



User Guide

IPSWITCH

Overview

| | |
|---|----|
| WhatsUp Gold Overview | 17 |
| Welcome to Ipswitch WhatsUp Gold | 17 |
| WhatsUp Gold editions | 19 |
| New in Ipswitch WhatsUp Gold..... | 23 |
| Sending feedback | 23 |
| Finding more information and updates..... | 24 |
| Getting Familiar with WhatsUp Gold | 25 |

Devices

| | |
|--|-----|
| Discovery Console | 47 |
| Learning about the Discovery Console | 47 |
| Discovering network devices | 48 |
| Using Device Roles..... | 62 |
| Managing device roles | 70 |
| Using Devices | 73 |
| Viewing devices in WhatsUp Gold | 73 |
| About device icons | 75 |
| Using Credentials | 75 |
| Searching for devices..... | 76 |
| Understanding group access and user rights for Find Device | 77 |
| Searching for devices with interface traffic | 77 |
| Using Device Groups | 79 |
| Using device groups..... | 79 |
| Creating device groups | 80 |
| Configuring Dynamic Groups..... | 81 |
| Dynamic Group examples | 83 |
| Using the Dynamic Group builder | 91 |
| Using Maps..... | 93 |
| Using the Map View..... | 93 |
| About Map View device limitations..... | 95 |
| Managing devices | 97 |
| Learning about devices..... | 97 |
| Using Device Properties | 118 |
| Working with Device Properties | 119 |
| Using Device Properties - Summary | 120 |
| Using Device Properties - General..... | 121 |

| | |
|--|-----|
| Device Properties - Performance Monitors..... | 121 |
| Using Device Properties - Active Monitors..... | 123 |
| Using Device Properties - Passive Monitors..... | 123 |
| Using Device Properties - Actions..... | 123 |
| Using Device Properties - Credentials | 124 |
| Using Device Properties - Polling | 125 |
| Using Device Properties - Virtualization..... | 126 |
| Using Device Properties - Notes | 127 |
| Using Device Properties - Custom Links | 127 |
| Using Device Properties - Attributes..... | 128 |
| Using the DeviceIdentifier attribute..... | 128 |
| Using Device Property - Menus..... | 129 |
| Using WhatsConfigured Device Properties - Tasks | 130 |
| Using Network Tools | 131 |
| Using the Ping tool | 132 |
| Using the Traceroute tool | 133 |
| Using the Lookup tool | 133 |
| Using the Telnet tool..... | 134 |
| Using the SNMP MIB Walker..... | 135 |
| Using the SNMP MIB Explorer..... | 138 |
| Using the MAC Address Tool..... | 139 |
| Using the Web Performance Monitor | 141 |
| Using the Web Task Manager | 144 |
| Monitoring Devices | 154 |
| Scenario: | 269 |
| Using Actions..... | 271 |
| Required for SMS Direct Actions..... | 282 |
| Select a Device | 307 |
| Dynamic Groups - Delete Devices..... | 307 |
| Configure Data Collection Advanced Settings..... | 307 |
| Using Network Tools to view real-time data | 308 |
| Network Interfaces..... | 308 |
| Add/Edit Network Interface..... | 308 |
| Ping Advanced Settings..... | 309 |
| Passive Monitor: Select Event Type | 309 |
| Monitor Properties - Select Monitor Type | 309 |
| Monitor Properties - Set Polling Interval and Dependencies | 309 |

| | |
|---|-----|
| Passive Monitor: Actions..... | 310 |
| Monitor Properties - Setup Actions for Device State Changes | 310 |
| Active Monitor Advanced Properties..... | 310 |
| APC UPS Performance Monitor | 311 |
| Select Action and State | 311 |
| Select Credentials..... | 311 |
| Device Dependencies | 312 |
| About Dynamic Group Properties..... | 313 |
| Using the Dynamic Group Rule Editor..... | 315 |
| MIB Walker Advanced Parameters | 317 |
| Add/Edit WMI Performance Counter | 321 |
| Select WMI Performance Counter for WMI monitor | 321 |
| Selecting a Performance Counter | 322 |
| Add/Edit SNMP Performance Counter | 322 |
| APC UPS Active Monitor | 323 |
| Diagnostic Tool | 326 |
| Re-enabling the Telnet protocol handler | 326 |
| Selecting a Performance Monitor Type..... | 326 |
| Add Custom Link | 327 |
| Add a Device Attribute..... | 327 |
| Bulk Field Change - Action Policy..... | 327 |
| Bulk Field Change - Active Monitor | 327 |
| Bulk Field Change - Active Monitor Properties..... | 328 |
| Bulk Field Change - Attribute..... | 328 |
| Bulk Field Change - Credentials | 329 |
| Bulk Field Change - Device Type | 329 |
| Bulk Field Change - Down Dependency | 329 |
| Bulk Field Change - Maintenance Mode..... | 329 |
| Bulk Field Change - Notes | 330 |
| Bulk Field Change - Passive Monitor | 330 |
| Bulk Field Change - Passive Monitor Properties..... | 331 |
| Bulk Field Change - Performance Monitor..... | 331 |
| Bulk Field Change - Polling Interval..... | 331 |
| Bulk Field Change - Up Dependency | 332 |
| Hub Transport Server Role thresholds..... | 332 |
| Outlook Web Access Server Role thresholds..... | 333 |
| Mailbox Server Role thresholds..... | 334 |

| | |
|---|-----|
| Selecting or Creating an Action | 335 |
| Setting Advanced Properties for a HTTP Content Monitor | 335 |
| Setting Advanced Properties for an Email Active Monitor | 336 |
| Configure CPU Threshold..... | 337 |

