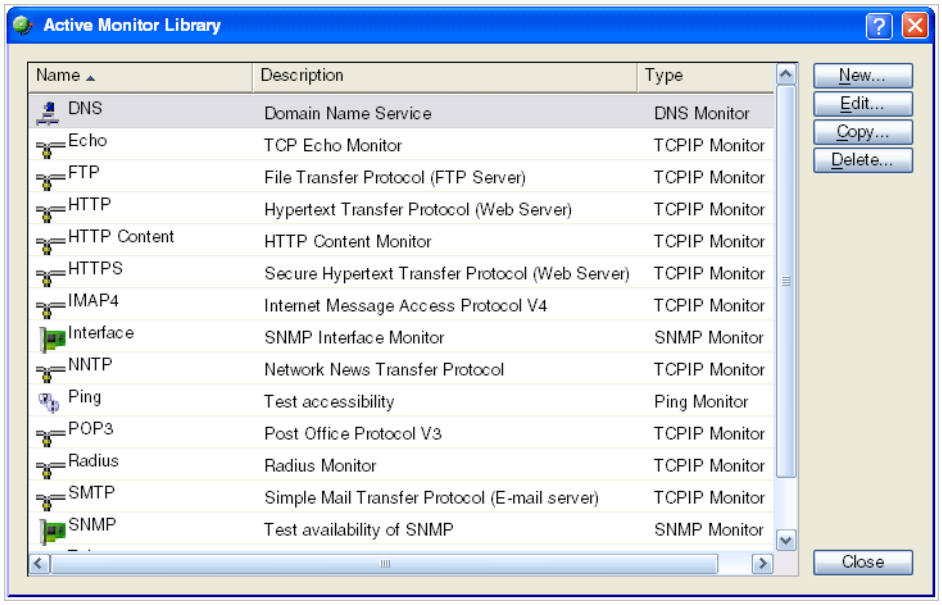
There are a few things to think about when you set up your Actions and Monitors. These will help you maximize the usefulness of the features and minimize problems.

- **Actions Coverage**. Set up your notification actions so that only the people that have to be notified are sent the alert. Consider creating vacation Action types that will not send alerts to people who cannot do anything about it.
- **Understanding SNMP**. It will take a little research, but when you find out which of your networked devices have SNMP capabilities, you can configure Monitors to listen for all types of information and trigger an Action accordingly.
- **Security Features**. Pay careful attention to your devices and services that are critical to the network security.
- **Network Resources**. WhatsUp Gold can be configured to perform an Action when your network resource availability diminishes across a certain threshold.
- **Assigning Actions to Devices or Monitors**. Assign actions to the device if you only want one notification when the device goes down. Assign an action to a specific Active Monitor if it requires special attention.

About the Active Monitor Library

The Active Monitor Library is the central storehouse of all Active Monitors that have been configured for your network. When changes are made to the Active Monitors listed in this dialog, the changes affect each instance of that particular monitor across your device groups.

Access the Active Monitor Library from the main menu of the WhatsUp Gold. In the web interface, click **Go > Configure > Active Monitor Library**.



This dialog is used to configure new or existing Active Monitor types. The list shows all types currently configured for use in WhatsUp Gold.

- Click **New** to configure a new type.
- Select an existing type, then click **Edit** to change the current configuration of a type.
- Select an ActiveMonitor type, then click **Copy** to make a copy of that type and add it to the list.
- 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.

- **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 the device. If the device does not respond, the monitor is considered down.
- **TCP/IP Monitor**. The TCP/IP monitor is used to monitor a TCP/IP service that either does not appear in the list of standard services or uses a non-standard port number.
- **NT Service Monitor**. The NT Service Monitor lets you check the status of a service on an 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 WhatsUp Professional, 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** lets 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 undergoes an unexpected rate of change.

For more information, see Using Ipswitch WhatsUp Gold v11 Premium Edition (on page 243).

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 an Active Monitor:

1 From the web interface main menu, click **Go > Configure > Active Monitor Library** to view the 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 opens.

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 add an Active Monitor to a device:

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

1 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.

2 In the Device Properties Active Monitor dialog, click **Discover**. WhatsUp Gold scans the device and creates a monitor for each network service found.

3 Manually assign an Active Monitor to the device:

a) In the Device Properties Active Monitor dialog, click **Add**. The Active Monitor Properties dialog opens.

b) Select the Active Monitor type you want to assignto the device, then click **Next**.

c) Set the polling properties for the monitor, then click **Next**.

d) Setup actions (on page 112) for the monitor state changes.

e) Click **Finish** to add the monitor to the device.

4 Add when you create a new device:

a) In the console click **File > New > New Device**. The Add New Device dialog opens.

- or -

In the web interface click **Go > Devices > New Device**. The Add New Device dialog opens.

b) Click **Advance**. The Device Discovery Properties dialog opens.

c) 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.

d) Click **OK**.

5 Use **Bulk Field Change** to add an active monitor to multiple devices:

a) Select the devices in the device list, then right-click on one of the selected items.

b) From the right-mouse menu, select **Bulk Field Change > Active Monitor**.

c) Select the active monitor type you want to add.

d) Click **OK**.

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 recommended 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 opens.
2. Select **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog box opens.
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.

- 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 opens.

   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 opens.
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 (on page 133)= keyword.
- To expect a string from a port, use the SimpleExpect (on page 134)= or the Expect (on page 131)= keyword.

- To comment out a line, use the # symbol as the first character of the line.
- To have conditional responses on "error" or "success" of a step within the scripts, use Flow Control Keywords (on page 132).

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 (on page 134) 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 (on page 136) 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
`\x##`	Binary value in Hexadecimal. For example, \x1B is escape
`\\`	The "\" character
`\t`	The tab character (\x09)
`\r`	The return character (\x0D)
`\n`	The new line character \x0A)

WhatsUp Gold versions 7 and 8 users: The %### decimal syntax for specifying binary octets has been replaced with the \x## hexidecimal syntax. Migrated definitions will be converted automatically.

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 (on page 131) 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
.	dot	Matches any one character
[...]	character class	Matches any character inside the brackets. Example, [abc] matches "a", "b", and "c"
[^...]	negated character class	Matches any character except those inside the brackets. Example, [^abc] matches all characters except "a", "b", and "c". See below for alternate use - the way ^ is used controls its meaning.
–	dash	Used within a character class. Indicates a range of characters. Example: [2-7] matches any of the digits "2" through "7". Example: [0-3a-d] is equivalent to [0123abcd]
\	escaped character	Interpret the next character literally. Example: 3\.14 matches only "3.14". whereas 3.14 matches "3234", etc.
\xnn	binary character	Match a single binary character. nn is a hexadecimal value between 00 and FF. Example: \x41 matches "A" Example: \x0B matches Vertical Tab

Quantifiers

Meta-character		Matches
?	question	One optional. The preceding expression once or not at all. Example: colou?r matches "colour" or "color" Example: [0-3][0-5]? matches "2" and "25"
*	star	Any number allowed, but are optional. Example: .* Zero or more occurrences of any character
+	plus	One required, additional are optional. Example, [0-9]+ matches "1", "15", "220", and so on
??, +?, *?		"Non-greedy" versions of ?, +, and *. Match as little as possible, whereas the "greedy" versions match as much as possible Example: For input string <html>content</html> <.*?> matches <html> <.*> matches <html>content</html>

Matching Position

Meta-character		Matches
^	caret	Matches the position at the start of the input. Example: ^2 will only match input that begins with "2". Example: ^[45] will only match input that begins with "4" or "5"
$	dollar	At the end of a regular expression, this character matches the end of the input. Example: >$ matches a ">" at the end of the input.

Other

Meta-character		Matches
|	alternation	Matches either expression it separates. Example: H|Cat matches either "Hat" or "Cat"
(...)	parentheses	Provides grouping for quantifiers, limits scope of alternation via precedence. Example: (abc)* matches 0 or more occurrences of the the string abc Example: WhatsUp (Gold)|(Professional) matches "WhatsUp Gold" or "WhatsUp Professional"
\0, \1, ...	backreference	Matches text previously matched within first, second, etc, match group (starting at 0). Example: <{head}>.*?</\0> matches "<head>xxx</head>".
!	negation	The expression following ! does not match the input Example: a!b matches "a" not followed by "b".

Abbreviations

Abbreviations are shorthand Meta-characters.

Abbreviation	Matches
\a	Any alphanumeric character: ([a-zA-Z0-9])
\b	White space (blank): ([\\t])
\c	Any alphabetic character: ([a-zA-Z])
\d	Any decimal digit: [0-9]
\D	Any non decimal digit [^0-9]
\h	Any hexadecimal digit: ([0-9a-fA-F])
\n	Newline: (\r|(\r?\n))
\p	Any punctuation character: ,./\';:"!?@#$%^&*()[]{}- _=+|<>!~
\P	Any non-punctuation character
\q	A quoted string: (\"[^\"]*\")|(\'[^\']*\')

\s	WhatsUp Gold style white space character [\\t\\n\\r\\f\\v]
\S	WhatsUp Gold style non-white space character [^ \\t\\n\\r\\f\\v]
\w	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 (on page 138) 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 Imail v1.3" back from the host, you could use "220 host" as a response string (i.e. `SimpleExpect=220 host`, or `Expect=^220 host`).

Note: Some services are based on binary protocols (such as DNS) and 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 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**. 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 (on page 146) that you can use to poll for specific information about the device in context.

We have provided several code samples (on page 139) for you to create useful active script monitors for your devices.

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 (on page 138) 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.

Monitor	Code

How to return the results of the script back to WhatsUp Pro.
 	
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"`

Logging a message to the WhatsUp Gold event viewer. Note: In order to view Context.LogMessage entries, you must have selected **Debug On** in the event viewer.	JScript: `Context.LogMessage("This is the message");`
Accessing the Device ID.	JScript: `var nDeviceID = Context.GetProperty("DeviceID");`
Accessing the IP address of the device.	JScript: `var sAddress = Context.GetProperty("Address");`

Accessing 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");`

Accessing the WhatsUp Pro database.	This sample uses the device ID in context and access 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");`
	`}`

Use WMI to see who is currently logged on a device.	You can set the monitor to be down if the logged on user is not the expected user. If no one is logged in, then it's also 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 " & _`

Use SNMP to monitor the total bandwidth utilization on an interface (in + 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 inteface indexed by nIfIndex.`
	`// ifSpeed is in bits per second.`
	`function getIfSpeed(nIfIndex)`
	`{`
	`var oResult = oSnmpRqst.Initialize(nDeviceID);`
	`if(oResult.Failed)`
	`{`
	`return null;`
	`}`
	`return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.5." + nIfIndex));`
	`// ifSpeed`
	`}`
	`// Function to get SNMP ifInOctets for the interface indexed by nIfIndex (in bytes).`
	`// Returns the value polled upon success, null in case of failure.`
	`function getInOctets(nIfIndex)`
	`{`
	`var oResult = oSnmpRqst.Initialize(nDeviceID);`
	`if(oResult.Failed)`
	`{`
	`return null;`
	`}`
	`return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.10." + nIfIndex));`
	`// inOctets`
	`}`
	`// Function to get SNMP ifOutOctets for the interface indexed by nIfIndex (in bytes).`
	`// Returns the value polled upon success, null in case of failure.`
	`function getOutOctets(nIfIndex)`
	`{`
	`var oResult = oSnmpRqst.Initialize(nDeviceID);`
	`if(oResult.Failed)`
	`{`
	`return null;`
	`}`
	`return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.16." + nIfIndex));`
	`// outOctets`
	`}`
	`// Helper function to get a specific SNMP object (OID in sOid).`
	`// Returns the value polled upon success, null in case of failure.`
	`function SnmpGet(sOid)`
	`{`
	`var oResult = oSnmpRqst.Get(sOid);`
	`if(oResult.Failed)`

Monitoring an SNMP agent running on a non standard port (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 );`
	`    }`
	`}`

Accessing 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"]);`

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 (on page 139) for you to create useful Active Script Monitors for your devices.

Methods	

`LogMessage(sText);`	This method allows for a message to be written to the WhatsUp Gold debug log.
	Example:
	JScript:
	`Context.LogMessage( "Checking Monitor name using Context.GetProperty()");`
	VBScript:
	`Context.LogMessage "Checking Address using Context.GetProperty()"`

`PutProperty(sPropertyName);`	This method allows you to store a value in the INMSerialize object. This value is retained across polls.
	Example:
	JScript:
	`var nCount = parselnt(nNum) +1;`
	`Context.PutProperty("MyNumeric",nCount);`

`SetResult(nCode, sText);`	This method allows for a result code and result message to be set. This is how you can tell the WhatsUp Gold system if the monitor succeeded or not.
	Important: Every script should have a result, otherwise it will report back positively.
	Example:
	JScript:
	`Context.SetResult(0, "  Everything is OK");`
	`//Success`
	`Context.SetResult(1, "  Really big big error");`
	`//Failure`
	VBScript:
	`Context.SetResult 1, "  Really big big error"`

Properties

```
GetProperty(sPropertyName);
```

This property offers access to many device specific aspects. You obtain access to these items using the names listed. These names are case sensitive.

"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

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);
```

This property returns an open connection to the WhatsUp Gold database.

Examples:

This example gets the Open connection and reads some values out of the WhatsUp Gold "Device" table using the deviceID context. Please 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");
}
```

CHAPTER 10

Using Passive Monitors

In This Chapter

About Passive Monitors

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). Since these messages/events can occur at any time, a Passive Monitor Listener "listens" for them, and notifies WhatsUp Gold when they occur.

The first step to use this function is to Configure the Passive Monitor Listeners (on page 152).

After the listeners have been configured, you can Configure Passive Monitors (on page 154) for individual devices.

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.

Configuring Passive Monitor Listeners

A Passive Monitor Listeners listen 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 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. They could contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.
- **Windows Event Log Monitor**. This could be monitoring when a service is started or stopped, if there was a logon failure recorded, or any other entry in the Windows Event Log.

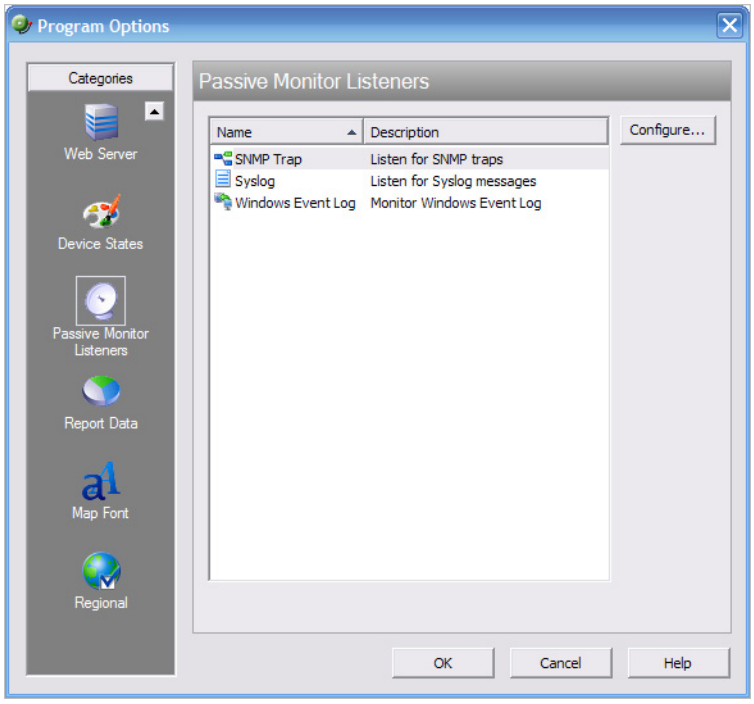
Before you can configure Passive Monitors, you must configure listeners.

To configure a listener:

1 In the WhatsUp Gold console, select **Configure > Program Options**. The Program Options dialog opens.

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 opens.

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.

Using the Passive Monitor Library

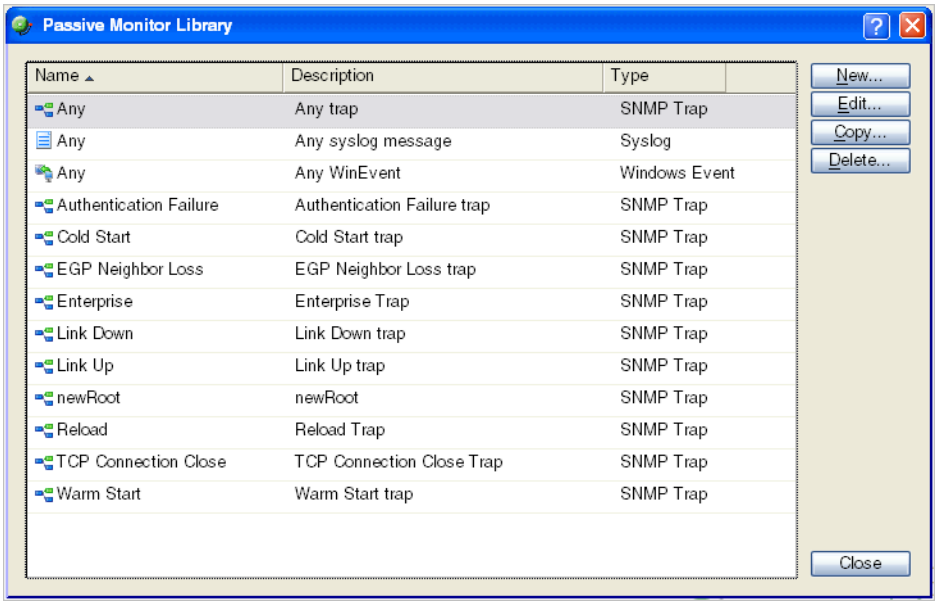
The Passive Monitor Library dialog displays the Passive Monitor types that have been created for WhatsUp Gold. These types are specific configurations of SNMP traps, Windows Log Events, and Syslog Events. After the Monitor types have been configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog.

