

---

# Ipswitch WhatsUp Professional and Premium Edition 2006

**User's Guide**

Software Version 2

**Ipswitch Inc.**

**Web: [HTTP://www.ipswitch.com](http://www.ipswitch.com)**

**10 Maguire Rd, Suite 220**

**Phone: 781.676.5700**

**Lexington, MA 02421**

**Fax: 781.676.5710**

## **Copyrights**

©1995-2006 Ipswitch, Inc. All rights reserved.

Ipswitch WhatsUp Professional and WhatsUp Professional Premium Edition 2006  
User's Guide

This manual, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the expressed prior written consent of Ipswitch, Inc.

The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. also assumes no liability for damages resulting from the use of the information contained in this document.

IMail, the IMail logo, WhatsUp, the WhatsUp Professional logo, WS\_FTP, the WS\_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

## **Production History**

March 2005

First edition.

November 2005

Second edition.

# Contents

## Chapter 1 Welcome

How it Works .....	1
WhatsUp Professional Premium Edition .....	1
New in WhatsUp Professional 2006 .....	2
Finding More Information .....	3

## Chapter 2 Installation and Configuration

First-time Install .....	5
Upgrading .....	5
System Requirements .....	6
Requirements for WhatsUp Professional .....	6
Requirements for MSDE 2000 .....	7
Installation Notes .....	7
Installing or Upgrading .....	7
Activating the WhatsUp Application .....	9
Migrating Data from WhatsUp Gold .....	10
Uninstalling .....	10
MSDE Database .....	11
Database Utilities .....	12
Database Backup and Restore .....	12
Database Performance Tool .....	12
Database Table Maintenance .....	13
Alternative Database Setups .....	13
Upgrading a Non-Default Configuration of MSDE 2000 or SQL Server 2000 .....	14
Creating a new WhatsUp Database on an Existing SQL Server on the Same Computer .....	17
Creating a New WhatsUp Database on an Existing SQL Server on a Remote Computer .....	19
Installing a New SQL Server Instance and Creating a New What- sUp Database .....	21
Configuring the Web Interface to use Microsoft IIS .....	22

## Chapter 3 Migrating from WhatsUp Gold

Philosophy Changes.....	25
Terminology Changes.....	26
Migrating Data from WhatsUp Gold to WhatsUp Professional.....	26
Using the Migration Utility.....	27

## Chapter 4 Device Discovery

Using the Wizard.....	29
Scan Types.....	29
Device Discovery - A Simulation.....	30
Discover Devices.....	30
Adding a Single Device.....	34
Manual Addition - A Simulation.....	34
Click and Drag.....	36
Active Discovery.....	37
Example: Configuring Active Discovery.....	37

## Chapter 5 Devices

Device Troubleshooting?.....	41
Device Services.....	41
Device Properties.....	42
Device Properties - General.....	42
Device Properties - Performance Monitors.....	43
Device Properties - Active Monitors.....	44
Device Properties - Passive Monitors.....	45
Device Properties - Actions.....	46
Device Properties - Credentials.....	47
Device Properties - Polling.....	48
Device Properties - Notes.....	51
Device Properties - Menu.....	52
Device Properties - Attributes.....	53
Device Types.....	54
Device Groups.....	55
Organizing Device Groups.....	55
Dynamic Groups.....	56
Editing Multiple Devices - Bulk Field Change.....	56
Acknowledgements.....	58
Acknowledging a State Change.....	59
Credentials Overview.....	59

## Chapter 6 Using the WhatsUp Professional Console

Console Overview .....	61
Device View .....	62
Device Icons.....	63
Organizing Devices and Device Groups.....	64
Map View .....	64
Device Layout.....	65
Adding Annotations to a Map.....	66
Link Lines .....	66
How to Create Connecting Links.....	67
Attached Lines .....	68
Report View .....	69

## Chapter 7 Using the Web Interface

Connecting to the Web Interface .....	71
Web Interface Overview .....	72
Managing Web Users.....	74
Device Group Access Rights .....	76
Web Interface Operations and Device Group Access Rights .....	78
Managing the Web Server .....	80
Securing the Web Interface.....	81
Configuring the Web Interface to use IIS.....	81

## Chapter 8 Performance Monitors

Performance Monitor Library .....	83
Configuring Performance Monitors .....	85
Configuring a single device .....	85
Configuring multiple devices.....	86
Performance Reporting .....	86
Device Status Report.....	87
Group and Device Performance Reports .....	88
Top 10 Report .....	88
Example: Monitoring Router Bandwidth .....	88
Configuring the Monitor .....	89
Viewing the Data .....	90
Example: Troubleshooting a Slow Network Connection .....	91
Custom Performance Monitors .....	93
To create custom performance monitors (to be used system wide) .....	93

To create a custom performance monitor to use on a single device.....	95
Example: Custom Performance Monitors.....	95
Enabling SNMP on Windows Devices.....	96
To install SNMP Monitoring.....	96
To enable SNMP Monitoring.....	96

## Chapter 9 Active Monitors

Monitors and Actions.....	99
Active Monitor Library.....	100
Supported Active Monitors.....	101
Assigning Active Monitors.....	101
Deleting Active Monitors.....	102
Group and Device Active Monitor Reports.....	103
Example: Monitoring Network Printer	
Toner Levels.....	104
Configuring the Monitor.....	104

## Chapter 10 Passive Monitors

Configuring Passive Monitor	
Listeners.....	105
Passive Monitor Library.....	106
Configuring Passive Monitors.....	107
Using the Trap Definition Import Tool.....	108
Group and Device Passive Monitor Reports.....	108

## Chapter 11 Actions

Action Library.....	109
Action Types.....	110
Action Strategies.....	111
Using Actions - A Simulation.....	112
Configure the Action.....	112
Test the Action.....	114
Assigning an Action to a Device.....	116
Assigning an Action to a Monitor.....	118
Blackout Periods.....	119
Action Policies.....	119
Implicit Action Policy.....	120
.....	121
Using Other Types of Actions.....	121
Percent Variables.....	122

## Chapter 12 Reports

Collecting Performance Data .....	125
Report List .....	126
Saving a Report .....	129
Recurring Reports .....	129
Creating Custom Reports .....	130
Step 1 - Add the report to the Report database table. ....	130
Step 2 - Open the Custom Report Template. ....	130
Step 3 - Add custom report content to the template.....	132
Step 4 - Save the new report file. ....	135
Sample Report.....	135

## Chapter 13 Premium Edition

Exchange Monitor.....	139
Why use it? .....	139
How to get started using the Exchange Monitor.....	140
Examples.....	140
SQL Server Monitor .....	142
Why use it? .....	142
How to get started using SQL Server Monitor .....	142
Example .....	143
WMI Monitor.....	144
Why use it? .....	145
About WMI.....	145
WMI Support Links .....	145
Troubleshooting WMI .....	146



# Welcome

Welcome to Ipswitch WhatsUp Professional and WhatsUp Professional Premium Edition 2006. This guide provides general information about using the product, as well as specific instructions on how to configure the application to work best in your network environment.

## How it Works

WhatsUp Professional 2006 is a powerful network monitoring solution designed to help you protect your growing business. WhatsUp Professional uses a relational database to store information about the devices on your network that are being monitored by the application. That information allows the application to effectively watch over your network by actively polling devices and services, or by listening for messages sent across your network.

Depending on the response from this polling, WhatsUp Professional then fires Actions based on the device state change that is invoked by the response or message.

WhatsUp Professional provides a series of reports that lets you view real-time and historical data based on the devices and monitors configured in your database.

## WhatsUp Professional Premium Edition

The Premium Edition is available for separate purchase. It provides all of the network monitoring capabilities of WhatsUp Professional 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.

# Chapter 1

## In this Chapter

---

How it Works

WhatsUp Professional  
Premium Edition

New in WhatsUp Professional

Finding More Information

---

- 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 on our web site at:

<http://www.ipswitch.com/products/network-management.asp>

## New in WhatsUp Professional 2006

These features were introduced in the release of Ipswitch WhatsUp Professional 2006:

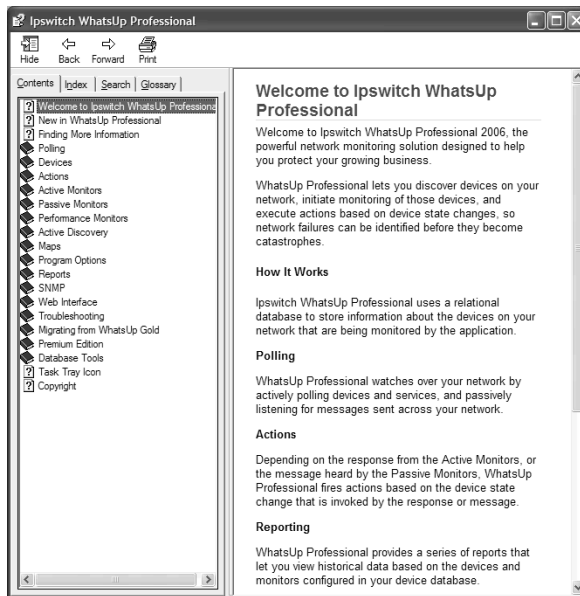
- Enhanced reporting capabilities that show how devices are performing over time, for example:
  - Top 10 Report
  - CPU Utilization Report
  - Disk Utilization Report
  - Interface Utilization Report
  - Memory Utilization Report
- Monthly Recurring Reports and Recurring Reports based on smaller intervals.
- Recurring Actions let you send a current status "snapshot" via an Action, such as pager, email, SMS, or beeper.
- SSL Monitoring lets you monitor any TCP/IP monitor (that supports SSL) through an SSL connection. For example, monitor secure web content via HTTPS.
- Custom monitoring (Active Script Monitor) and actions (Action Script) let you create monitors or actions for specific devices using standard scripting syntax (VBScript/JScript).
- SNMPv3 support allows polling of SNMP values from an SNMPv3 device for higher security.
- Dynamic Device Groups let you group devices by a specified property, such as "all routers," for easier management and reporting.
- MAC Address Finder/Reporter maps MAC (interface hardware) addresses to IP addresses and shows who is connected to the switch.
- Web Alarms provide a visible and audible alarm on the web interface.
- Router Bandwidth Monitoring shows current interface utilization as well as tracking utilization over time.

- Credentials Library allows centrally managed SNMPv1, SNMPv2, and SNMPv3 connection credentials, and WMI connection credentials.
- Implicit Action Policy lets you create an action policy that is global to all devices.
- Database Performance and Maintenance tools.
- Additions to Bulk Field Change let you edit multiple devices to change properties for Credentials, Performance Monitors, and Active Monitors.

## Finding More Information

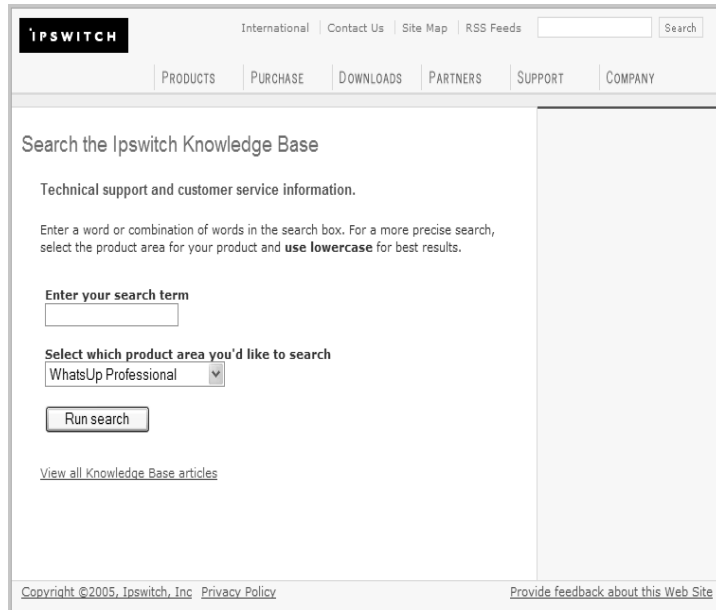
The documentation for WhatsUp Professional consists of three different parts, each part fitting a specific user need, and containing a specific type of information.

**Online Help for the console:** contains dialog assistance, general configuration information, and procedures that explain how to use the features. The Table of Contents is organized by functional area, and can be reached by selecting it from the main menu, or by pressing the [F1] key in any dialog.



**Online help for the web interface:** contains dialog assistance, procedures that explain how to use features, Table of Contents, Index, and Glossary.

**Knowledge Base:** You can search the Ipswitch Knowledge Base of technical support and customer service information. The URL is: <http://support.ipswitch.com/kb/>



The screenshot shows the Ipswitch Knowledge Base search interface. At the top left is the Ipswitch logo. To its right are navigation links: International, Contact Us, Site Map, RSS Feeds, and a search box with a Search button. Below this is a horizontal menu with links for PRODUCTS, PURCHASE, DOWNLOADS, PARTNERS, SUPPORT, and COMPANY. The main content area is titled "Search the Ipswitch Knowledge Base" and includes the text "Technical support and customer service information." Below this is a search instruction: "Enter a word or combination of words in the search box. For a more precise search, select the product area for your product and use lowercase for best results." There is a text input field for the search term, a dropdown menu for the product area (currently showing "WhatsUp Professional"), and a "Run search" button. A link for "View all Knowledge Base articles" is located below the search form. The footer contains the copyright notice "Copyright ©2005, Ipswitch, Inc Privacy Policy" and a link to "Provide feedback about this Web Site".

# Installation and Configuration

## Chapter 2

Installing WhatsUp Professional 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 WhatsUp Professional 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 MSDE.
- Creates a Data Source Name (DSN), which tells WhatsUp Professional where to find the WhatsUp database.
- Installs the WhatsUp Professional application.

Read the “System Requirements” on page 6, then follow the steps in “Installing or Upgrading” on page 7.

### Upgrading

If you are upgrading from a previous version of 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:

- An MSDE 2000 WhatsUp instance is installed on the computer on which you are installing WhatsUp Professional.
- The WhatsUp database exists on the database server.
- A DSN is configured for the WhatsUp database.

### In this Chapter

---

System Requirements

Installation Notes

Installing or Upgrading

Uninstalling

MSDE Database

Alternative Database Setups

Configuring the Web Interface to Use Microsoft IIS

---

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

Read the “System Requirements” on page 6, then follow the steps in “Installing or Upgrading” on page 7, and if necessary, configure the database manually as shown in “Alternative Database Setups” on page 13.

## 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 Professional installation has completed. For more information, see “Alternative Database Setups” on page 13.

# System Requirements

## Requirements for WhatsUp Professional

- Supported operating systems are: Windows 2003 Server; Windows XP SP1 or later; Windows 2000 SP4.

**Note:** If you have Windows XP Service Pack 2 installed, you need to read the release notes regarding issues with this Service Pack *before you install*.

- 265 MB of free disk space

**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.

- 256 MB Memory (RAM)
- To use pager, SMS, or beeper actions, a local modem and phone line is required (WhatsUp Professional 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:

<http://www.microsoft.com/speech/download/sdk51/>

- Microsoft Internet Explorer 5.01 or greater
- Microsoft Windows Scripting Host 5.6
- To download Windows Scripting Host, go to:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnanchor/html/scriptinga.asp>

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

## Requirements for MSDE 2000

- MSDE has a 2 GB data limit. Make sure you select a large capacity drive for data storage.
- MSDE 2000 requires that Microsoft Internet Explorer 5.0 or later be installed. A minimum installation is sufficient, and Internet Explorer does not have to be the default browser.
- File and print sharing must be active to install MSDE 2000. To verify:
  - Select **Start > Settings > Network Connections**.
  - Select **Advanced > Advanced Settings**.
  - 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 on 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 Professional 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.

- 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**, and then enter the CD path followed by `AutoRun.exe`. For example: `D:\AutoRun.exe`
- If you downloaded WhatsUp Professional from our Web site, run the downloaded installation application.

### 3 Read the Welcome screen.

The Welcome screen shows an estimate of how long it takes to install the application, displays an Activation message, and displays buttons that provide access to release notes and this guide (User's Guide).

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 will install 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 9.

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. (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 13.

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

Click **Next** to continue.

### 6 Select the installation directory for the WhatsUp Professional application files.

The default path is `C:\Program Files\Ipswitch\Whatsup Professional 2006`. It is recommended that you use the default, but you can choose a different path. Some users prefer to put application files on a partition separate from the operating system, which is usually installed on the C: drive.

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

If you have previously installed WhatsUp Professional, 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.

- 8 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.
- 9 Click **Install** to install the WhatsUp Professional application files.

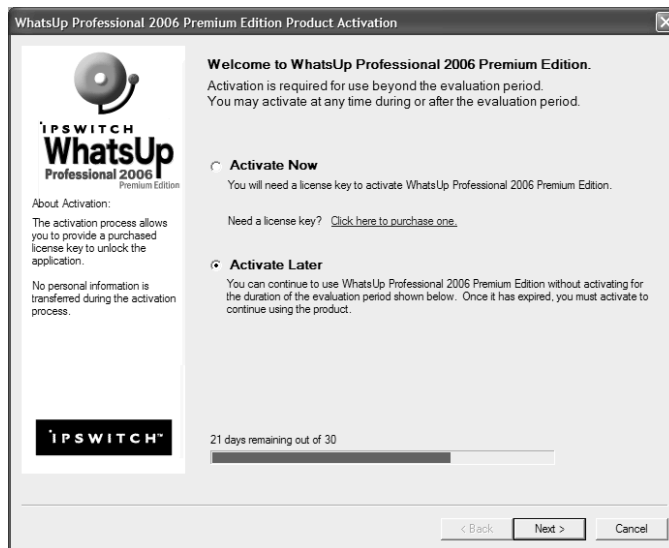
WhatsUp Professional gives you the option to go back and change options or cancel prior to completing the installation.

- 10 Installation of the core application is complete. You can read the Release Notes (which you should already have done!) and you can launch WhatsUp Professional. Make your selections, then click **Finish**.

If you choose to launch now, the next screen introduces you to the Discover Devices wizard, which lets you set options on how to discover your network. If you choose to postpone these steps, click the **Cancel** button. For information on how to use the Discover Devices wizard, see “Devices” on page 41.

## Activating the WhatsUp Application

If you have not activated the product, when you start WhatsUp, a welcome screen displays the following options:



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**

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

#### **Offline activation**

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

For more information about licensing, go to:

[http://www.ipswitch.com/support/cs\\_center.html](http://www.ipswitch.com/support/cs_center.html)

## **Migrating Data from WhatsUp Gold**

Chapter 3 of this guide describes how to migrate data from WhatsUp Gold versions 7 and 8 to WhatsUp Professional 2006. You must complete the WhatsUp Professional installation before migrating your data.

## **Uninstalling**

To uninstall WhatsUp Professional, click **Start > Settings > Control Panel**, then select **Add or Remove Programs**. Select Ipswitch WhatsUp Professional, then select **Remove** when prompted.

The following dialog shows the uninstall options:



- If you are upgrading from WhatsUp Professional v1.0, or the SP1a release, you do not need to uninstall.
- If you have a beta or other test version of the 2006 release, before installing the new version, you should uninstall and select the first option, which removes the application but leaves your network data intact.

## MSDE Database

The WhatsUp Professional 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, new developers learning how to build data-driven applications, and Web sites serving up to 25 concurrent users.”

For more information, go to: <http://www.microsoft.com/sql/msde/>

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

- WhatsUp Professional CD-ROM

- Microsoft Developer Network. Go to <http://msdn.microsoft.com> and search on **MSDE** to find information on MSDE and the latest downloads.

**Note:** Microsoft has issued a patch to MSDE 2000. Go to the Microsoft website for more information, and for instructions on how to download this patch.

<http://support.microsoft.com/?kbid=815495>

## Database Utilities

You can use the WhatsUp database utilities to back up and restore the database and to perform database maintenance and troubleshooting. These Utilities, described in the following sections, are available from the WhatsUp Professional main menu, by selecting **Tools > Database Utilities**.

### Database Backup and Restore

Through this feature, you can back up your complete WhatsUp Professional SQL 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.

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.

If you want to back up the 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.

This WhatsUp feature does a complete backup and restore, so any change that you make after the backup will be overwritten when the restore process is complete.

To access this feature:

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

### 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, much in the same way that disk fragmentation causes your computer to run slower.

From the WhatsUp Professional main menu, select **Tools > Database Utilities > Tools**, then select the Performance category.

For a detailed description, see the help topic: Database Performance Tool

## Database Table Maintenance

This feature lets you purge expired data from data tables in your database.

To access this feature, from the WhatsUp Professional main menu, select **Tools > Database Utilities > Tools**, then select the Table Maintenance category.

For a detailed description, see the help topic: Database Tools Table Maintenance

## Alternative Database Setups

Though we strongly recommend using the default database, which is MSDE 2000, you can configure WhatsUp Professional to use a custom database. This requires manually configuring the database, so you need to know how to set up your particular database program. You may want to do this if you want to:

- Use a database other than MSDE 2000
- Run the database on a computer separate from the one on which you will install WhatsUp Professional.

Supported databases:

- MSDE 2000
- Microsoft SQL Server 2000

Here's an overview of what you need to manually configure the database. The following sections expand on each of these steps.

- 1** Make sure the database server is installed on the appropriate computer. We recommend installing as the named instance: "WhatsUp"
- 2** Create a database called WhatsUp.
- 3** Create or edit the DSN that tells WhatsUp Professional 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 Professional or on a separate computer.

The following sections outline the steps required given different scenarios.

## Upgrading a Non-Default Configuration of MSDE 2000 or SQL Server 2000

Features in WhatsUp Professional 2006 mandate an update of the original database schema. The following procedure steps through how to upgrade an installation of WhatsUp Professional that is a non-default configuration. A non-default configuration is one that does not meet the following conditions:

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

All other configurations are considered a non-default configuration.

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

The WhatsUp Professional installation program will notify you if the database is in a non-default configuration. The procedures differ depending on whether the database server is on the same computer as WhatsUp Professional.

**Note:** Before updating the database schema, we recommend that you take the time to backup your existing data. To back up the data, do one of the following:

- If you are working on the computer on which WhatsUp Professional is installed, in WhatsUp Professional, select **Tools > Database Utilities > Back up SQL Database**.

- Execute the following SQL Command within the SQL Server Query Analyzer (this tool is part of the Enterprise Manager that can be found on the SQL Server CDs):

```
BACKUP DATABASE WhatsUp TO DISK='{path}\db_backup.dat'
```

ex: `BACKUP DATABASE WhatsUp TO DISK='C:\db_backup.dat'`

- Use the `osql` command to back up the database:

```
Osql -E -D <DSN> -Q "BACKUP DATABASE WhatsUp TO  
DISK= '{path}\db_backup.dat'"
```

Or,

```
Osql -E -S <machine\instance name> -Q "BACKUP DATABASE WhatsUp TO  
DISK= '{path}\db_backup.dat'"
```

To upgrade the database from the WhatsUp Professional 2005 schema version to WhatsUp Professional 2006 schema version, follow these steps:

- 1 If your WhatsUp database is not on the same computer as WhatsUp Professional, copy the *DB Scripts* directory and its contents 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.
- 3 Run the upgrade scripts, in one of the following ways:
  - a Run the VB script (as shown in Step 4). The VB script executes each script in sequence.
  - b Run each upgrade script manually (as shown in Step 4).

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

Before running the scripts, close the WhatsUp Professional application; then shut down the WhatsUp Engine (right-click the task tray icon, and select **Close**).

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

#### VB Script:

To execute the VB Script that follows, you must have the Windows Scripting Host (v5.6) installed on the system where you plan to execute "upgrade\_db.vbs." If your system does not have the Windows Scripting Host installed, you must either download the Windows Scripting Host from Microsoft, or manually run the upgrade scripts as detailed below.

To download Windows Scripting Host, go to:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnanchor/html/scriptinga.asp>

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

Note: If the SQL Server and WhatsUp Professional are on the same machine, then run `upgrade.vbs` without specifying any arguments.

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

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

where the argument, <sql server name>, specifies the computer name/database instance name.