Home

| | |
|---|-----|
| Understanding and using dashboards | 339 |
| Learning about dashboards | 339 |
| Overview of dashboard report categories | 340 |
| Adding dashboard reports to a dashboard view | 342 |
| Searching for dashboard reports..... | 345 |
| Working with dashboard views..... | 346 |
| Changing dashboard content | 348 |
| Using the dashboard report menu | 348 |
| Configuring a dashboard report..... | 349 |
| Moving dashboard reports within a dashboard view..... | 350 |
| Navigating dashboard views | 351 |
| Types of dashboards..... | 352 |
| About types of dashboards | 352 |
| Home Dashboard | 353 |
| Device Status dashboard..... | 354 |
| Top 10 Dashboard..... | 356 |
| Using Favorites | 358 |
| Using the Favorites toolbar | 358 |
| Adding Favorites | 358 |
| Editing Favorites | 360 |
| Dashboard reports | 362 |
| CPU Utilization reports..... | 363 |
| Custom Performance Monitor reports | 369 |
| Disk Utilization reports..... | 374 |
| Flow Monitor reports | 382 |
| General reports | 407 |
| Interface Errors and Discards reports..... | 423 |
| Interface Utilization reports..... | 431 |
| Inventory reports..... | 441 |
| Memory Utilization reports..... | 445 |
| Performance-Historic reports | 451 |

| | |
|--|-----|
| Performance-Last Poll reports | 469 |
| Ping Availability and Response Time reports..... | 481 |
| Problem Areas reports..... | 489 |
| Problem Areas Specific Device | 501 |
| Remote/Central reports | 507 |
| Split Second Graph reports..... | 536 |
| Threshold reports..... | 552 |
| Top 10 reports | 561 |
| Virtualization reports | 570 |
| Wireless reports | 577 |
| ELM reports..... | 585 |
| Dashboard Report - Remote Site | 587 |
| Creating and modifying user accounts | 587 |
| Using the Remote/Central dashboard reports | 589 |

Monitoring

| | |
|--|-----|
| Working with monitor reports | 592 |
| Viewing device reports..... | 592 |
| Viewing group reports | 594 |
| Changing the report date range..... | 597 |
| Using Business Hours settings in monitor reports | 598 |
| Viewing real-time data in monitor reports..... | 600 |
| About report refresh intervals | 601 |
| Changing the date range | 602 |
| Using the Zoom tool | 603 |
| Using paging options | 604 |
| Changing preferences | 604 |
| Using the WhatsUp Gold toolbar buttons..... | 606 |
| Configuring monitor report charts | 606 |
| Resizing and sorting report columns | 607 |
| Disabling Instant Info popups | 608 |
| Understanding the Graph Types | 610 |
| Using Favorites | 612 |
| Using the Favorites toolbar | 612 |
| Adding Favorites | 612 |
| Editing Favorites | 614 |

| | |
|---|-----|
| Using WhatsUp Gold monitor reports..... | 616 |
| List of reports and logs..... | 616 |
| Learning about monitor reports..... | 619 |
| Device Properties - Performance Monitors..... | 622 |
| Using the Performance Monitor Library | 624 |
| Scheduling reports | 625 |
| Exporting reports and logs | 626 |
| Emailing reports and logs | 627 |
| Printing reports and logs..... | 628 |
| Viewing scheduled reports..... | 628 |
| Performance monitor reports | 630 |
| Learning about performance monitors..... | 630 |
| CPU Utilization..... | 631 |
| Disk Utilization | 633 |
| Memory Utilization | 636 |
| Custom | 639 |
| Network monitor reports..... | 641 |
| Learning about network monitors..... | 641 |
| Interface Utilization | 642 |
| Interface Traffic | 644 |
| Ping Response Time | 647 |
| Ping Availability | 650 |
| Interface Discards..... | 654 |
| Interface Errors | 656 |
| Using Device monitor reports..... | 659 |
| Learning about Device monitors..... | 659 |
| Active Monitor Availability..... | 659 |
| Active Monitor Outages..... | 662 |
| Device Uptime..... | 663 |
| Device Health..... | 665 |
| State Change Acknowledgment..... | 666 |
| State Change Timeline | 667 |
| Top 10 Dashboard..... | 669 |
| Remote Site Log..... | 670 |
| Report body..... | 670 |
| Remote Site Status..... | 670 |
| Report Body..... | 671 |

| | |
|-------------------------------------|-----|
| Diagnostic Report | 671 |
| Maximum report records..... | 671 |
| Business Hours report settings..... | 672 |
| WhatsConnected Device Info | 672 |
| Device State Legend | 674 |

Logs

| | |
|---|-----|
| Working with logs..... | 676 |
| Learning about Logs | 676 |
| Selecting a device to view logs | 677 |
| Changing the report or log date range | 678 |
| Changing the date range | 678 |
| Using paging options | 679 |
| Navigating between logs | 680 |
| Printing reports and logs..... | 680 |
| Using the WhatsUp Gold toolbar buttons..... | 680 |
| Using Manage Web Server..... | 681 |
| Managing Action Policies..... | 682 |
| Viewing payload details..... | 683 |
| Changing preferences | 684 |
| Using WhatsUp Gold System Logs | 686 |
| Action Log..... | 687 |
| Error Logs | 688 |
| SNMP Trap Log..... | 692 |
| Syslog..... | 694 |
| Windows Event Log..... | 696 |
| Activity Log..... | 698 |
| Scheduled Report Log | 699 |
| Recurring Action Log | 700 |
| Web User Activity Log | 701 |
| WhatsVirtual Event Log..... | 702 |
| Using WhatsUp Gold Group / Device Logs..... | 704 |
| Actions Applied..... | 704 |
| Blackout Summary Log | 705 |
| Monitors Applied..... | 707 |
| Quarterly Availability Summary | 708 |
| State Summary | 710 |

Alert Center

| | |
|--|-----|
| Working with Alert Center reports | 713 |
| Using Alert Center reports | 713 |
| Filtering the Items Report | 713 |
| Using the Item History report | 714 |
| Updating Alert Center items | 715 |
| A note about notifications | 717 |
| Understanding resolving items - examples..... | 717 |
| Filtering the Log Report..... | 718 |
| Configuring Alert Center records to expire | 719 |
| Using the Alerts Home reports | 720 |
| Using the Performance CPU threshold report..... | 721 |
| Using the Performance Custom threshold report..... | 721 |
| Using the Performance Disk threshold report..... | 721 |
| Using the Performance Interface threshold report..... | 722 |
| Using the Interface Errors and Discards threshold report | 722 |
| Using the Performance Memory threshold report..... | 723 |
| Using the Performance Ping Availability threshold report | 723 |
| Using the Ping Response Time threshold report..... | 724 |
| Using the SNMP Trap threshold report | 724 |
| Using the Syslog threshold report | 725 |
| Using the Windows Event Log threshold report..... | 725 |
| Using the Flow Monitor Conversation Partners threshold report..... | 726 |
| Using the Flow Monitor Custom threshold report..... | 726 |
| Using the Flow Monitor Failed Connections threshold report..... | 727 |
| Flow Monitor Interface Traffic threshold report..... | 727 |
| Using the Flow Monitor Top Sender/Receiver threshold report..... | 728 |
| Using the Blackout Summary threshold report..... | 728 |
| Using the WhatsUp Health threshold report..... | 729 |
| Failover threshold report..... | 729 |
| Using the WhatsConfigured Threshold report | 729 |
| WhatsVirtual events threshold report..... | 730 |
| Configuring notifications..... | 731 |
| Using Alert Center and actions..... | 731 |
| Alert Center Percent Variables..... | 732 |
| Using Alert Center Notification Policy options..... | 733 |
| Configuring a notification policy..... | 734 |