To access the Passive Monitor Library:

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

  - or -

- From the main menu bar of the WhatsUp Gold console, click **Configure > Passive Monitor Library**.



- Click **New** to create a new passive monitor type.
- Select a monitor type in the list, then click **Edit** to change the settings.
- Select a monitor type in the list, then click **Copy** to create a new monitor type based on the selected type.
- Select a monitor type, then click **Delete** to remove it from the list.

Configuring Passive Monitors

To add/edit a Passive Monitor manually:

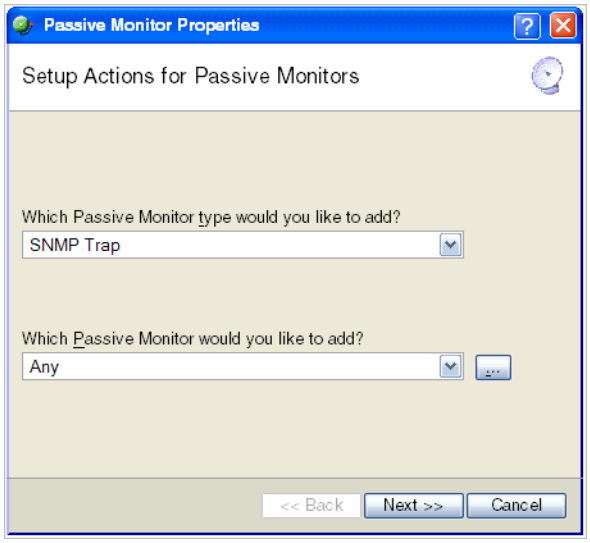
1. From the WhatsUp Gold web interface, click **Go > Configure > Passive Monitor Library**.
2. Click **New** to configure a new Passive Monitor.

   - or -

   Select a monitor from the list, then click **Edit** to make changes to an existing configuration. The configuration dialog for the selected monitor type opens.
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:

1. Right-click the device to which you want to assign a passive monitor, then click **Properties**. The Device Properties dialog opens.
2. Click **Passive Monitors**. The Device Properties Passive Monitor dialog opens.
3. Click **Add**. The Passive Monitor Properties dialog opens.



4. Select the Passive Monitor type and Passive Monitor you want to assign, then click **Next**. The Setup Actions for Passive Monitors dialog opens.
5. Click **Add** to setup a new action for the passive monitor. The Select or Create Action dialog opens. 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.

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 197).

- SNMP Trap Log
- Syslog Entries
- Windows Event Log
- Passive Monitor Error Log

Are you missing traps or logs, or receiving blank emails generated from an Action on a Passive Monitor?

Receiving SNMP Traps

WhatsUp Gold has an internal SNMP trap handler, which when enabled, listens for and accepts SNMP traps that are addressed to it. 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 236).

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, you need to turn off the SNMP trap service.

CHAPTER 11

Using Performance Monitors

In This Chapter

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:

- 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, 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.

Learning about the Performance Monitor Library

The Performance Monitor Library is a central storehouse of all global Performance Monitors that have been configured for your network. 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.

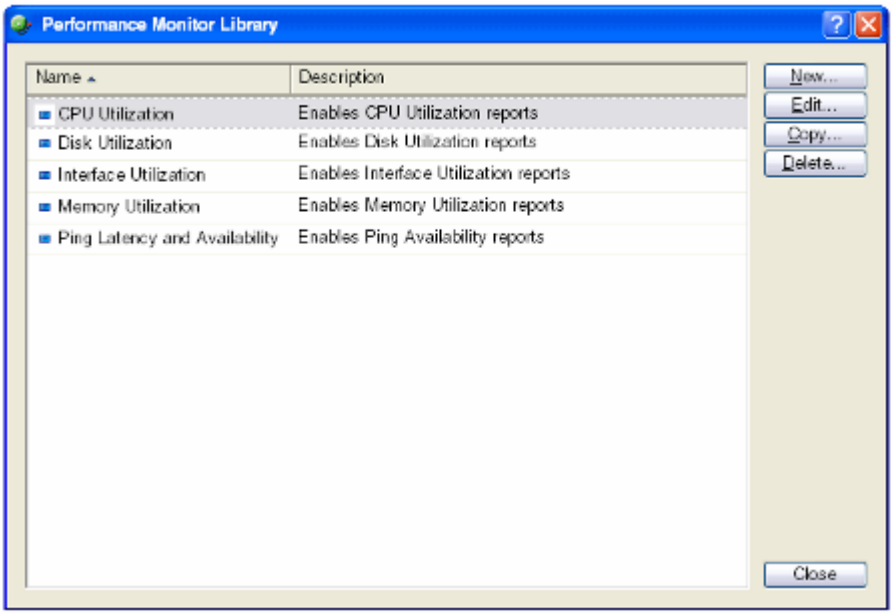
You can use the Performance Monitor Library to configure and manage performance monitors. When custom Performance Monitors are changed, the changes affect each instance of that particular monitor across your device groups.

To access the Performance Monitor Library dialog:

- From the WhatsUp Gold console main menu, select **Configure** > **Performance Monitor Library**.

  - or -

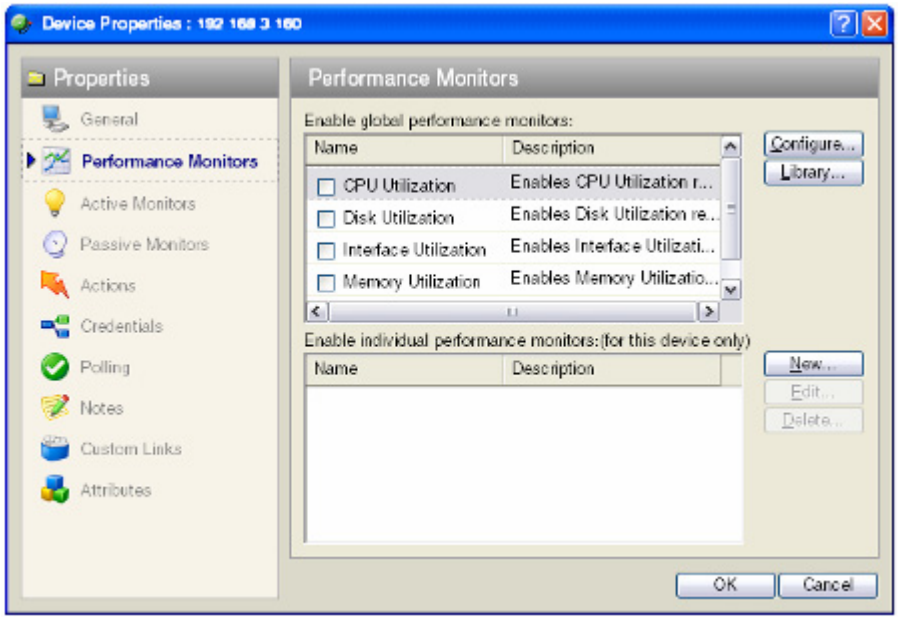
- From the WhatsUp Gold web interface, select **Go > Configure > Performance Monitor Library**.



To configure Performance Monitors for the devices they are assigned to:

1 Right-click a device you want to configure. The shortcut menu opens.

2 Click **Properties**. The Device Properties dialog opens.



- 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.

Enabling SNMP on Windows Devices

Before you can collect performance data on a Windows PC, you must first install and enable the Microsoft SNMP Agent on the device itself.

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 opens.
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 (on page 85) for connecting to this device.

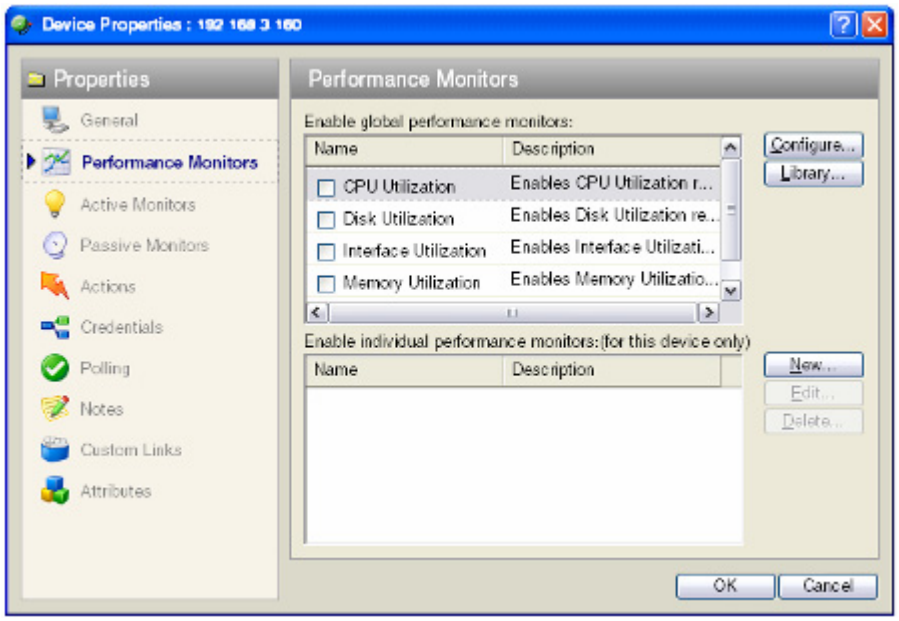
6 On the **General** tab, click **Start** to start the service (if necessary).

7 Click **OK** to close the dialog.

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.

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:

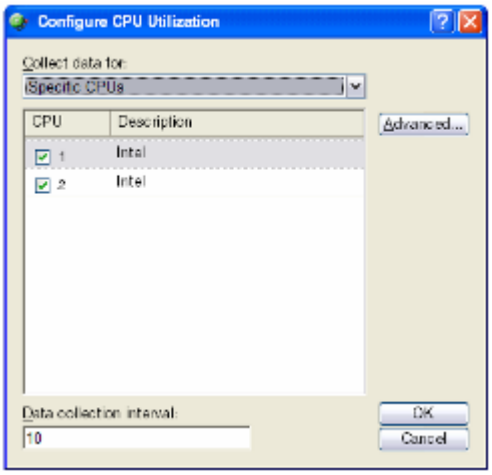
1 In Device View, select a device from the device list.

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**.

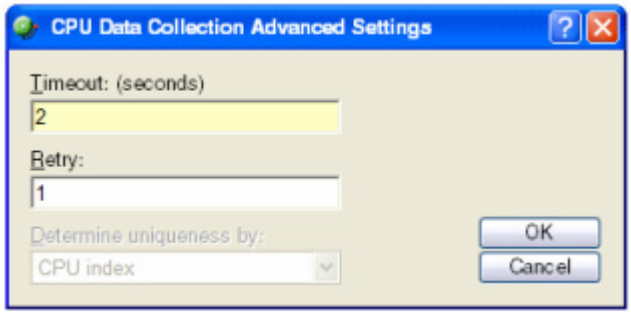
On the monitor configuration dialog, select the specific item you want to monitor by making a selection in the **Collect data for** drop-down list. Depending on the monitor, you can select to collect data for **All**, **Active**, **Specific**,or **Default** interfaces, memories, cpus, or disks.



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.

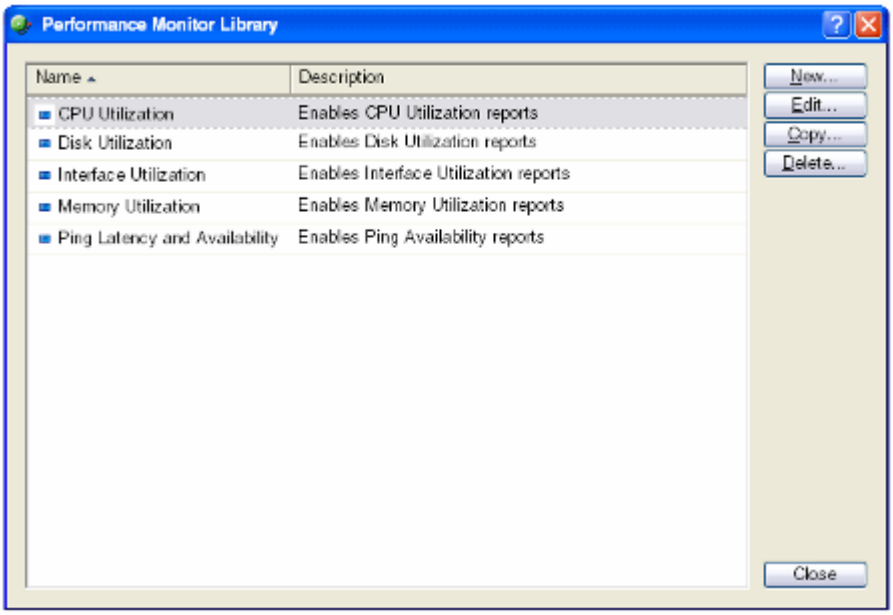
For information on the Active Script Performance Monitor, please see Adding custom performance monitors to the Performance Monitor Library (on page 164).

Adding custom Performance Monitors to the Performance Monitor Library

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. 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 In the WhatsUp Gold web interface from the **Go** menu, go to **Configure** > **Performance Monitor Library**.



2 In the Performance Monitor Library, click **New.**

3 Select the monitor type: SNMP, WMI, or Active Script Performance Monitor.

4 Follow the instructions below for the type of monitor you choose.

To configure an SNMP monitor:

1 On the Add SNMP Performance Counter dialog, enter a **Name** and **Description** for the monitor as it will appear in the Performance Monitor Library.

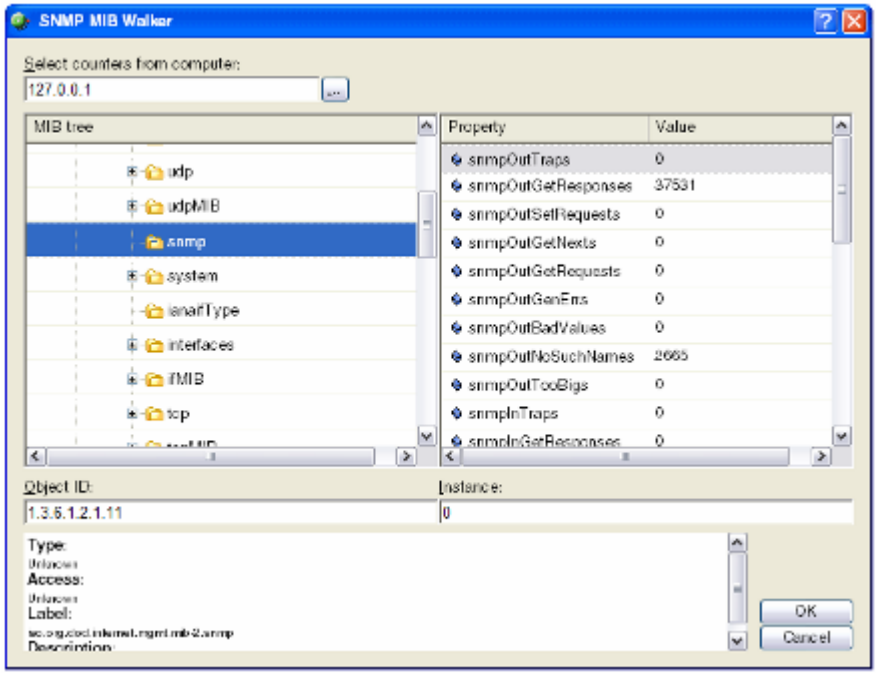
2 Either enter the OID and instance or click the **Browse (...)** button next to the **Instance** box to go to the SNMP MIB Walker dialog.

3 In the MIB Walker dialog, enter the share name or IP address of the computer in 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 Walker 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 the **Performance counter** and **Instance** box in the Add SNMP Performance counter dialog.

10 Verify the configuration and click **OK** to add the monitor to the Performance Monitor Library.

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.