For example:

```
cscript upgrade_db.vbs -E -S
computer123\MySQLServerInstanceName
-d whatsapp
```

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

#### 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 from Step 1 in the previous procedure.

No trailing slash ( \ ) should be used in the replacement string.

Some of the upgrade scripts will have no placeholders; some will have more than one.

Save each updated file.

- 2 Run the scripts by using SQL Server Enterprise Manager (available on the SQL Server CD).

**IMPORTANT!!!** Open the SQL Server Enterprise Manager and select the server running the "WhatsUp" database. From the Enterprise Manager, open the SQL Server Query Analyzer, and select the **WhatsUp** 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, and then execute by pressing the F5 key, in order.

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.

Following successful execution of both scripts, your WhatsUp Professional 2006 database will have been updated and should be ready for use by WhatsUp Professional 2006. All data previously collected should be present within the updated database.

- 3 To confirm 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. You can now launch NMConsole.exe or start the application via the program shortcuts.

## Creating a new WhatsUp Database on 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 Professional.

You must first complete the WhatsUp Professional 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 Professional console, select **Tools > Database Utilities > Back Up SQL Database**. Enter a name for the backup file, for example: 2005cleanDB.dat

Or, from the command line, enter:

```
osql -E -D whatsup -Q "backup database to
disk='C:\2005cleanDB.dat'"
```

- b** Restore the backup to your SQL Server. From the command line, go to the directory where you saved the backup file, and enter:

```
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:\2005cleanDB.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 WhatsUp Professional installation. To do this:

- a** At the DOS prompt, navigate to the directory where WhatsUp Professional is installed, and enter: Nmservice /Service:

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 Ipswitch WhatsUp Professional 2006 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**.

## Creating a New WhatsUp Database on 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 WhatsUp Professional installation, then configure Microsoft SQL Server 2000.

- 1 Move the database to the SQL Server instance.

Backup the clean MSDE 2000 WhatsUp database.

From the WhatsUp Professional console, select **Tools > Database Utilities > Back Up SQL Database**. Enter a name for the backup file, for example: 2005cleanDB.dat

OR, from the command line, enter:

```
osql -E -D whatusp -Q "backup database to  
disk='C:\2005cleanDB.dat'"
```

- 2 Turn on TCP/IP.

On the computer on which Ipswitch WhatsUp Professional 2006 was installed, from Windows Explorer select **C:\Program Files\Microsoft SQL Server\80\tools\bin\SVRNETCN.exe**.

- a Click the General tab and enable TCP/IP.
  - b You must now stop and restart the SQL server.
- 3 On the WhatsUp Professional computer, create a System Data Source Name (DSN).
  - a On the computer on which Ipswitch WhatsUp Professional 2006 was installed, click **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.



## Installing a New SQL Server Instance and Creating a New WhatsUp Database

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

- 1 Backup the clean MSDE 2000 WhatsUp database.

From the WhatsUp Professional console, select **Tools > Database Utilities > Back Up SQL Database**. Enter a name for the backup file, for example: 2005cleanDB.dat

OR, from the command line, enter:

```
osql -E -D whatusp -Q "backup database to  
disk='C:\2005cleanDB.dat' "
```

- 2 Uninstall MSDE at **Add/Remove Programs > Microsoft SQL Desktop Engine**. Then delete the whatusp.mdf and whatusp.ldf files in C:\Program Files\Microsoft SQL Server\MSSQL\$WHATUSP\Data
- 3 Install SQL Server, and during install please specify the instance name: WhatsUp. From the Services Control manager, start MSSQL\$WHATUSP service - (**Control Panel > Administrative Tools > Services**).
- 4 Restore the backup to your SQL Server.