| | |
|---|-----|
| Configuring an Alert Center email notification | 736 |
| Configuring an Alert Center SMS Direct notification | 738 |
| Configuring an Alert Center SMS Action notification | 741 |
| Configuring email notification message settings..... | 743 |
| Stopping a running notification policy | 744 |
| Using the Email Action | 745 |
| Using the SMS Direct Action | 745 |
| Using the SMS Action | 746 |
| Configuring thresholds..... | 747 |
| Configuring Alert Center thresholds..... | 748 |
| Selecting threshold devices | 749 |
| Configuring performance thresholds | 753 |
| Configuring passive thresholds | 770 |
| Configuring Flow Monitor thresholds | 777 |
| Configuring system thresholds..... | 790 |
| Notification Policy Graph View..... | 799 |
| Threshold Devices..... | 800 |
| Alert Center Item Details | 801 |
| Netflow database record types | 802 |
| Reducing the WhatsUp database size | 802 |
| Reducing the number of raw, hourly, or daily data records | 803 |
| Reducing the number of host records..... | 803 |
| Restarting the Flow Collector service..... | 803 |
| Reducing performance monitors | 804 |
| WhatsUp discovery service is down | 804 |
| WhatsUp web service SQL queries exceed threshold..... | 804 |
| WhatsUp web service is down..... | 806 |
| WhatsUp web service HTTP responses exceed threshold..... | 806 |
| WhatsUp polling service SQL queries exceed threshold | 808 |
| WhatsUp polling service is down | 809 |
| Troubleshooting the WhatsUp Health Threshold | 810 |
| Changing how long report data is stored | 811 |
| Reducing passive monitor records | 811 |
| Reducing expired records | 814 |
| Database Tools Table Maintenance..... | 814 |
| Program Options - Report Data..... | 815 |
| Configure CPU Utilization | 816 |

| | |
|--|-----|
| Configure Disk Utilization | 816 |
| Configure Memory Utilization | 817 |
| Configure Ping Latency and Availability..... | 817 |
| Configure Data Collection Advanced Settings..... | 817 |
| Creating global custom performance monitors | 818 |
| Creating device-specific custom performance monitors | 818 |
| Reducing ActiveMonitorStateChangeLog | 818 |
| Reducing StatisticalInterface | 819 |
| Bulk Field Change - Performance Monitor..... | 820 |
| Configure Interface Data Collection..... | 823 |
| Monitored devices exceeds license limit..... | 824 |
| Flow Threshold Hosts | 825 |
| Select Notification Type..... | 826 |
| Reducing performance monitor records | 826 |
| Reducing PassiveMonitorActivityLog | 827 |
| Configure VMware event listener | 829 |

Admin

| | |
|---|-----|
| Using WhatsUp Gold Admin features | 832 |
| Using Admin features | 832 |
| Home..... | 834 |
| Using Admin Console | 834 |
| Opening NM Console from the Web interface | 834 |
| Libraries | 835 |
| Using the Monitor Library | 835 |
| Using the Credentials Library..... | 836 |
| Scheduled..... | 842 |
| Adding and editing a Recurring Action | 842 |
| Using Admin Scheduled features..... | 843 |
| System Administration | 845 |
| Managing WhatsUp Gold server options | 845 |
| Using the SNMP MIB Manager..... | 845 |
| Setting LDAP credentials..... | 848 |
| Translation Groups | 851 |
| Managing users and groups..... | 852 |

| | |
|--|-----|
| Options..... | 865 |
| Configuring Email settings..... | 866 |
| Changing preferences | 867 |
| Managing dashboard views | 868 |
| Using the Program Options..... | 871 |
| Setting Advanced Options..... | 881 |
| Types of SNMP Trap Monitors..... | 882 |
| Common SNMP Traps..... | 882 |
| Select computer..... | 883 |
| FTP server user permissions | 883 |
| WMI | 884 |
| Event Viewer | 884 |
| Payload Definition..... | 884 |
| SMS Providers | 884 |
| Setting Modem Connection Preferences | 884 |
| Configure Memory Threshold..... | 885 |
| Configure Disk Performance - Exchange | 885 |
| Configure System Thresholds..... | 886 |
| Configure Links Thresholds | 886 |
| Configure Queues Thresholds | 887 |
| Adding Custom Thresholds | 887 |
| FTP server user permissions | 887 |
| Configure Disk Performance | 888 |
| Configure Disk space Threshold | 888 |
| Configure System Threshold | 888 |
| Configure Buffers Threshold | 888 |
| Configure Locks Threshold | 888 |
| Configure Cache Threshold | 889 |
| Configure Transactions Threshold | 889 |
| Configure Users Threshold | 889 |
| Configure Alerts Threshold..... | 889 |
| SQL Server Services..... | 890 |
| Selecting a Device | 891 |
| Selecting computers | 891 |
| Configuring CPU Threshold..... | 892 |
| Setting Advanced Properties for a HTTP Content Monitor | 892 |
| Setting Advanced Properties for an Email Active Monitor..... | 892 |

| | |
|--|-----|
| Selecting a blackout period | 894 |
| Importing a MIB file | 894 |
| Hub Transport Server Role Thresholds | 894 |
| Select Action Type | 896 |
| WinEvent Condition | 896 |

Using SNMP Features

| | |
|--|-----|
| SNMP overview..... | 898 |
| Enabling SNMP on Windows devices | 899 |
| Monitoring an SNMP Service | 899 |
| About the SNMP Agent or Manager | 900 |
| About the SNMP Management Information Base | 900 |
| About SNMP Object Names and Identifiers | 901 |
| Using the SNMP MIB Manager | 901 |
| Using the SNMP MIB Manager to troubleshoot MIB files | 902 |
| About the SNMP operations | 904 |
| Using a custom name for SNMP device interfaces | 905 |
| Configuring a custom name (ifAlias) for an SNMP device interface | 905 |
| About SNMP Security | 908 |
| Using the Trap Definition Import Tool | 908 |

Extending WhatsUp Gold with custom scripting

| | |
|---|-----|
| Extending WhatsUp Gold with scripting..... | 909 |
| Scripting Active Monitors | 910 |
| Using the Context object with Active Monitors..... | 911 |
| Example Active Script Active Monitors | 913 |
| Scripting Performance Monitors | 926 |
| Using the Context object with Performance Monitors..... | 928 |
| Example Active Script Performance Monitors | 931 |
| Scripting Actions..... | 936 |
| Using the Context object with Actions | 937 |
| Example Active Script Actions | 939 |