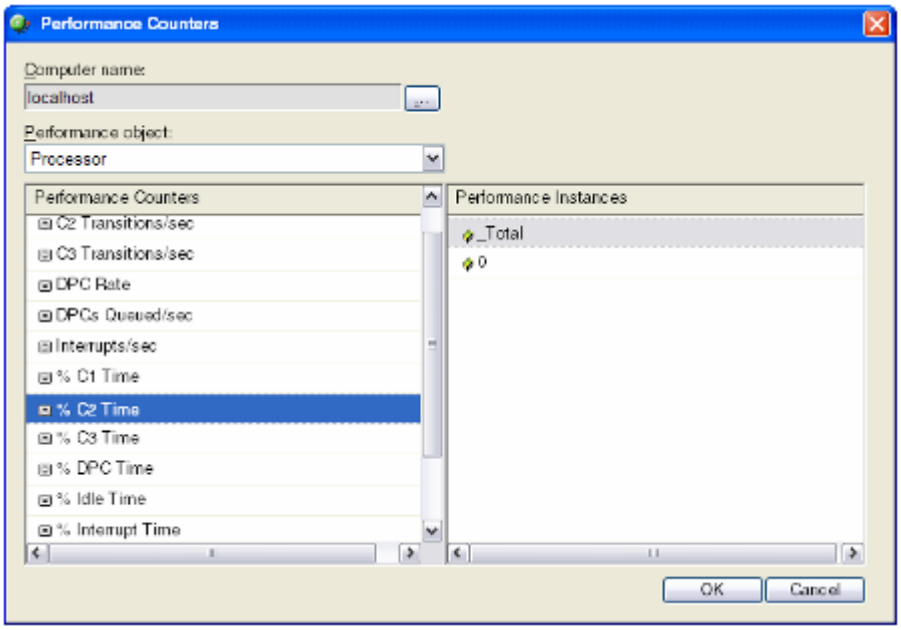
2 Click the **Browse (...)** button next to the **Instance** box.

3 In the dialog that appears, enter the share name or IP address of the computer in which you want to connect.

4 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.

5 Enter the password for the login used above and click **OK** to connect to the computer.

6 Use the **Performance counter** tree to navigate to the performance counter you want to monitor.



7 Once 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 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.

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** drop down menu.

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** drop-down menu.

7 If needed, adjust the **Timeout** and **Retries** count for connection to the device.

8 Click the **Browse (...)** button next to the Instance box. 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** drop down menu.

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** drop-down menu.

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 (on page 162) 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 the WhatsUp Gold reports, please see Using Full Reports (on page 197).

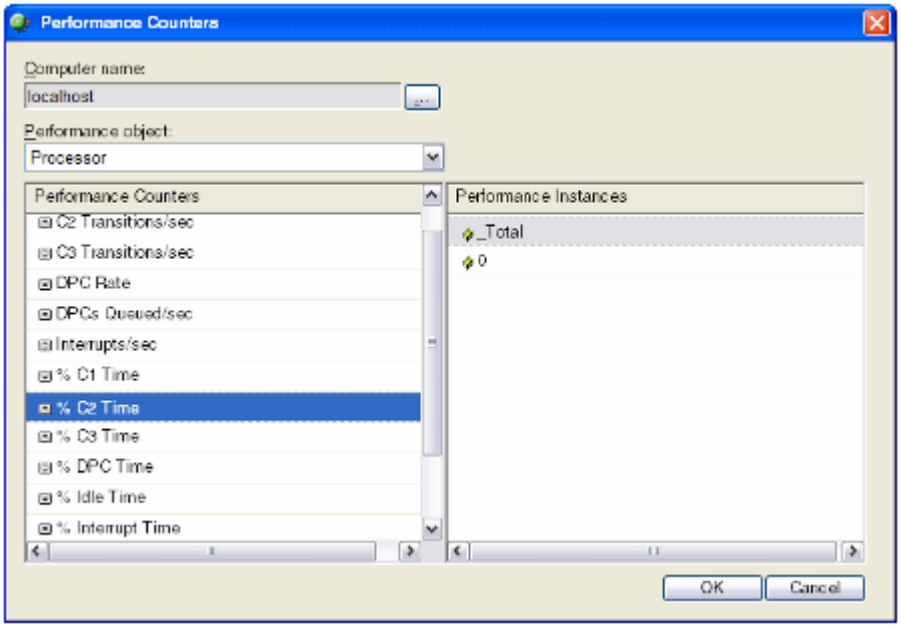
Performance Monitors gather specific types of data on the devices they are assigned to. System wide monitors are configured using the Performance Monitor Library, but you can also create specific SNMP and WMI monitors to be used on a per-device basis.

To create custom performance monitors for system-wide use:

1. On the WhatsUp Gold web interface, go to **Go > 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:

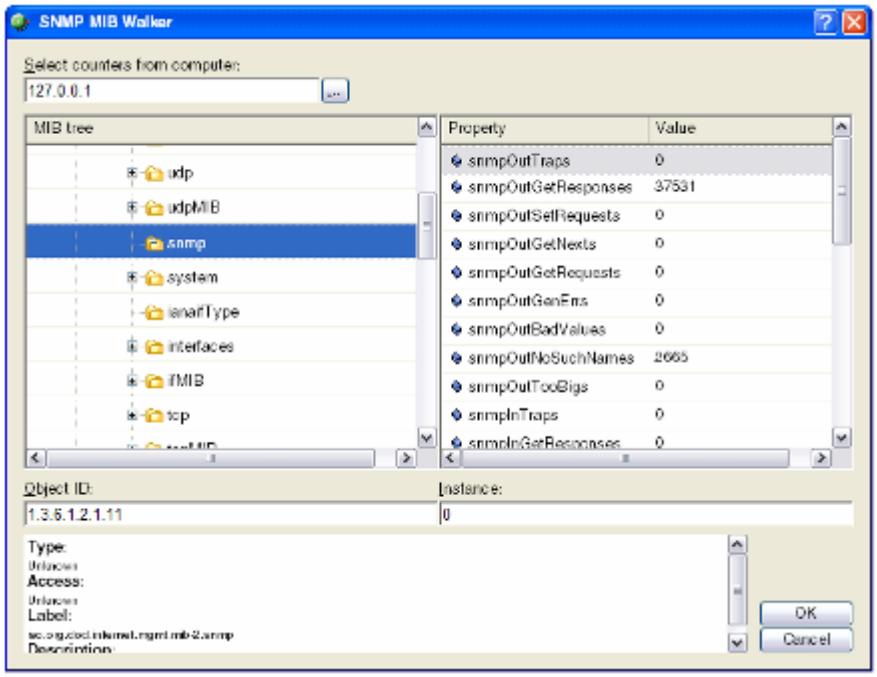
1. On the Add Performance Counter dialog, enter a name and description for the monitor.
2. Click the **Browse (...)** button next to the **Instance** box to go to the Select Performance Counter dialog.
3. Click the **Browse (...)** button next to **Select counters from computer** box. The Select Computer dialog appears.
4. Enter the share name or IP address of the computer you want to connect to.
5. 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.
6. Enter the password for the login used above and click **OK** to connect to the computer.
7. Use the Performance counter tree to navigate to the performance counter you want to monitor.



8. After you select the performance counter, select the specific instance you want to monitor.
9. Click **OK** to add the counter and instance to the Add Performance Counter dialog.
10. 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 the **Instance** box 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 you want to connect to.
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 Walker 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 the Performance counter and Instance box 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.

Ipswitch uses a BitSight2 temperature sensor from Ravica to monitor the temperature and humidity in our testing labs. Since the device is SNMP enabled, we added a device for the sensor to our 'Office' group and enabled SNMP on that device.

With the device in the group, we created a Custom SNMP Performance Monitor for that device.

Since the OID for temperature and humidity monitoring is included with the documentation for the device, we did not have to add the MIB to the MIB directory. Instead, we simply entered the OID into the Add SNMP Performance Counter dialog.

When the performance monitor is running, data is collected by the application and displayed on the Custom Performance Monitor report. Once you have several hours of data, you might have graph that looks like this:

Example: monitoring router bandwidth

Through the Performance Monitoring system, you have the ability to configure the application 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**.

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 on enabling SNMP, see "Enabling SNMP on Windows devices (on page 161)."

Configuring the monitor

Because the Interface Utilization performance monitor is one of the default performance monitors installed with WhatsUp Gold, there is no global configuration required before setting the monitor up for a device itself. Once your SNMP credentials have been established for the device, you are ready to configure and enable the monitor to start gathering data.

1. On the WhatsUp Gold web interface, select the device you want to gather performance data for and then right-click.
2. Select **Properties** from the right-menu.
3. Select **Performance Monitors** on the Device Properties dialog.
4. Select the Interface Utilization monitor from the list.
5. Click **Configure** to set up the monitor for the device. WhatsUp Gold scans the device and discovers the interfaces on the device.

   Once the scan is complete, 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 (see "Enabling SNMP on Windows Devices" on page 96).
6. 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.
7. (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.
8. On the Configure Interface Data Collection dialog, enter a time interval (in minutes) 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."
9. Click **OK** to save the Interface Utilization configuration.

Viewing the data

WhatsUp Gold will take several polling cycles before it has enough data to produce meaningful graphs (with a 10 minute poll interval, this may mean a few hours.) Once enough data has been gathered, there are several reports you can use to view this data.

- **By Device**. For device-specific data, view the Interface Utilization report (shown below); 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.

We first describe the scenario, then the steps taken by the network administrator to solve the problem.

Scenario:

A developer working in Augusta, GA on an Atlanta-based propriet 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 montors (on page 162).

CHAPTER 12

Using Active Discovery

In This Chapter

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:

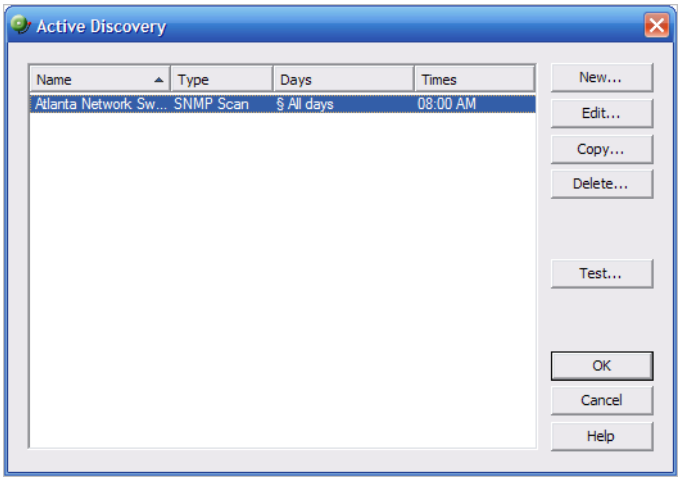
- Active Discovery Log report shows the success or failure of the Active Discovery task, and any devices and/or Monitors found during that scan.
- Active Discovery Results report shows all new items found in the latest scan, or all unprocessed items from previous scans. Through this report, you can add 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, in the Report view.

Configuring Active Discovery

To configure an active discovery task:

1 From the WhatsUp Gold console main menu, select **Configure > Active Discovery**. The Active Discovery dialog opens.



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 179).

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 opens.

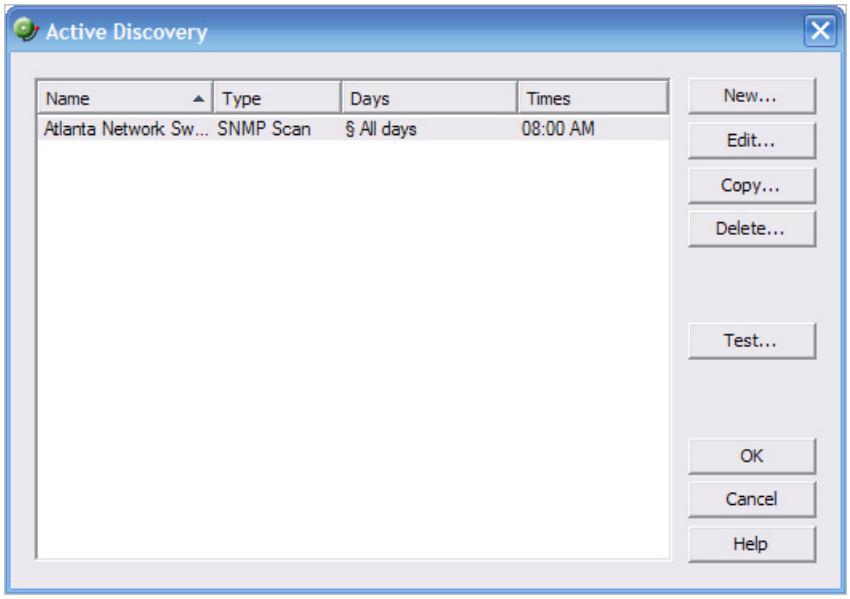
2 Click **New** to add a new task.

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 opens.

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 opens.
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 opens.
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.

CHAPTER 13

Using Maps

In This Chapter

Using 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**.

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 (on page 47) 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.

Using device layout

Map View has a number of options you can use to organize your view of devices. Arrange options (on page 182) are available from the Arrange menu on the main menu bar and right-click menu. Display options (on page 182) 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 (on page 46) (such as lines, text, circles) and attached lines (on page 48) to create custom map views.

Lock position (see "Using the lock position" on page 184) 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

Specifies the font used for device display names. Click **Change Font** to open the standard Windows font selection dialog box. Select the font properties you want to use and click **OK**. 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 (on page 182) 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.

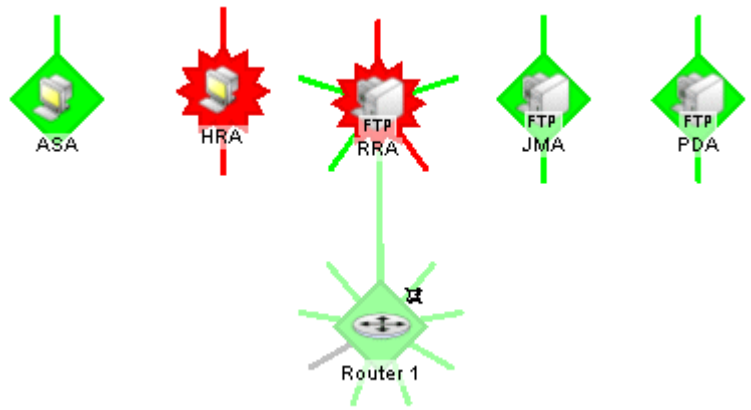
For example, to clean-up a map, after completing discovery, you can try the following display options:

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

In Map View, 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 (see "Connecting links" on page 187) to device RRA and this link is currently up. Also shown are eight unconnected links (on page 187), 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.

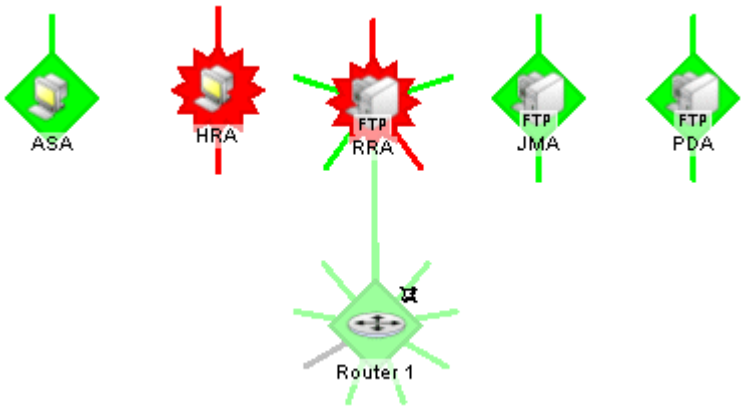
By default, links can be rendered in one of three colors:

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

Using link lines

In Map View, 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 (see "Connecting links" on page 187) to device RRA and this link is currently up. Also shown are eight unconnected links (on page 187), 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 can be rendered in one of four colors:

- **Green** indicates a service (such as, but not limited to, Interface) that is up. This includes services that have not yet been polled.
- **Red** indicates a service that is down.
- **Gray** indicates a service listed in the devices' Active Monitors list, but not currently monitored.

- **Orange** indicates that the device is currently in maintenance mode.

Using attached lines

Attached lines show an arbitrary connection between devices and move with the device. These 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 (on page 47).

To draw an attached line:

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

Note: The root 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 (on page 47) 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 (on page 47), 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.

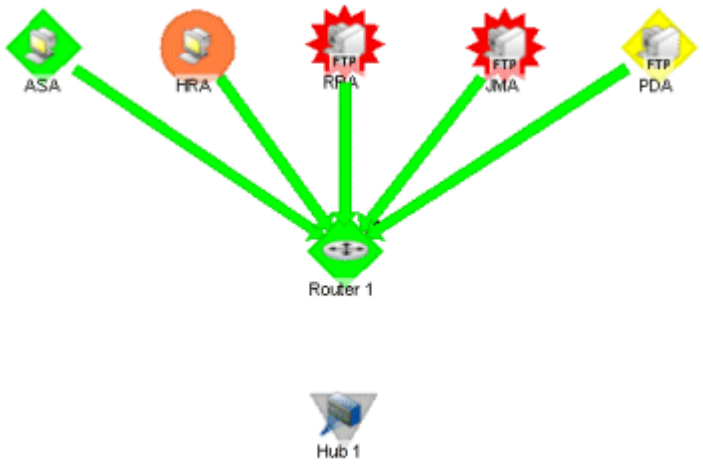
3 **Automatically**, when you right-click a device, then click **Properties > Active Monitors > Discover**.