```
osql -E -S <sql server name> -Q "restore database whatusp  
from disk='<the .dat file>' with Move 'whatusp_dat' to  
'<location for the mdf file>', Move 'whatusp_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 whatusp from disk='D:\2005cleanDB.dat' with Move  
'whatusp_dat' to 'D:\Program Files\Microsoft SQL  
Server\MSSQL$mySqlServerInstanceName\Data', Move  
'whatusp_log' to 'D:\Program Files\Microsoft SQL  
Server\MSSQL$mySqlServerInstanceName\Data' "
```

- 5 Configure the Data Source Name (DSN).
  - a On the computer on which Ipswitch WhatsUp Professional 2006 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 Professional has the account information needed to log on to the database. The NMCONFIG dialog appears.
  - 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"

## Configuring the Web Interface to use Microsoft IIS

Follow these steps to run the WhatsUp Professional Web Interface through a Microsoft IIS (Internet Information Server) web server.

- 1 Allow MSDE to use SQL Server Authentication.
  - a Click **Start > Run** and enter: Regedit, then click Ok. The Registry Editor appears.
  - b Go to the following key:  
  
HKLM\Software\Microsoft\Microsoft SQL Server\WHATSUP\MSSQLServer  
  
and set the value for **LoginMode** to **2** (decimal).
  - c Close the Registry Editor.
- 2 Restart the MSSQL\$WHATSUP service (in the Services dialog in the Windows Control Panel).
- 3 Specify a username and password for WhatsUp Professional to use when connecting to MSDE.

Run NmConfig.exe and specify username = *sa* and password = *wug\_sa*. This is using the built-in account that was installed by the WhatsUp Professional installation. You can specify any username, as long as the user has proper permissions on the WhatsUp database. We recommend that you change the password.

- 4 Make sure that Microsoft IIS does not have any of the WhatsUp Professional COM objects or DLLs loaded. This can be done by restarting IIS.
- 5 Create a virtual directory in IIS named NmConsole which points to the WhatsUp web root directory.
  - a Go to **Control Panel > Administrative Tools > Internet Information Services**. Right-click on **Default Web Site** and choose **New > Virtual Directory**.
  - b Enter the path: <install path>\HTML\1033\NmConsole
- 6 Enable Parent Paths for the default web site (to support use of the relative paths used to navigate in the WhatsUp web interface).
  - a Run inetmgr.exe, then expand Websites. Right-click the default web site, then select **Properties**.
  - b Select **Home Directory > Configuration > Options**, then select **Enable Parent Paths**.

If the SQL instance has a user and password set and you have run NmConfig (Step 3), then you do not have to do the following step (Step 7). However, you must modify the default DSN to use SQL authentication.

- 7 Set Authentication for the virtual directory you set up in step 5. To do this:
  - a 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.
  - c Click **OK**, then **OK** again to save your changes.
- 8 Set the the internal web server to port 8080, or disable it.
  - a In the WhatsUp Professional console, select **Configure > Program Options**.
  - b In the General tab, do one of the following: Set **Enable web server on port to 8080**; or clear the selection to disable the internal server.
- 9 To connect to the Web interface, open a browser and enter the following address in the Address box:  
`http://localhost/NmConsole`



# Migrating from WhatsUp Gold

## Chapter 3

WhatsUp Professional goes well beyond being a newer version of WhatsUp Gold. WhatsUp Professional 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 WhatsUp Gold to WhatsUp Professional, you will immediately notice the visible changes made to the application. However, the philosophy changes may take a little longer to grasp.

## Philosophy Changes

In WhatsUp Gold, 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 the device being polled by each map.)

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

In Gold, maps handled the polling of the devices on that map. In Professional, there is a single database that stores all device information across all device groups.

### In this Chapter

---

Philosophy Changes

Terminology Changes

Using the Migration Utility

---

In short, the Device List has replaced the WhatsUp Gold Maps as the main interface between the user and the polling engine. This gives the users the ability to make dependencies across their network, and to have devices appear in multiple groups with the same information in each entry.

## Terminology Changes

The following table is a comparison between terminology used previously in WhatsUp Gold, and what is used now in WhatsUp Professional.

WhatsUp Gold	WhatsUp Professional
Events	Passive Monitors
Monitors and Services	Active Monitors
Notifications	Actions
Map	Device Group or Device Map

## Migrating Data from WhatsUp Gold to WhatsUp Professional

The WhatsUp Gold to WhatsUp Professional Data Migration Utility migrates information from WhatsUp Gold versions 7 or 8 data files to the WhatsUp Professional 2006 database. These items that can be migrated through the use of 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 during the operation of WhatsUp Professional, and can be run multiple times. Each time the utility is run, imported maps and devices will be duplicated in the WhatsUp Professional database, but duplicate definitions are not imported or updated. If a definition already exists in the WhatsUp Professional database, the definition is ignored, even if the definition was updated in WhatsUp Gold in the meantime.

## Using the Migration Utility

Access the Migration Utility from the WhatsUp Professional Console main menu by selecting **Tools > WhatsUp Gold Data Migration**. The migration utility is actually a wizard that walks you through each step in the process.

### Back up first!

Before you migrate data into the WhatsUp Professional database, you should back up the current database using the Back Up SQL Database utility. The migration utility will not damage the database, but some of the results may be confusing if you are not familiar with new WhatsUp Professional terminology.

To back up the database: from the WhatsUp Professional main menu, select **Tools > Database Utilities > Back up SQL Database**.

### Selecting the data source

Select the path to the WhatsUp Gold install that you want to migrate into the WhatsUp Professional database. The path can be any drive that is local, or a connected mapped drive, on the WhatsUp Professional computer.

This directory contains the WhatsUp Gold configuration definitions, but not your WhatsUp Gold map files. You are given the ability to select your map files in the next dialog in this utility.

Be aware that, although Notification Library definitions are migrated, modem settings for pagers, beepers, and SMS notifications will not be migrated during this process, as these settings reside in the registry. When the migration utility finishes, you will need to add the modem settings for these notifications by using the Actions Library (**Configure > Actions Library**) in WhatsUp Professional.

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

### Selecting Maps to transfer

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

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

**Warning:** 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 cannot 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 the database restore.

**Note:** If devices are duplicated in the imported WhatsUp Gold map files, WhatsUp Professional 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, creating shortcuts in the device groups for each duplicated device.

## Viewing the migration report

Once the utility completes the migration of the maps and configuration definitions, the migration utility displays the migration report.

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

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 search the Knowledge Base for a potential work-around.

Trigger time warnings may affect 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 WhatsUp Gold Settings and then re-import.

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

**Note:** Remember that maps are already live in your database, and are already being polled and alerts are active.

# Device Discovery

## Using the Wizard

Through the Device Discovery wizard, you can scan your network for devices, using the protocol(s) and settings you choose. Once the devices are found, you select the ones you want to monitor, and WhatsUp Professional creates a device in the database for each. Device groups are created based on subnetworks that are found during the scan.

The wizard begins by default after installation. After this initial Discovery, you can go back at any time for another Discovery by going to the menu bar and selecting **File > Discover Devices**.

## 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 Professional 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 Professional 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

# Chapter 4

## In this Chapter

---

Using the Wizard

Scan Types

Device Discovery - A Simulation

Adding a Single Device

Active Discovery

---

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 “Device Discovery - A Simulation” on page 30.

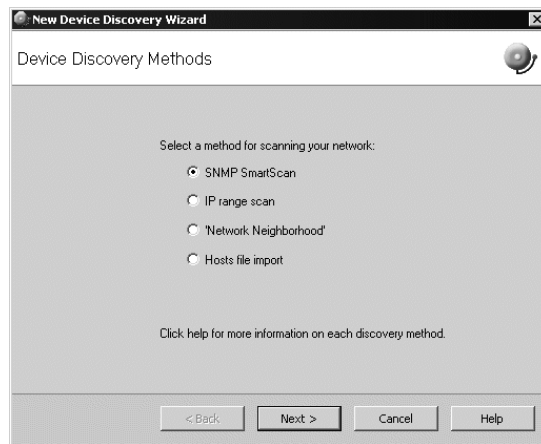
## Device Discovery - A Simulation

This section describes how to use the Device Discovery wizard using 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 will have to:

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

### Discover Devices

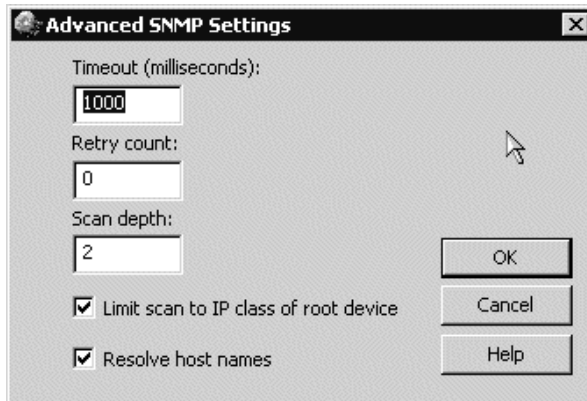
- 1 Select **File > Discover Devices**. The New Device Discovery Wizard appears.



- 2 Select **SNMP SmartScan** as the method for scanning your network, and click **Next**. The SNMP SmartScan settings dialog appears.
- 3 In the **SNMP Enabled Router** box, enter the IP address of the SNMP enabled router you want to use for this scan.
- 4 In the **SNMP read Communities** box, enter the proper read community string for that router. If an incorrect string is entered, WhatsUp Professional 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 which 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 wish to change the scan's default timeouts in milliseconds, retry counts, and scan depth.



Click 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 the **Resolve host names** option if you wish to populate the list of discovered devices with host names in addition to IP addresses. Click **OK**. You are returned to the SNMP SmartScan settings dialog.

- 6 Click **Next**. The Active/Performance Monitors to Scan dialog appears. Select the type of Active Monitor you wish to use in this scan process. Let's select Ping and HTTP as our Active Monitors to be used in the scan process.



The Ping monitor polls the device on a regular basis to establish whether it is Up or Down.

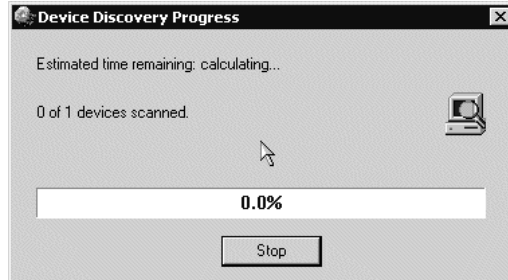
By default, WhatsUp professional sends a ping command to each viable IP address in the range configured during the first section of this wizard. If the device responds, WhatsUp Professional then scans for the monitors listed on this dialog. If no device responds, discovery moves on to the next IP address. 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 will take longer if this option is selected.

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.

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.

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

- 7 Click **Next**. The Device Discovery displays the estimated remaining scan time and the scan's progress. You can cancel this Device Discovery by clicking **Stop**.



- 8 When the Discovery is over, the **Devices to Monitor** window appears, listing all of the devices just discovered. Note that if any of the devices have already been entered into the database, a shortcut to that 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.

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

- 9 Click **Next**. The Action Policy Selection dialog appears.

For an example of how to create Action Policies, see “Actions” on page 109.

- 10 Complete the remaining screens in the wizard.

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

- 11 Click **Finish** to begin monitoring your devices. A progress bar appears while devices are added to the database; then the Device View appears.

For information on device views, see “Device View” on page 62.

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

## Adding a Single Device

There are three ways to add devices, one at a time, to the monitoring database:

- In the Map view, right-click and select **New > New Device**, or in the Device view, right-click and select **New Device**.
- You can display the Device Types (list of device icons) in the left hand pane, then click and drag one to the Device or Map view.
- From the main menu, select **File > New > New Device**, or press <Ctrl+N>.

### Manual Addition - A Simulation

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

- 1 Start by selecting the Device Group to which you want to add a device. Then, click the Map View tab (at the bottom of the console) to display the map for the group.
- 2 Either press <CTRL+N> or right-click on the Map View and select **New > New Device**.
- 3 The Add New Device dialog appears. Type the IP address or host name for the device into the box.



Optionally, click **Advanced**, to set any of the Active Monitor Scan Properties.

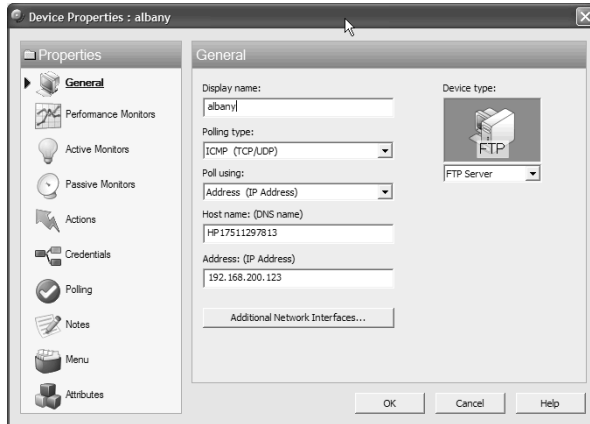
Any monitors for which the **Use in discovery** option is selected will be checked when the device is added.

Click **OK** to add the device.

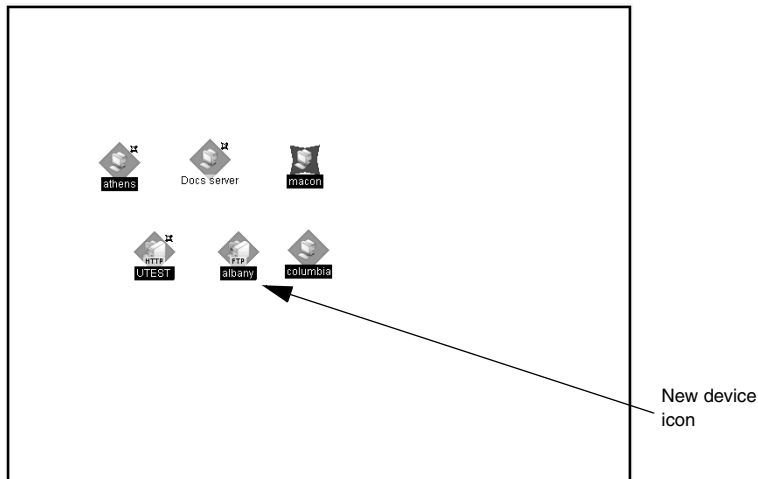
If the device already exists in another group, you will get a message to that effect. If you want to add a short cut for the device in this new group, click **Yes**.

The Device Properties dialog appears.

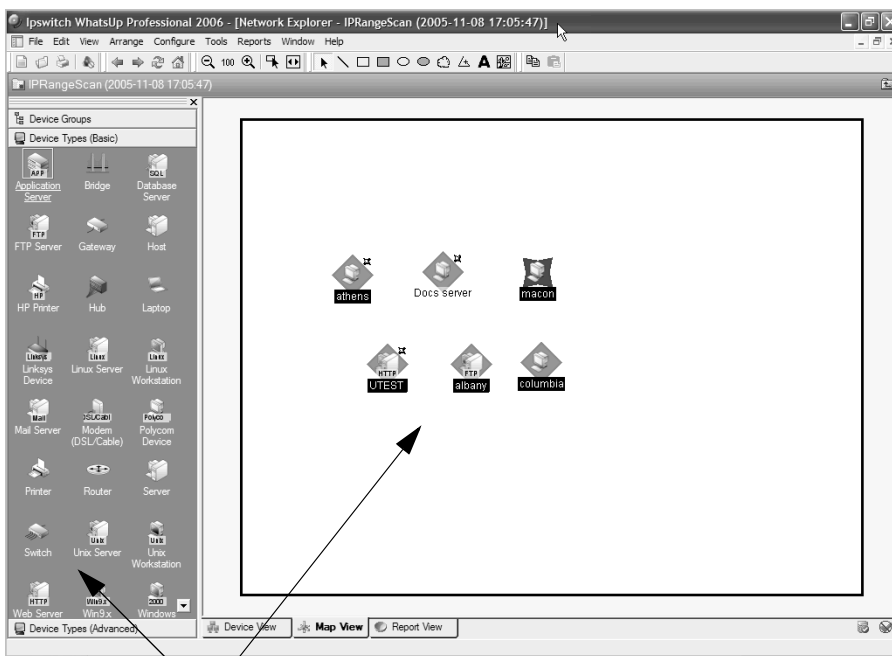
- 4 You can either accept the default Properties populated when you added the device, or modify them. If you accept them, click **OK**. For information on the Device Properties dialog, see “Device Properties” on page 42.



When you click **OK**, the new device icon appears in the Map View.



## Click and Drag



Click and drag the device icon.

- 1 In the left viewing pane, select **Device Types (Basic)** or **Device Types (Advanced)**, depending on which device type you desire.
- 2 Drag the device icon to the map. When the icon is dragged into the Map view, the Add New Device dialog appears. The rest of the steps are identical to those in “Manual Addition - A Simulation” on page 34.

# Active Discovery

With Active Discovery, you can schedule WhatsUp Professional to scan your network for new monitors and Devices on a regular basis. Newly discovered items are added to the Active Discovery Results report, and WhatsUp Professional 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 Professional 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 Professional 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 e-mail is generated and sent to the address you provide during Active Discovery configuration. The e-mail contains links to the reports that are populated by the scan:

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

If an e-mail notification is not specified (in the wizard), these reports are also available in the System report list, in the Report view.

## Example: Configuring Active Discovery

In this example, we set up an Active Discovery task to scan our Atlanta network every morning and send an e-mail update to the network administrator.

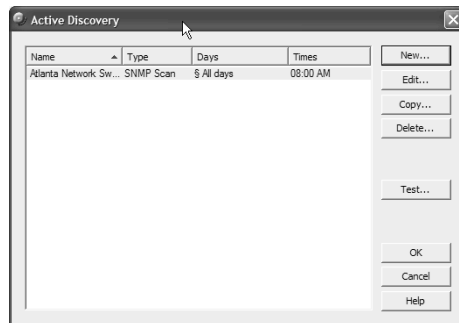
- 1 From the WhatsUp Professional main menu, select **Configure > Active Discovery**. The Active Discovery dialog appears.
- 2 Click **New** to add a new task.

We completed the Add Active Discovery Task wizard 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
SNMP SmartScan	SNMP enabled router: 192.168.2.1 SNMP read communities: public Windows credentials: none
Active/Performance Monitors	Active Monitors: FTP, HTTP SMTP, Ping Performance Monitors: CPU Utilization, Disk Utilization, Interface Utilization

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.



From the e-mail, click the Active Discovery Results link to view the report. In our example, the report shows the following:

The screenshot shows the 'System Active Discovery Results' report in Internet Explorer. The report is divided into two main sections: 'devices found' and 'services found'.

**devices found**

Date	Host Name	IP Address	Description
7/26/2005 10:04:05 AM	pc185-ati.ipswitch.gabn.net	216.104.153.165	pc185-ati.ipswitch.gabn.net found. Services found: Ping
7/27/2005 10:04:10 AM	pc145-ati.ipswitch.gabn.net	216.104.153.145	pc145-ati.ipswitch.gabn.net found. Services found: Ping
8/4/2005 10:04:20 AM	pc173-ati.ipswitch.gabn.net	216.104.153.173	pc173-ati.ipswitch.gabn.net found. Services found: Ping
8/15/2005 10:04:15 AM	pc136-ati.ipswitch.gabn.net	216.104.153.136	pc136-ati.ipswitch.gabn.net found. Services found: Ping
8/26/2005 10:04:16 AM	pc186-ati.ipswitch.gabn.net	216.104.153.186	pc186-ati.ipswitch.gabn.net found. Services found: Ping,HTTP
12/1/2005 10:04:45 AM	NM01	192.168.3.33	NM01 found. Services found: Ping - Performance monitors found: Ping Latency and Availability
12/1/2005 10:04:45 AM	WKS187	192.168.3.32	WKS187 found. Services found: Ping,SNMP,POP3,SMTP,interface(2) Broadcom 54g MacPerformance 802.11g - Packet Scheduler Miniport (192.168.3.32),interface(3) National Semiconductor DP93815-Based PCI Fast Ethernet Adapter - Packet Scheduler Miniport...

**services found**

Date	Host Name	IP Address	Description
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	DNS
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	SNMP
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	Echo
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	FTP
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	POP3
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	SMTP
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	Time
7/16/2005 10:04:09 AM	pc190-ati.ipswitch.gabn.net	216.104.153.190	Telnet

- Select the Discovery results (devices, services, or monitors found) you want to add to your device group, then click **Add**.

For more information on Active Discovery, please see the WhatsUp Professional online help.



# Devices

In WhatsUp Professional, devices are virtual representations of resources (computers, servers, hubs, etc.) that are connected to your computer through a LAN, a wireless network, or even over the Internet. WhatsUp Professional watches these devices through the network connection. When those network resources can't be reached by WhatsUp Professional, the device is considered down, and an Action can be configured to fire.

## Device Troubleshooting?

WhatsUp Professional is not a troubleshooting tool. It will tell you when your network goes up or down, but will not tell you what made your network go down. For that, you will need to inspect the afflicted resource and its documentation.

## Device Services

WhatsUp Professional 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, e-mail 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.

# Chapter 5

## In this Chapter

---

Device Troubleshooting?

Device Services

Device Properties

Device Types

Device Groups

Dynamic Groups

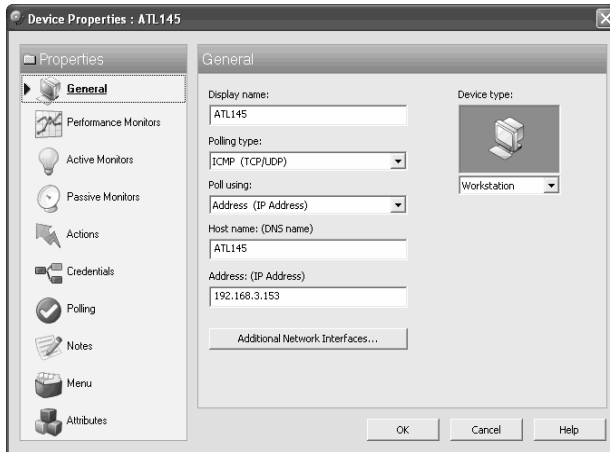
Editing Multiple Devices - Bulk Field Change

Acknowledgements

Credentials Overview

---

# Device Properties



You can modify individual device properties by right-clicking on the device icon in either Device or Map View, and selecting **Properties**. There are 10 separate Properties available. Their descriptions follow. Click the icons in the left viewing pane to view or modify each property.

## Device Properties - General

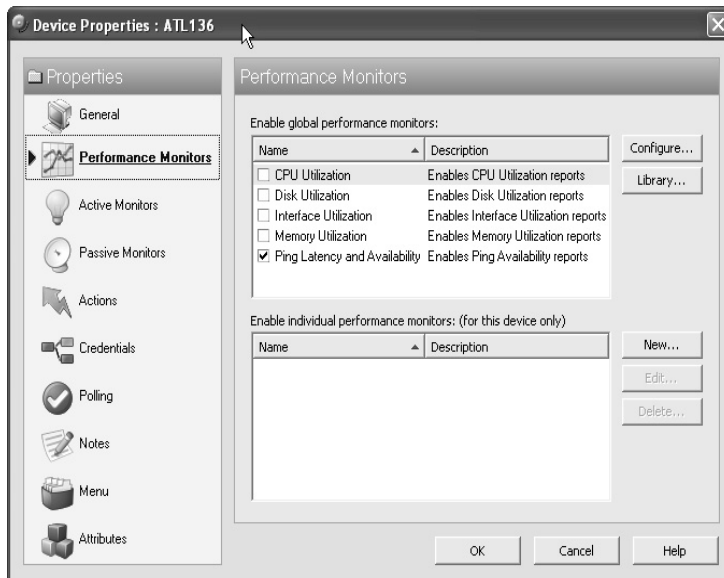
The General section of the device properties dialog box lists, or allows you to modify, basic information for the selected device.

- **Display name** - An identifying name for the current device. This name is populated during Discovery, but can be changed at any time. Changing the name will not change how the device is polled, only how it is displayed in WhatsUp Professional.
- **Polling type** - Select the type of polling you want WhatsUp Professional 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 whether you want WhatsUp Professional to use the IP address or the 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.

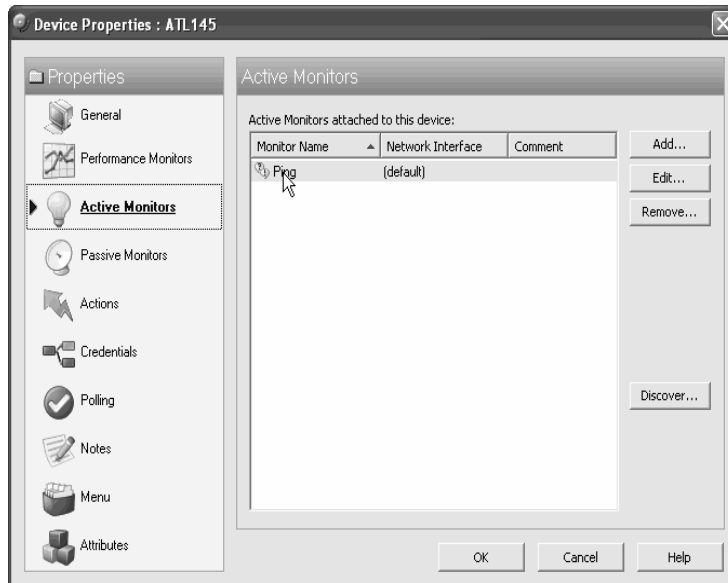
## Device Properties - Performance Monitors



This dialog is used to display and manage Performance Monitors for this device. This list is populated by entries in the Performance Monitor Library.

For more detailed information, see Chapter 8 - “Performance Monitors.”

## Device Properties - Active Monitors

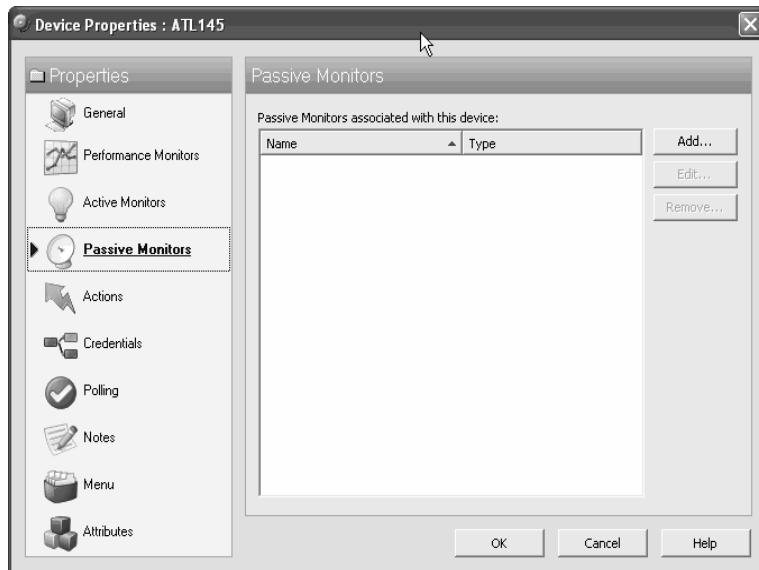


This dialog is used to display and manage Active Monitors for this device. There are several ways that an Active Monitor can be added to this list:

- 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.
- Click **Discover** to have WhatsUp Professional scan the device for Active Monitors.

For more detailed information, see Chapter 9 - “Active Monitors.”

## Device Properties - Passive Monitors



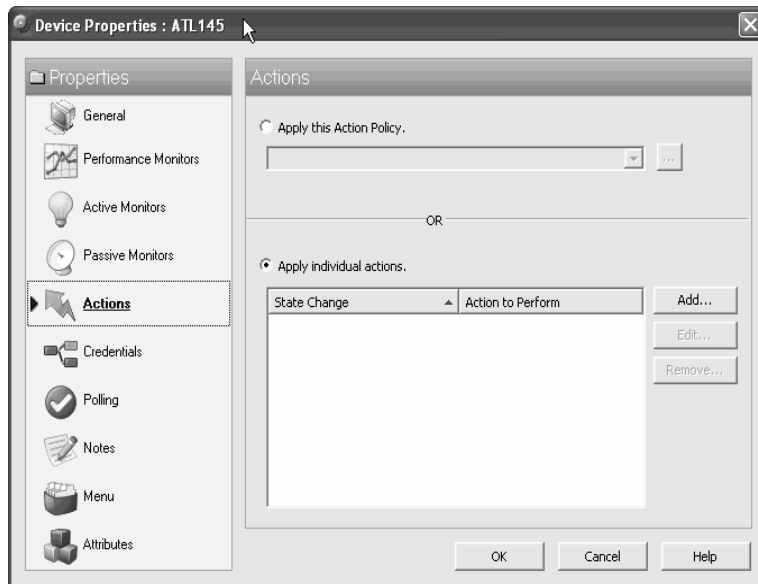
Some elements on a network may not provide a clear up or down status when queried. For example, a message may get logged to the system's Event Log by another application (such as an anti-virus application alerting when a virus is found). Because these messages/events can occur at any time, a Passive Monitor Listener “listens” for them, and notifies WhatsUp 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 and click **Edit** to change the configuration.
- Select a Passive Monitor and click **Remove** to remove the monitor from the device.

For more detailed information, see Chapter 10 - “Passive Monitors.”

## Device Properties - Actions



On this dialog, you can select an Action Policy to use on the selected device or configure actions specifically for this device.

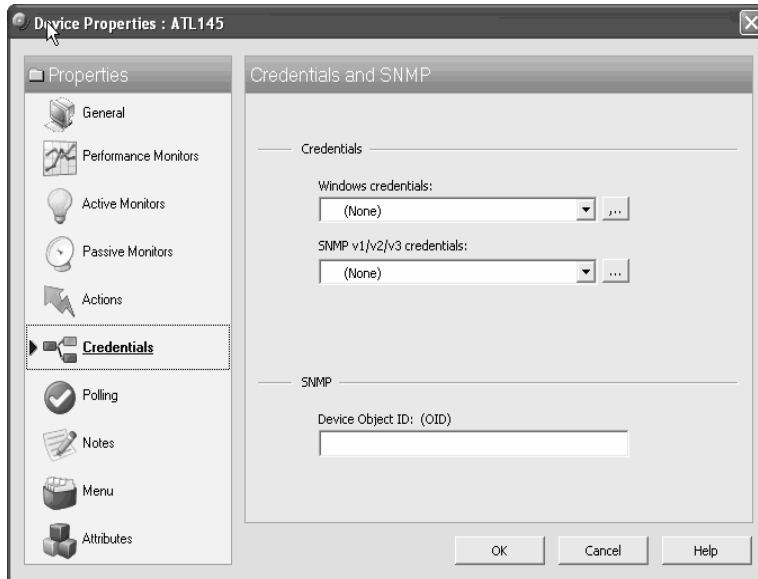
To apply an Action Policy to the device, select one from the action policy pull-down menu. You can also create a new action policy or edit an existing action policy, by clicking the **Browse** button next to the pull-down menu box.

Alternatively, configured actions 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.

- Click **Add** to configure an action for the device.
- Select a configured action and click **Edit** to change the settings for that action.
- Select a configured action and click **Remove** to delete the action from the list. Removing the action from the list also deletes all records for this action (on this device) from the Action Log.

See Chapter 11 - “Actions” for more detailed information.

## Device Properties - Credentials



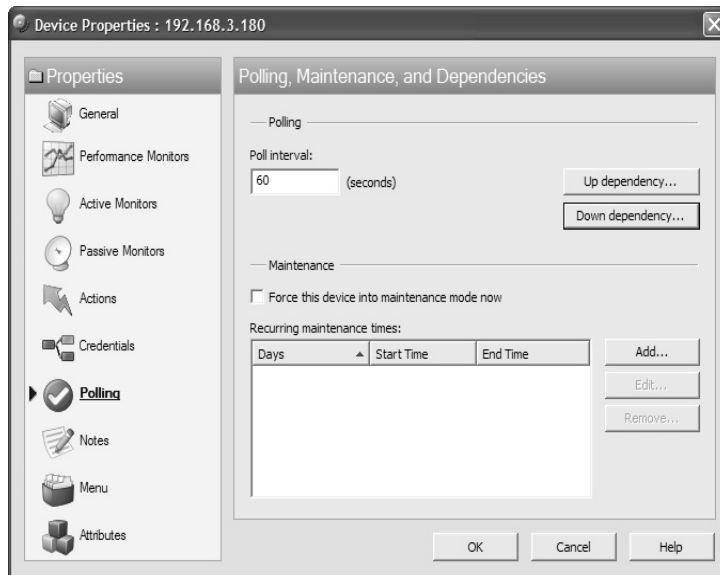
This dialog displays SNMP and Windows credential information for the current device.

**Note:** SNMP manageable devices appear on the map view with a white star in the top right corner of its icon.

- **Windows credentials** - Select the Windows credential that you need to use to connect to this device.
- **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 the device is SNMP manageable, then the correct credential is selected automatically. If any of these conditions are not met, **(None)** will be 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 on credentials, see “Credentials Overview” on page 58.

## Device Properties - Polling



Briefly, polling is the term used for the monitoring of discovered devices in WhatsUp Professional. This dialog allows you to configure polling options and/or schedule maintenance times for the selected device.

### Polling

- **Poll interval** - This number determines how often WhatsUp Professional will poll the selected device. Enter the number of seconds you want to pass between polls.

### Maintenance

With this section, you can manually set the maintenance state on a device, or schedule a weekly maintenance state for a certain time period. Any device placed in maintenance mode will not be polled, and actions will not be 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 background color.

- **Manually put this device into maintenance mode now** - Select this option to put the device in maintenance mode. Clear the option to resume polling the device.
- **Scheduled 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 and click **Edit** to change a scheduled time.
- Select an entry and click **Remove** to delete a scheduled time from the list.

## Dependencies

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

There are two types of dependencies:

- **Up Dependency** can be thought of as describing that something is “behind” something else. The dependent 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 dependent devices in front will not be polled unless the device further down the line is down.

An important reason you might want to set dependencies on another device, is to limit notification actions being fired.

For example: if you place devices behind a router (up dependent on the router) those devices will not be polled unless that router is up. If the router goes down, the devices will be placed in the unknown state. Without the dependency, the devices behind the router would fire actions when they become unreachable due to the router going down. With the dependency, only actions on the router will fire.

## Setting Dependencies

There are two ways to set dependencies in the WhatsUp Professional console:

### Using Device Properties:

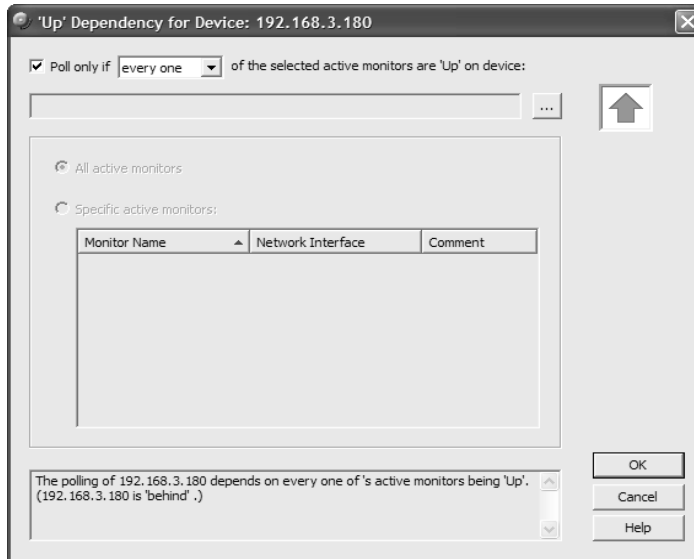
- Double-click on a device in the Device or Map View to display Device Properties, and click the Polling Icon.
- Click either the **Up Dependencies** or **Down Dependencies** button to bring up the Device Dependencies dialog and configure the dependency.

### Using the Map View:

- Right-click on a selected device and **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.
- Select **Display > Polling Dependency Arrows** to view the dependency between the two devices.

In 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 dependencies there.

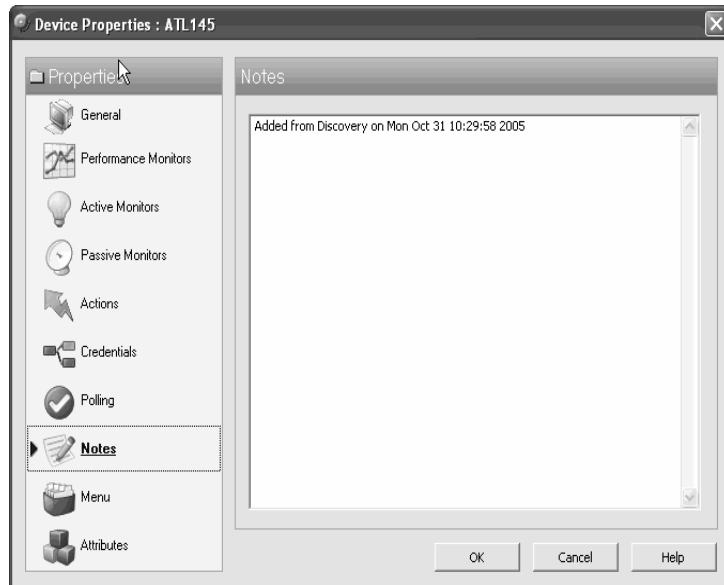
The Device Dependencies dialog is the same for both up and down dependencies with the exception that one sets up dependencies and the other sets down dependencies. Up dependencies is signified with an upward green arrow icon, while down dependencies is signified with a downward red arrow.



- Check 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 the 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 wish to associate with the dependency.

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

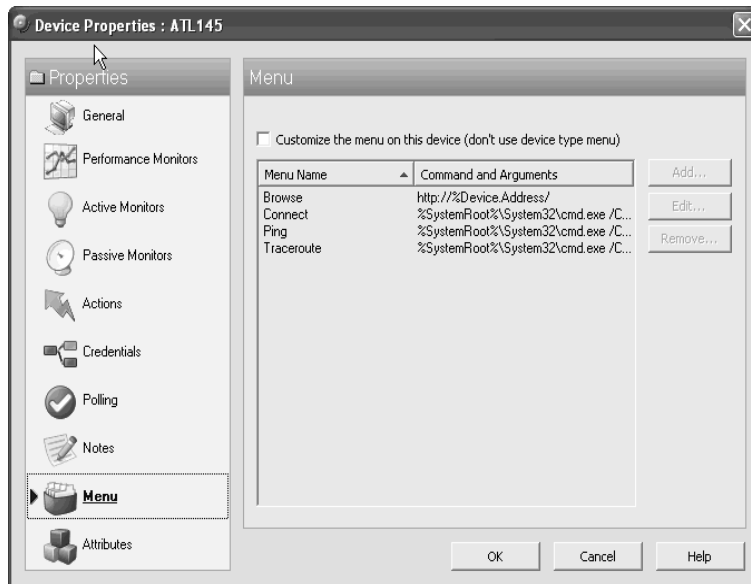
## Device Properties - Notes



This section of the Device Properties dialog gives you the ability to enter free-form notes to the device database. By default, the first line of the Notes box shows when the device was added to the database. If viewing the Notes on a device shortcut, you will still see the date and time the device was added to the database, not when the shortcut was created.

You may want to record historical information about a device, physical location information, or perhaps notes relating to the actions configured for the device. The use of this section is completely up to you.

## Device Properties - Menu

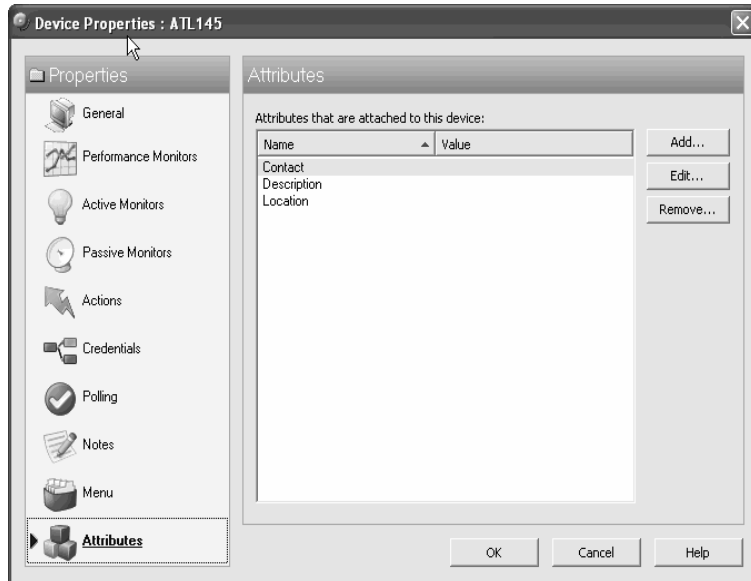


Use this dialog to create a context menu for a device. Once a new menu item has been configured, it appears on the right-mouse menu when you right-click on that device in the device list. When you select the menu item, the associated command is launched with the arguments that have been entered in its 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. Once an item has been configured, it appears in the Custom Links menu in the left-hand navigation section of the page when that device is viewed. When the link is clicked, the browser opens the link in the same window.
  - Click **Add** to add a new menu item.
  - Select an item and click **Edit** to change the settings.
  - Select an item and click **Remove** to remove it from the list.

**Note:** 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.

## Device Properties - Attributes

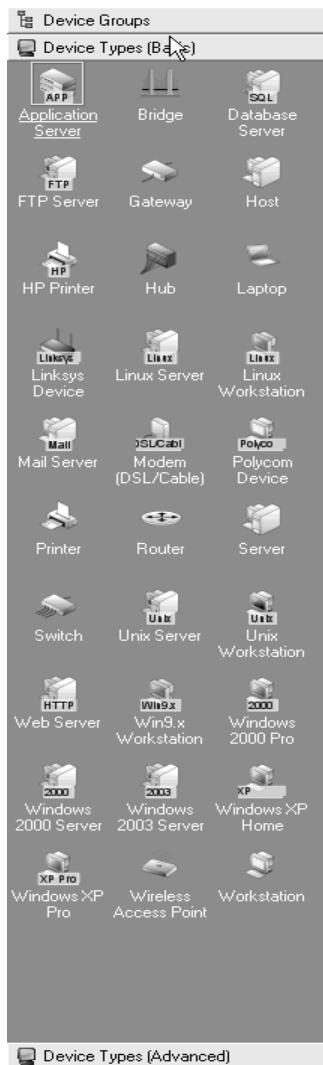


This dialog lists attributes added to a device, such as contact person, location, etc. The first attributes in the list are added by WhatsUp Professional when the device is added to the database, either by the Device Discovery wizard, or through another means.