Using the SNMP API

| | |
|---|-----|
| CoreAsp.SnmpRqst..... | 942 |
| CoreAsp.ComResult..... | 945 |
| CoreAsp.ComSnmpResponse..... | 945 |
| Example scripts using the SNMP API..... | 946 |
| Troubleshooting the SNMP API..... | 949 |

Troubleshooting and Maintenance

| | |
|--|-----|
| Troubleshooting your network | 951 |
| Maintaining the Database | 952 |
| About the database tools..... | 952 |
| Recovering from a "Version Mismatch" error | 955 |
| Task Tray Application fails on Windows Vista..... | 955 |
| Co-located SQL Server and WhatsUp Gold server clocks must be synchronized..... | 956 |
| Connecting to a Remote Desktop | 956 |
| WhatsUp Gold engine message | 956 |
| Troubleshooting SNMP and WMI connections..... | 957 |
| Re-enabling the Telnet protocol handler..... | 958 |
| Passive Monitor payload limitation..... | 958 |
| Receiving entries in the SNMP Trap Log | 959 |
| Recommended SMS modems and troubleshooting tips..... | 959 |
| Uninstalling Ipswitch WhatsUp Gold..... | 961 |
| Troubleshooting the WhatsUp Health Threshold..... | 962 |

Using WhatsUp Gold Flow Monitor

| | |
|--|-----|
| Flow Monitor Overview | 964 |
| Welcome to WhatsUp Gold Flow Monitor | 964 |
| What is Flow Monitor? | 965 |
| How does Flow Monitor work?..... | 965 |
| System requirements..... | 967 |
| Flow Monitor Home | 968 |
| Preparing network devices | 972 |
| Determining which network devices to monitor | 972 |
| Manually configuring devices to export flow data to Flow Monitor | 973 |
| Configuring sFlow enabled devices to export flow data to Flow Monitor..... | 975 |
| About Flexible NetFlow | 979 |

| | |
|--|------|
| About Network Based Application Recognition (NBAR)..... | 983 |
| About CBQoS | 984 |
| Viewing potential Flow Monitor sources..... | 988 |
| Using Flow Monitor to Configure Cisco NetFlow Devices..... | 989 |
| Managing Flow Sources | 992 |
| About Flow Sources | 992 |
| Configuring Flow Monitor to listen for NetFlow data..... | 993 |
| Viewing Flow Sources..... | 994 |
| Configuring a Flow Source..... | 996 |
| Creating flow sources | 1004 |
| Managing Flow Monitor Settings | 1006 |
| Flow Monitor Settings | 1006 |
| Configure Flow Monitor to listen for NetFlow data | 1011 |
| Setting the logging level | 1011 |
| Data retention strategy and tuning..... | 1012 |
| Configuring data retention settings..... | 1014 |
| Configuring Applications..... | 1018 |
| Monitoring traffic on non-standard ports | 1018 |
| Configure Applications | 1019 |
| Map Ports to Application..... | 1021 |
| Configuring Flow Groups..... | 1022 |
| Using Flow Groups..... | 1022 |
| Flow Groups | 1023 |
| Flow Group | 1023 |
| Configuring Type of Service..... | 1025 |
| Flow Types of Service..... | 1025 |
| Edit Flow Type of Service..... | 1026 |
| Managing unclassified traffic | 1027 |
| Classifying traffic that is considered unclassified | 1027 |
| Flow Unclassified Traffic | 1028 |
| Configuring Data Export Settings..... | 1030 |
| Flow Export Settings | 1030 |

| | |
|---|------|
| Maintaining Flow Databases | 1032 |
| Flow Database Table Maintenance..... | 1032 |
| Stopping or restarting the collector | 1034 |
| Backing up and restoring the Flow Monitor databases | 1035 |
| Using the database backup and restore backup utility for Flow Monitor | 1035 |
| Managing users and user rights | 1036 |
| Using Flow Monitor reports | 1038 |
| About the Flow Monitor Reports group | 1038 |
| About the Interface Details report | 1039 |
| Flow Monitor Interface Overview report | 1048 |
| Flow Log | 1052 |
| Flow Bandwidth Usage report..... | 1056 |
| Flow Interface Usage Report | 1059 |
| About the NBAR and CBQoS Reports..... | 1061 |
| Using Scheduled Reports: printing, exporting, and emailing reports | 1064 |
| Using Flow Monitor dashboard reports | 1066 |
| Understanding Flow Monitor dashboard reports | 1066 |
| Navigating dashboard reports | 1068 |
| Configuring dashboard reports | 1073 |
| Exporting dashboard report data..... | 1075 |
| Linking to Flow Monitor reports from WhatsUp Gold workspace reports | 1076 |

Using WhatsVirtual

| | |
|--|------|
| Welcome to Ipswitch WhatsVirtual | 1080 |
| Welcome to Ipswitch WhatsVirtual..... | 1080 |
| Using WhatsVirtual..... | 1081 |
| STEP 1: Purchase and enable the WhatsVirtual license | 1081 |
| STEP 2: Create Credentials and Perform Discovery..... | 1081 |
| STEP 3: Manage and monitor virtual devices | 1087 |
| STEP 4: View the WhatsVirtual maps | 1097 |
| STEP 5: View the WhatsVirtual reports..... | 1099 |

Other Plugins

| | |
|--|------|
| Using WhatsConfigured | 1102 |
| Welcome to WhatsConfigured | 1103 |
| Accessing WhatsConfigured Features in WhatsUp Gold | 1104 |
| Using WhatsConfigured reports | 1105 |
| Using Task Scripts..... | 1108 |
| Using Tasks | 1111 |
| Using Policies | 1123 |
| Using Archive Search | 1127 |
| About Device Properties - Tasks | 1129 |
| Using Alert Center with WhatsConfigured | 1132 |
| Managing WhatsConfigured and TFTP services | 1134 |
| The WhatsConfigured Custom Script Language | 1135 |
| Using WhatsConfigured Comments..... | 1137 |
| Using WhatsConfigured Variables | 1138 |
| Using WhatsConfigured Commands..... | 1141 |
| Script Examples..... | 1153 |
| About the WhatsConfigured Custom Script Language..... | 1154 |
| Task Status | 1154 |
| About the WhatsConfigured Diff Viewer | 1155 |
| Using WhatsConnected..... | 1157 |
| WhatsConnected Task Log | 1157 |
| WUG Device Viewer | 1159 |
| Using ELM Reports | 1165 |
| Using Event Log Management (ELM) Reports in WhatsUp Gold | 1166 |