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.

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 (on page 47)) and provide visual indications of polling dependencies (on page 91).

Here is an example of a Map View.



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.

The above image shows a device that is considered up because the device is accessible, but a monitor configured on the device is down.

You can also use Map View to:

- Indicate relationships among devices by using annotation objects.
- Change the layout (on page 183) 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 acknowledge, the icon returns to the above appearance.

For more information, see Using Map View (on page 181).

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 Professional\2007\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.

CHAPTER 14

Using the Program Options

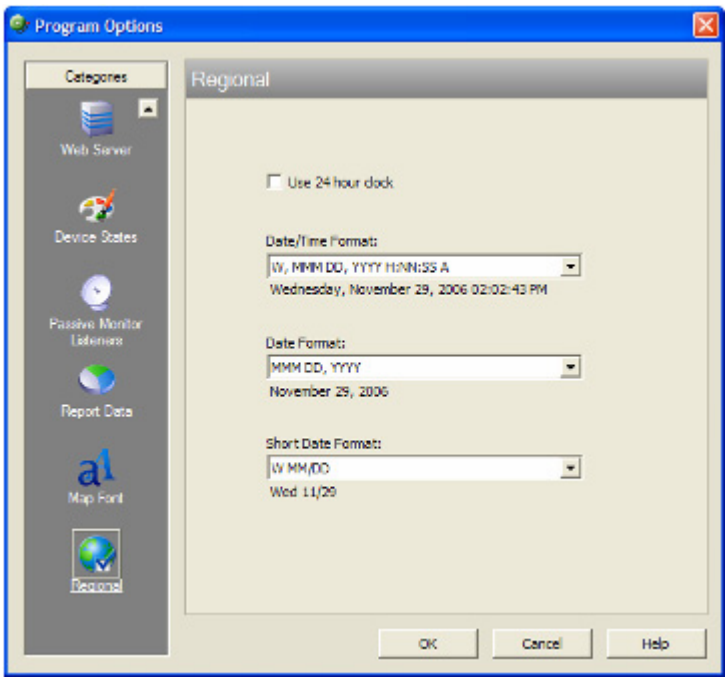
In This Chapter

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**.

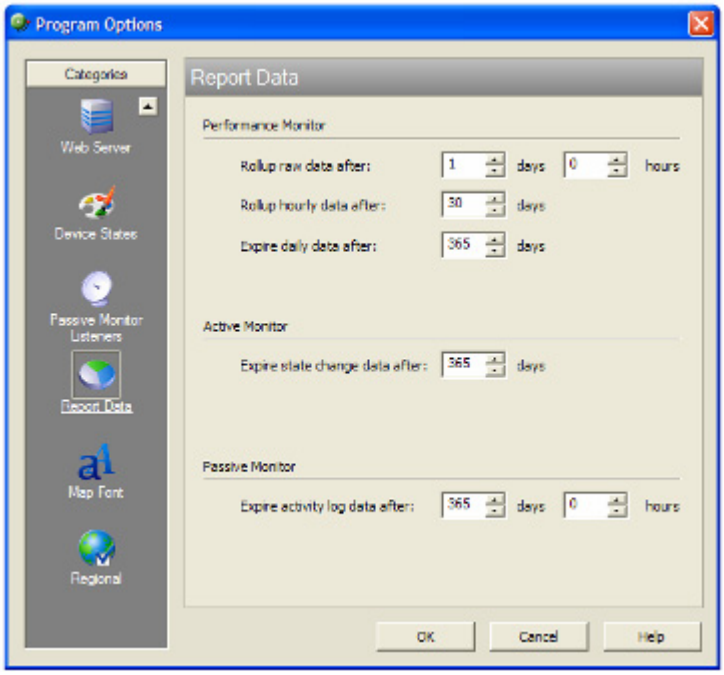
These formats can be seen in use on several of the reports available on the Reports view.

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.

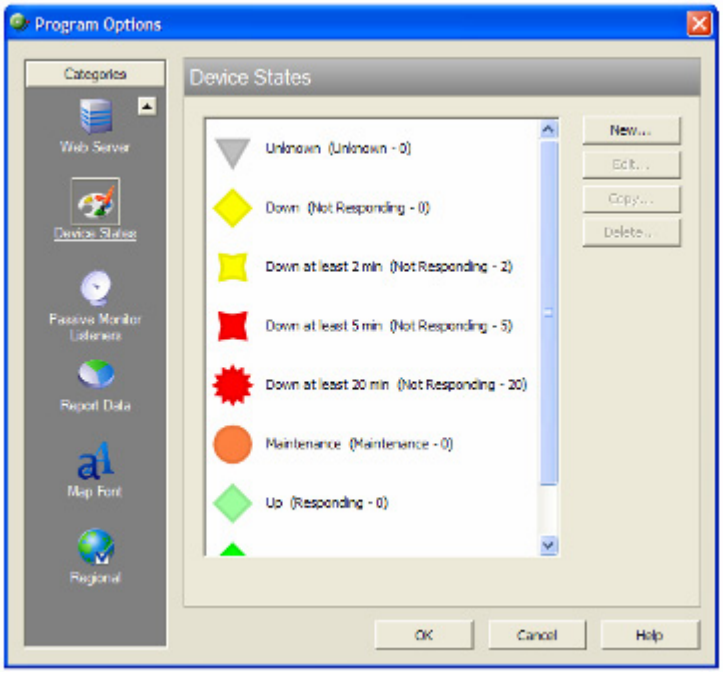
4 Click **OK** to save the changes.

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.

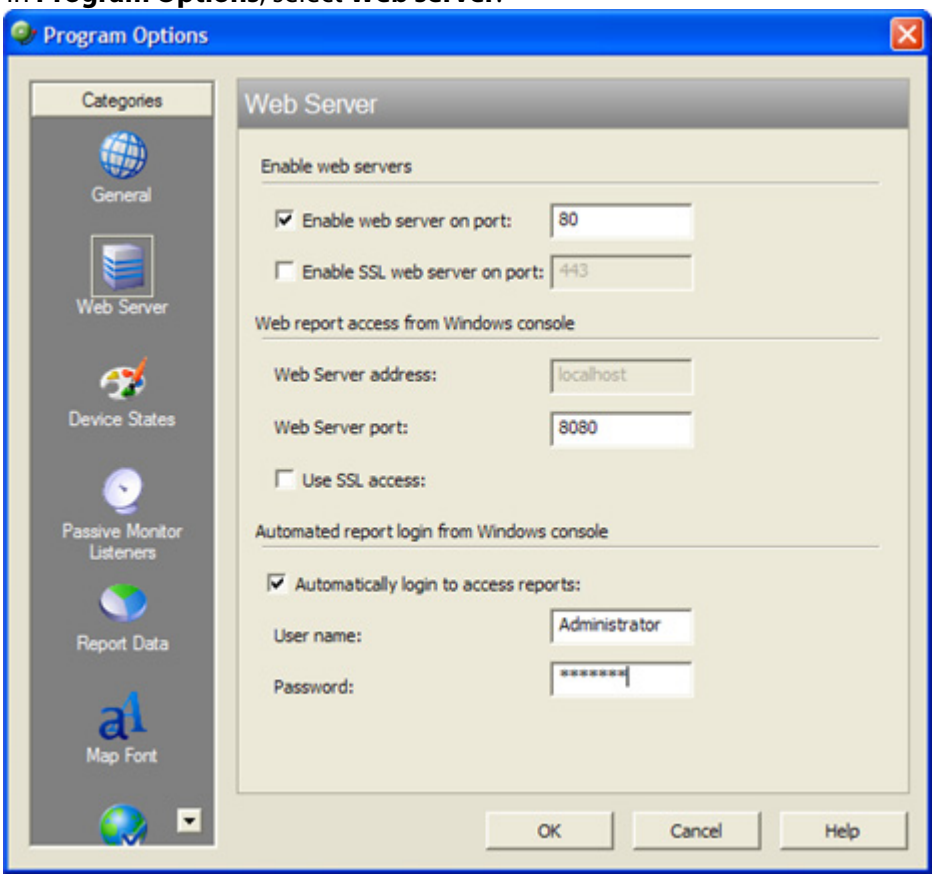
If the default settings do not fit your needs, click **Add** to create a new device state, using the internal state and state time that you need.

Stopping and starting the secure web server

To stop and restart the secure web server:

1 From the main menu, select **Configure > Program Options.**

2 In **Program Options**, select **Web server**.



3 Select **Use SSL access** to start the server with SSL.

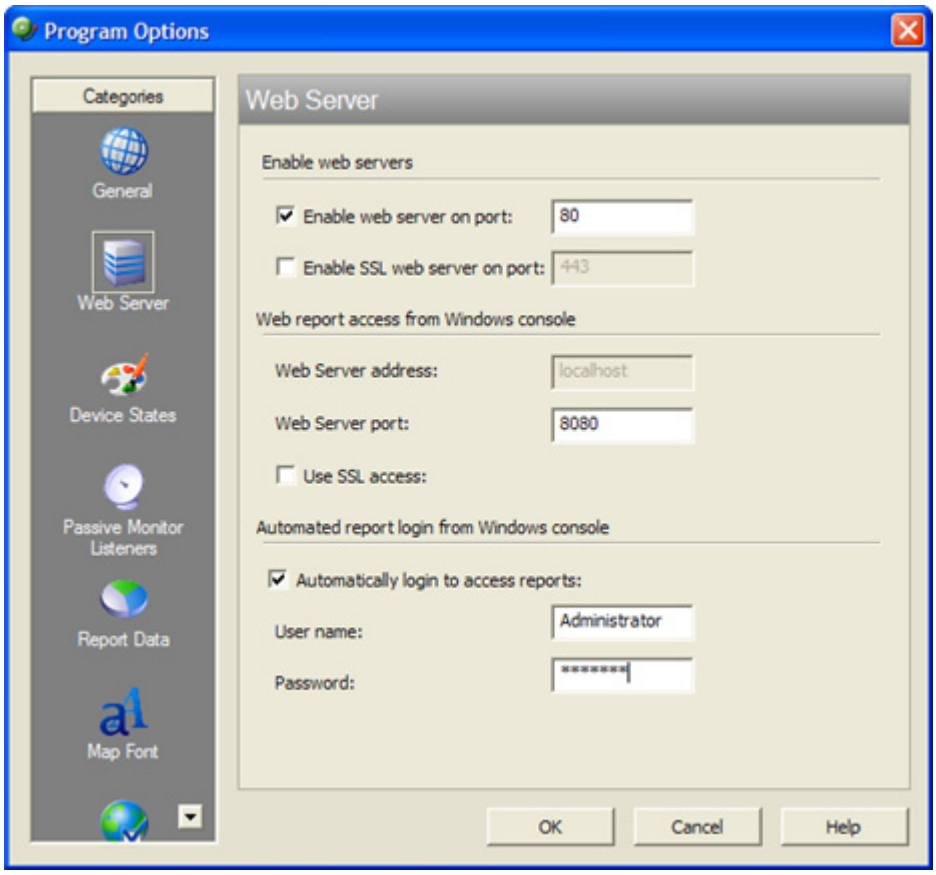
4 Click **OK**.

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

Stopping and starting the web server

To stop and restart the Web server:

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



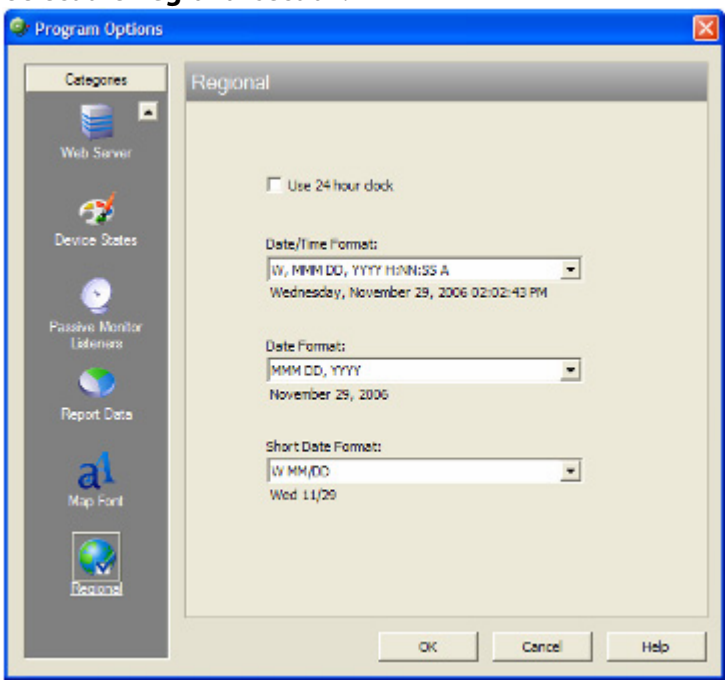
3. Select **Enable web server on port:** to start the server, then clear the option to stop the server.
4. Click **OK** to save your changes.

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

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**.

CHAPTER 15

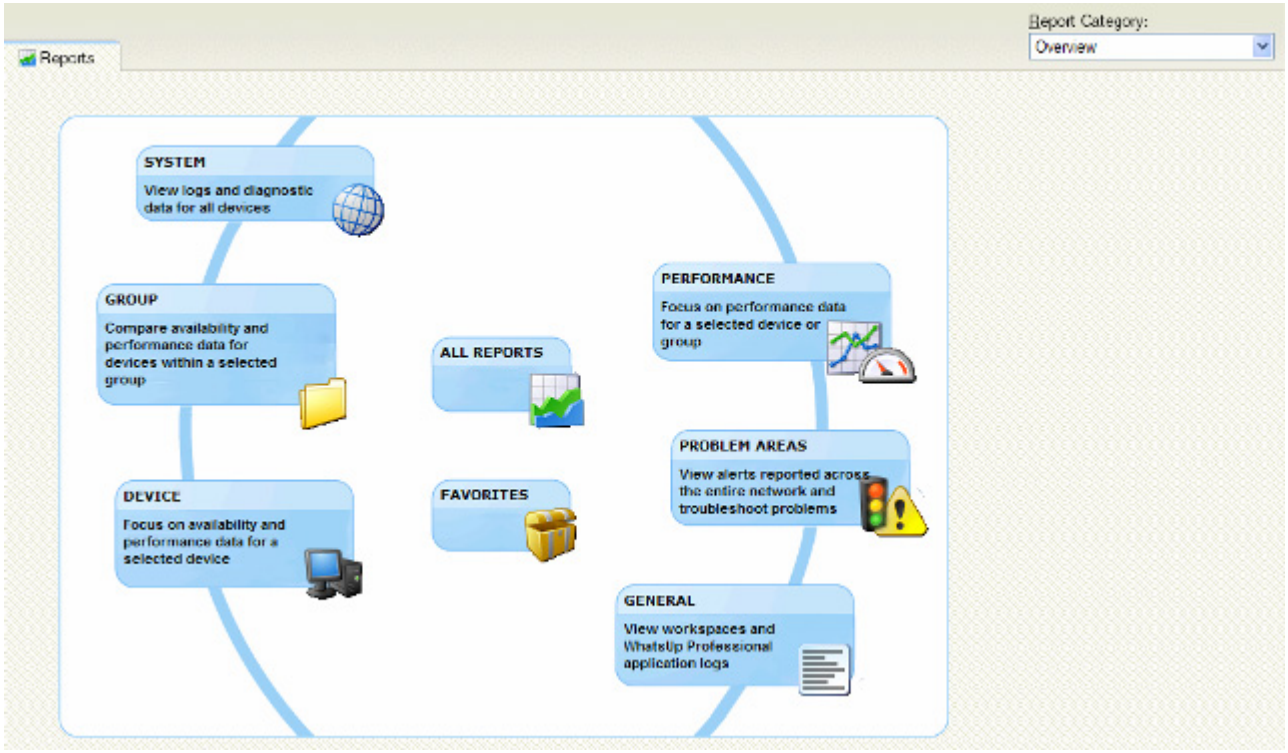
Using Full Reports

In This Chapter

Learning about full reports

In WhatsUp Gold, full reports are used to troubleshoot and monitor performance and historical data that has been collected during the operation of the application. These reports can help you troubleshoot problem areas on your network and give you easy access to important network information. Full reports are accessible from both the console and the web Interface, but beginning in v11, reports are only viewable from the web interface.

Full 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.



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 in two ways: scope of the information displayed within a report, and the type of information displayed within a report.

There are three categories for full reports based on the scope of information displayed within a report:

- **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.
- **Group**. These reports display information relating to a specific device group. For example, the Group State Change Timeline and the Group Actions Applied reports.
- **Device**. These reports display information relating to a specific device. For example, the Device Status Report.

There are three categories for full reports based on the type of information displayed within a report:

- **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.