- Click **Add** to create a new attribute for the device.
- Select an existing attribute and click **Edit** to change the attribute.
- Select an existing attribute and click **Remove** to remove the attribute from the device.

# Device Types

In the left-hand pane of the WhatsUp Professional console interface, the Device Types (icons representing the types of devices you might have on your network) appear. You can click the tab at the bottom of the pane to switch from **Device Types (Basic)** to **Device Types (Advanced)**. To use these icons on existing devices, see “Device Properties” on page 42 in this chapter.



# Device Groups

## Organizing Device Groups

In essence, device groups are organizational folders that allow you to 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. Double clicking a device opens Device Properties.

### 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. In other words, there may be more than one reference in the My Network tree to one device. However, you can configure this same device 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.



The green square in the right-hand corner of the folder icon indicates that all monitors on all devices are Up.



The red square in the right-hand corner of the folder icon indicates that at least one monitor is Down.

## Renaming a Device Group

Right-click on the group in the My Network tree or Device View and select **Rename** from the menu.

## Dynamic Groups

This feature gives users the ability to create device groups based on whatever criteria they 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 run on the WhatsUp database, and can display real-time data if viewed through a report that is set to automatically refresh.

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

To configure dynamic groups:

- 1 Right-click on the device list in the WhatUp Professional Console.
- 2 Select **New Dynamic Group** or **Properties** from the right-mouse menu. The Dynamic Group dialog appears.
- 3 Enter a name for the group, and enter an SQL query in the Filter box that identifies the devices you want to appear in that group.
- 4 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.

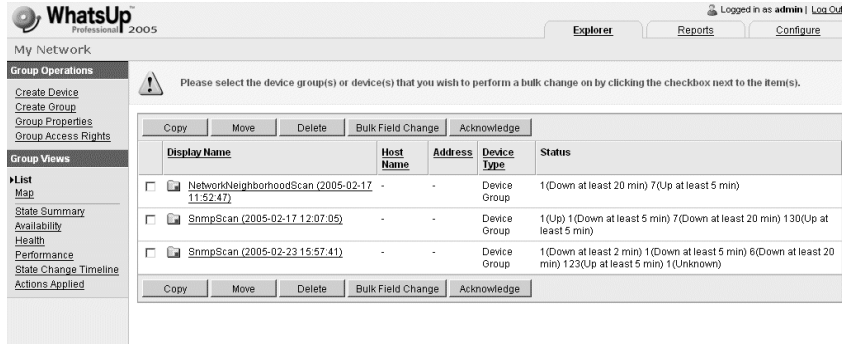
## Editing Multiple Devices - Bulk Field Change

The Bulk Field Change feature gives you the ability to make changes to multiple devices and device groups, if you have administrative privileges to these devices or device groups. To edit multiple devices:

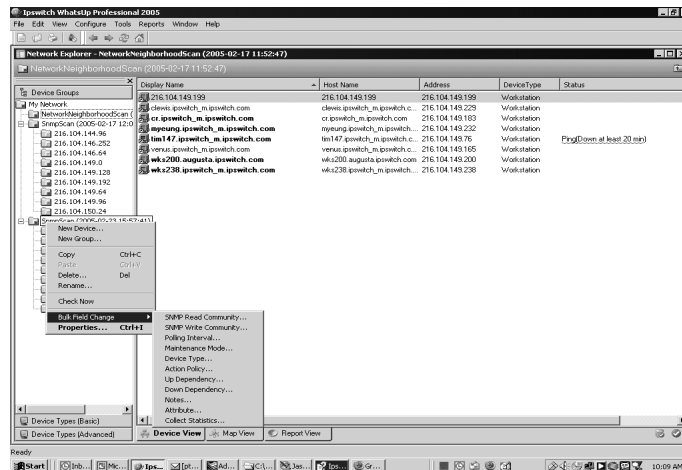
- In the Console, select the devices and device groups you want to change, then right-click and select Bulk Field Change from the right-click menu.

**Note:** When you select a device group, every device in that group and in any subgroup in that group will reflect the bulk field change.

- In the Web interface, select the devices or groups whose field you wish to change and click the **Bulk Field Change** button.



- In the Console, select the field you want to change from the right-mouse menu. In the Web interface, click the select the checkbox(es) for the field you want to change.



- On the dialog for that setting, enter the configuration information that you want set.
- Click **OK** to commit the changes and return to the device list.

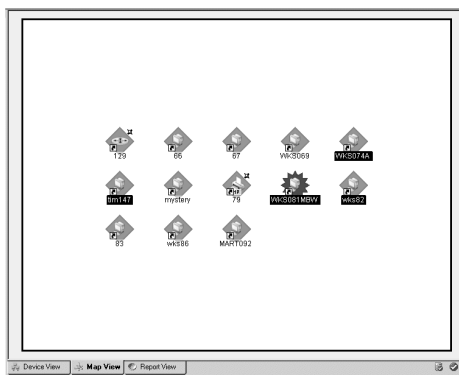
The following are the items that can be modified through Bulk Field Change.

- Action Policy
- Attribute
- Collect Statistics

- Device Type
- Up/Down Dependency
- Maintenance Mode
- Notes
- Polling Interval
- Active Monitor
- Active Monitor Properties
- Performance Monitor
- Credentials

## Acknowledgements

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

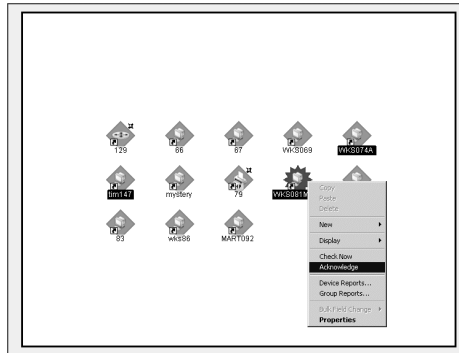


Once the device is in Acknowledgement mode, it will remain so until you actively acknowledge it.

**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.

## Acknowledging 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 in the Report View and select the devices you want to acknowledge. Once the devices are selected, click **Clear** to remove the devices from the report, thereby acknowledging the state change.

## Credentials Overview

The Credentials system stores login or community string information for Windows and SNMP devices in your WhatsUp database. The system supports SNMP v 1, 2, and 3. Credentials are configured in the Credentials Library (found on the console main menu at Configure > Credentials) 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.



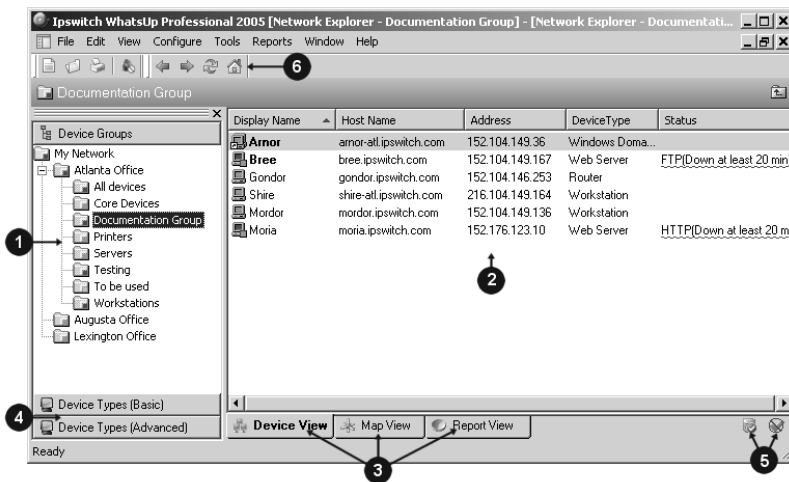
# Using the WhatsUp Professional Console

## Chapter 6

The WhatsUp Professional Console is your 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 Professional Console.



### In this Chapter

Console Overview

Device View

Map View

Report View

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

- 2 **View pane.** This pane displays the selected device group based on the view from the tabs below (see #3). If the Report view is selected, your WhatsUp Professional reports are displayed in this pane.
- 3 **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.
  - **Report View.** Use the Report View to troubleshoot and monitor performance and historical data collected during the operation of WhatsUp Professional.
- 4 **Device Type Groups.** Click the Basic or Advanced tab to view the device types contained in that section. These types can be dragged into the view pane to create a new device based on that device type.
- 5 **Polling Indicator Icons.** These icons indicate the current state of the poll engine.



Poll engine is  
connected



Poll engine is not  
connected



Polling is enabled









Polling is disabled

- 6 **WhatsUp Professional 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**.

## Device View

With a similar look and feel to Windows Explorer, WhatsUp Professional'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 alpha-








Display Name	Host Name	Address	DeviceType	Status
 <b>Arnor</b>	arnor-atl.ipswitch.com	152.104.149.36	Windows Doma...	Ping(Down); DNS(Down); I
 <b>Bree</b>	bree.ipswitch.com	152.104.149.167	Web Server	Ping(Down); HTTP(Down)
 <b>Gondor</b>	gondor.ipswitch.com	152.104.146.253	Router	Ping(Down); Interface(1)(D
 <b>Mordor</b>	mordor.ipswitch.com	152.104.149.136	Workstation	Ping(Down)
 <b>Moria</b>	moria.ipswitch.com	152.176.123.10	Web Server	Ping(Down); HTTP(Down)
 <b>Shire</b>	shire-atl.ipswitch.com	216.104.149.164	Workstation	

betical order. 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.

## Device Icons

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

	(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 “Devices” on page 41.

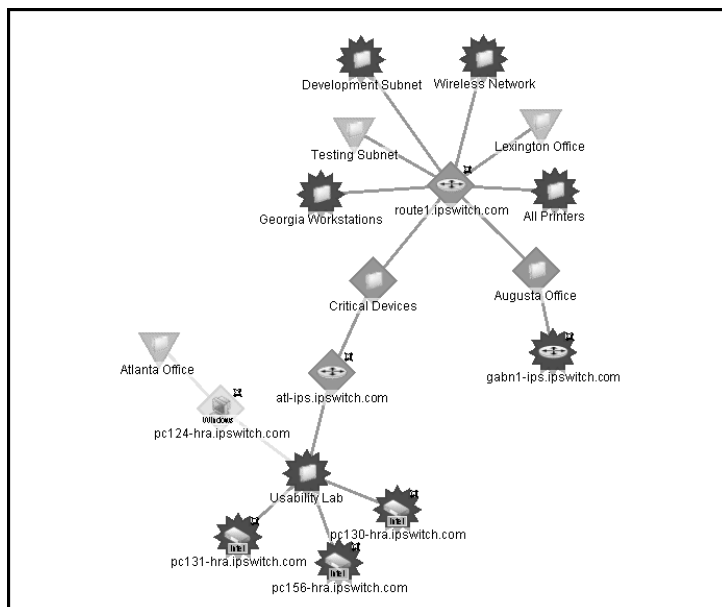
## Organizing Devices and Device Groups

While in the Device View, you can quickly and easily organize your devices and device groups, simply by dragging the device you want in a particular group to that device group folder. Once you 'drop' the icon or icons, a menu appears, asking if you want to Move or Copy those devices. If you move the devices, they are deleted from the previous device group. If you share 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.

## Map View

Through the Map View of WhatsUp Professional, you have the ability to 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 those devices being polled multiple times. In short, there is an enormous amount of flexibility in the way this feature can be used.



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

## Device Layout

The WhatsUp Professional 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.



Map View Arrange Toolbar

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**.

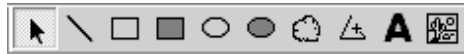
If you have a large set of devices or want to represent a topology specific to your network, you can also use the graphics annotations (such as lines, text, circles) and attached lines to create custom map views.

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.

See the application's Online Help for more information on how to use specific features of the Map View, including grouping, using grid lines, and further manipulating of annotation objects.

## Adding Annotations to a Map

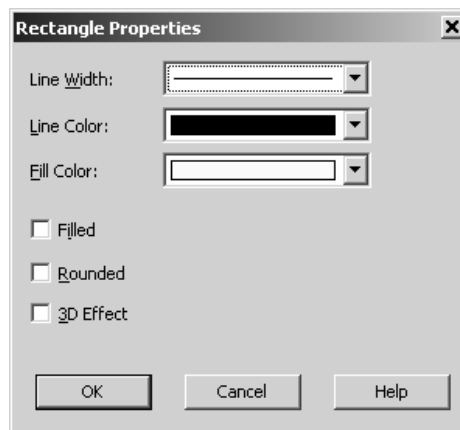
Annotations are graphical tools that let you customize a map view. You can add text, shapes, lines, and graphics to visually organize a set of devices.



Map View Annotation Toolbar

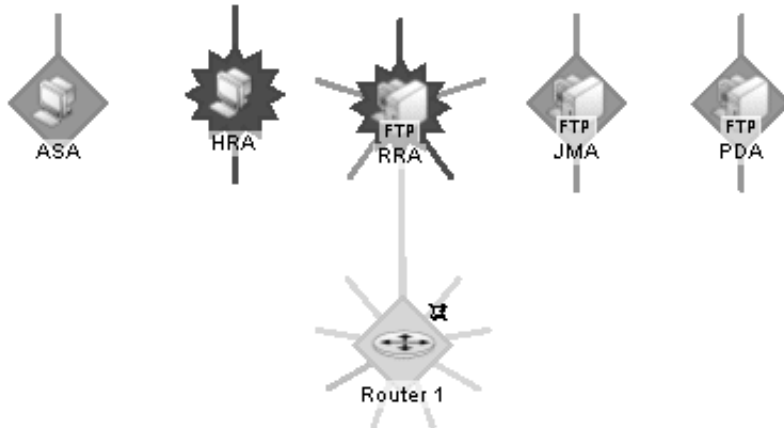
In the Map View toolbar, click an annotation icon to make it the active tool. Then, you can drag the cursor on a map to create a line, rectangle, circle, polygon, or network cloud.

To change an annotation's properties, such as border width and color, select the annotation, and then select Properties from the right mouse menu.



## Link Lines

In Map View, you can use Link lines to monitor the status 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 shows a map with link lines displayed.



- Router 1 shows a connecting link to device RRA and this link is currently up. Also shown are eight unconnected links, all of which represent interfaces on the router. One of the unconnected links is disabled.
- JMA is a workstation that shows two unconnected links that are currently up. If you look in Device Properties, Active Monitors, you'll see these are the Ping and FTP monitors.
- RRA is an FTP Server that is currently down and shows five unconnected links, two of which are down.

Links are rendered in the color of their device state:

- 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.

## How to Create Connecting Links

There are three ways to set up the connecting link lines:

- Manually, using **Link to** on the right-click menu for a device. (**Disconnect link to** remove them.)

- a Select a monitor for which you want to display a link line, then click **OK**. The link line cursor appears.
  - b Move the cursor to another device and click to create a link.
- Automatically, during Device Discovery when using SNMP SmartScan.

**Note:** The "Interface" service must be included in the scan.

- Automatically, when you click the **Discover** button in the **Device Properties > Active Monitors** dialog. These link lines are not connected to any other device.

When using 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 allows the scan to identify all the interfaces on the device. If scanning a specific device (**Device Properties > Active Monitors** dialog), select Credentials in device properties and enter the SNMP Read community. Then, go to the Active Monitors dialog and click **Discover**.

When creating links manually, you are always creating a connected link. If there already was an unconnected link for that 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, as it assumes you meant that monitor.

To display unconnected link lines, right-click in the map view and choose **Display > Unconnected Links**.

## 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 reflections of true connectivity between the two devices; that is done with link lines (See "Link Lines" on page 66).

To draw an attached line:

- 1 In Map View, right-click a device to display the menu.
- 2 Select **Attach > Attach to**.
- 3 Click the device icon to which you want to attach a line.

WhatsUp Professional draws an attached line between the two devices.

## Report View

Use the Report View to troubleshoot and monitor the performance and historical data collected by WhatsUp Professional. Reports can be viewed in the WhatsUp Professional console or the Web Interface, and they can be e-mailed on a regular basis to an e-mail address you specify through the Recurring Report feature.

For more information on the different reports that are available, see “Reports” on page 125.



# Using the Web Interface

Through the Web Interface, you can remotely configure your network, just as if you were sitting at the WhatsUp Professional computer and using the console. Although some of the navigation methods are different, the general functions and configuration procedures are identical.

In addition, the Web interface can be used to let your entire IT staff take ownership of the monitoring of different sections of your network, all using the same install of the WhatsUp Professional application.

## Connecting to the Web Interface

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

For example, if your IP address of your WhatsUp Professional computer is 156.104.152.177, to connect to the interface, in your Web browser you would enter: `http://156.104.152.177`

The port number (default is 80) can be changed in the WhatsUp Professional console by selecting **Configure > Program Options** from the main menu. Select the General section and enter your new port number in the **Enable web server on port** box. If you change the port number, you must enter it as part of the URL, for example: `http://156.104.152.177:8080`

## Access Problems

If you are having trouble connecting to the logon screen of the Web interface, you might want to make sure that there is no port conflict. Changing the port number as described above will fix that problem. Another common mistake is neglecting to enable the Web server itself. To enable the Web server, navigate to the WhatsUp Professional Console main menu, select **Configure > Program Options**. Select the **General** section and select the **Enable web server** option.

# Chapter 7

## In this Chapter

---

Connecting

Overview

Web Users

User Rights

Web Server Configuration

Web Interface Security

Configuring the Web Interface to use IIS

---

## Default Logon

WhatsUp Professional comes with two default user accounts you can use to try out the application. You should change these passwords as soon as you implement the application in a production environment.

Default Admin Account	Default Guest Account
Username : admin Password: admin	Username: guest Password: (no password, leave blank)

## Web Interface Overview

The following is a breakdown of the main features found in the WhatsUp Professional Web interface.

The screenshot displays the WhatsUp Professional 2006 web interface. The top navigation bar includes 'Explorer', 'Reports', 'Configure', and 'Tools'. The main content area shows a 'Web Alarm' notification for 'Shire' and 'Mordor' devices. Below the notification is a table of devices with columns for 'Display Name', 'Host Name', 'Address', 'Device Type', and 'Status'. The 'List Map' view selector is highlighted in the left sidebar.

Display Name	Host Name	Address	Device Type	Status
<input type="checkbox"/> Aragorn	Aragorn	152.128.3.145	Workstation	
<input type="checkbox"/> Arda	152.128.3.158	152.128.3.158	HP Device	
<input type="checkbox"/> Arnor	arnor-atf.ipswitch.com	152.128.3.100	Workstation	
<input type="checkbox"/> Gondor	Gondor	152.128.3.180	HP Printer	
<input type="checkbox"/> Mordor	Mordor	152.128.3.132	Intel Device	Interface[12:Port 12](Down at least 20 min)
<input type="checkbox"/> Shire	shire-atf.ipswitch.com	152.128.3.97	Server	Ping(Down) Interface[1:ethernet1](Down)
<input type="checkbox"/> WKS188	WKS188	152.128.3.188	Workstation	

- 1 Group/Device Operations.** Select a link in this section to make changes to the current group or device, depending on what you have selected in the main pane.
- 2 View Selector.** Choose the view you want to see the current group in. This option is not available when viewing device properties.
  - a List View.** View the group as a list of devices. This is the view seen in the graphic above.

- b Map View.** View the group as a map file. You cannot make changes to the map in the Web interface. This has to be done in the WhatsUp Professional Console.
- 3 Group/Device Reports.** Select a report from this list to view historical data for the selected group or device.
- 4 Main Pane.** This is the main operating pane for the Web interface. Notice that when you are viewing a device group, you can click the device name in the list (or on the map) to access the device properties for that device.
- 5 Tab Bar.** Select one of the three tabs to access that section of the Web interface.
  - a Explorer.** Provides access to devices and device groups.
  - b Reports.** Provides access to a variety of reports for the entire system, groups or specific devices.
  - c Configure.** Opens the System Configuration page, which allows you to change program options and define or edit Monitors, Actions, Devices and Notifications.
  - d Tools.** Provides access to the network tools.
- 6 Group View Button Bar.** When viewing a group in the list view, these buttons appear at the top and bottom of the device list.
  - a Copy.** Select a device or device group and click **Copy** to create copies of that device or device group in another device group. Multiple copies of the same device share the same database entry, so you only have to make changes to one copy for all of the devices to be changed. This also means that WhatsUp Professional only polls the device once, no matter how many device groups it appears in.
  - b Move.** Select a device or device group and click **Move** to move the items from the current group to another.
  - c Delete.** Select a device or device group and click **Delete** to remove those items from the current device group. If that device is the only entry in the database, the device will be removed from the database as well.
  - d Bulk Field Change.** Select two or more devices or any number of device groups and click **Bulk Field Change** to make configuration changes to multiple device entries at once. For more information, see “Editing Multiple Devices - Bulk Field Change” on page 56.
  - e Acknowledge.** If a device name appears in bold in the device list, select that device and click **Acknowledge** to acknowledge that a state change has occurred. For more information on the Acknowledgement system, see “Acknowledgements” on page 58.
- 7** When viewing devices and groups in the **Explorer** tab, a history of your path through the application is available.

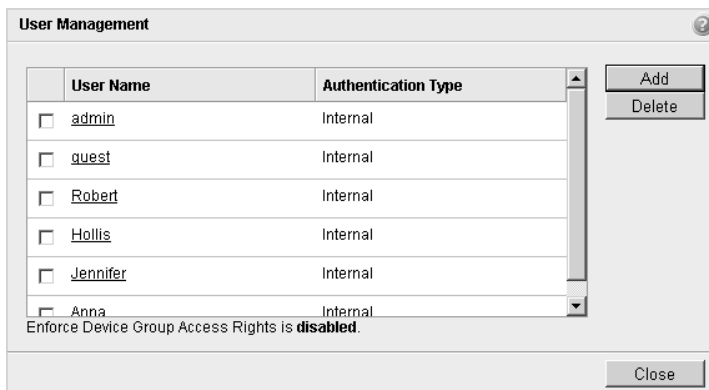
- 8 This section displays the current user and a link to **Log Out** of the Web interface.
- 9 This section only appears when the Web alarm action fires. A Web Alarm is an action type that plays a sound over the web interface when a device state change occurs. All users logged in via the web interface will see these alarms. The type is configured in the Actions Library, and can be associated to any device or monitor like any other action. The difference between the Web Alarm action and other actions is that the default Web Alarm is placed in the Implicit Action policy at installation.

This section allows you to dismiss or mute the alarms that have been fired. Clicking the Mute or Mute All buttons only stop the current sound being played. It does not stop the sound for future occurrences of the Web Alarm.

## Managing Web Users

The Web User Management system allows you to restrict access to your WhatsUp Professional Web interface to only those people who have an account set up. User permissions are configured for those users, limiting what operations they can perform through the Web interface.

Access the User Management page by clicking **Configure** on the Tab bar and from the System Configuration page, select **Manage Users**.



Click **Add** to create a new user, or click a user name to edit the settings for that user. The Edit/Create User page appears.

**Create User**

User name:  
Robert

Authentication type:  
 Internal  LDAP

Internal password:  
.....

Confirm password:  
.....

Home Group:  
My Network

Users are given group read access rights for their home group.

**User Rights**

<input type="checkbox"/> Manage Users	<input type="checkbox"/> Configure LDAP Credentials
<input type="checkbox"/> Manage IP Security	<input checked="" type="checkbox"/> Change Your Password
<input checked="" type="checkbox"/> Configure Monitors	<input checked="" type="checkbox"/> Configure Actions
<input checked="" type="checkbox"/> Manage Groups	<input checked="" type="checkbox"/> Manage Devices
<input checked="" type="checkbox"/> Access Group and Device Reports	<input type="checkbox"/> Manage Web Server
<input type="checkbox"/> Access System Reports	<input type="checkbox"/> Manage Recurring Actions

OK Cancel

- **User Name.** Enter the name of the user.
- **Authentication Type.** Select the method of authenticating the user.
  - **Internal.** Use WhatsUp Professional's internal user database.
  - **LDAP.** Use an external LDAP database. LDAP credentials must be configured for this to work.
- **Internal Password.** Enter the user's password (only if **Authentication Type** is set to **Internal**).
- **Confirm Password.** Enter the user's password again.
- **Home Group.** Select the device group that the user will see when they log into the WhatsUp Professional Web interface. If they have the correct group access rights, they will be able to navigate out of this group.
- **Device Group Settings.** (This section is only visible after a user has been created. After initial creation, you are prompted to set device group permissions.) Click **Set Device Group Access Rights** to make a change to the groups to which the user has read and write access.
- **User Rights.** Select which options to which you wish to give the user access.

**Note:** If you grant the **Manage Group** option, the **Manage Device** option is always selected as well.

## User Rights

The following rights can be given to a user:

- **Manage Users.** Create and edit users for use in the Web Interface.
- **Manage IP Security.** Allow or refuse access to the Web Interface to specific IP addresses.
- **Configure Monitors.** Configure active monitors for devices in the database.
- **Manage Groups.** Create, edit, or remove device groups, if the user has access to the groups.
- **Access Group and Device Reports.** View group and device reports for the groups to which the user has access.
- **Access System Reports.** View system reports.
- **Configure LDAP Credentials.** Allows user to configure LDAP credentials for the Web Interface.
- **Change Your Password.** Allows users to change their own password.
- **Configure Actions.** Create and edit actions in the Action Library.
- **Manage Devices.** Add new devices and edit existing devices in the groups to which the user has access.
- **Manage Web Server.** Change the configuration of the Web server.
- **Manage Recurring Actions.** Create, edit, or remove Recurring Actions, if the user has access to the groups.

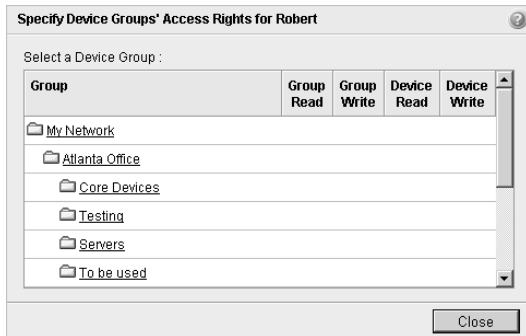
## Device Group Access Rights

You can further limit your Web users through **Device Group Access Rights** to be able to view or manipulate only certain device groups in your database. There are two ways to assign these rights: the first is by user and the second is by group.

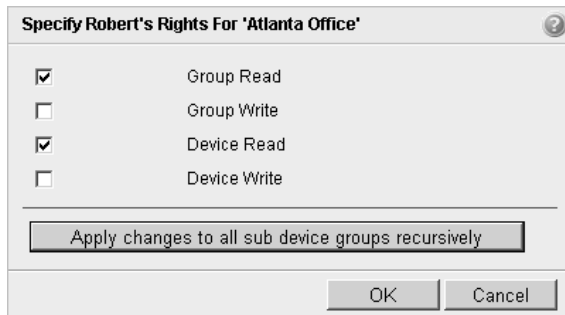
### Assigning Access Rights by User

- 1 In the Manage Users dialog, select the user to whom you want to assign rights.

- 2 In the Edit User dialog, click **Set Device Group Access Rights**. The page that appears shows all device groups in your database.



- 3 Select the group to which you want to assign rights.



- 4 Select the rights you want to give to that user for the selected group. Click **Apply changes to all sub device groups recursively** to give these rights to all subgroups in the current group.

**Note:** Access rights will not be enforced until the **Enforce Device Group Access Rights** option is selected in **Configure > Manage Web Server**.

## Assigning Access Rights by Group

- 1 In the **Explorer** tab of the Web interface, select the group to whom you want to assign rights.

**2** In the Group Operations list, select **Group Access Rights**.

User	Group Read	Group Write	Device Read	Device Write
admin	✓	✓	✓	✓
guest				
Robert				
Hollis				
Jennifer				
Anna				

Select the user to whom you want to give current group access rights. Current rights appear in the user list next to the user's name.

Specify Robert's Rights For 'Atlanta Office'

Group Read

Group Write

Device Read

Device Write

Apply changes to all sub device groups recursively

OK Cancel

**3** Select the rights you want to give to that user for the selected group. Click **Apply changes to all sub device groups recursively** to give these rights to all subgroups in the current group.

**Note:** Access rights will not be enforced until the **Enforce Device Group Access Rights** option is selected in **Configure > Manage Web Server**.

## Web Interface Operations and Device Group Access Rights

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

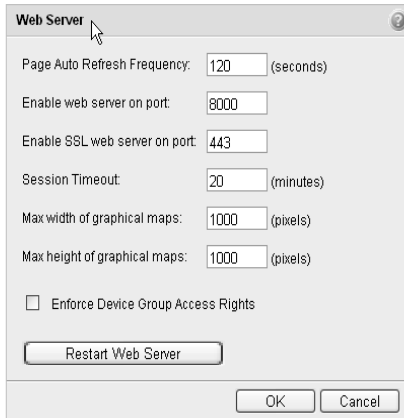
- List, Map, and Group reports in the **Group Views** menu require Group Read access.

- Create Group and Group Properties in the **Group Operations** menu require Group Read Write access.
- Copy Group requires Group Read in the source group, and Group Read Write in the destination group. (Permissions to groups and subgroups are copied, not inherited, from the new parent).
- Move Group requires Group Read Write in both the source and the destination groups. (Permissions of the group and subgroups remain the same.)
- Delete Group requires Group Read Write, Device Read Write recursively. (Device Read Write may not be required if the group is empty).
- Create Device requires Group Read Write and Device Read Write. If the device already exists in other group(s), you must also have Group Read Write and Device Read Write in one or more of those groups.
- Copy Device requires Group Read in the source group and Group Read Write in the destination group. The level of device permissions must be the same in both groups. Downgrade from Device Read Write to Device Read is also permitted.
- Move Device requires Group Read Write in both the source and the destination groups. The level of device permissions must be the same in both groups. Downgrade from Device Read Write to Device Read is also permitted.
- Viewing Device Properties and Device Reports requires Device Read.
- Modifying Device Properties, Bulk Field Change, and Acknowledgement require Device Read Write.

**Note:** Access rights will not be enforced until the **Enforce Device Group Access Rights** option is selected in **Configure > Manage Web Server**.

# Managing the Web Server

The following is a list of items that can be configured on your Web server.



The screenshot shows a 'Web Server' configuration window with the following settings:

- Page Auto Refresh Frequency: 120 (seconds)
- Enable web server on port: 8000
- Enable SSL web server on port: 443
- Session Timeout: 20 (minutes)
- Max width of graphical maps: 1000 (pixels)
- Max height of graphical maps: 1000 (pixels)
- Enforce Device Group Access Rights
- Restart Web Server button
- OK and Cancel buttons

- **Page Auto Refresh Frequency.** Enter, in seconds, how often you want device list, map and report pages to reload and refresh their data.
- **Enable Web server on port.** Enter the port you would like the WhatsUp Professional Web server to use for standard connections. The default value is 80, but you can enter any port number (for example, if you are running WhatsUp Professional on a server that also has a public Web server, you will want to enter a different port).
- **Enable SSL web server on port.** Enter the port you would like the WhatsUp Professional Web server to use for SSL-secured connections. The default value is 443, but you can enter any port number.
- **Max Width of Graphical Maps.** Enter the maximum width of maps viewed through the Web browser. The size is in pixels, and the default is 1000.
- **Max Height of Graphical Maps.** Enter the maximum height of maps viewed through the Web browser. The size is in pixels, and the default is 1000.
- **Session Timeout.** Enter, in minutes, the amount of time to pass after which WhatsUp Professional ends the session of an inactive Web user.
- **Enforce Device Group Rights.** Select this option to enforce device group rights on Web users. If this is selected, users will only be able to view the device groups for which they have rights. Clear this option to allow user access to all groups.
- **Restart Web Server.** Click this button to restart the Web server.

## Securing the Web Interface

Beyond the User Accounts, there are other security features included with the WhatsUp Professional Web Interface.

- **IP Security.** Specify an IP address or set of IP addresses that are either granted access to the Web site or are denied access. Addresses which are in both/neither the allow and deny lists are allowed.
- **SSL.** Use the SSL Web server to secure the information passed from the WhatsUp Professional Web server to the computer that you are using to access the interface.