About the Dashboard Screen Manager

| | |
|--|------|
| Ipswitch Dashboard Screen Manager overview | 1173 |
| How does the Dashboard Screen Manager work? | 1174 |
| What is a Dashboard playlist? | 1174 |
| Installing the Dashboard Screen Manager | 1175 |
| Opening the Dashboard Screen Manager | 1176 |
| Configuring a Dashboard Screen Manager playlist..... | 1176 |

Copyright notice

WhatsUp Gold Overview

In This Chapter

| | |
|---|----|
| Welcome to Ipswitch WhatsUp Gold..... | 17 |
| WhatsUp Gold editions | 19 |
| New in Ipswitch WhatsUp Gold..... | 23 |
| Sending feedback..... | 23 |
| Finding more information and updates..... | 23 |
| Getting Familiar with WhatsUp Gold..... | 25 |

Welcome to Ipswitch WhatsUp Gold

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

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

Discovery and Mapping

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

Device roles do two things:

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

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

Polling/Listening

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

Actions/Alerts

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

Logs and Dashboards

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



WhatsUp Gold Interfaces

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

- **Windows console interface.** The console is a Windows application, through which you can configure and manage WhatsUp Gold and its database.
- **Web interface.** The web interface provides access to WhatsUp Gold functionality (via HTTP or HTTPS) from a web browser.
- **Mobile interface.** You can now conveniently view your network's status from a mobile device at any time through WhatsUp Gold Mobile Access.

WhatsUp Gold editions

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

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

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

| | Standard Edition | Premium Edition | MSP Edition | Distributed Edition |
|--|------------------|-----------------|-------------|---------------------|
| Application and Hardware Management | | | | |
| Monitor Microsoft Exchange | | ● | ● | ● |
| Monitor SQL Server and MySQL | | ● | ● | ● |
| Monitor applications via WMI | | ● | ● | ● |
| Monitor device hardware, such as cooling systems, power supplies, and temperature monitors | | ● | ● | ● |
| Monitor printers and APC UPS devices | | ● | ● | ● |
| Monitor web content | | ● | ● | ● |
| Monitor device network statistics | | ● | ● | ● |

| | Standard Edition | Premium Edition | MSP Edition | Distributed Edition |
|---|------------------|-----------------|-------------|---------------------|
| Monitor device file and folder properties | | ● | ● | ● |
| Monitor email and FTP servers | | ● | ● | ● |
| Monitor wireless access points (WAPs) | | ● | ● | ● |
| Monitor Unix/Linux environments over SSH | | ● | ● | ● |
| Real-time Monitoring | | | | |
| View real-time data about devices in logs and Dashboard reports | | ● | ● | ● |
| Quickly access real-time data via InstantInfo popups | | ● | ● | ● |
| Monitor performance data with the Web Performance Monitor | | ● | ● | ● |
| View real-time information about tasks running on a device using the Web Task Manager | | ● | ● | ● |
| Distributed Monitoring | | | | |
| Monitor devices on networks segmented across multiple geographic locations | | | ● | ● |
| View report data from multiple remote sites from one central location | | | ● | ● |

| Optional Plug-ins | | | | |
|--|---|---|---|---|
| <p>WhatsUp Gold Flow Monitor. This plug-in provides insight into how efficiently your network is performing and how bandwidth is utilized, giving you detailed information to assess network quality of service and quickly resolve traffic bottlenecks.</p> <p>For more information, see the WhatsUp Gold Flow Monitor User Guide on the <i>WhatsUp Gold web site</i> (http://www.whatsupgold.com/NetFlowMonitor).</p> | ● | ● | ● | ● |
| <p>WhatsUp Gold WhatsConfigured. This configuration management plug-in automates, and reduces the time and effort required to backup, compare, and upload configuration files for networking devices and alerts when configuration changes are detected.</p> <p>For more information, see the <i>WhatsUp Gold web site</i> (http://www.whatsupgold.com/).</p> | ● | ● | ● | ● |
| <p>WhatsUp Gold WhatsVirtual. This plug-in lets you monitor virtual environments using WhatsUp Gold. The WhatsVirtual plugin provides WhatsUp Gold with the ability to discover, map, monitor, alert, and report on virtual environments.</p> <p>For more information, see the <i>WhatsUp Gold web site</i> http://www.whatsupgold.com/WhatsVirtual.</p> | ● | ● | ● | ● |
| <p>WhatsUp Gold VoIP Monitor. This plug-in delivers the ability to monitor and report on your network's capacity to support and maintain acceptable performance for VoIP call quality.</p> <p>For more information, see the <i>WhatsUp Gold web site</i> (http://www.whatsupgold.com/products/Voip_Monitor).</p> | ● | ● | ● | ● |

| Optional applications | | | | |
|---|---|---|---|---|
| <p>WhatsUp Gold WhatsConnected. This plug-in is a Layer 2/3 network mapping tool that discovers, maps and documents your network down to the individual port, making it simple to visualize the physical topology and understand device interconnections.</p> <p>For more information, see the <i>WhatsUp Gold web site</i> (http://www.whatsupgold.com/products/WhatsConnected).</p> | ● | ● | ● | ● |
| Access from mobile devices | | | | |
| <p>WhatsUp Gold Mobile Access. Allows you to conveniently view your network's status from a mobile device at any time.</p> <p>For more information, see the <i>WhatsUp Gold Mobile Access User Guide</i> (http://www.whatsupgold.com/wug15ma).</p> | ● | ● | ● | ● |

WhatsUp Gold optional plug-ins are available for use with any of the WhatsUp Gold editions. These plug-ins broaden your monitoring and reporting capabilities to give you a more complete picture of your network and its many components. For more information, see the *WhatsUp Gold web site* (<http://www.whatsupgold.com/>).

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

- **WhatsUp Gold WhatsConnected** plug-in for WhatsUp Gold provides layer 2/3 network discovery and topology mapping to visually depict device connectivity down to the individual port. It also employs deep device scanning that provides detailed information about discovered devices in a simple device list view, a device category view, and a detailed topology view. You can publish any of the network maps as a network diagram in Microsoft® Visio™ or export detailed device information to WhatsUp Gold to automate the creation of detailed network topology map views. WhatsConnected also includes Layer 2 Trace and IP/MAC Finder tools to validate connection paths and report real-time availability data on devices. For more information, see the *WhatsUp Gold web site* (<http://www.whatsupgold.com/products/WhatsConnected>).
- **WhatsUp Gold VoIP Monitor** plug-in for WhatsUp Gold measures your network's ability to provide the quality of service (QoS) necessary for your VoIP calls on your LAN and WAN links. After a simple setup, the VoIP Monitor accesses Cisco IP SLA (service level agreement) enabled devices to monitor VoIP performance and quality parameters including jitter, packet loss, latency, and other performance values. The plug-in's full integration with WhatsUp Gold allows you to easily view graphs and metrics for bandwidth and interface utilization and troubleshoot network issues that affect VoIP performance. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/products/Voip_Monitor).