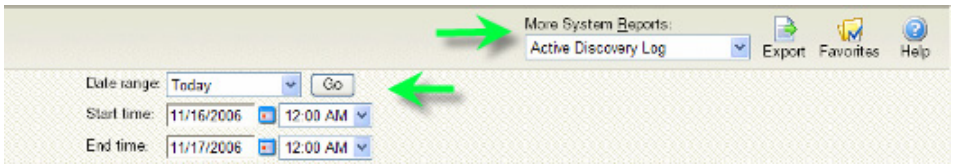
Note: By default, performance data is not collected for the monitors assigned to the devices in your database. To begin collecting performance data for a device, right-click on a device on the Devices tab and select **Properties** from the context menu. In the Device Properties dialog, select **Performance Monitors**. No information will be displayed in performance reports until you have done this.

- **Problem Areas**. These are trouble-shooting reports that allow you to investigate network issues. For example, the Group Active Monitor Outage and the Passive Monitor Error Log.
- **General**. These reports display information on your WhatsUp Gold settings and diagnostics, as well as device-specific and user-configured details. The Home, Top 10, and Device Status workspaces/full reports all fall in the General category.

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.

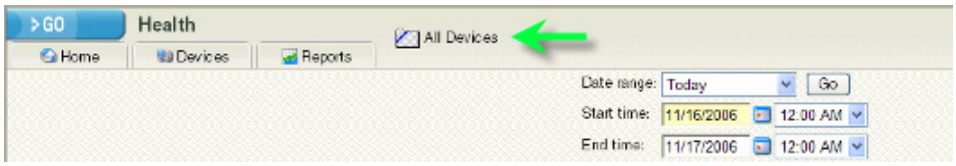
Favorites. Allows you to add a report to your list of Favorites.

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.

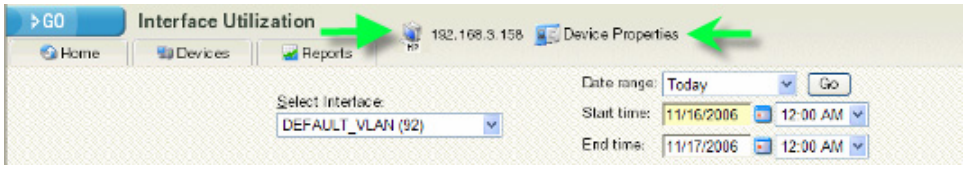
The **More Group Reports** drop-down menu allows you to easily jump to other group reports, or to bring up the report picker to select from all full reports.

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 two 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.

List of full reports

The following is a list of all reports that are available in Ipswitch WhatsUp Gold v11.

(P) = Performance

(PA) = Problem Areas

(G) = General

System reports	
Action Log (PA)	A record of all Actions that WhatsUp attempts to fire.
Active Discovery Log (G)	A record of all Active Discovery task results.
Activity Log (G)	A history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the selected time period.
General Error Log (PA)	A record of error messages generated by WhatsUp.
Passive Monitor Error Log (PA)	A record of Passive Monitor errors reported by WhatsUp.
Performance Monitor Error Log (PA)	A record of Performance Monitor errors reported by WhatsUp.
Recurring Action Log (G)	Results of Recurring Action executions.
Recurring Report Log (G)	Results of Recurring Report executions.
SNMP Trap Log (PA)	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 (PA)	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 (PA)	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 (G)	Shows the history of user activity on the system.
Windows Event Log (PA)	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	
Actions Applied (G)	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 (PA)	Compare the amount of time the Active Monitors on your devices have been available.
Active Monitor Outage (PA)	Compare the amount of time the Active Monitors on your devices have been down.
CPU Utilization (P)	CPU utilization statistics for devices by group.
Disk Utilization (P)	Disk space utilization statistics for devices by group.
Health	The current status of monitored devices in the selected group, along with each Monitor configured to those devices.
Interface Utilization (P)	Interface traffic and utilization for devices by group.
Memory Utilization (P)	Memory utilization statistics for devices by group.
Ping Availability (P)	Ping availability statistics for devices by group.
Ping Response Time (P)	Ping response times for devices by group.
State Change Timeline (PA)	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 (G)	A summary of device states organized by device group.

Device reports	
Active Monitor Availability (PA)	Find out when the Active Monitors on your device have been accessible.
CPU Utilization (P)	CPU utilization statistics for a device.
Custom Performance Monitors (P)	View information on your devices collected by Performance Monitors.
Device Status (G)	A detailed look at a specific device.
Disk Utilization (P)	Disk space and utilization statistics for a device.
Health (PA)	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 (P)	Interface traffic and utilization statistics.
Memory Utilization (P)	Memory utilization statistics for a device.
Performance Monitor Error Log (PA)	A record of Performance Monitor errors for an individual device.

Ping Availability (P)	Availability statistics for a device.
Ping Response Time (P)	Ping response times for an individual device.
SNMP Trap Log (PA)	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 (PA)	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 (PA)	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 (PA)	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.

Printing, exporting, and saving full reports

All full reports can be printed and many can be exported into text or Microsoft Excel. 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 delimeter** 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:

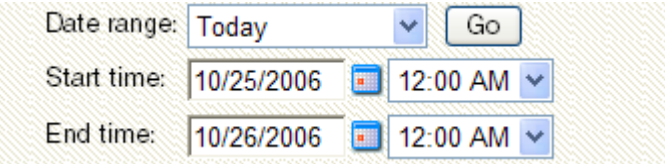
While viewing the full report you wish to save:

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.**

Changing the report date range

Date/Time picker

Use the date/time picker at the top of the report to select a date range. The date and time format for the date on this report matches the format specified in **Program Options > Regional**.



Zoom tool

Use the report Zoom tool to page left or right, or to zoom-in or zoom-out on a report.

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

Through this feature, you can configure WhatsUp Gold to send reports to email addresses at regularly scheduled intervals.

Configuring Recurring Reports

To create a new Recurring Report:

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 will want to enter in the **URL box**.
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 WhatsUp Gold 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.

CHAPTER 16

Understanding and Using Workspaces

In This Chapter

Learning about workspaces

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

Device and Home workspaces

Device 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.

Home workspaces can display both Home and Device workspace reports. You can place any workspace report on a universal 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.

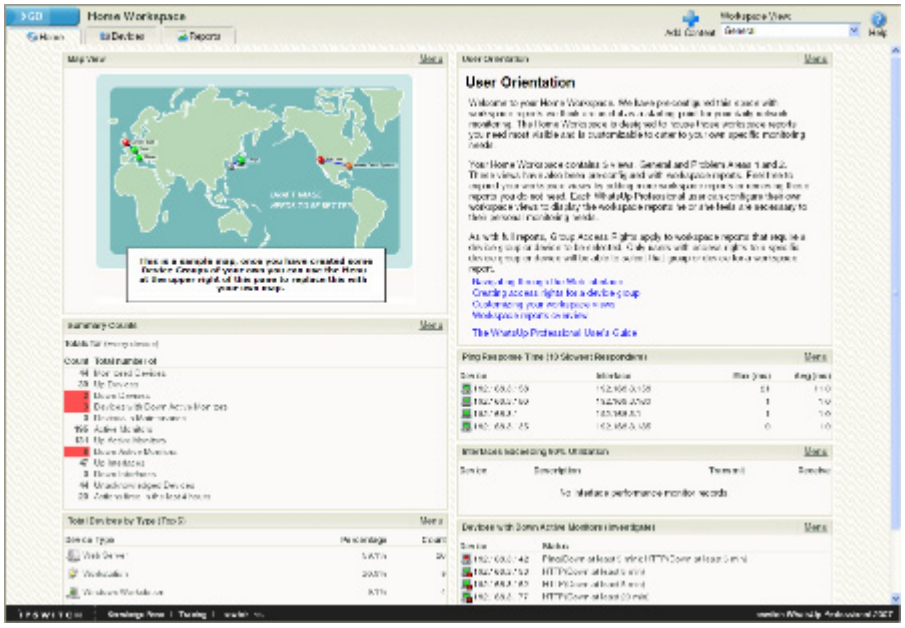
About pre-configured workspaces

Ipswitch WhatsUp Gold v11 comes to you with 3 pre-configured workspaces:

- Home workspace
- Device Status workspace
- Top 10 workspace

The 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.



Home contains three pre-configured "views" that you can customize to your own specifications:

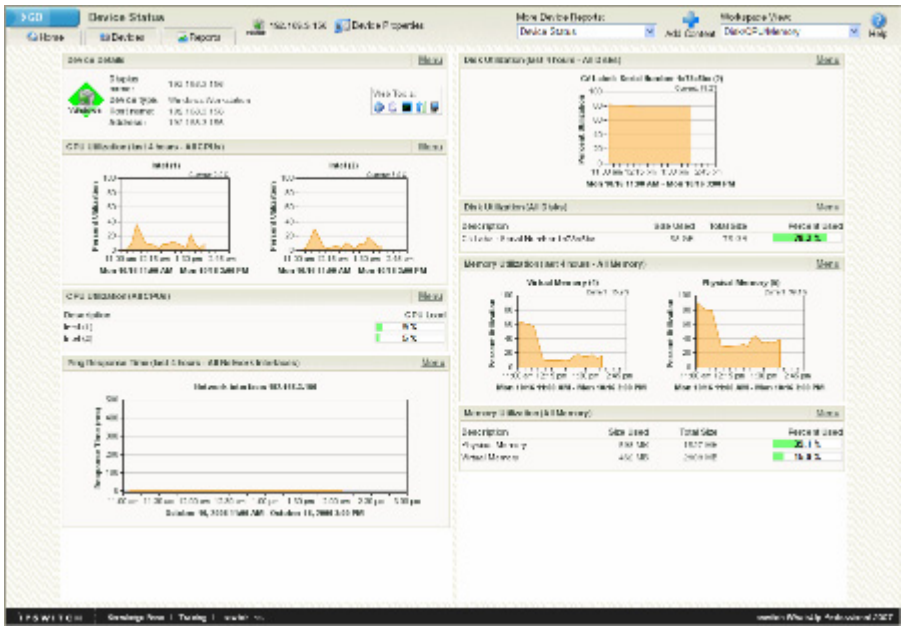
- General
- Problem Areas 1
- Problem Areas 2

Each workspace view includes several default workspace reports that you can decide to keep, alter, expand, or remove.

You can also create your own workspace views for the Home workspace through the Manage Workspace Views (on page 210) dialog.

The Device Status workspace

The WhatsUp Gold Device Status workspace displays the Device Status full report for a network device. You can change the device-in-context, but the workspace reports in each workspace view remain the same.



The Device Status workspace also has several pre-configured workspace views:

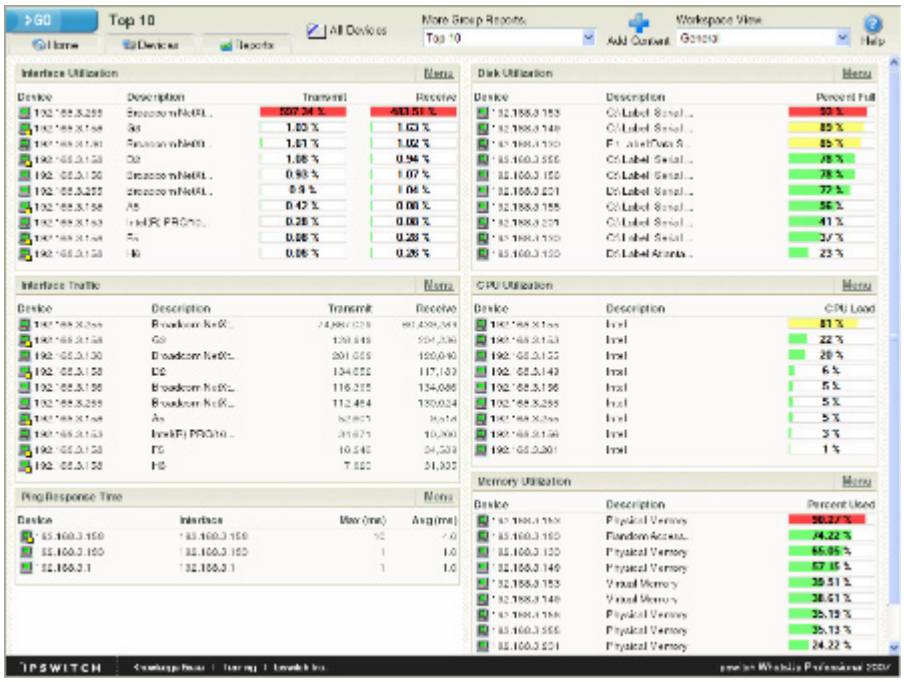
- General
- Disk/CPU/Memory
- Problem Areas
- Router/Switch/Interface

The Top 10 workspace

The WhatsUp Gold displays the Top 10 full report for your network devices. The Top 10 full report is a collection of workspace reports that focus 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

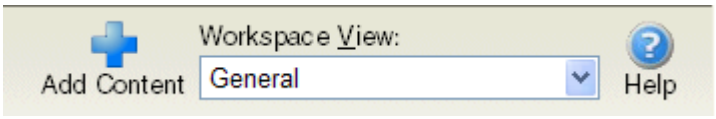


Unlike the Home and Device Status workspaces, the Top 10 workspace is designed with only the General workspace view. You can customize the general view in the same way you can other workspace views by removing the default workspace reports and/or adding other Top 10 and Threshold workspace reports.

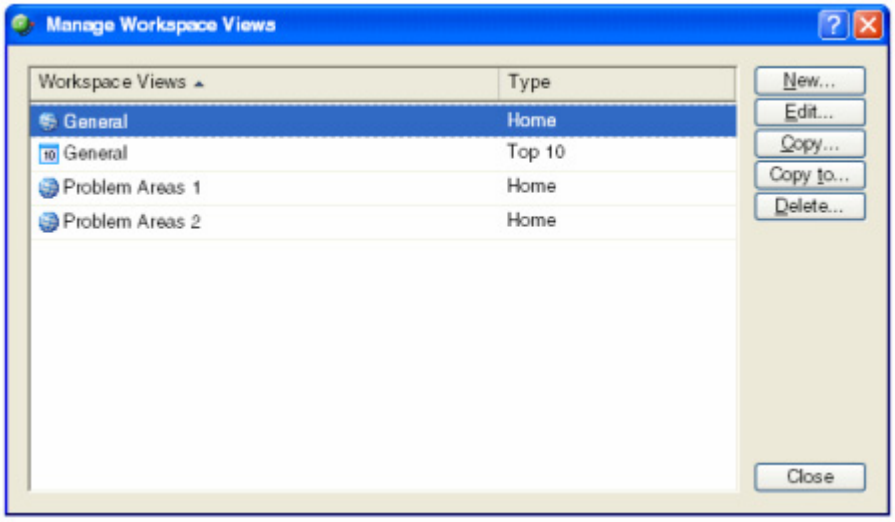
Managing workspace views

WhatsUp Gold gives you the ability to 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 these views as needed.

From the **Workspace View** drop-down menu, select **Manage Workspace Views**.



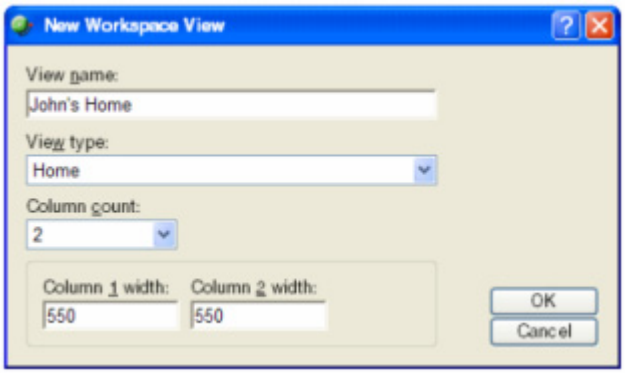
In the Manage Workspace Views dialog, you can create new workspace views, and edit, copy, or delete an existing workspace view.



- 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 to another user.
- 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 opens.



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 opens.

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).

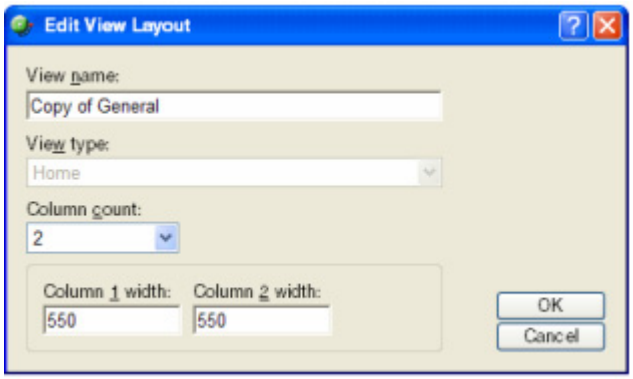
Note: Workspace view types cannot be edited after a view is created.

- **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 opens.



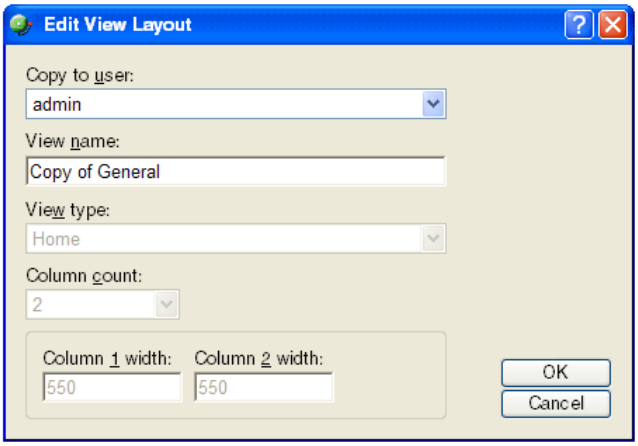
2 Enter the appropriate information in the following fields:

- **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 opens.