### A Note About Web Security

WhatsUp Professional 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 (server.key and server.crt) are installed with every copy of WhatsUp Professional. Therefore, your encrypted session may not be as secure as it could be.

These certificate/key 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 Professional Install Directory>\data\SSL directory and should be updated with your own files.

## Configuring the Web Interface to use IIS

You can configure the WhatsUp Professional Web Interface to run through a Microsoft IIS (Internet Information Server) Web server. For more information, see “Configuring the Web Interface to use Microsoft IIS” on page 22.



# Performance Monitors

Performance Monitors in WhatsUp Professional gather statistics about the devices running on your network, then use that data to create real-time reports trending the utilization and availability of different device resources. You can configure monitors for the following:

- CPU Utilization
- Memory Utilization
- Interface Utilization
- Disk Utilization
- Ping Availability

The system also lets you create custom monitors that you can use to monitor any performance counter made available through WMI or SNMP.

## Performance Monitor Library

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

To access this dialog, from the WhatsUp Professional Console main menu, select **Configure > Performance Monitor Library**.

# Chapter 8

## In this Chapter

---

Performance Monitor Library

Performance Reporting

Configuring Performance Monitors

Example: Monitoring Router Bandwidth

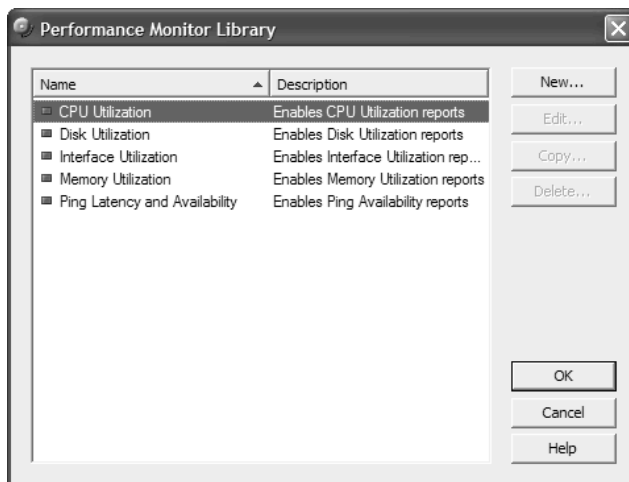
Example: Troubleshooting a Slow Network Connection

Custom Performance Monitors

Example: Custom Performance Monitors

Enabling SNMP on Windows Devices

---



There are two types of Performance Monitors:

- WhatsUp Professional 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, but cannot be edited or changed from their default settings. These monitors are ready to be added to devices, as described in “Configuring Performance Monitors” on page 85.
- Custom monitors are monitors that you create to monitor any WMI or SNMP performance counter. Custom monitors can be added in two ways: when added in the Performance Monitor Library, the custom monitor is available for use on any device; when added via the **Device Properties > Performance Monitors** dialog, the custom monitor is available only to that device.

For more information on creating custom performance monitors, see “Custom Performance Monitors” on page 93.

You can use the Performance Monitor Library to do the following:

These functions apply only to custom monitors that you create in the Performance Monitor Library. Default monitors in the library cannot be edited or removed: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

- Click **New** to configure a new custom Performance Monitor.
- Select an existing custom monitor and click **Edit** to change its current configuration.

- Select a custom Performance Monitor and click **Copy** to make a copy of that monitor and add it to the list.
- Select a custom Performance Monitor and click **Delete** to remove it from the list.

## Configuring Performance Monitors

To configure these monitors for use on specific devices, you must use either the **Device Properties > Performance Monitors** to configure a single device, or **Bulk Field Change > Performance Monitors** to configure multiple devices.

Before you configure a monitor, check the following:

- Make sure that SNMP or WMI monitoring is enabled for the device.

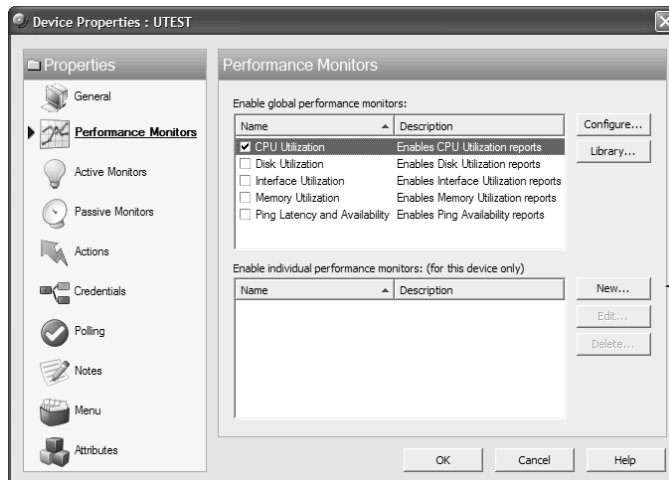
For more information on SNMP monitoring, see “Enabling SNMP on Windows Devices” on page 96.

For more information on WMI monitoring, see “About WMI” on page 145, and the WhatsUp Professional release notes.

- Set the credentials for accessing the device via SNMP or WMI. For more information, see “Credentials Overview” on page 59.

### Configuring a single device

- 1 Double-click the device icon to access that device's Device Properties.
- 2 Click **Performance Monitors** to view that page of the dialog.



CPU Utilization monitor is selected for this device.

A custom monitor created here would apply to this device only.

- 3 Select the Performance Monitor you want to add to this device and click **Configure**. You can configure the system-wide monitors in the top section, and device specific monitors in the bottom section. The configuration dialog for that monitor appears.
- 4 Optionally, make any changes on the monitor configuration dialog. For the default monitors, you may need to make changes if there are multiple resources (CPUs, interfaces, disks).
  - a In the **Collect data for** drop-down list, depending on the monitor, you can select **All items**, **Active items**, or **Specific items**. If you select Specific items, the list is enabled and you can select or clear any item in the list. This is particularly useful for the Interface Utilization monitor where a device may have many interfaces.
  - b Select the **Data collection interval**. This is the amount of time between performance polls.
  - c Click **Advanced** to change connection settings on the device.
  - d Click **OK** to save the changes.
- 5 On the Device Properties page, click **OK**.

## Configuring multiple devices

- 1 Select the devices you want to configure performance monitors for.
- 2 Right-click on a selected monitor and select **Bulk Field Change > Performance Monitors**.
- 3 In the Bulk Field Change: Performance Monitors dialog, select the changes you want to make for each type of monitor; **No change**, **All** (begin collecting statistics on all items on all selected devices,) or **None** (stop collecting statistics on all selected devices.)
- 4 If **All** is selected, you can change the collection interval for the selected devices.
- 5 Click **OK** to make the selected changes.

## Performance Reporting

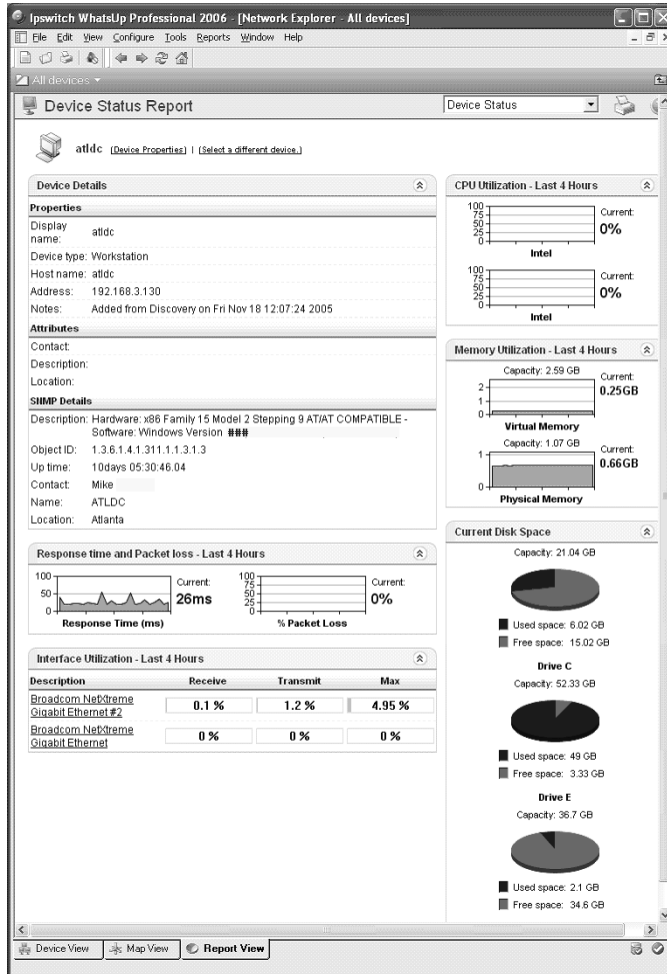
Through the Performance Monitoring feature, the application can be configured to collect specific types of data on your SNMP and WMI enabled devices. Once that data is gathered, you can generate reports to see the results of the performance monitoring. The following explains the different ways you can view and access this information.

## Device Status Report

This report details the current status (a snapshot) of one device within a group. The sections within the report only contain data if those performance monitors have been enabled for the device on **Device Properties > Performance Monitors**.

To access the Device Status report, click the Report view tab and select either All Reports or Device Reports on the Report view toolbar.

You can also access the Device Status report by selecting **Device** from the Reports menu or by right-clicking on a device and selecting Device Reports.



## Group and Device Performance Reports

These reports display information for devices or device groups that have performance monitors configured and enabled. Access these reports from the Report View.

**CPU Utilization** - This report displays CPU utilization percentages collected during the selected time period from the device or device group displayed at the top of the report.

**Disk Utilization** - This report displays disk utilization percentages collected during the selected time period from the device or device group displayed at the top of the report.

**Interface Statistics** - This report displays interface utilization information collected during the selected time period from the device or device group displayed at the top of the report.

**Memory Utilization** - This report displays memory utilization collected during the selected time period from the device or device group displayed at the top of the report.

**Ping Availability** - This report displays ping availability data collected during the selected time period from the device or device group displayed at the top of the report.

**Ping Response Time** - This report ping response time data collected during the selected time period from the device or device group displayed at the top of the report.

## Top 10 Report

This collection of reports displays the top devices based on the criteria of each report section. Configure how you want this report to look by clicking the **Configure** link. This link takes you to the Configure Top 10 Reports page. Through this page, you can change the order of the reports, the number of items in each report, and which column the report appears in.

To access the Top 10 reports, click the **Report view** tab and select either All Reports or System Reports on the Report view toolbar.

## 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 and set up for the device in **Device Properties > Credentials**. 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 for PCs, see “Enabling SNMP on Windows Devices” on page 96.

## Configuring the Monitor

Because the Interface Utilization performance monitor is one of the default performance monitors installed with WhatsUp Professional, 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 In the WhatsUp Professional console, double-click the device you want to gather performance data for.
- 2 Click Performance Monitors to access that section of the Device Properties.
- 3 Select the Interface Utilization monitor from the list.
- 4 Click **Configure** to set up the monitor for the device. WhatsUp Professional scans the device and discovers the interfaces on the device.

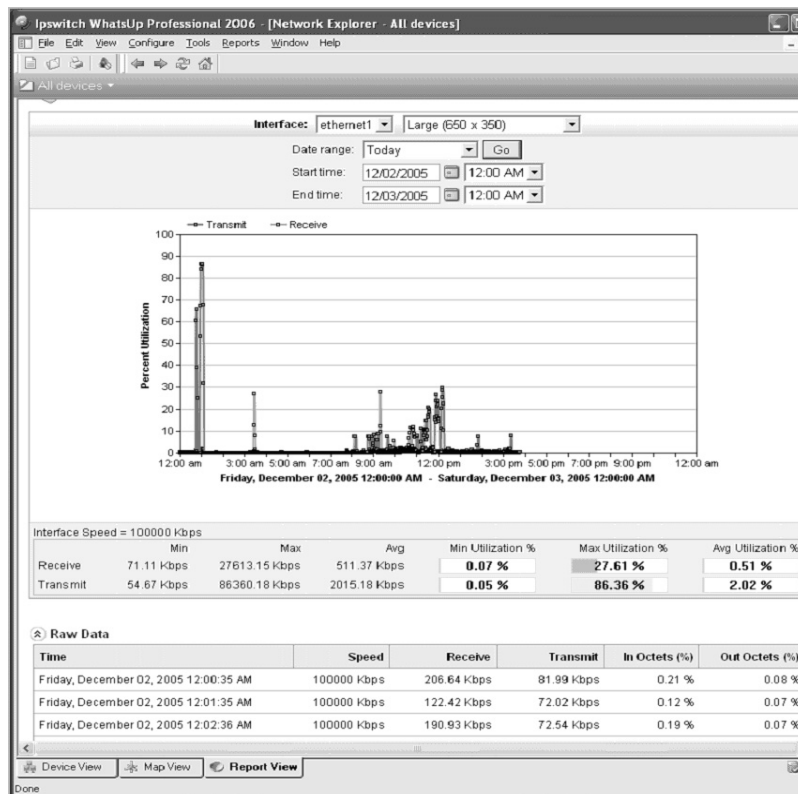
Once the scan is complete, the Configure Interface Data Collection dialog appears. If the credentials for the device are not configured properly, the scan will fail (return to the Credentials Library to fix it.) If the device is not SNMP-enabled, the scan will fail (see “Enabling SNMP on Windows Devices” on page 96).

- 5 Select the interfaces you want to collect data for. From the **Collect data for** pull-down, select All, Active, or Specific. If you select Specific, select just the interfaces you want to monitor in the list below. By default, active interfaces will be measured.
- 6 (Optional) Click **Advanced** to change the retry and timeout settings for the SNMP connection to the device. Click **OK** to save the changes to the Advanced Settings.
- 7 On the Configure Interface Data Collection dialog, enter a time interval (in minutes) you want the application to wait between polls. The default is 10 minutes. See, “Program Options - Report Data for more information on data collection and roll-up.”
- 8 Click **OK** to save the Interface Utilization configuration.

## Viewing the Data

WhatsUp Professional 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.

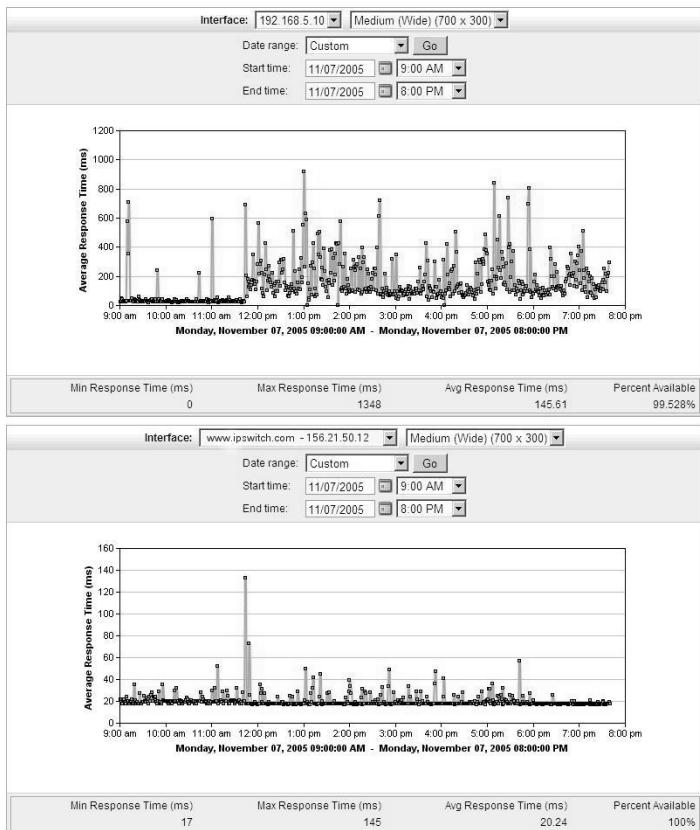
We first describe the situation, then the steps taken by the network administrator to solve the problem.

A developer working in Augusta (GA) on an Atlanta project complained of a "slow network (T1) connection" between Augusta and Atlanta, saying it took 40 minutes to check in (to the source library) a few files.

The network administrator in the Atlanta office followed up by taking the following steps:

- 1** Goes to the WhatsUp Professional console, which has been set up to monitor critical devices in the Atlanta office, as well as connections to other Ipswitch sites.
- 2** Checks the Ping Response Time report for the connection from the WhatsUp Professional console (in Atlanta) to the Augusta primary server, which shows increased response time starting at 11:45 AM.

Note that this connection has been configured with appropriate performance monitors and gathering data for weeks. To set up this type of monitoring for a connection, configure the Ping Latency and Availability monitor on a device that is on the other end of the connection as seen from the device on which you run the WhatsUp console. See “Configuring Performance Monitors” on page 85 for more information.



Something has happened on the network at 11:45am today and has not stopped all afternoon.

Note that this appears to affect traffic between Atlanta and Augusta - however looking at the same timeline between Atlanta and Lex - we do not see the same slowdown.

Seems to suggest that something is causing the Augusta end of the network to be slow - something that went into effect at 11:45am.

Dave is seeing the link from Augusta to Atlanta being painfully slow.

- To confirm that this behavior is not caused by our net provider, the network administrator makes the same check (Ping Response Time) for the connection from the WhatsUp Professional console (in our internal network) to a primary server (www.ipswitch.com) at our Lexington site. This shows a small spike at 11:45, then a return to a normal baseline.

In comparing the Ping Response Time reports for the two connections, the network administrator confirms that the problem is local to our Augusta office. The report for the Atlanta to Augusta connection shows a spike at 11:45 AM and then an increased baseline, that continues until 11:00 PM that night. The report for the Atlanta to Lexington connection shows a smaller spike at 11:45 AM, then a return to normal baseline. It does not reflect the significant jump from the baseline seen on the Augusta connection.

The historical data on Atlanta to Augusta connection shows a significant jump from baseline from 11:45 to 11:00 pm, then back to normal baseline and continues normal the next day.

Be aware of differences in scale when comparing reports. In our example, the two reports show different values on the Y-axis, which seem to minimize the difference in the baselines.

- 4 As a next step, now that the cause of the slow connection has been isolated to the Augusta site, the network administrator checks the Interface Bandwidth Utilization report for servers on the Augusta network, and further isolates the problem to one server.

## Custom Performance Monitors

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 (to be used system wide)

- 1 In the WhatsUp Professional console, go to **Tools > Performance Monitor Library**.
- 2 In the Performance Monitor Library, click **New**.
- 3 Select the monitor type: SNMP or WMI.
- 4 Configure the monitor:

#### 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 Once 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.

### 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.

Once the monitor has been added to the library, you can enable that monitor through **Device Properties > Performance Monitors** for that device.

## To create a custom performance monitor to use on a single device

- 1 In the WhatsUp Professional console, double-click the device icon you want to create the monitor on. The Device Properties for that device appears.
- 2 Click Performance Monitors to access that section of device properties.
- 3 Click **New** next to the Individual performance monitors list.
- 4 Select the monitor type: SNMP or WMI.
- 5 Follow the directions above for creating either an SNMP or WMI monitor.

You can suspend or enable data collection on that monitor by selecting or clearing the checkbox next to the monitor name.

### Example: Custom Performance Monitors

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

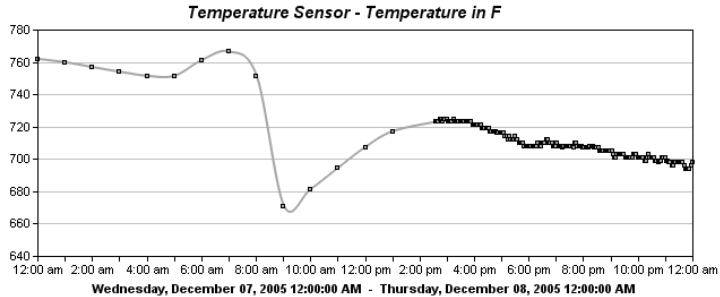
With the device in the group, we created a Custom SNMP Performance Monitor for that device.

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.

The screenshot shows a dialog box titled "Add SNMP Performance Counter". It contains the following fields and controls:

- Name:** A text box containing "Temperature Monitor".
- Description:** A text box containing "Enables Custom Performance Monitor reports".
- Performance counter:** A text box containing "1.3.6.1.4.1.3854.1.2.2.1.16.1.14".
- Instance:** A text box containing "0".
- Collection interval:** A spin box set to "10".
- Timeout: (seconds):** A spin box set to "3".
- Retries:** A spin box set to "1".
- Buttons:** "OK", "Cancel", and "Help" buttons are located on the right side of the 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:



## Enabling SNMP on Windows Devices

Before you can collect performance data on a Windows PC, you must first install and enable an SNMP agent on the device. This section describes how to install and enable the Microsoft SNMP Agent, though you can use another SNMP agent.

### To install SNMP Monitoring

- 1 From the Windows Control Panel, select Add or Remove Programs.
- 2 Select 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 Once the install wizard is complete, click **Finish** to close the window.

### To enable SNMP Monitoring

In the Control Panel, select Administrative Tools.

- 1 Double-click Services to open it.
- 2 In the Services (Local) list, double-click SNMP Service to view the Properties.

- 3 On the Agent tab, enter the name of the person responsible for the upkeep and administration of the computer, and enter the location of the computer. These items are returned during some SNMP queries.
- 4 On the Security tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like WhatsUp to read information about the computer. This community string will be later used to create credentials for connecting to this device.
- 5 On the General tab, click **Start** to start the service (if necessary.)
- 6 Click **OK** to close the dialog.

You can test the device by connecting to it through SNMP View



# Active Monitors

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.

## Monitors and Actions

The Monitors and the Action systems work together in WhatsUp Professional to help you stay informed about what is happening in 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 a touch of creativity, a network administrator should be able to tailor the Monitors and Actions systems to watch over all of their important devices, and to troubleshoot problems that may arise.

## Taking Advantage of the Relationship

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

- **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 can't 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 sorts of information, and trigger an Action accordingly.
- **Security Features.** Pay careful attention to your devices and services that are critical to the security of your network.
- **Network Resources.** WhatsUp Professional can be configured to perform an Action when your network resource availability diminishes across a certain threshold.

# Chapter 9

## In this Chapter

---

Monitors and Actions

Active Monitor Library

Assigning Active Monitors

Deleting Active Monitors

Group and Device Active Monitor Reports

Example: Monitoring Network Printer Toner Levels

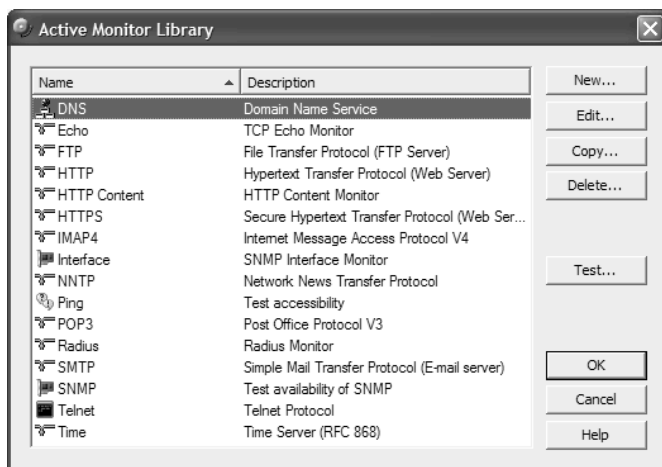
---

- **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.

## 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, those changes affect each instance of that particular monitor across your device groups.

Access the Active Monitor Library from the main menu of the WhatsUp Professional console. Select **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 Professional.

- Click **New** to configure a new type.
- Select an existing type and click **Edit** to change the current configuration of a type.
- Select an ActiveMonitor type and click **Copy** to make a copy of that type and add it to the list.
- Select an Active Monitor type and click **Delete** to remove it from the list.
- Select an Active Monitor and 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 Professional.

- **DNS Monitor.** This 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.** 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.** This monitor checks for a Telnet server on port 23. If no telnet service responds on this port, then the service is considered down.
- **Ping Monitor.** This monitor sends an ICMP (ping) command to the device. If the device does not respond, the Monitor is considered down.
- **TCP/IP Monitor.** This 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.
- **Active Script Monitor.** This monitor 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. Please be aware that Ipswitch does not support the scripts that you create, only the ability to use them in the Active Script Monitor.
- **NT Service Monitor.** This monitor allows you to check the status of a service on an Windows machine and attempt a restart of that service (if the appropriate Administrator permissions exist).

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

## 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 enough, so there is no need to make any changes to the Active Monitors in the library.

## Add/Edit an Active Monitor

- 1 From the main menu, select **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 that Monitor type appears.
- 3 Once 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.

## Assign an Active Monitor to a Device

There are three ways to add Active Monitors to devices:

- Selecting the Active Monitors you want to scan for during Device Discovery. When you select the discovered devices and add them to your database, WhatsUp Professional creates a Monitor for each network service found.
- Click the **Discover** button on the Active Monitor dialog of Device Properties. WhatsUp Professional will then scan the device and create a Monitor for each network service found.
- Manually assign an Active Monitor to the device:
  - a On the Active Monitor dialog of Device Properties, click **Add**. The Monitor Properties dialog appears.
  - b Select the Active Monitor type you want to assign. Click **Next**.
  - c Set the polling properties for the Monitor. Click **Next**.
  - d Setup actions for the Monitor.
  - e Click **Finish** to add the Monitor to the device.

## 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 yourself. This includes the default types that were added during initial installation of WhatsUp Professional. It is recommended that you only delete the custom Monitors that you create.

**Warning:** 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.

### To remove a Monitor from a device

- 1 Double-click the device from which you want to remove the Monitor. The Device Properties dialog appears.
- 2 Click the Active Monitor icon in Device Properties.
- 3 Select the Monitor you want to remove from the list.
- 4 Click **Remove**.
- 5 A warning dialog appears, stating that all data for that Monitor will be deleted if the Monitor is removed.
- 6 Click **OK** to remove the Monitor.

**Note:** If you wish 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.

## Group and Device Active Monitor Reports

These reports display information for devices or device groups that have active monitors configured and enabled. Access these reports from the Report View.

- 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 Professional you can create a custom SNMP Active Monitor that will notify you when toner levels are low.

### Configuring the Monitor

- 1 From the WhatsUp Professional console main menu, select **Configure > Active Monitor Library**. 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 In the **Active Monitor Library** dialog, click **New** and select **SNMP Monitor**,
- 3 In the **New SNMP Monitor** dialog, name the monitor TonerMonitor and describe it similarly. For the Object ID and Interface, 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 level. 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 by going to **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.

# 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 anti-virus 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 Professional when they occur.

## Configuring Passive Monitor Listeners

A Passive Monitor Listener is a separate executable that listens for an event to occur and then notifies WhatsUp Professional. 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, file changes, or application specific events.

WhatsUp Professional 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 come from non-UNIX devices as well. They might contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.
- **Windows Event Log Monitor.** This could be monitoring when a service is started or stopped, if there was a logon failure, or any other entry in the Windows Event Log.

# Chapter 10

## In this Chapter

---

Configuring Passive Monitor Listeners

Passive Monitor Library

Configuring Passive Monitors

Group and Device Passive Monitor Reports

---

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

- 1 From the WhatsUp Professional console, select **Configure > Program Options**.

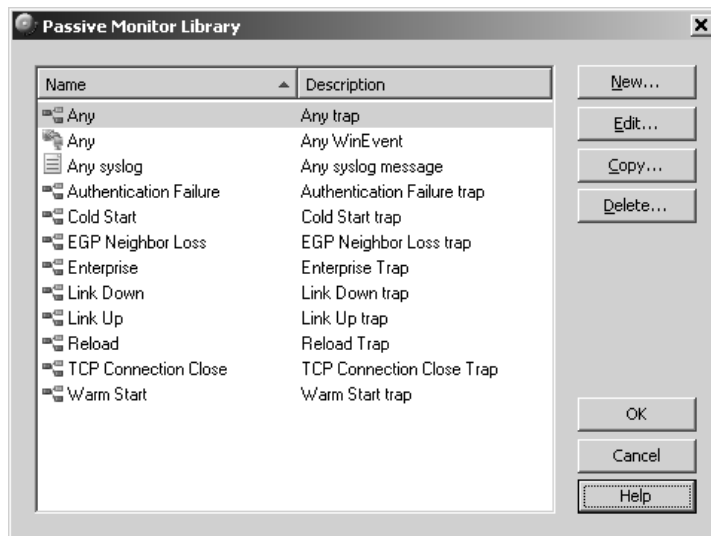
If the Windows SNMP Trap Service (Control Panel > Services) is running on the WhatsUp console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp passive monitor listener.

- 2 In Program Options, select **Passive Monitor Listeners**.
- 3 Select the listener you want to configure and click **Configure**.
- 4 Enter the appropriate information based on the listener being configured.
- 5 Click **OK** to save the changes.

## Passive Monitor Library

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

To access the Passive Monitor Library on the WhatsUp Professional console, select **Configure > Passive Monitor Library**.



- Click **New** to create a new type.
- Select a type in the list and click **Edit** to change the settings.

- Select a type and click **Copy** to create a new type based on the selected type.
- Select a type and click **Delete** to remove it from the list.

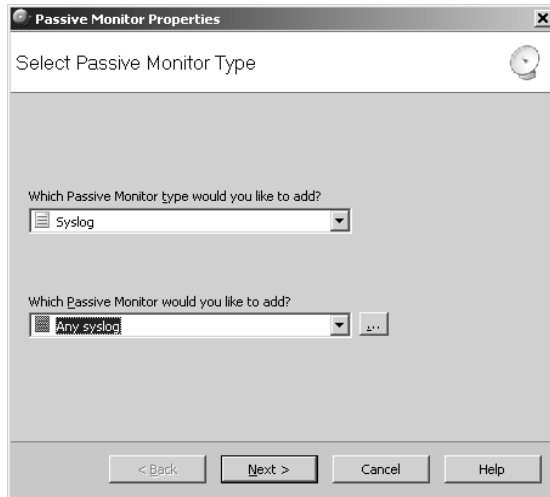
## Configuring Passive Monitors

### Add/Edit a Passive Monitor Manually

- 1 From the main menu, select **Configure > Passive Monitor Library** to view the Passive Monitor Library.
- 2 Click **New** to configure a new Passive Monitor, or select a Monitor from the list and click **Edit** to make changes to an existing configuration. The configuration dialog for that Monitor type appears.
- 3 Once 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.

### Assign a Passive Monitor to a Device

- 1 Double-click the device to display its properties. Select **Passive Monitors**, then click **Add**. The Passive Monitor Properties dialog appears.



- 2 Select the Passive Monitor and type you want to assign. Click **Next**.
- 3 Set up Actions for the Monitor.
- 4 Click **Finish** to add the Monitor to the device.

## Using the Trap Definition Import Tool

This tool allows you to import SNMP Trap definitions into your Passive Monitor Library. The list in this dialog is populated by the MIBs that are currently in the **\Program Files\Ipswitch\WhatsUp Professional\Data\Mibs** directory.

To import trap definitions, select the traps listed here and click **Import to passive monitor library**. Select **All Traps** to select all the traps in the list. Clear the option to de-select all of the traps.

When you click **Import to passive monitor library** the Trap Import Results dialog appears. Traps that already exist in the database will not be imported again.

To add traps to the list, copy the .txt file for that MIB into the **Program Files\Ipswitch\WhatsUp Professional\Data\Mibs**, then restart the console.

### Select trap definitions to import:

- **Trap Name** - The name of the trap to be imported.
- **Enterprise OID** - This is the same as the SNMP enterprise identifier in the trap, which is used for unique identification of traps for a particular application.
- **Generic** - Each trap has a generic type number. This number is part of the rule that determines the matching criteria for an incoming trap.
- **Specific** - Enterprise specific number that identifies the MIB.
- **MOIB Module** - The code type of MIB.

## Group and Device Passive Monitor Reports

These reports display information for devices or device groups that have passive monitors configured and enabled. Access these reports from the Report View.

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

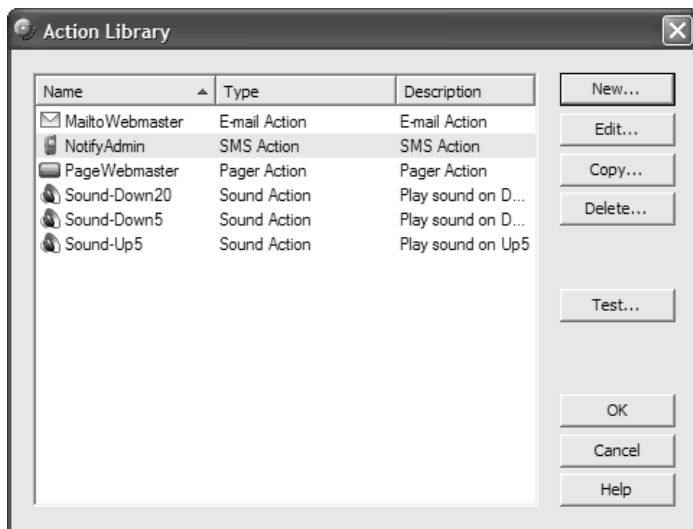
# Actions

Actions provide the mechanism for notifying you about changes in the status of a device or a Monitor, or for launching a program in response to a status change. For example, if your Web server device is down, you will get a visual indicator (the device icon changes color to red). You may also want to trigger an Action that plays a sound or sends an e-mail message to the Webmaster.

## Action Library

The Action Library is the central storehouse of all Actions that have been configured for your network. When changes are made to an Action listed in this dialog, those changes effect each instance of that particular Action across your device groups.

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



This dialog is used to configure a new or existing Action.