New in Ipswitch WhatsUp Gold

You can refer to the Ipswitch WhatsUp Gold *Release Notes* (<http://www.whatsupgold.com/WUG15relnotes>) to learn about the latest product features, system requirements, fixed in this release, known issues, and other information. Also see *About the WhatsUp Gold web interface* (on page 25) for highlight information on the web user interface.

Sending feedback

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

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

Finding more information and updates

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

- **Release Notes.** The release notes provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for installing, upgrading, and configuring WhatsUp Gold. The release notes are available at **Start > Programs > Ipswitch WhatsUp Gold > Release Notes** or on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/WUG15relnotes>).
- **Application Help for the console and web interface.** The console and web help contain dialog assistance, general configuration information, and how-to's that explain how to use the features. The Table of Contents is organized by functional area, and can be accessed from the main menu or by clicking **Help** in the console, or the **?** icon in the web interface.
- **Getting Started Guide.** This guide provides an overview of WhatsUp Gold, information to help you get started using the application, the system requirements, and information about installing and upgrading. The Getting Started Guide is available on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/wug15gsg>).
- **Additional WhatsUp Gold resources.** For a listing of current and previous guides and help available for WhatsUp Gold products, see the *WhatsUp Gold web site* (<http://www.whatsupgold.com/support/guides.aspx>).
- **WhatsUp Gold optional plug-ins.** You can extend the core features of WhatsUp Gold by installing plug-ins. For information on available plug-ins and to see release notes for each plug-in, see *WhatsUp Gold plug-ins documentation* (<http://www.whatsupgold.com/support/guides.aspx>).
- **Licensing Information.** Licensing and support information is available on the *MyIpswitch licensing portal* (<http://www.myipswitch.com/>). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.
- **Technical Support.** Use the WhatsUp Gold Support Site for a variety of WhatsUp Gold product help resources. From here you can view product documentation, search Knowledge Base articles, access the community site for help from other users, and get other Technical Support information. The Support Site is available on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/wugtechsupport>).

Getting Familiar with WhatsUp Gold

Using the WhatsUp Gold Web Interface

In This Chapter

| | |
|---|----|
| Accessing the web interface..... | 25 |
| About the WhatsUp Gold web interface | 25 |
| Organizing Devices, Device Groups, and Maps with drag-and-drop..... | 32 |
| About the Task Tray and Desktop Actions icon..... | 33 |

Accessing the web interface

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

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

`http://monitor1.ipswitch.com`

- or -

`http://monitor1.ipswitch.com:80`



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

There are two default users on the Web server:

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



Note: Microsoft Internet Information Services (IIS) is used for the WhatsUp Gold web server. For more information, see the *Configuring the web server* section of the *Installing and Configuring WhatsUp Gold* (http://www.whatsupgold.com/wugiis_15) guide.

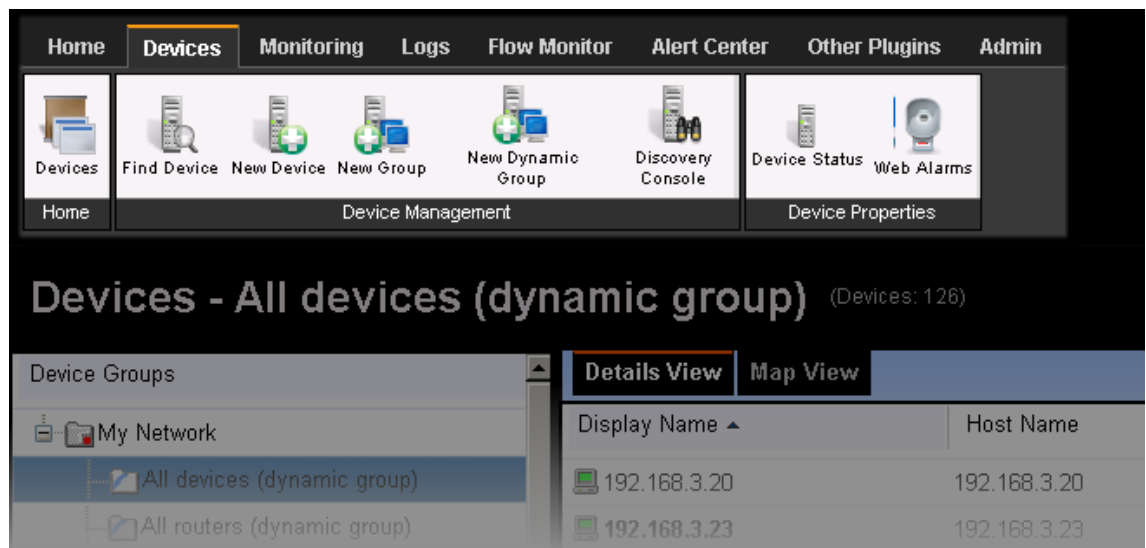
About the WhatsUp Gold web interface

The WhatsUp Gold web interface allows you to view and modify most WhatsUp Gold features from a web browser. You can discover network devices; configure monitors, alerts, and actions; view reports for devices and groups of devices, manage admin features, and more in the WhatsUp Gold web interface.