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.

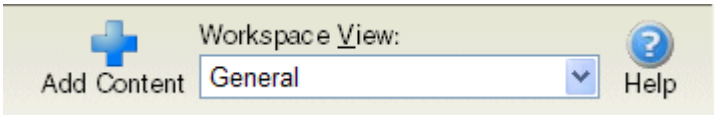
To delete a workspace view:

1 From the From the Manage Workspace Views dialog, click **Delete**.

2 Click **OK** on the dialog that follows.

Navigating through workspaces

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

New to Ipswitch WhatsUp Gold v11 are workspace reports, smaller versions of the full reports. These workspace reports are displayed within WhatsUp Gold workspace views. For more information, see Understanding and Using Workspaces (on page 207).

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 214).
- 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.

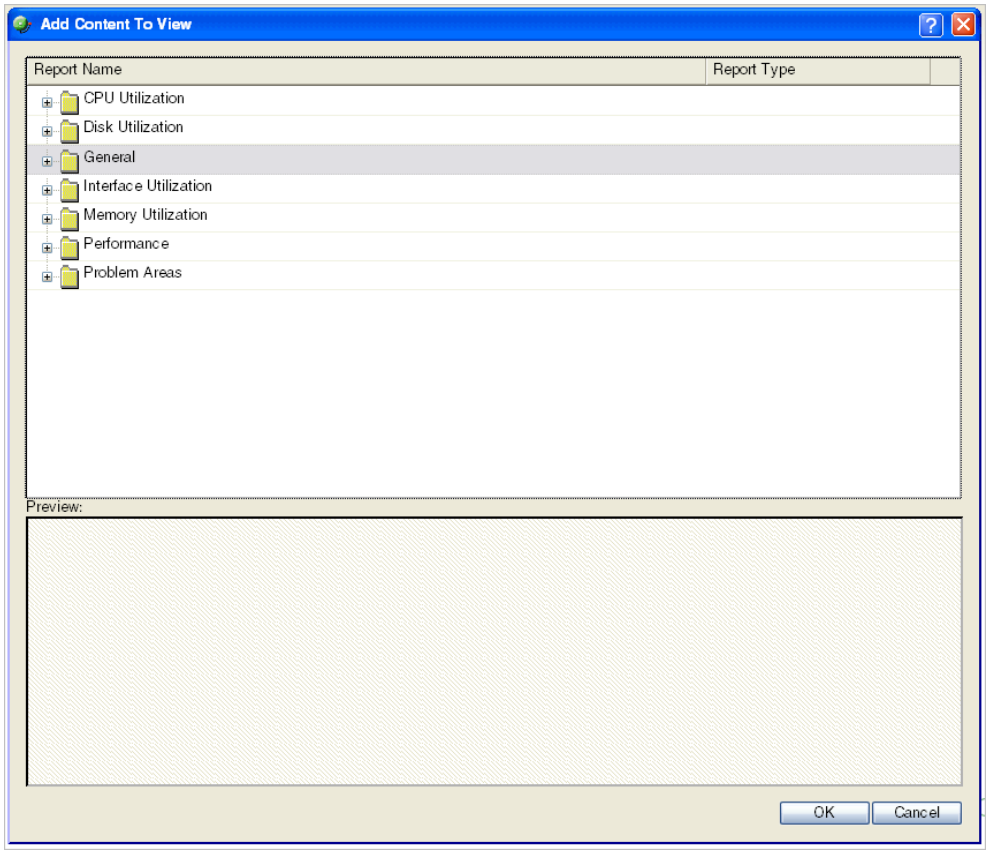
Adding workspace reports to a Device Status workspace

You can customize a Device Status workspace by adding additional reports to the workspace view.

To add a report to a Device Status workspace:

1 In the WhatsUp Gold web interface, right-click a device, then click **Device Status**. The Device Status Workspace page opens.

2 In the Workspace toolbar, click **Add Content**. The Add Content To View page opens.



3 Click the **+** button next to a report category folder, then click to select the report(s) you want to add to the Device Status workspace.

4 Click **OK** to save changes. The new report is added to the Device Status workspace.

CHAPTER 17

Using Workspace Reports

In This Chapter

Learning about workspace reports

Starting with the newest release, 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, but are not interactive: they only display data.

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.

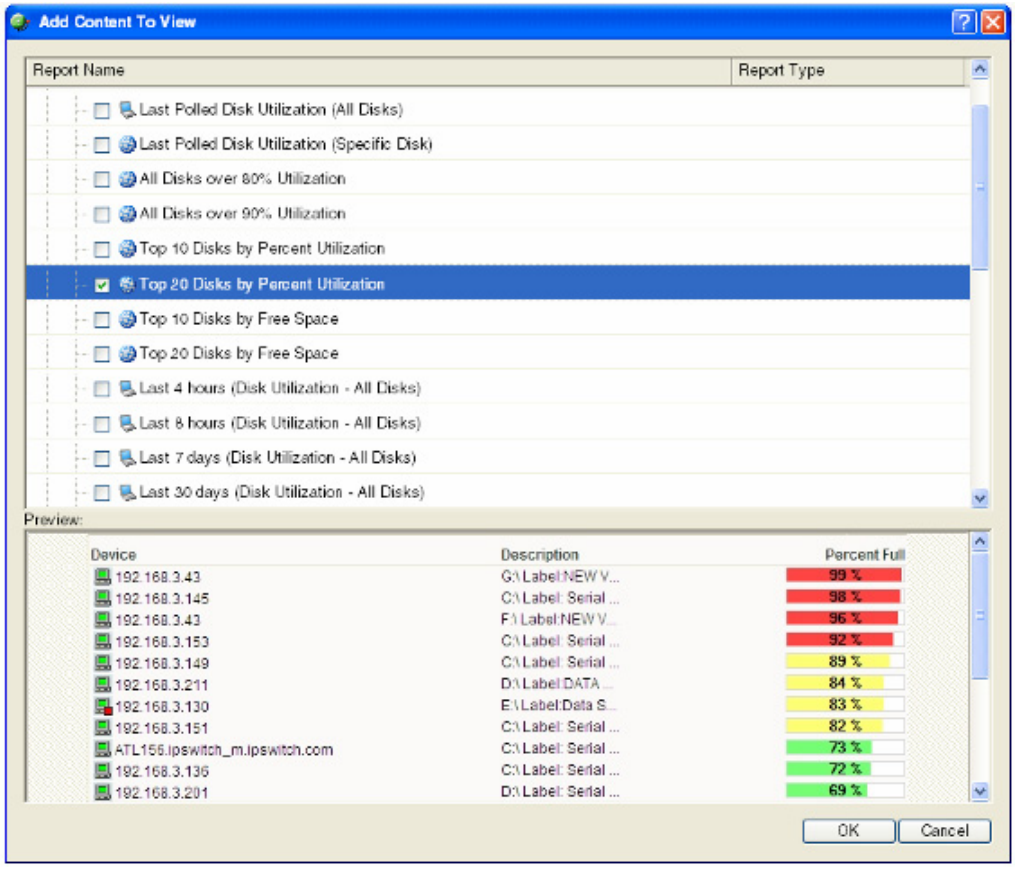
Workspace report categories

Workspace reports are broken down into 11 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**. 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.
- **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.

(H) = Home

(D) = Device

CPU Utilization workspace reports	
(H) Last Polled Values (specific CPU)	Shows the CPU utilization for a specific device CPU at the time of the last poll.
(H) All CPUs over 80% Utilization	Lists all network devices with a CPU utilization greater than 80%.
(H) All CPUs over 90% Utilization	Lists all network devices with a CPU utilization greater than 90%.
(H) Top 10 CPUs by Utilization	Lists the top 10 devices based on their current CPU utilization percentage.

(H) Top 20 CPUs by Utilization	Lists the top 20 devices based on their current CPU utilization percentage.
(D) Last 4 hours CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 4 hours.
(D) Last 8 hours CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 8 hours.
(D) Last 7 days CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 7 days.
(D) Last 30 days CPU Utilization (single device)	Details all CPU utilization percentages for one device over the last 30 days.
(H) Last 4 hours CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device over the last 4 hours.
(H) Last 8 hours CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device over the last 8 hours.
(H) Last 7 days CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device over the last 7 days.
(H) Last 30 days CPU Utilization (specific CPU)	Details a specific CPU's utilization percentages for one device of the last 30 days.

Custom Performance Monitor workspace reports	
(H) Last Polled Value (specific monitor)	Details information on a specific custom performance monitors at the time of the last poll.
(H) Top 10 with threshold	Lists the top 10 devices by a custom performance monitor threshold.
(H) Top 20 with threshold	Lists the top 20 devices by a custom performance monitor threshold.
(H) Top 20 by specific monitors	Lists the top 10 devices by a specific custom performance monitor.
(D) Last 4 hours (single device)	Details a device's custom performance monitors over the last 4 hours.
(D) Last 8 hours (single device)	Details a device's custom performance monitors over the last 8 hours.
(D) Last 7 days (single device)	Details a device's custom performance monitors over the last 7 days.
(D) Last 30 days (single device)	Details a device's custom performance monitors over the last 30 days.
(H) Last 4 hours (specific monitor)	Details a specific custom performance monitor over the last 4 hours.
(H) Last 8 hours (specific monitor)	Details a specific custom performance monitor over the last 8 hours.

(H) Last 7 days (specific monitor)	Details a specific custom performance monitor over the last 7 days.
(H) Last 30 days (specific monitor)	Details a specific custom performance monitor over the last 30 days.

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

(H) Last 7 days Disk Free Space (specific disk)	Details a specific disk's free space for one device over the last 7 days.
(H) Last 30 days Disk Free Space (specific disk)	Details a specific disk's free space for one device over the last 30 days.

General workspace reports	
(D) Device Attributes	Displays a device's attributes configured in **Device Properties > Attributes**.
(D) Device SNMP Details	Displays a device's SNMP details.
(D) Device Details	Displays a device's details configured in **Device Properties > General**.
(D) Device Custom Links	Displays any custom links assigned to a device in **Device Properties > Custom Links**.
(D) Device Dependencies	Shows the state of a device and any devices that are up or down dependent on that device.
(D) Device Active Monitor States	Lists all of a device's Active Monitors and their current state.
(D) Performance Monitor Summary	Displays a polling summary for the device-in-context.
(H) Map View	Displays a smaller version of a network map.
(H) Database Size	Displays a graphical representation of the WhatsUp Gold database at the time of the last poll.
(H) Custom Links	Displays any custom links that you add to the workspace report.
(H) Free Form Text/HTML	Displays any free form text or HTML code that you add to the workspace report.
(H) Web User Activity Log	Displays a log of when a user logs on or off the web interface, and the actions taken while logged on.
(H) Interface Details	Displays SNMP information reported by a specific network interface.
(H) User Orientation	Displays information regarding the new the new web interface, workspaces, and workspace reports.

Interface Utilization workspace reports	
(D) Last Polled Interface (single device)	Shows the interface utilization for all network interfaces at the time of the last poll.
(H) Last Polled Interface (specific interface)	Shows the interface utilization for a specific network interface at the time of the last poll.
(H) All Interfaces over 80% Bandwidth Utilization	Lists all network interfaces with a utilization greater than 80%.

(H) All Interfaces over 90% Bandwidth Utilization	Lists all network interfaces with a utilization greater than 90%.
(H) Top 10 Devices by Bandwidth Utilization	Lists the top 10 devices based on their current interface utilization.
(H) Top 20 Devices by Bandwidth Utilization	Lists the top 20 devices based on their current interface utilization.
(H) Top 10 Devices by Interface Traffic	Lists the top 10 devices based on their current interface traffic.
(H) Top 20 Devices by Interface Traffic	Lists the top 20 devices based on their current interface traffic.
(D) Last 4 hours Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 4 hours.
(D) Last 8 hours Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 8 hours.
(D) Last 7 days Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 7 days.
(D) Last 30 days Interface Utilization (single device)	Details all interface utilization percentages for one device over the last 30 days.
(H) Last 4 hours Interface Utilization (specific interface)	Details a specific interface's utilization for one device over the last 4 hours.
(H) Last 8 hours Interface Utilization (single device)	Details a specific interface's utilization for one device over the last 8 hours.
(H) Last 7 days Interface Utilization (specific interface utilization)	Details a specific interface's utilization for one device over the last 7 days.
(H) Last 30 days Interface Utilization (specific interface utilization)	Details a specific interface's utilization for one device over the last 30 days.

Inventory workspace reports	
(H) Total Devices by Type	Lists all monitored network devices by type and number.
(H) Total Active Monitors by Type	Lists all Active Monitors on the network by type and number.
(H) Total Passive Monitors by Type	Lists all Passive Monitors on the network by type and number.
(H) Total Performance Monitors by Type	Lists all Performance Monitors on the network by type and number.
(H) Total Actions Applied by Type	Lists all Actions on the network by type and number.
(H) Total Devices with Specific Attributes	Lists all devices with a specific attribute.
(H) Active Discovery Results	Once an Active Discovery is performed, the results are listed in this report.

Memory Utilization workspace reports	
(D) Last Polled Memory Utilization (single device)	Shows the memory utilization for all of device's memories at the time of the last poll.
(H) Last Polled Memory Utilization (specific aspect)	Shows the memory utilization for a specific network device at the time of the last poll.
(H) All Memories over 80% Utilization	Lists all network devices with a memory utilization greater than 80%.
(H) All Memories over 90% Utilization	Lists all network devices with a memory utilization greater than 90%
(H) Top 10 Devices by Memory Utilization	Lists the top 10 devices based on their current memory utilization.
(H) Top 20 Devices by Memory Utilization	Lists the top 20 devices based on their current memory utilization.
(D) Last 4 hours Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 4 hours.
(D) Last 8 hours Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 8 hours.
(D) Last 7 days Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 7 days.
(D) Last 30 days Memory Utilization (single device)	Details all memory utilization percentages for one device over the last 30 days.
(H) Last 4 hours Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 4 hours.
(H) Last 8 hours Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 8 hours.
(H) Last 7 days Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 7 days.
(H) Last 30 days Memory Utilization (specific aspect)	Details a specific memory's utilization for one device over the last 30 days.

Performance - Historic workspace reports	
(D) Custom Performance Monitor Values (last 4 hours - single device)	Details a device's custom Performance Monitor values over the last 4 hours.
(D) Interface Utilization (last 4 hours - single device)	Details all interface utilization percentages for one device over the last 4 hours.
(D) CPU Utilization (last 4 hours - single device)	Details all CPU utilization percentages for one device over the last 4 hours.

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

Performance - Last Poll workspace reports	
(D) Custom Performance Monitor Values (single device)	Shows the values for all of a device's custom Performance Monitors at the time of the last poll.
(D) Interface Utilization (single device)	Shows the interface utilization for all of a device's interfaces at the time of the last poll.
(D) CPU Utilization (single device)	Shows the CPU utilization for all of device's CPUs at the time of the last poll.
(D) Memory Utilization (single device)	Shows the memory utilization for all of a device's memories at the time of the last poll.
(D) Disk Utilization (single device)	Shows the disk utilization for all of a device's disks at the time of the last poll.
(H) Custom Performance Monitor Values (specific monitor)	Shows the values for a specific device custom Performance Monitor.
(H) Interface Utilization (specific interface)	Shows the utilization of a specific device interface at the time of the last poll.
(H) CPU Utilization (specific CPU)	Shows the utilization of a specific device CPU at the time of the last poll.
(H) Memory Utilization (specific aspect)	Shows the utilization of a specific device memory at the time of the last poll.

(H) Disk Utilization (specific disk)	Shows the utilization of a specific device disk at the time of the last poll.
(H) Ping Response Time (specific interface)	Shows the ping response time of a specific device interface at the time of the last poll.

Ping Availability and Response Time workspace reports	
(D) Last 4 hours (single device)	Shows the ping response time for all of a device's interfaces over the last 4 hours.
(D) Last 8 hours (single device)	Shows the ping response time for all of a device's interfaces over the last 8 hours.
(D) Last 7 days (single device)	Shows the ping response time for all of a device's interfaces over the last 7 days.
(D) Last 30 days (single device)	Shows the ping response time for all of a device's interfaces over the last 30 days.
(D) Last 4 hours (single device)	Shows the ping availability for all of a device's interfaces over the last 4 hours.
(D) Last 8 hours (single device)	Shows the ping availability for all of a device's interfaces over the last 8 hours.
(D) Last 7 days (single device)	Shows the ping availability for all of a device's interfaces over the last 7 days.
(D) Last 30 days (single device)	Shows the ping availability for all of a device's interfaces over the last 30 days.
(H) Last Polled Response Time (specific interface)	Shows the last ping response time of a specific device interface at the time of the last poll.
(H) Top 10 by Ping Response Time	Lists the top 10 devices based on their current ping response time.
(H) Top 20 by Ping Response Time	Lists the top 20 devices based on their current ping response time.
(H) Top 10 by Ping Packet Loss	Lists the top 10 devices based on their current ping packet loss.
(H) Top 20 by Ping Packet Loss	Lists the top 20 devices based on their current ping packet loss.
(H) Devices with Ping Response Time over 100msec	Lists all devices with a ping response time greater than 100 msec.
(H) Devices with Ping Response Time over 500msec	Lists all devices with a ping response time greater than 500 msec.
(H) Devices with Ping Packet Loss over 50%	Lists all devices with a ping packet loss greater than 50%.
(H) Devices with Ping Packet Loss over 75%	Lists all devices with a ping packet loss greater than 75%.
(H) Devices with Ping Availability over 75%	Lists all devices with a ping availability greater than 75%.