# Chapter 11

## In this Chapter

Action Library

Action Types

Action Strategies

Using Actions - A Simulation

Action Policies

Implicit Action Policy

Using Other Types of Actions

Percent Variables

- Click **New** to configure a new Action. Then, select the Action Type. For a description of each type, see “Action Types” on page 110.
- To change the configuration of an Action, select it, then click **Edit**.
- To create a new Action based on the existing one, select an existing Action, then click **Copy**.

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.

Some Actions, when triggered, send a message (for example, e-mail, pager, SMS). You are provided with a default message for these Actions, which you can modify as needed.

Once created, Actions can be assigned to a device, a 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.

For a step-by-step example of how to create and assign an Action, see “Using Actions - A Simulation” on page 112.

## Action Types

An Action assigned to a device or Monitor “fires” when a specified state change occurs. WhatsUp Professional supports the following types of Actions.

- **Sound:** Sound an alarm by playing a selected sound file on the WhatsUp Professional console.
- **Beeper:** Activate a beeper.
- **Pager:** Send a message to a pager.
- **E-mail:** Send an SMTP Mail message.
- **SMS:** Send a Short Message Service (SMS) notification to a pager or cell phone.
- **Winpopup:** Display a message in a pop-up window on a Windows NT system.
- **Syslog:** Send a message to a host that is running a Syslog server.
- **Text-to-Speech:** Send a text-to-speech notification to a speaker.
- **Program:** Run another program (executable) to take some action.
- **Service Restart:** Stop or restart a Windows NT Service.
- **Web Alarms:** Play a sound to notify of a device state change.
- **Script:** 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

Ipswith does not support the scripts that you create, only the ability to use them in the Script Action.

## 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 (for example, an e-mail, SMS, or pager message sent to inform the target of a state change).

Imagine the number of messages sent if external notifications are placed on a router and every device and monitor that uses that router for their connection to the Internet. If the router goes down, it will appear as if all of the devices are down, and messages will be sent for each of them. Consider using dependencies and limiting the external notifications to the router and the most important of the devices in the group.

- Don't 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. For example, you could create a **Down at least 60 mins** state, and sending an escalated message to show that the device is still down after an hour. This can be done through **Program Options > Device States**.

- 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. Find Action Policies on the console main menu at **Configure > Action Policies**.

- 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 wish to be notified if any 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 monitors itself. Remember that if you assign the action to both the monitor and the device, both actions will fire if the monitor goes down.

## Using Actions - A Simulation

This section describes how to configure an Action and assign it to a device, using the example of an E-mail Action.

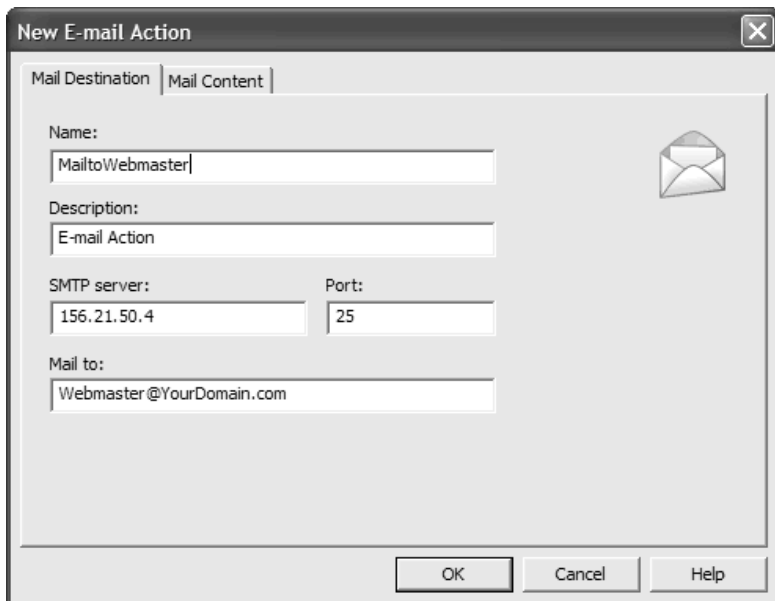
In the example, you want to be notified by e-mail if the web server device (the computer on which the web server is running) is down. To accomplish this, we will:

- Configure an E-mail Action
- Test the Action
- Assign the Action to the device

### Configure the Action

In this example, we are configuring an E-mail Action that will be assigned to a Web server device. If the device does not respond to polling for 2 or more minutes, the E-Mail Action is triggered and sends a message to the Webmaster.

- 1 Select **Configure > Action Library**.
- 2 Click **New**, then select **E-Mail Action** as the type. The New E-Mail Action dialog appears, with focus on the Mail Destination tab.

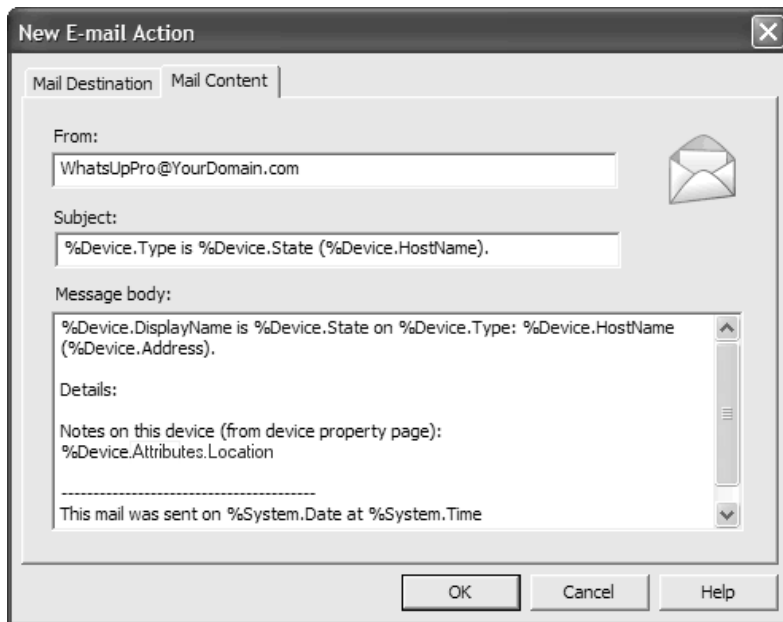


The screenshot shows a dialog box titled "New E-mail Action" with a close button (X) in the top right corner. The dialog has two tabs: "Mail Destination" (selected) and "Mail Content". The "Mail Destination" tab contains the following fields:

- Name: MailtoWebmaster
- Description: E-mail Action
- SMTP server: 156.21.50.4
- Port: 25
- Mail to: Webmaster@YourDomain.com

There is an envelope icon on the right side of the dialog. At the bottom are "OK", "Cancel", and "Help" buttons.

- 3 In the **Name** box, enter a unique name that identifies the Action, for example “Mailto Webmaster.” This name will be used to label the Action in other dialog boxes.
- 4 In the **Description** box, enter a short description of the Action. This is displayed in the Action Library along with the entry in the **Name** box.
- 5 In the **SMTP Server** box, enter the IP Address (or the DNS hostname) of the e-mail server for your domain. Port 25 is the standard port for SMTP communications; if your mail server uses a different port number, you can enter it in the **Port** box.
- 6 In the **Mail to** box, enter one or more e-mail addresses that are acceptable to your SMTP server. Separate each address with a comma; spaces are not allowed. The addresses should not contain brackets, braces, quotes, or parentheses.
- 7 Select the Mail Content tab (at the top of the dialog) to switch focus.



The screenshot shows a dialog box titled "New E-mail Action" with a close button (X) in the top right corner. It has two tabs: "Mail Destination" and "Mail Content", with "Mail Content" selected. The dialog contains the following fields and text:

- From:** WhatsUpPro@YourDomain.com
- Subject:** %Device.Type is %Device.State (%Device.HostName).
- Message body:**
  - %Device.DisplayName is %Device.State on %Device.Type: %Device.HostName (%Device.Address).
  - Details:**
  - Notes on this device (from device property page): %Device.Attributes.Location
  - 
  - This mail was sent on %System.Date at %System.Time

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- 8 The **From** address defines the sender of the message as:

*WhatsUpPro@YourDomain.com.*

You can change *YourDomain* to your company’s domain name, or you can enter any address acceptable to your e-mail server.

- 9 The **Subject** box shows a status message that states the type of device, its current state, and the hostname.

*%Device.Type is %Device.State (%Device.HostName)*

This message uses variables to show the type of device, its current state, and its hostname; for example: *Server is down (Web1.YourDomain.com)*.

You can use variables to customize the message in the Subject and in the Message Body. For more information on variables, see “Percent Variables” on page 122.

- 10** The **Message Body** box shows a detailed status message for the device.

*%Device.DisplayName is %Device.State on %Device.Type: %Device.HostName  
(%Device.Address)*

*Details:*

*%Device.Attributes.Location*

-----

*This mail was sent on %System.Date at %System.Time*

*Ipswitch WhatsUp Professional 2006*

In our example, when the Action is triggered, the e-mail will report a message like the following:

*Web1 is down on server: web1.YourDomain.com (156.21.50.4)*

*Details:*

*Lamar Bldg; 2nd floor*

-----

*This mail was sent on 02/17/2005 at 15:34:06*

*Ipswitch WhatsUp Professional 2006*

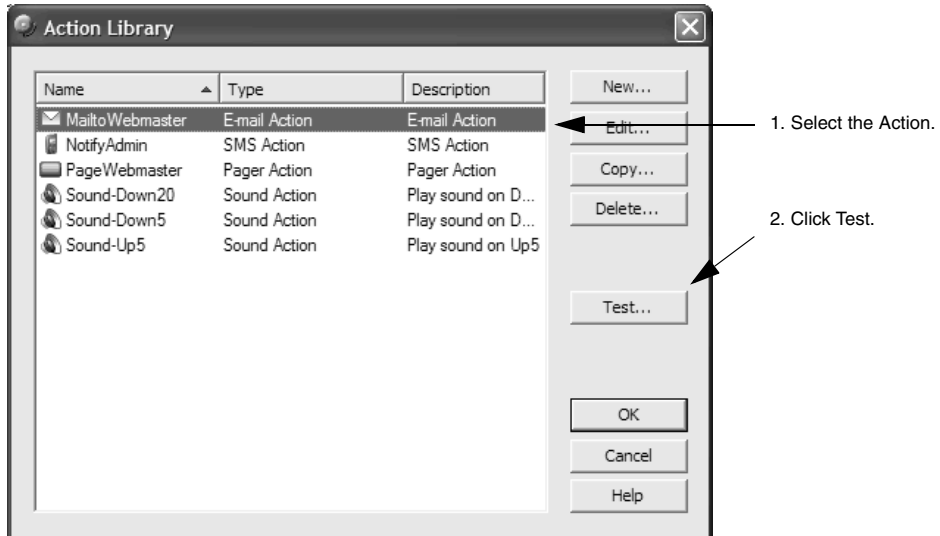
You can customize this message by adding or removing variables and text. For more information on variables, see “Percent Variables” on page 122.

- 11** Click **OK** to save the new Action.

The Name and Description of this Action now appears in the Action Library.

## Test the Action

To test the Action, select it in the Action Library, then click the **Test** button. WhatsUp Professional runs a test and responds with a Success or Fail message. This test verifies the information specified in the Action. For example, for an E-Mail Action, it verifies that the SMTP Server is accessible and will accept a message from the specified user account.



A message dialog shows the test results.

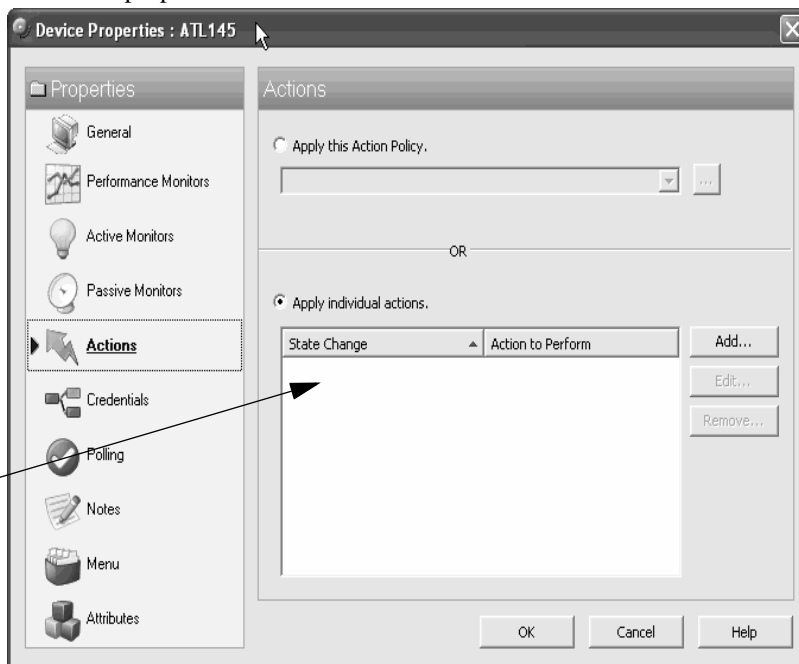


Note that this test is run by the WhatsUp Professional console (NMConsole.exe), but when an Action is triggered, it will be run by the service (NMService.exe). The best way to get accurate test results is to run both of these programs from the same Windows NT account.

## Assigning an Action to a Device

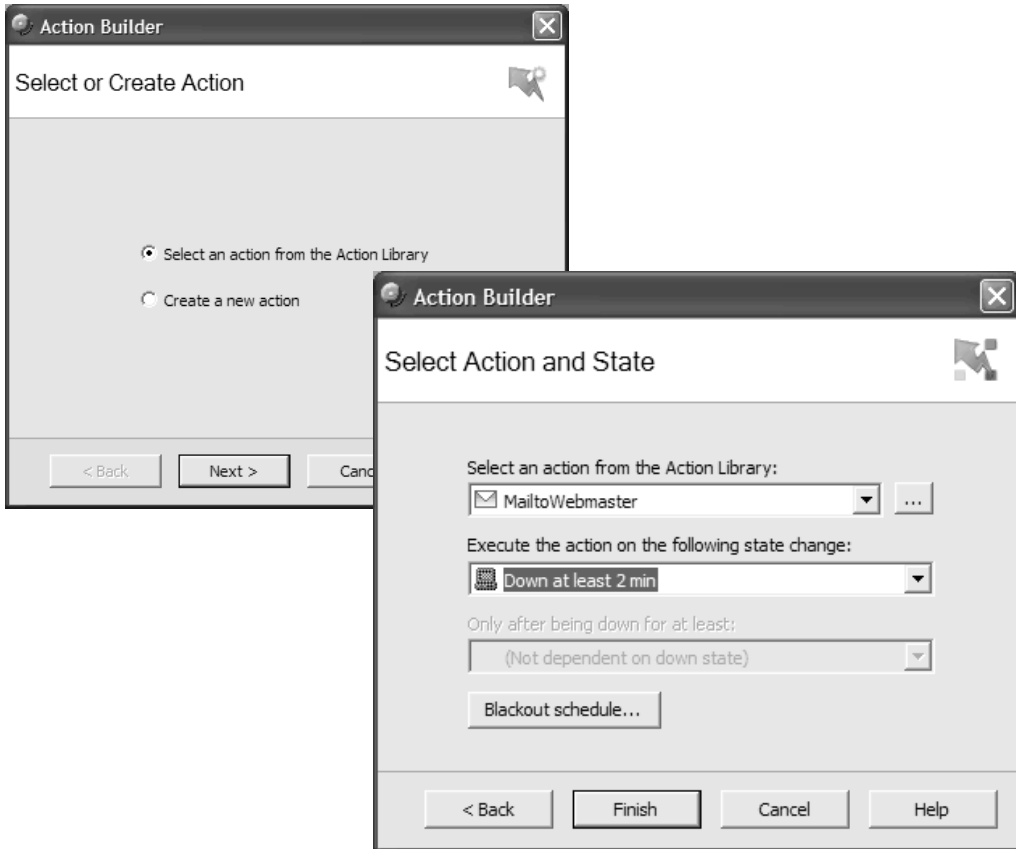
The next step in configuring an Action is to assign it to a device or Monitor. In our example, we assign the **MailtoWebmaster** Action to the Web1 device. If Web1 goes down, the Action sends an e-mail to the webmaster.

- 1 In the Device List, select the Web1 device, then right-click and select **Properties** from the menu. The Device Properties appear.
- 2 Select the Actions properties.



There are currently no Actions assigned to this device.

- 3 Select **Apply individual Actions**, then click **Add**. The Action Builder wizard appears.



- 4 Select **Select an Action from the Action Library**, then click **Next**.
- 5 Select the **MailtoWebmaster** Action, then select to trigger this action when the web server has been **Down at least 2 min**.
- 6 Click **Finish** to assign this Action to the Web1 server.

The Action is now shown on the Action properties for the device.

When the Web1 device is down for more than 2 minutes, the Action sends an e-mail message similar to the following:

*Web1 is down on server: web1.YourDomain.com (156.21.50.4)*

*Details:*

*Lamar Bldg; 2nd floor*

-----  
*This mail was sent on 02/17/2005 at 15:34:06*

*Ipswitch WhatsUp Professional 2006*

## Assigning an Action to a Monitor

You can also assign an Action to an Active or Passive Monitor. For example, you might create an Active Monitor to monitor the HTTP service on your Web server. Thus, you could know if the Web service went down, which may or may not mean that the Web server device is down.

Using our Web1 device example, we assign the **MailtoWebmaster** action to the HTTP Active Monitor:

- 1 In the Device List, right-click the Web1 device, then select **Properties** from the menu.
- 2 Select the Active Monitor properties.
- 3 Select the HTTP Monitor, then click **Edit**. The Monitor Properties appears.
- 4 Select **Apply individual actions**, then click **Add**. The Action Builder appears.
- 5 Select **Select an action from the Action Library**, then click **Next**.
- 6 Select the **MailtoWebmaster** action, then select it to execute on **Down at least 2 minutes**, then click **Finish**.

The Action is now shown in the Action properties of the Active Monitor.

- 7 Edit the content of the **MailtoWebmaster** action so it reports the Active Monitor status. Add the following text and variables to the message body:

*Monitors that are down include: %Device.ActiveMonitorDownNames*

*Monitors that are up include: %Device.ActiveMonitorUpNames*

When the HTTP Active Monitor (on Web1) is down for more than 2 minutes, the Action sends an e-mail message similar to the following:

*Web1 is down on server: web1.YourDomain.com (156.21.50.4)*

*Monitors that are down include: HTTP Active Monitor*

*Monitors that are up include:*

*Details:*

*Lamar Bldg; 2nd floor*

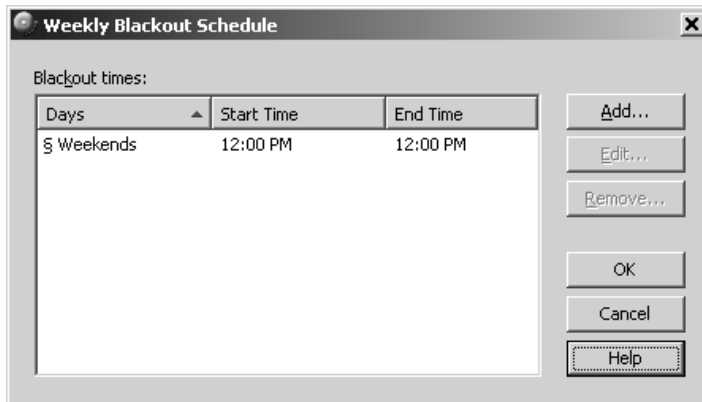
*This mail was sent on 02/17/2005 at 15:34:06*

*Ipswitch WhatsUp Professional 2006*

## Blackout Periods

You can create a Blackout period to have WhatsUp Professional 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 e-mail when there is no one to receive it.

This dialog is found in the Action Builder wizard.



Click add or edit to configure a blackout period, then select the day and time you want the Action to be placed in blackout period, and when you want WhatsUp Professional to begin using the Action. You can select multiple days for a single time period.

## Action Policies

You can use Action Policies to stack multiple Actions together in a single policy. You can then assign that Action Policy 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.

The Action Policy dialog shows the Action Policies that you can assign to any device or monitor. This is where you create a new action policy, modify an existing policy, or delete a policy.

To create an Action Policy:

- 1 From the menu bar, select **Configure > Action Policies**. The Action Policies dialog appears.
- 2 On the Action Policies dialog, click **New**.

- 3 In the New Action Policy dialog, enter a name in 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 Add existing Actions to the Action Policy, or create new Actions, then add them. 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 the **Only execute first action** option, WhatsUp Professional tries each action for that state from top to bottom until it finds one which succeeds.
- 8 Once all of the Actions have been added, click **OK** to create the Policy and add it to the active list.

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.

- 9 Assign the Action Policy to a device or monitor.

## Implicit Action Policy

With the Implicit Action policy, WhatsUp Professional automatically assigns actions to all devices in your database. By default, the Implicit Action policy is populated with a Web Alarm action, but that can be removed. 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 Professional 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.

## Using Other Types of Actions

Our simulation showed how to create an E-mail Action, test it, and apply it to a device. You would follow basically the same process if you wanted to use any of the other Actions.

Actions like beeper, pager, sound, and WinPopup are similar to the E-mail Action we just covered. See the Help system for step-by-step procedures on creating these Actions. Some Actions may be used in other ways, which are briefly explained below:

- **SMS Actions:** You can send a message using SMS (Short Message Service). SMS is similar to paging. However, SMS messages do not require the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability.

WhatsUp Professional transmits the SMS message to the Provider, and the provider forwards it to the cell phone. WhatsUp Professional does not broadcast SMS messages directly.

- **Service Restart:** You can start or stop an NT service when another device or a Monitor does not respond to polling. Example: You can monitor a device's Web server using HTTP. If it goes down, WhatsUp Professional can start a backup Web server (as an NT service).
- **Program:** You can define Program Actions to launch an external application when a device goes down or comes back up. Example: You may have a "Trouble Ticket System" that you want WhatsUp Professional to interface with. This system logs trouble tickets for a network technician. When a device goes down, this notification executes a program that will log a trouble ticket.
- **Syslog:** When a device does not respond to polling, you can send a Syslog message to a host that is running a Syslog server.
- **Text to Speech:** You can send a speech notification when a device does not respond to polling. This notification will audibly alert you via a speaker using a computer-generated voice.
- **Sound:** You can create custom sound actions by dropping .wave files into the Program Files\Ipswitch\WhatsUp Professional 2005\Data\Sounds directory.

## Percent Variables

When an Action is triggered, a message (or command) is sent either to a person or to another program. Use the message variables (percent variables) to specify what information should be in the message. For example, the default e-mail message reports the following information:

In the Subject line:

*%Device.Type is %Device.State (%Device.HostName).*

In the Message Body:

*%Device.ActiveMonitorDownNames is %Device.State on %Device.Type:  
%Device.HostName (%Device.Address).*

*Details:*

*Monitors that are down include: %Device.ActiveMonitorDownNames*

*Monitors that are Up include: %Device.ActiveMonitorUpNames*

*Notes on this device (from device property page):*

*%Device.Notes*

-----

*This mail was sent on %System.Date at %System.Time*

*Ipswitch WhatsUp Professional 2006*

You can customize a message by adding any of the variables in the following table.

<b>% Variable</b>	<b>Description</b>
<code>%ActiveMonitor.Argument</code>	SNMP instance number.
<code>%ActiveMonitor.Comment</code>	The human readable name that coincides with the network switch.
<code>%ActiveMonitor.Name</code>	The name of the Active Monitor that fired an Action. This is only used when an Action is associated directly with an Active Monitor, and not the device as a whole.
<code>%ActiveMonitor.NetworkInterfaceAddress</code>	IP Address for the network interface.
<code>%ActiveMonitor.Payload</code>	The payload returned by an Active Monitor. This is only used when an Action is associated directly with an Active Monitor and not the device as a whole.
<code>%ActiveMonitor.State</code>	The current status of the monitor, such as "Down at least 5 min." This variable only works on an Action or Action Policy that has been assigned directly to the Active Monitor (as opposed to the device in general.)

% Variable	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.Attribute	<p>Info Line 1 Device properties.</p> <p>Append the category to the end of the variable.</p> <p>Example: <i>%Device.Attribute.Contact</i></p> <p><b>Note:</b> To avoid an error return, when placing %Device.Attribute in quotation marks, place a space between the last letter and the closing quotation mark.</p> <p>Default categories:</p> <ul style="list-style-type: none"> <li>• * - Returns all attributes</li> <li>• Info1 - Upgrade path from v8</li> <li>• Info2 - Upgrade path from v8</li> <li>• Contact - Contact info from SNMP.</li> <li>• Location - Location info from SNMP</li> <li>• Description - Description info from SNMP</li> </ul>
%Device.Address	The IP address from Device properties.
%Device.Type	Device Type (from General of Device properties)
%Device.HostName	Host Name (from General of Device properties)
%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	<p>The type of Passive Monitor (Syslog, Windows Event, or SNMP Trap)</p> <p>See the definition in Help</p>
%Device.Notes	Notes. (Notes are from the Device properties Notes).
%Device.DatabaseID	Returns the database ID of a device.

% Variable	Description
%Device.DisplayName	Display Name (from <b>Device Properties &gt; General</b> )
%Device.SNMPOid	SNMP Object identifier. This is the word "unknown" if SNMP Object box is blank.
%Device.Status	The state's description (such as "Down at least 2 min" or "Up at least 5 min")
%Device.SNMPReadCommunity	SNMP Community
%Device.State	The state's description (such as "Down at least 2 min" or "Up at least 5 min")
%Device.SNMPWriteCommunity	SNMP Write Community (from SNMP section of Device Properties)
%Device.ActiveMonitorUpNames	Full service names of all Up monitored services on a device
%Device.ActiveMonitorDownNames	List of Down services using the abbreviated name if available
%System.NumberofDownDevices	Number of Down devices
%System.DisplayNamesDownDevices	Display names of devices with Down Monitors
%System.NumberofUpDevices	Number of Up devices
%System.DisplayNamesUpDevices	Display names of Up devices
%System.Date	The current system date. The format follows regional settings.
%System.Time	The current system time. The format follows regional settings.
%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', ...'  Ex. ARNOR: FTP, HTTP, Ping
%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', ...'  Ex. ARNOR: FTP, HTTP, Ping
%System.NumberofDownMonitors	Shows the number of down monitors on your network.
%System.NumberofUpMonitors	Shows the number of up monitors on your network.

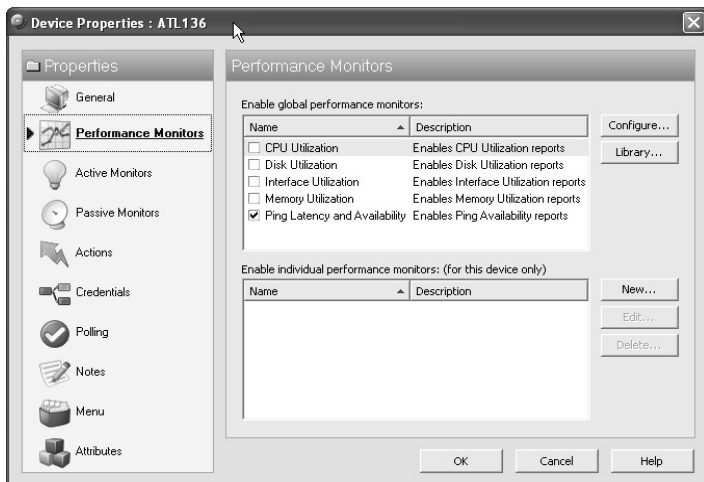
# Reports

In WhatsUp Professional, reports are used to troubleshoot and monitor performance and historical data that has been collected during the operation of the application. Reports can be viewed in the console or the Web Interface, and they can be e-mailed on a regular basis to an e-mail address you specify through the Recurring Report feature.

## Collecting Performance Data

By default, performance data is not kept for the Monitors assigned to the devices in your database.

To begin collecting performance data for a device, in Device view, right-mouse click on a device. In the right-mouse menu select **Properties**. In the Device Properties dialog, select **Performance Monitors**.



Use this dialog to configure Performance Monitors for the current device. The list is populated by entries in the Performance Monitor Library. If you would like to add a new entry into the library for

# Chapter 12

## In this Chapter

Collecting Performance Data

Report List

Recurring Reports

Creating Custom Reports

use on all of your devices, click **Library**. If you want to add a customized WMI or SNMP Performance Monitor to be used only on this device, use the **Enable individual performance monitors** section of the dialog.

Select data you want to collect by clicking the selection box next to the Performance Monitor you want to gather data on.

If you select a specific Performance Monitor without configuring the monitor manually, the default collection type is automatically selected. The collection type refers to which item on the current device is being monitored (this does not pertain to the custom WMI and SNMP monitors that may appear.)

For information on configuring Performance Monitors, see “Performance Monitors” on page 83.

## Report List

The following is a list of all reports that are available in WhatsUp Professional.

System Reports	
Action Log	A record of all Actions that WhatsUp attempts to fire.
Active Discovery Log	A record of all Active Discovery task results.
Active Discovery Results	Process items (devices, monitors) found during Active Discovery.
Activity Log	A history of system-wide configuration and application initialization messages generated by WhatsUp Professional for the time period displayed at the bottom of the report.
Diagnostic	Performs system and application checks.
General Error Log	A record of error messages generated by WhatsUp.
Passive Monitor Error Log	A record of Passive Monitor errors reported by WhatsUp.
Performance Monitor Error Log	A record of Performance Monitor errors reported by WhatsUp.
Recurring Action Log	Results of Recurring Action executions.
Recurring Report Log	Results of Recurring Report executions.
SNMP Trap Log	A history of SNMP traps that have occurred during the time period displayed at the bottom of the report. 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	When a device state changes, regardless of any action that has been placed on the device, WhatsUp Professional 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	Syslog events logged during the time period displayed at the bottom of the report. If the Syslog Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Syslog Entries log.
Top 10	A collection of Top 10 reports; for example, top devices by ping packet loss, top interfaces by traffic volume.
Web User Activity Log	Shows the history of user activity on the system.
Windows Event Log	Shows Windows events logged for all devices during the time period displayed at the bottom of the report. If the Windows Event Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Windows Event Log.
<b>Group Reports</b>	
Actions Applied	Shows how Actions are applied to devices and monitors in a group.
Active Monitor Availability	Compare the amount of time the Active Monitors on your devices have been available.
Active Monitor Outage	Compare the amount of time the Active Monitors on your devices have been down.
CPU Utilization	CPU utilization statistics for devices by group.
Disk Utilization	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 Bandwidth Utilization	Interface traffic and utilization for devices by group.
Memory Utilization	Memory utilization statistics for devices by group.
Ping Response Time	Ping response times for devices by group.
State Change Timeline	A timeline of when each Monitor on a device in the selected group changed from one state to another during the displayed time period.

State Summary	A summary of device states organized by device group.
Actions Applied	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.
<b>Device Reports</b>	
Active Monitor Availability	Find out when the Active Monitors on your device have been accessible.
CPU Utilization	CPU utilization statistics for a device.
Custom Performance Monitors	View information on your devices collected by Performance Monitors.
Device Status	A detailed look at a specific device.
Disk Utilization	Disk space and utilization statistics for a device.
Health	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 Bandwidth Utilization	Interface traffic and utilization statistics.
Memory Utilization	Memory utilization statistics for a device.
Ping Availability	Availability statistics for a device.
Ping Response Time	Ping response times for an individual device.
SNMP Trap Log	A history of SNMP traps that have occurred for the selected device during the time period displayed at the bottom of the report. 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	This report shows a timeline of when each Monitor on the selected device changed from one state to another during the displayed time period.
Syslog Entries	This report shows syslog events logged for the selected device during the displayed 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	This report shows Windows events logged for the selected device during the time period displayed at the bottom of the report. If the Windows Event Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Windows Event Log.
-------------------	--

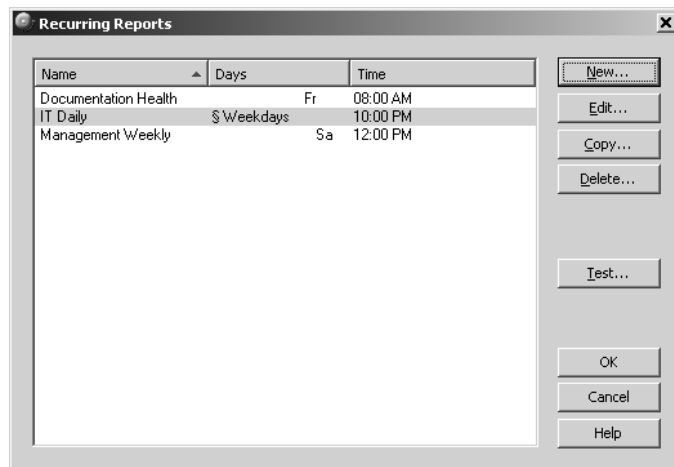
## Saving a Report

Using Windows Internet Explorer, you can save a report for later viewing.

To do this, open the report through the Web interface, then select **File > Save As** in Windows Internet Explorer. Save the file as an .mht (Web Archive, single file) file.

## Recurring Reports

Through this feature, you can configure WhatsUp Professional to send reports to e-mail addresses at regularly scheduled intervals. Each entry represents a different e-mail address or report that is to be sent.



- Click **New** to create a new recurring report.
- Select an entry and click **Edit** to make changes that entry.
- Select an entry and click **Copy** to create a copy of that entry. You can then edit the new copy as needed.
- Click **Delete** to remove a recurring report.
- Select an entry and click **Test** to test the recurring report.

## Creating Custom Reports

In WhatsUp Professional, you have the ability to create customized reports to display informational and historical data about the network and the devices you are monitoring through the application. To create these reports, you should be experienced with ASP, JScript, and SQL and have the means to identify the database entries you want to write into the parameters of the report.

Follow these steps to create a custom report and have that report appear in the lists and menus in the application, based on the report type you assign:

- 1 Add the report to the Report database table.
- 2 Open the Custom Report Template.
- 3 Add custom report content to the template.
- 4 Save the new report file in the WhatsUp Professional Reports directory.

### Step 1 - Add the report to the Report database table.

Once the report entry is in the database, the report name appears in the report pull-down menu in the Report view of the console, and in the report lists throughout the application. Without this entry, you will not be able to test the report as you create it.

nReportID	Identity column. This is assigned by the database.
sName	Enter a name for the report.
sDescription	Enter a description of the report.
sFilename	The file name of the report, relative to the Reports directory.
nReportType	An integer value. Valid report types: 1 = Device Reports 2 = Group Reports 3 = System Reports
sCategories	The names of the report categories, separated with a comma. A link to the report will be added in the category groups specified.

### Step 2 - Open the Custom Report Template.

Download the Custom\_Report\_Template.asp file from the Solutions Guide at [http://www.ipswitch.com/support/whatsup\\_professional/guides/index.asp](http://www.ipswitch.com/support/whatsup_professional/guides/index.asp) and open it, or copy the text below and paste it into an HTML or text editor.

### *Simple Custom Report Template*