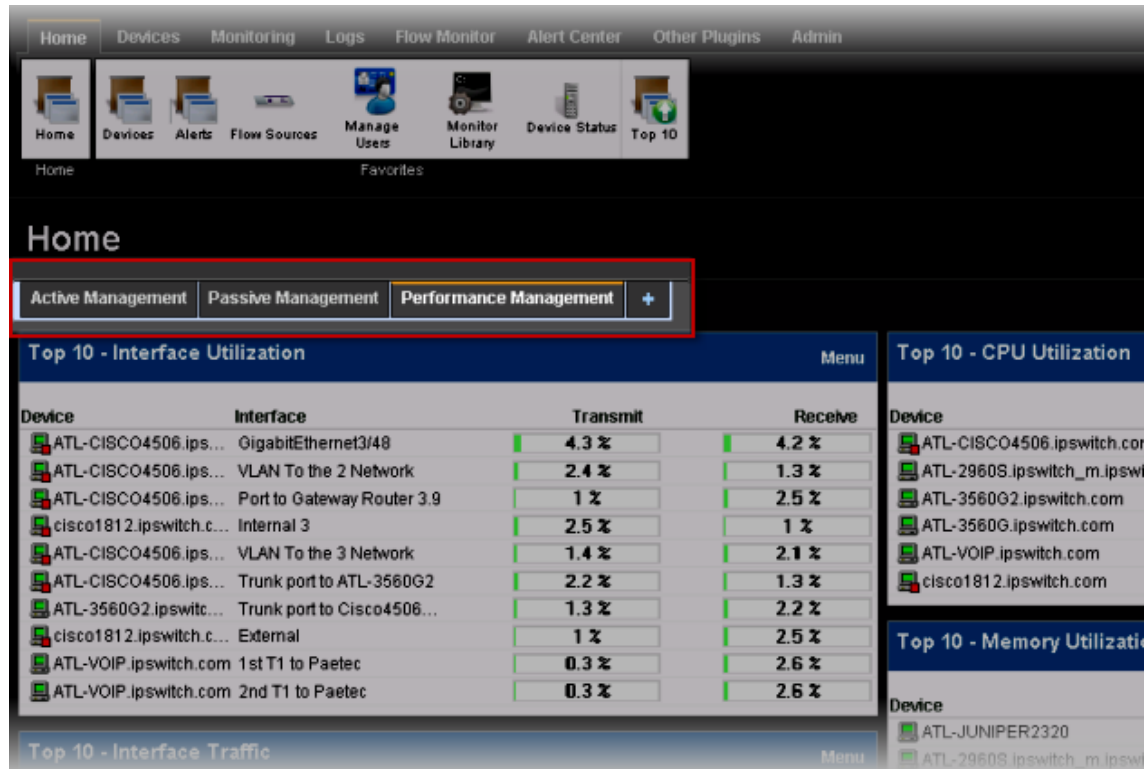
Reporting features are available in the web interface. Full reports and dashboard reports provide information about device status and performance. Full reports are located in the Monitoring and Logs tabs and dashboard reports are located in the Home tab under the **Home** button.

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

- **Where is the GO menu?** The Go menu has been replaced by new tabs and a functional navigation bar to help you access the web interface application features easily.



- **Workspace reports are now dashboard reports.** Dashboard reports are much like workspace reports in previous versions of WhatsUp Gold. You can add up to 15 reports to a single view and it's easier to add and manage dashboard views. Each dashboard view is accessed from a tab at the top of the view.



You can add and delete dashboard views to organize dashboard reports into groups.

- Click **Edit View** to add a new dashboard view (tab).
- Click **Add Content** to add a new dashboard report to the dashboard view. For more information, see the Dashboard help.



- **How do I collapse the navigation bar to make more viewable content pane space?** Click an active or selected tab to collapse the navigation bar and click again to expand the navigation bar again.

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

Home

ATL-VOIP.ipswitch.com (192.168.3.4)
Cisco cisco1841 Router

Active Monitors - 0 Down

- Interface - Connect to Port G5/12 on Cisco 4506 (192.168.3.4) Up for 43 days
- Ping Up for 43 days
- Fan Up for 43 days
- HTTD Up for 30 days

Performance Monitors

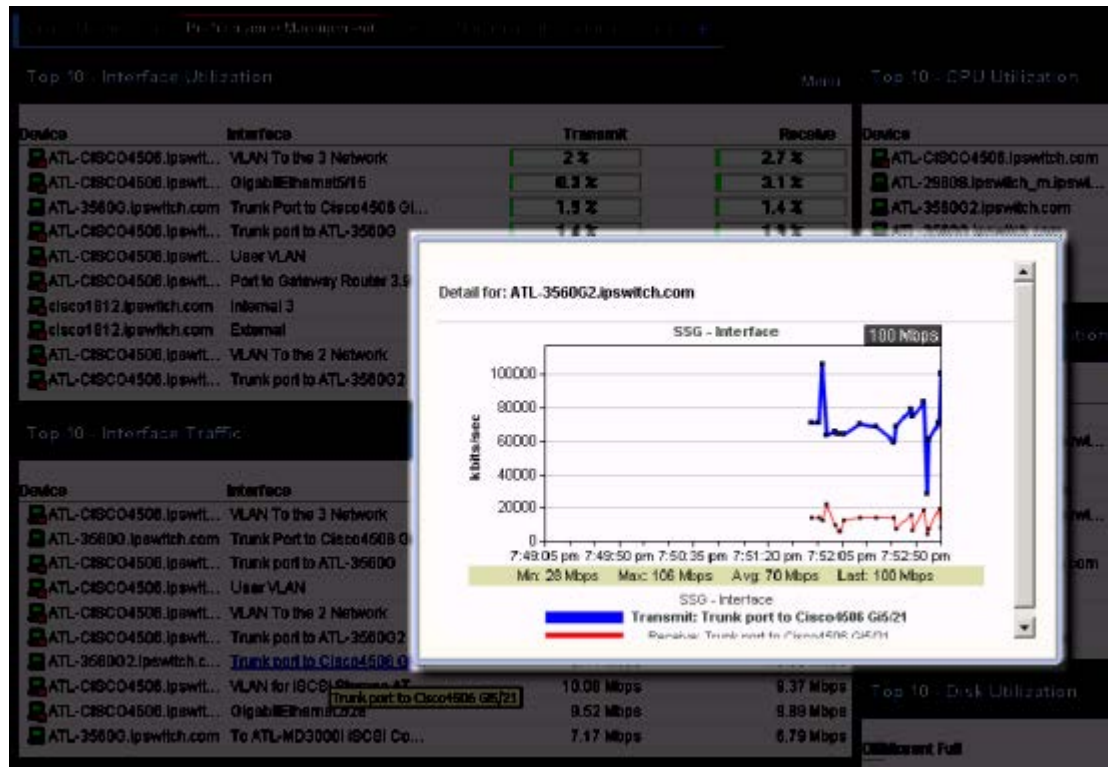
- CPU Utilization 11% Polled 7 minutes ago
- Ping Latency and Availability 0 ms Polled 7 minutes ago
- Memory Utilization 22.86% Polled 7 minutes ago
- Interface Utilization 0.01% Polled 6 minutes ago