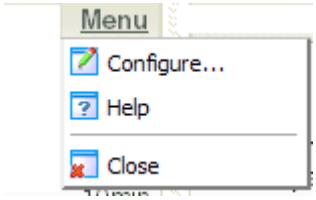
Problem Areas workspace reports	
(D) Devices with Down Active Monitors	Displays a device's down Active Monitors.
(D) All Down Interfaces	Displays a device's down interfaces.
(D) Tail of State Change Log	Displays the tail of the State Change Log for a specified device.
(D) Tail of Syslog	Displays the tail of the Syslog full report for a specified device.
(D) Tail of Windows Event Log	Displays the tail of the Windows Event Log for a specified device.
(D) Tail of SNMP Trap Log	Displays the tail of the SNMP Trap Log for a specified device.
(D) Tail of Action Activity Log	Displays the tail of the Action Activity Log for a specified device.
(D) Tail of Passive Monitor Error Log	Displays the tail of the Passive Monitor Error Log for a specified device.
(D) Web Alarms	Displays any web alarms fired for a specified device.
(H) All Completely Down Devices	Displays down devices for a specified device group.
(H) All Down Interfaces	Displays down interfaces for a specified device group.
(H) Devices with Down Active Monitors	Displays devices with down Active Monitors within a specified device group.
(H) Unacknowledged Devices	Displays unacknowledged devices within a specified device group.
(H) Devices that have fired an Action in the last X hours	Displays devices that have fired an action over the selected time period.
(H) Tail of State Change Log	Displays a tail of the State Change Log for your network.
(H) Summary Counts	Displays a summary of a specified device group.
(H) Tail of Syslog	Displays the tail of the Syslog full report for your network.
(H) Tail of Windows Event Log	Displays the tail of the Windows Event Log for your network.
(H) Tail of SNMP Trap Log	Displays the tail of the SNMP Trap Log for your network.
(H) Tail of Action Activity Log	Displays the tail of the Action Activity Log for your network.
(H) Tail of Passive Monitor Error Log	Displays the tail of the Passive Monitor Error Log for your network.
(H) Map View	Displays a smaller version of a network map.
(H) Device Group Mini Status	Lists all devices in a device group and displays their status by color.
(H) Web Alarms	Shows a snap shot of the most recent web alarms fired on your network.
(H) General Error Log	Displays the tail of the General Error Log for your network.

Threshold workspace reports	
(H) Ping Response Time	Displays the top devices based on their current ping response time thresholds.
(H) Ping Packet Loss	Displays the top devices based on their current ping packet loss thresholds.
(H) CPU Utilization	Displays the top devices based on their current CPU utilization percentage thresholds.
(H) Memory Utilization	Displays the top devices based on their current memory utilization percentage thresholds.
(H) Disk Utilization	Displays the top devices based on their current disk utilization percentage thresholds.
(H) Disk Free Space	Displays the top devices based on their current disk free space thresholds.
(H) Interface Utilization	Displays the top devices based on their current interface utilization percentage thresholds.
(H) Interface Traffic	Displays the top devices based on their current interface traffic thresholds.
(H) Custom WMI/SNMP	Displays the top devices based on their current custom WMI/SNMP thresholds.
(H) Ping Availability	Displays the top devices based on their current ping availability thresholds.

Top 10 workspace reports	
(H) Ping Response Time	Displays the top devices based on their current ping response time.
(H) Ping Packet Loss	Displays the top devices based on their current ping packet loss.
(H) CPU Utilization	Displays the top devices based on their current CPU utilization.
(H) Memory Utilization	Displays the top devices based on their current memory utilization.
(H) Disk Utilization	Displays the top devices based on their current disk utilization.
(H) Disk Free Space	Displays the top devices based on their current disk free space.
(H) Interface Utilization	Displays the top devices based on their current interface utilization.
(H) Interface Traffic	Displays the top devices based on their current interface traffic.
(H) Custom WMI/SNMP	Displays the top devices based on their current custom WMI/SNMP.
(H) Ping Availability	Displays the top devices based on their current ping availability.

About the workspace report menu

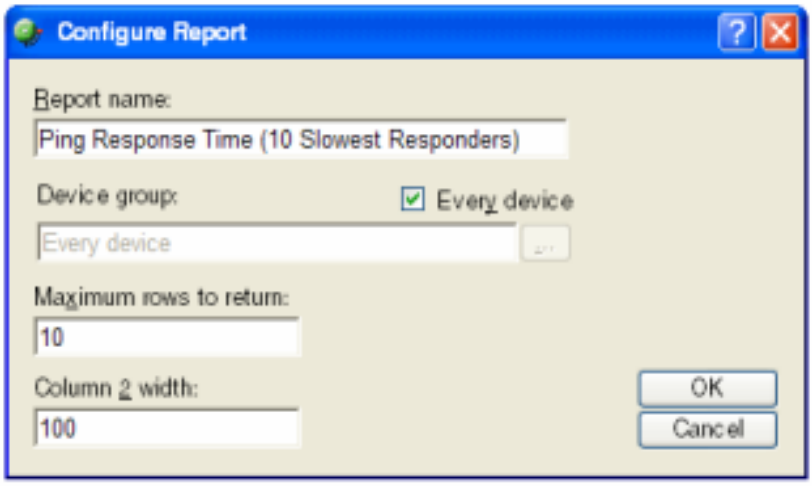
Each workspace report has a menu on the right side of its title bar. From the Workspace Report Menu, you can access help for a specific workspace report, go to the configuration dialog for a report, or close the report. Closing the report removes it from a workspace view. Keep in mind that after you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



Configuring a workspace report

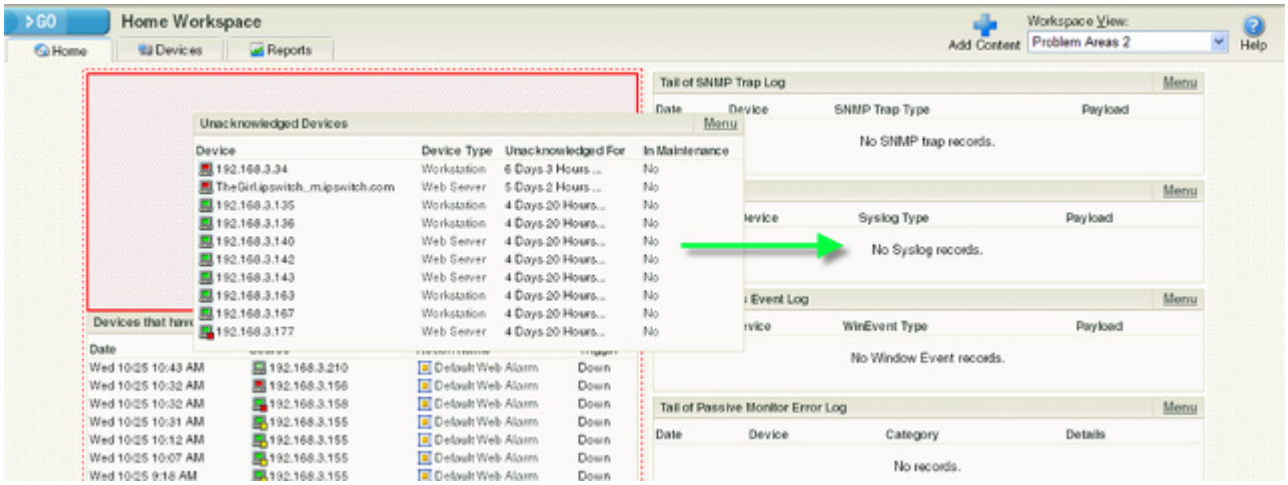
Workspace reports are designed for customization to fit your own specific display needs. From a workspace report's menu, select **Configure** to bring up its Configuration dialog. On the Configuration dialog, you'll have the chance to do a number of things including:

- Changing the report title
- Selecting a device or device group for the report
- Changing the height and width of the report
- Changing the width of certain report columns



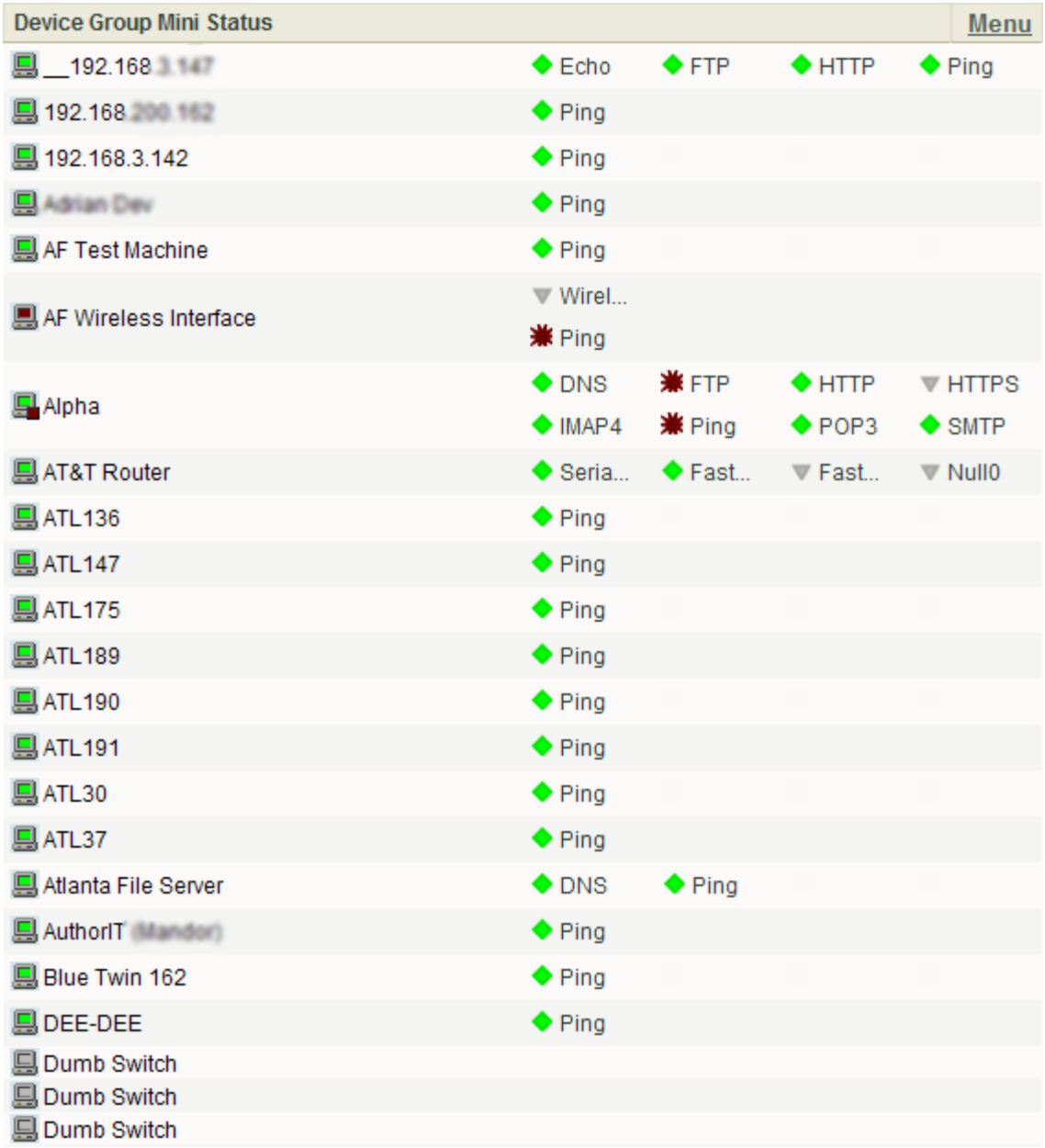
Moving Workspace Reports within a workspace

Ipswitch WhatsUp Gold v11 supports click-and-drag within the web interface. You can move a workspace report from one column of a workspace view to another by selecting it and dragging it to another area of the workspace view. These location changes are saved: workspace reports will appear in the same location in which you moved them after logging out from the web interface, or after moving between workspace views.



Device Group Mini Status workspace report

WhatsUp Gold includes a report similar to What's Up Gold's Mini Status report. In the newest release, it is represented as the Device Group Mini Status workspace report. This 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.



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 have the option to display Active Monitors

associated with the devices in a selected group, which is useful in pin-pointing 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 over 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.

CHAPTER 18

Using SNMP

In This Chapter

SNMP overview

The Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a device (a host, gateway, server, etc.).

A monitoring or management application on the remote user's system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device can provide information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the Management Information Base (MIB). The MIB defines the SNMP objects that can be managed and the format for each object.

The SNMP protocol together with the MIB provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. For a detailed description of SNMP, see Request for Comments (RFC) 1157. For a description of the MIB, see RFC 1213. The MIB information used by WhatsUp Gold is contained in MIB files in the MIB directory.

Monitoring SNMP Service

You can select SNMP on a device's **Services** dialog box (**Properties > Services**) and monitor it just as you can monitor any TCP service. This checks to see if the SNMP service is running on the device.

To monitor whether SNMP is running on a device

First, you need to add an SNMP Active Monitor to the device.

To assign an SNMP Active Monitor to a device:

1. In the Device Properties Active Monitor dialog, click **Add**. The Active Monitor Properties dialog opens.
2. Select the SNMP Active Monitor, then click **Next**.
3. Set the polling properties for the monitor, then click **Next**.
4. Set up an Action for the monitor state changes.
5. 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 or manager software must be installed and enabled on any devices for which you want to receive SNMP information. Windows NT 4.0 and Windows 98, 2000, ME, and XP provide an SNMP agent. Network systems manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

About the SNMP Management Information Base (MIB)

The MIB contains the essential objects that make up the "management information" for the 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 the processing of IP packets, 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.

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.

About SNMP Security

In WhatsUp Gold, credentials are used like passwords to limit access to a devices SNMP data. The credentials system supports SNMP v1, 2, and 3.

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

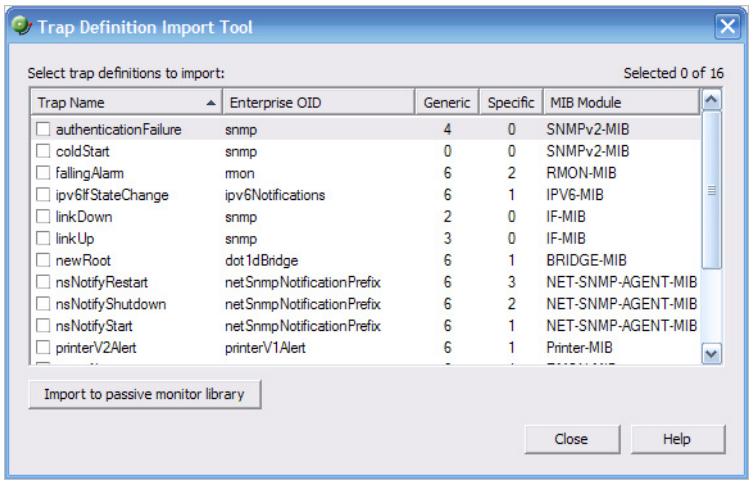
This tool lets you import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your WhatsUp Gold MIB folder: `\Program Files\Ipswitch\WhatsUp\Data\Mibs` folder.

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.

CHAPTER 19

Migrating from Version 7 or 8 of WhatsUp Gold

In This Chapter

Information for WhatsUp Gold v8 and earlier users

The information below, describes many of the changes that you will encounter while moving to this new version of the WhatsUp product line.

WhatsUp Gold v8 and earlier vs. Ipswitch WhatsUp Gold v11 today

Ipswitch WhatsUp Gold v11 offers a completely redesigned User Interface, a new polling engine, a new database structure for storing information about devices, and a new philosophy of user interaction. Processes have been streamlined to make the application easier to use, and more robust in its functionality. When moving from file-based WhatsUp Gold v7 or v8 to database-based Ipswitch WhatsUp Gold v11, you will immediately notice the changes made to the application. The philosophy changes may take a little longer to grasp.

Philosophy changes

In WhatsUp Gold v8 and earlier, everything was centered around device maps. Those maps were used to monitor devices, edit device entries, and display relational information between the devices on the map. If you had multiple locations, or even multiple subnets in each location, you had to have several maps open in your WhatsUp window to monitor them all at once. Furthermore, maps were independent of each other, meaning that you could not have dependencies across maps or have the same device entry on multiple maps (without being polled by each map.)