```
<%@ language="jscript" %>
<!--#include file="../StandardIncludes/
    ApplicationContext.inc" -->
<!--#include file="../utility/Sql.inc"-->
<!--#include file="../StandardIncludes/Header.inc"-->
<%= app.GetReportHeader(
    "CustomReport.asp",
    "Custom Report Title",
    "icnChartPie32.gif")
%>
```

### *Report Content*

```
<%= rc.getReportFooter() %>
<!--#include file="../StandardIncludes/Footer.inc"-->
```

## Include File Descriptions

The following describes the include files that appear in the Custom Report Template. To make sure the report looks and functions like the default reports, these includes, and the commands calling them must remain unchanged.

The code for the includes assume the default install directory structure. All of the calls use the following as the root directory:

```
<<Install directory>>\HTML\1033\NmConsole\
```

### **ApplicationContext.inc**

This include defines the functions that appear below:

**rc.getReportHeaderFromDBCUSTOM(sTitle, sIconName)**

Returns an HTML string that opens the report table.

sTitle = The title of the report.

sIconName = The report icon relative to the Reports/Images directory.

**rc.getReportFooter()**

Returns an html string that closes the reports table.

**app.GetDeviceID()**

Returns the device ID currently in context.

**app.GetDeviceGroupID()**

Returns the device group ID currently in context.

**app.SetScreenTitle(sTitle, sTab, bAutoRefresh)**

Sets the title of the current page.