While maps are still used today, they are now graphical representations of Device Groups, and are one of two ways to display the devices in those groups. The primary means of viewing devices is through the Device List view. This view has a familiar folder and item feel to it, and is very useful when handling many groups or large numbers of devices.

In WhatsUp Gold v8 and earlier, maps handled the polling of the devices on that map. Today, there is a single database that stores all device information, across all device groups and a polling engine that polls them all.

In short, the Device List and group tree has replaced the traditional WhatsUp Gold Maps as the main interface for the user. This gives the user the ability to make dependencies across their network, regardless of grouping; and to have devices appear in multiple groups, with the same information in each device entry.

Terminology changes

The following is a comparison between terminology used in WhatsUp Gold v8 and earlier, and the current product.

WhatsUp Gold v8 and earlier	Ipswitch WhatsUp Gold v11
Events	Passive Monitors
Monitors and Services	Active Monitors
Notifications	Actions
Map	Device Group or Device Map

Import utility

To start the Import utility, from the WhatsUp Gold console, select **Tools > WhatsUp Gold v7/v8 File Data Import**. The Import wizard opens.

This utility migrates data from WhatsUp Gold 7 or 8 into the database. The following is a list of the items that are imported with this utility:

- Maps
- Service Definitions
- Events Library Definitions
- Notification Library Definitions
- Custom Device Type Definitions
- Trap Definitions

This utility can be run at any time, and can be run multiple times. Each time the utility is run, imported maps and devices will be duplicated, but definitions are not duplicated or updated. For example, If XYZ email action exists in the database, the imported XYZ data is ignored, even if the definition was updated in WhatsUp Gold v7/v8 in the meantime.

Back up the database

Before you click **Next**, we recommend that you back up your database, using the **Back up SQL database** utility. Nothing harmful happens to your database as a result of this migration, though results may be a bit confusing if you are not familiar with the new application and terminology.

Note: As soon as the migration utility is run, items added to the database begin polling, even if the migration wizard has not yet completed. Data imported is "live" as it is imported.

Data Source

- Data Source is the third dialog in the WhatsUp Gold v7/v8 Data Migration Utility.

On this dialog, select the path to the WhatsUp Gold v7/v8 installation that you want to migrate into the database. The path can be any drive that is local or mapped from the WhatsUp Gold v7/v8 computer. The drive must be mapped, as the UNC name is not recognized as a valid drive.

This directory contains the WhatsUp Gold v7/v8 configuration definition files. You can select your map files in the next dialog in this utility.

For remotely mapped directories, be aware that modem settings for pagers and beepers will **not** be imported during this process, as these settings reside in the remote computer's registry. In this case, be sure to review the pager/beeper definitions once imported to ensure modem settings are correct.

Note: There may be an issue with custom icons, sound files, background images, and program notifications being imported when migrating WhatsUp Gold v7/v8 data from a remote drive. Since the WhatsUp Gold v7/v8 definition files may reference absolute directory locations, from the perspective of the remote computer, these types of files may need to be copied manually and re-setup for use in the current product.

Maps to transfer

- Maps to Transfer is the fourth dialog in the WhatsUp Gold v7/v8 Data Migration Utility.

Browse and select the map files that you want to import into the database. These files can reside on any mapped drive on your network, and may be any valid map file type (wup, xml, or ini.) Select all or a subset of maps to import.

If you only want to import definitions and not your WhatsUp Gold maps, you may leave this list blank.

Note: Be certain you are ready to begin importing data before you click **Next.** As soon as the process begins, data is being written to the database, and can not be 'backed out' without restoring a previously backed up database. You can stop the process, but any data written to the database will stay there until it is removed manually or overwritten during a database restore.
If devices are duplicated in the imported WhatsUp Gold map files, this utility creates duplicate devices for each that is found. Each device instance will be polled as if it were a different device. You may want to condense these entries after completing the migration, and create "shortcuts" in the device groups instead of each duplicated device.

Report of Migration Results

- Migration Results is the fifth dialog in the WhatsUp Gold Data Migration Utility.

This dialog displays messages that the migration utility generates during the upgrade process.

Be sure to review the results and review any warning or error that you may find. If there is an error with an imported file, review the map file that was indicated.

If there is an SQL error, be aware that the problem may be an unexpected setup or condition and you may need to contact Ipswitch Technical Support or the Knowledge Base for potential work-around.

Trigger time warnings may effect your desired notification settings. Review those triggers and determine which best suits your needs. You can change those settings to a predefined state change, or create a new one to more closely match your original WhatsUp Gold v7/v8 settings and them re-import.

If you would like to view this log later, you can access it at any time from the <install directory>/data/logs directory, as it contains a history of all migration attempts. This log is also useful for customer support calls.

Finished

Click **Finish** to close this utility.

Important: Remember that maps are already live in your database, and are already being polled and alerts are active. Clicking **Cancel** now does not roll back changes to a pre-migration state. Data is live and is being used. To revert, you can restore the backed up database.

CHAPTER 20

Using Ipswitch WhatsUp Gold v11 Premium Edition

In This Chapter

What is in Ipswitch WhatsUp Gold v11 Premium Edition?

The Premium Edition is available for separate purchase. It provides all of the network monitoring capabilities of WhatsUp Gold and extends the product to allow additional monitoring of applications and servers, including:

- Microsoft® Exchange™ and Microsoft SQL Server: lets 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 undergoes an unexpected rate of change.

For more information about the Premium Edition, and for purchase information, see the network management product pages (http://www.ipswitch.com/products/network-management.asp) on the Ipswitch website.

Monitoring a Microsoft Exchange Server

The Exchange Monitor is a module to WhatsUp that 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.

Note: Exchange Monitor is part of the WhatsUp Gold Premium Edition, which extends WhatsUp Gold to provide application monitoring of Microsoft Exchange and Microsoft SQL servers, as well as any WMI-enabled application.

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 follows:

1. Determine which Exchange parameters (on page 246) to monitor.
2. Determine which Exchange services (on page 247) 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 (Only if WhatsUp Gold Premium Edition has been activated):

1 Go to the Active Monitor Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Active Monitor Library**.

  - or -

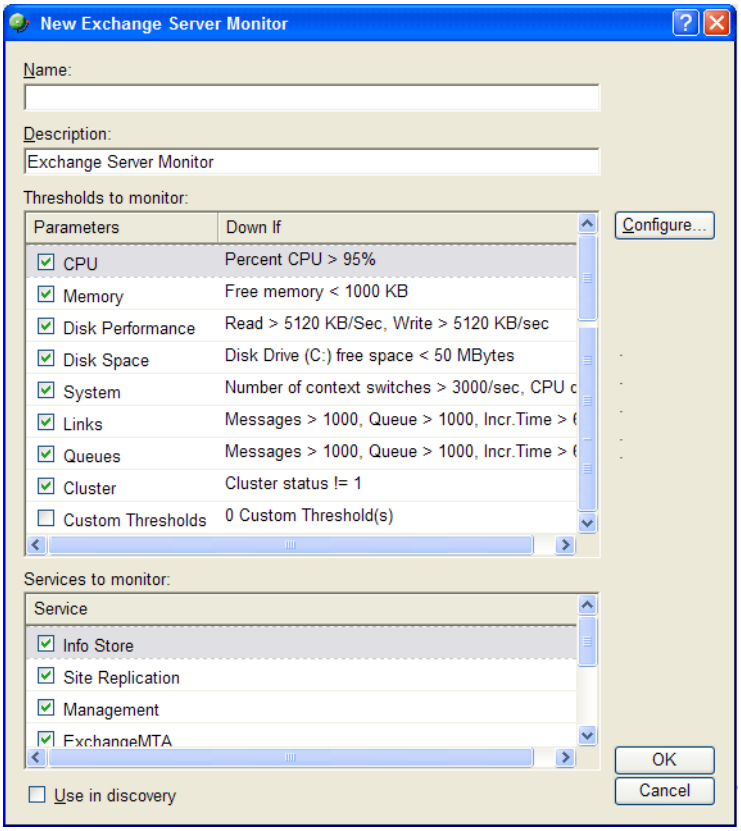
- From the main menu bar of the WhatsUp Gold console, select **Configure > Active Monitor Library**. The Active Monitor Library appears.

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 opens.

b) Select **Exchange Monitor** from the list. The New Exchange Monitor Server dialog opens.



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 (see Thresholds table (on page 246)).

f) Select the services to monitor (see Services table (on page 247)).

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 opens.

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 96).

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

If you have created other Active Monitors in WhatsUp Gold, you'll find that the Exchange Monitor works in much the same way.

To monitor what's happening with the operating system on the Exchange server, we'll 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, we check thresholds for the CPU, Memory, and System parameters. We also have this monitor check the state of the System Attendant service.

1 In the web interface, select **Go > Configure > Active Monitor Library**, then click **New**. The Select Active Monitor Type dialog opens.

2 Select Exchange Monitor and click **OK**. The New Exchange Server Monitor dialog opens.

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.

3 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 opens.

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 96).

After you complete the wizard, the monitor immediately begins to monitor the Exchange server.

For status information on your Exchange Monitor, you can check any of the Active Monitor Reports:

- Active Monitor Availability
- Active Monitor Outage
- Health
- State Change Timeline
- State Summary
- Workspace reports

Monitoring Microsoft SQL Server

The SQL Server Monitor is a module to WhatsUp that lets you monitor the Microsoft® SQL Server application. The SQL Server Monitor provides real-time information about the state and health of Microsoft SQL Server applications on your network.

Note: SQL Server Monitor is part of the WhatsUp Gold Premium Edition, which extends WhatsUp Gold to provide application monitoring of Microsoft Exchange and Microsoft SQL servers, as well as any WMI-enabled application.

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 (on page 43), you can detect a looming problem before it causes an application or service failure.

How to get started using SQL Server Monitor

Here is a basic approach to using the 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 (Only if WhatsUp Gold Premium Edition has been activated):

1 Go to the Active Monitor Library:

- In the WhatsUp Gold web interface, select **Go > Configure > Active Monitor Library**.

  - or -

- From the main menu bar of the WhatsUp Gold console, select **Configure > Active Monitor Library**. The Active Monitor Library appears.

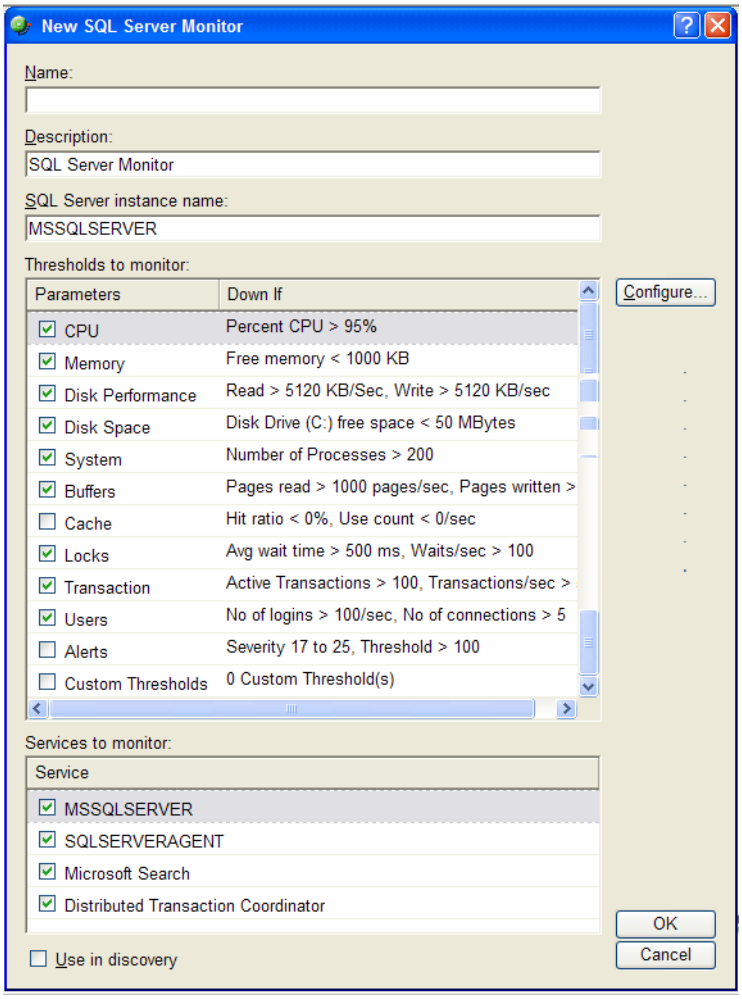
Tip: The Active Monitor Library is the starting point for creating any Active Monitor in WhatsUp Gold. This dialog shows all of the Active Monitors in your database.

2 Add an SQL monitor:

a) Click **New**. The Select Active Monitor Type dialog opens.

b) Select SQL Service Monitor and click **OK**.

c) The New SQL Service Monitor dialog opens.



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 will monitor.

g) Select the thresholds to add to the monitor (see Thresholds table (on page 252)).

h) Select the services to add to the monitor (see Services table (on page 252)).

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 opens.

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 96).

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

If you have created other monitors or services in WhatsUp, you'll find that the SQL Monitor works in much the same way.

To monitor user activity, we'll create a monitor called "SQLUser," then select Users as the only parameter to monitor.

1. In the web interface, select **Configure > Active Monitor Library**, then click **New**. The Select Active Monitor Type dialog opens.
2. Select SQL Server Monitor and click **OK**. The New SQL Server Monitor dialog opens.
   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.
3. 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 opens.

      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 96).

After you complete the wizard, the monitor immediately begins to monitor the SQL Server application.

For status information on your SQL Server monitor, you can check any of the Active Monitor Reports:

- Active Monitor Availability
- Active Monitor Outage
- Health
- State Change Timeline
- State Summary
- Workspace reports

Monitoring WMI-enabled applications

The WMI Monitor is a module to WhatsUp that 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 WhatsUp Gold to provide application monitoring of Microsoft Exchange and Microsoft SQL servers, as well as any WMI-enabled application.

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, your users will be unable to 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 get started using WMI Monitor

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.

Example: WMI Monitor

If you have created other Active Monitors in WhatsUp Gold, you'll find that the WMI Monitor works in much the same way.

Here is our scenario: A device on your network has been illegally logged into through a 'brute force' attack where someone used 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 that is accessed is on your domain or has sensitive information stored on it. To keep this from happening again, you decide that you need to know immediately when such attacks are attempted.

By creating a custom WMI Active Monitor that checks the appropriate performance counters on a Windows device, you can have WhatsUp Gold notify you when this type of attack occurs, so you can do something about it before they get in.

To configure this type of Active Monitor:

1. Using the WhatsUp Gold web interface, create the WMI monitor.
   a) In the web interface, select **Go > Configure > Active Monitor Library**, click **New**. The Select Active Monitor Type dialog opens.
   b) Select **WMI Monitor** and click **Ok**. The Add WMI Monitor dialog opens.
   c) In the **Name** box, enter "ErrorsLogon" to identify that this monitor checks for logon errors.
   d) Click the **Browse** (**…**) button next to **Instance** to access the Performance Counters dialog.
   e) Enter the share name or IP address of the computer you want to connect to.
   f) 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.

g) Enter the password for the login used above and click **OK** to connect to the computer. The Performance Counters dialog opens.

h) In the **Performance object** box, select Server.

i) In the Server folder, select the performance counter named: ErrorsLogon

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 opens.

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 96).

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.

CHAPTER 21

Troubleshooting

In This Chapter

Database Performance Tool

This is a database troubleshooting tool that 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 database 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 MSDE as the WhatsUp Gold database, this section also displays the percentage of the 2GB 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. More information can be found in Microsoft's "Books On-Line" for SQL Server (http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp).

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.) More information can be found in Microsoft's "Books On-Line" for SQL Server (http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp).

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 it the entire subnet, or a single device ?
- Is it the entire device, 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 if it is a monitor or the device that is down. If it is the device, all of the monitors will appear down.
- Check out the Ping monitor. If it is up, you can be certain that the connection between the network and that device is up.
- If it is a monitor that appears to be down, begin by trying to restart the service on the device the monitor is running on. This is on the actual device itself, not through WhatsUp Gold.

WhatsUp Gold engine message

This message means that Ipswitch WhatsUp Gold v11 is not operating properly, because the Ipswitch WhatsUp Gold v11 Engine service has stopped.

To restart the service:

1. Open the Windows **Control Panel**.
2. Select **Administrative Tools > Services**. The Services window appears.
3. Select **Ipswitch WhatsUp Engine**, then click **Start**.

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-mouse 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.

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 RPCPingTimout registry value:

1. Go to **Start > Run > Regedit.exe**
2. From the Registry Editor go to:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Network Monitor\WhatsUp Engine\2007\Settings`

3 Within the Settings folder, select **RPCPingTimeout** and right-click. From the right-mouse 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.

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.

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 262).

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.

Index

E

G

I

M

N

O

P

R

S

T

U

V

W