```
sTitle = The title of the page.  
sTab = The selected tab. For reports this is best set to  
null.  
bAutoRefresh = Set to true if you wish the report to  
refresh.
```

**Note:** The bAutoRefresh parameter will only work if it precedes `<!--#include file="../StandardIncludes/Header.inc"-->`

### Sql.inc

#### **var oRs = ExecSQL(sCommandText)**

Executes a specified query, SQL statement, stored procedure, or provider-specific text.

The results are stored in the Recordset object (oRs) if it is a row-returning query. A closed Recordset object will be returned if it is not a row-returning query.

**Note:** The returned Recordset is always a read-only, forward-only Recordset.

### Header.inc & Footer.inc

The header include provide standard `<html>` and `<body>` tags. The footer include closes these tags.

## Step 3 - Add custom report content to the template.

The report is a product of the device or group context and the SQL commands necessary to retrieve data from the database. The context makes sure that the device or group you are trying to run the report against is the correct one. System reports do not require the context.

Insert the following ASP code as needed.

## Group Reports

The following shows how to obtain a group name for the report header.

```
<%
var nDeviceGroupID, oGroupInfoRS, sGroupName
nDeviceGroupID = app.GetDeviceGroupID();
oGroupInfoRS = ExecSQL(
    "SELECT DeviceGroup.sGroupName FROM DeviceGroup "
    + " WHERE DeviceGroup.nDeviceGroupID = "
    + nDeviceGroupID
    );
if(oGroupInfoRS.EOF)
    ValidateDeviceGroup(
        true,
        app.REPORT_TYPE_GROUP
    );
sGroupName = oGroupInfoRS.Fields("sGroupName")+" ";
oGroupInfoRS.Close();
app.SetScreenTitle(
    "Custom Report for Group " + sGroupName,
    null, true);
%>
```

The **ValidateDeviceGroup()** function is included with :

```
<!--#include file="../utility/StandardFunctions.inc"-->
    This function ensures that the device group in context is a valid device group. If it is not,
    then the method will display an error message and intelligently redirect the user.
```

The html code to display the group in context:

```
<table cellpadding="0" cellspacing="0" border="0"
class="contentTbl">
    <tr>
        <td class="content-headerCell">
            Current Group :
            <%= sGroupName %>
            <%= GetGroupSelectorLink() %>
        </td>
    </tr>
</table>
```

The **GetGroupSelectorLink()** function is included with :

```
<!--#include file="../utility/ReportsStandardFunctions.inc"-->
    This function displays a link to be able to select a different group.
```

## Device Reports

```

<%
var nDeviceID, oDeviceInfoRS, nDeviceTypeID, sDeviceName,
nWorstStateID;
nDeviceID = app.GetDeviceID();
oDeviceInfoRS = ExecSQL(
    "SELECT sDisplayName, nDeviceTypeID, nWorstStateID
    FROM Device "
    + "WHERE nDeviceID = " + nDeviceID + " AND
    ISNULL(bRemoved, 0) = 0"
);
if(oDeviceInfoRS.EOF) ValidateDevice(true,
app.REPORT_TYPE_DEVICE);
nDeviceTypeID =
    parseInt(oDeviceInfoRS.Fields("nDeviceTypeID"));
sDeviceName = oDeviceInfoRS("sDisplayName") + "";
nWorstStateID = parseInt(oDeviceInfoRS("nWorstStateID"));
oDeviceInfoRS.Close();
app.SetScreenTitle("Custom Report for Device "
    + sDeviceName, null, true);

%>

```

The **ValidateDevice()** function is included with :

```

<!--#include file="../utility/StandardFunctions.inc"-->

```

This function ensures that the device in context is a valid device. If it is not, then the method will display an error message and intelligently redirect the user.

The **GetReportsMonitorDeviceStateIconLarge()** and **GetDeviceSelectorLink()** functions are included with :

```

<!--#include file="../utility/ReportsStandardFunctions.inc"-->

```

**GetReportsMonitorDeviceStateIconLarge()** gets the image src for the device icon. This is used below in the section Getting the State Icon. **GetDeviceSelectorLink()** displays a link to be able to select a different device.

The html code to display the device in context:

```

<table cellpadding="0" cellspacing="0" border="0">
<tr>
    <td class="content-headerCell">
        <%= sDeviceName %>
        <%= GetDeviceSelectorLink() %>
    </td>
</tr>
</table>

```

```
</table>
```

The **GetDeviceSelectorLink()** function is included with :

```
<!--#include file="../utility/ReportsStandardFunctions.inc"-->
```

This function displays a link to be able to select a different device.

## Getting the State Icon

If you need to display the state icon in the report, add this code to the report content.

```
<%  
var sDeviceImageSrc =  
GetReportsMonitorDeviceStateIconLarge(  
    nWorstStateID,  
    nDeviceTypeID,  
    "FFF8DC"  
);  
%>
```

Insert the following HTML where you want the device icon to appear on the report:

```

```

## SQL Commands

SQL commands are used to retrieve data from the database and display it in the report. Write these commands and place them in the report after the context is declared.

## Step 4 - Save the new report file.

Once the report is complete, save it as an .asp file using the filename added to the database in step 1. The default path to the report directory is:

```
<<Install directory>>\HTML\1033\NmConsole\Reports
```

## Sample Report

The following is a sample report that you can use to familiarize yourself with the commands and functions of the reporting system. The report itself displays general device properties of the device that is put in context by the application. Please note that though attempts were made to keep the sample code in a format that would allow for easy copy and pasting, some code lines are simply too long to hold true to their correct format on the printed page. Copying and pasting this code as is from the sample report will return errors.

```

<!--
Sample Device Details Report
Enter this into the WhatsUp database Report table:
  sName : Sample Device Report
  sDescription : Device details sample report
  sFilename : _sampleDeviceReport.asp
  nReportType : 1
//-->
<!--
This section is from the template
//-->
<%@ language="jscript" %>
<!--#include file="../StandardIncludes/
      ApplicationContext.inc" -->
<!--#include file="../utility/Sql.inc"-->
<!--#include file="SelectReport.inc"-->
<!--#include file="../utility/StandardFunctions.inc"-->
<!--#include file="../utility/ReportsStandardFunctions.inc"--
>
<%
// This section places the device in context.
var nDeviceID, oDeviceInfoRS, nDeviceTypeID, sDeviceName,
nWorstStateID;
nDeviceID = app.GetDeviceID();
oDeviceInfoRS = ExecSQL(
  "SELECT sDisplayName, nDeviceTypeID, nWorstStateID "
  + "FROM Device "
  + "WHERE nDeviceID = " + nDeviceID
  + " AND ISNULL(bRemoved, 0) = 0"
);
if(oDeviceInfoRS.EOF)
  ValidateDevice(true, app.REPORT_TYPE_DEVICE);
nDeviceTypeID =
  parseInt(oDeviceInfoRS.Fields("nDeviceTypeID"));
sDeviceName = oDeviceInfoRS("sDisplayName") + "";
nWorstStateID = parseInt(oDeviceInfoRS("nWorstStateID"));
oDeviceInfoRS.Close();
app.SetScreenTitle(
  "Details for Device " + sDeviceName, null, true
);

//This section gets the state change icon.
var sDeviceImageSrc = GetReportsMonitorDeviceStateIconLarge(
  nWorstStateID,
  nDeviceTypeID,
  "FFF8DC"
);

```

```

//This section contains the SQL commands written for the
report.
var sSQL = "Select "
  + "Device.sDisplayName, "
  + "DeviceType.sDisplayName AS sTypeName, "
  + "sNetworkName, "
  + "sNetworkAddress, "
  + " sNote "
  + "FROM Device "
  + "INNER JOIN NetworkInterface ON "
  + "NetworkInterface.nNetworkInterfaceID = "
  + "Device.nDefaultNetworkInterfaceID "
  + "INNER JOIN DeviceType ON "
  + "DeviceType.nDeviceTypeID = Device.nDeviceTypeID "
  + "WHERE Device.nDeviceID = " + app.GetDeviceID();
var oDeviceRs = ExecSQL(sSQL);
%>
<!--#include file="../../StandardIncludes/Header.inc"-->
<!-- More from the template //-->
<%= rc.getReportHeader(
  "_sampleDeviceReport.asp",
  "Device Details Report",
  "icnChartPie32.gif")
%>
<!-- This section controls the formatting of the data as it
appears on the report page itself, after it has been
generated.
/-->
<table cellpadding="0" cellspacing="0" border="0"
class="contentTbl">
  <tr>
    <td class="deviceReportCell">
      <table cellpadding="0" cellspacing="0" border="0">
        <tr>
          <td></td>
          <td class="content-headerCell">
            <%= sDeviceName %>
            <%= GetDeviceSelectorLink() %>
          </td>
        </tr>
      </table>
    </td>
  </tr>
  <tr>
    <td class="deviceReportCell">

```

```

<table cellpadding="0" cellspacing="0" border="0">
  <tr>
    <td valign="top" align="right">Device Name:
    </td>
    <td><%= oDeviceRs("sDisplayName") %></td>
  </tr>
  <tr>
    <td valign="top" align="right">Device type:
    </td>
    <td><%= oDeviceRs("sTypeName") %></td>
  </tr>
  <tr>
    <td valign="top" align="right">Network name:
    </td>
    <td><%= oDeviceRs("sNetworkName") %></td>
  </tr>
  <tr>
    <td valign="top" align="right">Network
    address:</td>
    <td><%= oDeviceRs("sNetworkAddress") %></td>
  </tr>
  <tr>
    <td valign="top" align="right">Note:</td>
    <td>
      <% var sNote = oDeviceRs("sNote")+""; %>
      <%= sNote.replace(/(\r\n|\r|\n)/g, '<BR>') %>
    </td>
  </tr>
</table>
</td>
</tr>
</table>
<!-- The rest is from the template //-->
<%= rc.getReportFooter() %>
<%
oDeviceRs.close();
%>
<!--#include file="../../StandardIncludes/Footer.inc"-->

```

# Premium Edition

The Premium Edition is available for separate purchase. It provides all of the network monitoring capabilities of WhatsUp Professional 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 on our web site at:

<http://www.ipswitch.com/products/network-management.asp>

## Exchange Monitor

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.

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 Professional 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

# Chapter 13

## In this Chapter

---

Exchange Monitor

SQL Server Monitor

WMI Monitor

---

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 to monitor.
- 2 Determine which Exchange services to monitor.
- 3 Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination.

To start, it may be simpler to create one monitor for each parameter or service that you want to monitor. 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 that the monitor will be reported Down if any of the parameters or services that you selected to monitor in Step 3 are down.

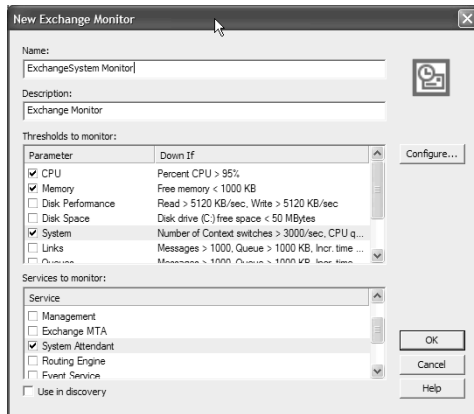
## Examples

If you have created other Active Monitors in WhatsUp Professional, 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 "ExchangeSystem" 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 Select **Configure > Active Monitor Library**, then click **New**. The Select Active Monitor Type dialog appears.
- 2 Select Exchange Monitor and click **OK**. The New Exchange Monitor dialog appears.



- a 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.
  - b Select the CPU parameter, then click **Configure**. The CPU Threshold dialog appears. Enter an appropriate threshold and click **OK**.
  - c Select the Memory parameter, then click **Configure**. The Memory Threshold dialog appears. Enter an appropriate threshold for the amount of free memory and click **OK**.
  - d Select the System parameter, then click **Configure**. The System Threshold dialog appears. Enter an appropriate threshold and click **OK**.
  - e Click **OK** to add the ExchangeSystem monitor to the Active Monitor library.
- 3 Add the ExchangeSystem monitor to your Exchange server device.
    - a In your device list, find the device that represents the Exchange server. Double-click the device to display its properties, then select Active Monitors.
    - b Click **Add**. The Active Monitor wizard appears.
    - c Select the ExchangeSystem monitor, and continue with the wizard to configure any actions for the monitor.

For more information on setting up an action, see “Actions” on page 109.

Once 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

## SQL Server Monitor

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.

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?

The SQL Server Monitor extends monitoring to parameters reported by Microsoft SQL Server (and Microsoft MSDE), allowing you to get an early warning of a degradation in performance. For example, you can monitor system parameters on your SQL Server database server to see if performance is within an expected range, and if not, you can intervene before the SQL Server fails. In other words, you can detect a looming problem before it causes an application or service failure.

### How to get started using SQL Server Monitor

Here is a basic approach to using the SQL Server Monitor:

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.

- 1 Determine which SQL parameters to monitor.

- 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 logs and notifications. 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 a 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 that the monitor will be reported Down if any of the parameters or services that you selected to monitor in Step 4 are down.

## Example

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 Select **Configure > Active Monitor Library**, then click **New**. The Select Active Monitor Type dialog appears.
- 2 Select SQL Server Monitor and click **OK**. The New SQL Server Monitor dialog appears.

Parameters	Down If
<input type="checkbox"/> Cache	Hit ratio < 0%, Use count < 0/sec
<input type="checkbox"/> Locks	Avg wait time > 500 ms, Waits/sec > 100
<input type="checkbox"/> Transactions	Active transactions > 100, Transactions/sec > 5
<input checked="" type="checkbox"/> Users	No. of logins > 100/sec, No. of connections > 5
<input type="checkbox"/> Alerts	Severity 17 to 25, Threshold > 100
<input type="checkbox"/> Custom Thresholds	0 Custom Threshold(s)

- a** 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.
    - b** Click the **Users** parameter to select it, then click **Configure**. The Users Threshold dialog appears. 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.
    - c** 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. Double-click the device to display its properties, then select Active Monitors.
    - b** Click **Add**. The Active Monitor wizard appears.
    - c** 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 “Actions” on page 109.

Once 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

## WMI Monitor

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.

WMI Monitor is part of the WhatsUp Professional Premium Edition, which extends WhatsUp Professional 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?

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.

The Exchange Monitor and the SQL Server Monitor, which were created by Ipswitch, are examples of custom WMI monitors. You can use the WMI Monitor feature to create a monitor for most Windows applications.

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.

## About WMI

Windows Management Instrumentation (WMI) is a Microsoft Window's standard for retrieving information from computer systems running Windows.

WMI comes installed by default on Windows 2000, 2003, and XP systems.

## WMI Support Links

For more information about WMI, click the following links to the Microsoft Support Center.

### **General description of WMI**

([http://msdn.microsoft.com/library/en-us/wmisdsk/wmi/about\\_wmi.asp?frame=true](http://msdn.microsoft.com/library/en-us/wmisdsk/wmi/about_wmi.asp?frame=true))

### **How to Set Security in Windows XP Pro When Installed in a Workgroup**

(<http://support.microsoft.com/default.aspx?scid=KB;EN-US;q290403>)

### **WMI Scripts Generate "Permission Denied" Error Message**

(<http://support.microsoft.com/default.aspx?scid=KB;EN-US;q282949>)

## Troubleshooting WMI

Sometimes remote connectivity cannot be established with WMI without testing.

Microsoft provides some tools for troubleshooting WMI. A simple tool to use is called Wbemtest.

This tool is found in the folder: %SYSTEM%\system32\wbemfolder

To use WbemTest:

- 1 Run **wbemtest**.
- 2 Click **Connect**.
- 3 Set the **Namespace** to \\MACHINE\root\cimv2 (where MACHINE is the local or remote target machine)
- 4 Set the **Credentials** to a username and password that have administrative access on the target machine. (Leave Authority blank.)
- 5 Set **Impersonation Level** to Impersonate.
- 6 Set **Authentication Level** to Packet.
- 7 Click **Connect**.

If successful, there will be no errors, and the namespace will be listed as \\MACHINE\root\cimv2.

If unsuccessful, errors will be displayed. These errors can be fixed by applying the information in this page, or by consulting the Microsoft Knowledge Base at <http://support.microsoft.com>.

- 8 To close **WbemTest**, click **Exit**.

The information in this Troubleshooting topic comes courtesy of [Somix Technologies, Inc.](#), makers of OSTivity, a web-based Asset Management and Inventory System.

# INDEX

- A**
  - Actions 109
    - Action Library 109
    - Action Policies 119
    - Action Strategies 111
    - Action Types 110
    - Assigning an Action to a Device 116
    - Assigning an Action to a Monitor 118
    - Blackout Periods 119
    - Configuring 112
    - Other Types of Actions 121
    - Percent Variables 122
    - Testing 114
    - Using Actions 112
  - Activating WhatsUp 9
  - Active Discovery 37
    - IP Range Scan 37
    - SNMP SmartScan 37
  - Active Monitors 99
    - Active Monitor Library 100
    - Assigning 101
      - Add/Edit 102
    - Deleting 102
    - Supported Active Monitors 101
  - Alternative Database Setups 13
- B**
  - Bulk Field Chang 56
- C**
  - Console 61
    - Overview 61
- D**
  - Database Utilities 12
    - Database Backup and Restore 12
    - Database Performance Tool 12
    - Database Table Maintenance 13
  - Device Discovery 29
    - Adding a Single Device 34
    - Scan Types 29
    - Wizard 29
  - Device Groups 55
    - Dynamic Groups 56
    - Organization 55
      - Device State 55
      - Discovery 55
      - Map View 55
      - Renaming a Device Group 56
  - Device Types 54
  - Device View 62
    - Device Icons 63
    - Organizing Devices and Device Groups 64
  - Devices 41
    - Acknowledgements 58
      - Acknowledging a State Change 59
    - Device Properties
      - Actions 46
      - Active Monitors 44
      - Attributes 53
      - Credentials 46, 47
      - General 42
      - Menu 52
      - Notes 51
      - Passive Monitors 45
      - Performance Monitors 43
      - Polling 48
      - Device Services 41
      - Troubleshooting 41
- I**
  - Installation
    - Custom Database 6
    - First-time Install 5
    - Installation Notes 7
    - Upgrading 5
  - Installing or Upgrading 7
  - IP Range Scan 37
- K**
  - Knowledge Base 4
- M**
  - Map View 64
    - Adding Annotations to a Map 66
    - Attached Lines 68
    - Device Layout 65
    - Link Lines 66
  - Microsoft IIS 22
  - Microsoft SQL Server 1
  - Migrating
    - Data 26
    - Migration Utility 27
  - Migrating from WhatsUp Gold 10, 25
  - Migration
    - Terminology Changes 26
  - MSDE Database 11

- O**
- Online Help
    - Console 3
    - for the console 3
  - Online help
    - for the web interface 3
- P**
- Passive Monitors 105
    - Configuring 107
      - Add/Edit a Passive Monitor Manually 107
      - Assign a Passive Monitor to a Device 107
    - Configuring Passive Monitor Listeners 105
    - Passive Monitor Library 106
    - SNMP Passive Monitor (SNMP Trap) 105
    - Syslog Passive Monitor 105
    - Using TrapImport.exe 108
    - Windows Event Log Monitor 105
  - Performance Monitors 83
    - Configuring 85
      - multiple devices 86
      - single device 85
    - Enabling SNMP on Windows Devices 96
      - To enable SNMP Monitoring 96
      - To install SNMP Monitoring 96
    - Performance Monitor
      - Library 83
      - Performance Reporting 86
        - Device Status Report 87
        - Group and Device Performance Reports 88
        - Top 10 Report 88
  - Premium Edition 1, 139
    - Exchange Monitor 139
    - SQL Server Monitor 142
    - WMI Monitor 144
- R**
- Report View 69
  - Reports 125
    - Collecting Statistical Data 125
    - Creating Custom Reports 130
    - Recurring Reports 129
    - Report List 126
    - Saving a Report 129
- S**
- SNMP SmartScan 37
  - System Requirements 6
    - Requirements for MSDE 2000 7
    - Requirements for WhatsUp Professional 6
- U**
- Uninstalling 10
- W**
- Web Alarm 120
  - Web alarm 74
  - Web Interface 71
    - Configuring to use IIS 81
    - Connecting 71
    - Access Problems 71
    - Default Logon 72
  - Device Group Access
    - Rights 76
      - Assigning Access Rights by Group 77
      - Assigning Access Rights by User 76
  - Managing the Web Server 80
  - Managing Users 74
    - User Rights 76
  - Overview 72
  - Securing the Web Interface 81