Group Membership

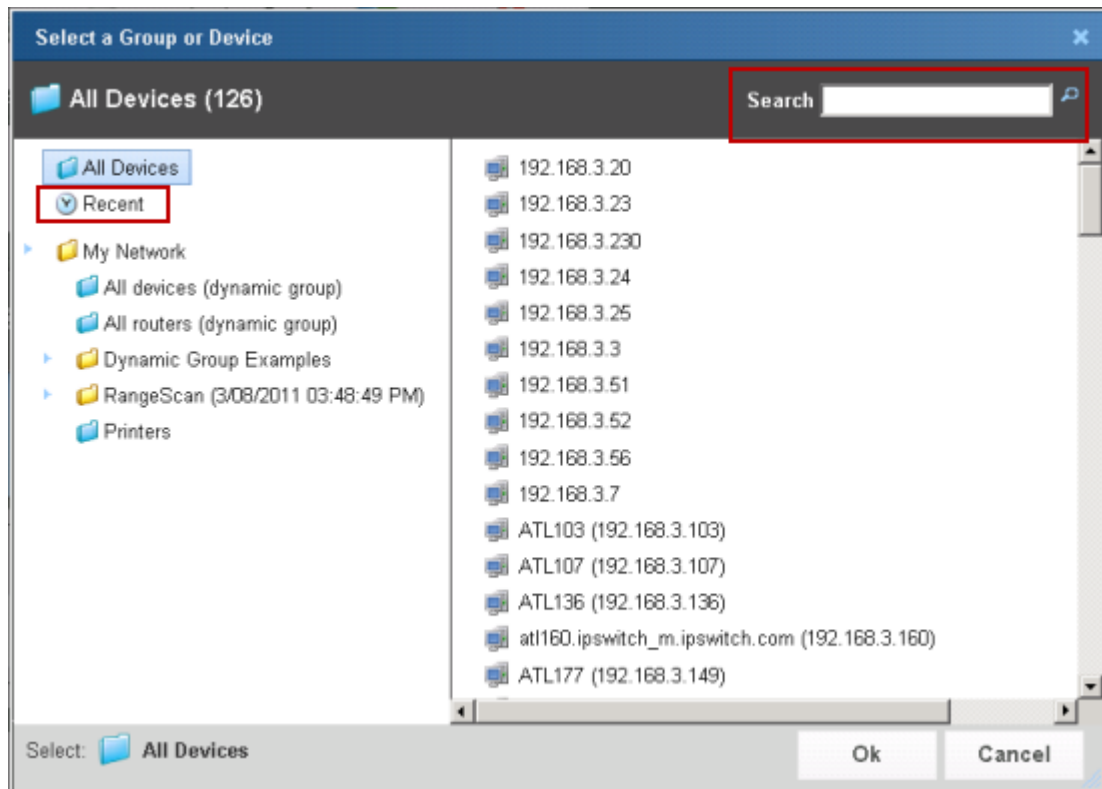
- RangeScan (3/08/2011 03:48:49 PM)
- Layer 2 topology map

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

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



- **Device picker** performs faster, provides search capabilities, and a list of recently selected devices.



- **The new Admin Panel** provides visibility into the WhatsUp Gold services and databases. Click **Admin > Admin Panel** to access it.

Admin Panel

Services

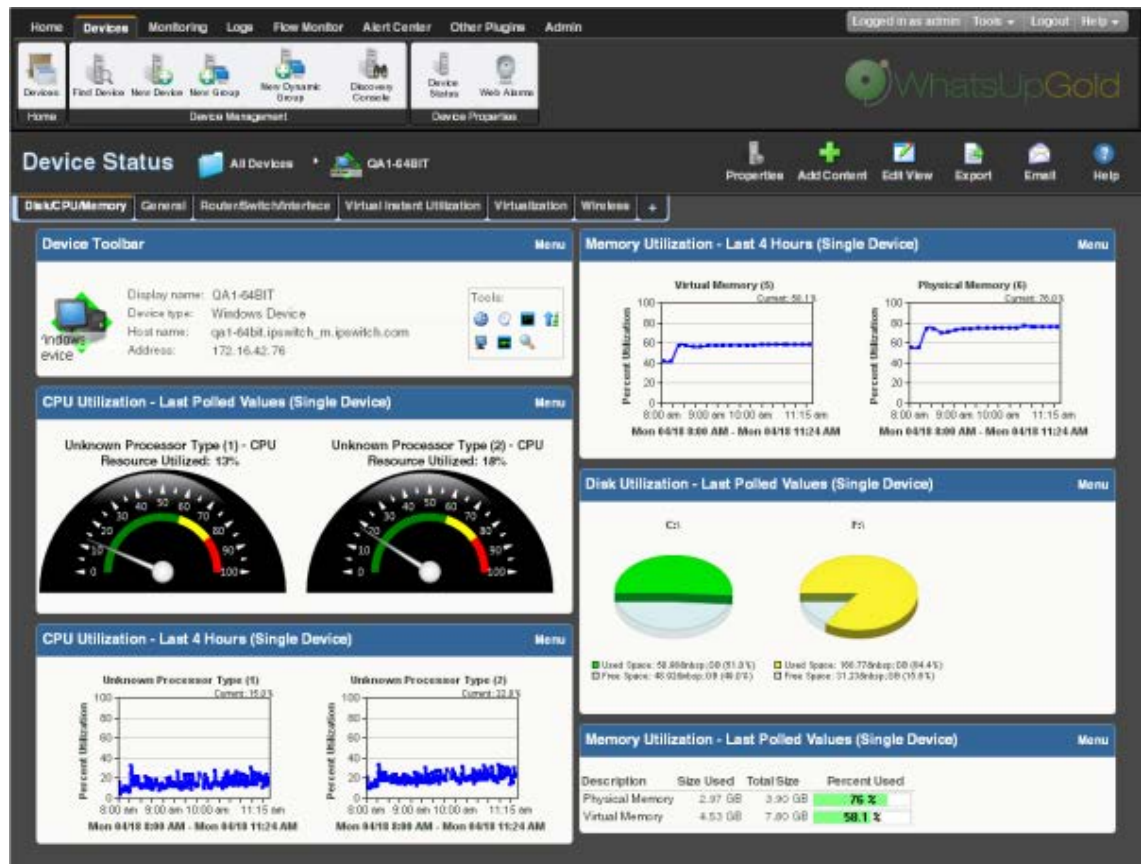
| Description | Process Name | Status |
|---------------------------------------|--------------------------|---------|
| Polling Engine | nmsservice.exe | Running |
| Flow Collector | bwcollector.net.exe | Running |
| Alert Center | alertcenterservice.exe | Running |
| Trivial File Transfer Protocol Server | tftpsservice.exe | Running |
| Whats Configured | networkconfigservice.exe | Running |
| Discovery | discoveryservice.exe | Running |
| Failover Manager | nmfailover.exe | Stopped |

Start
Stop
Restart

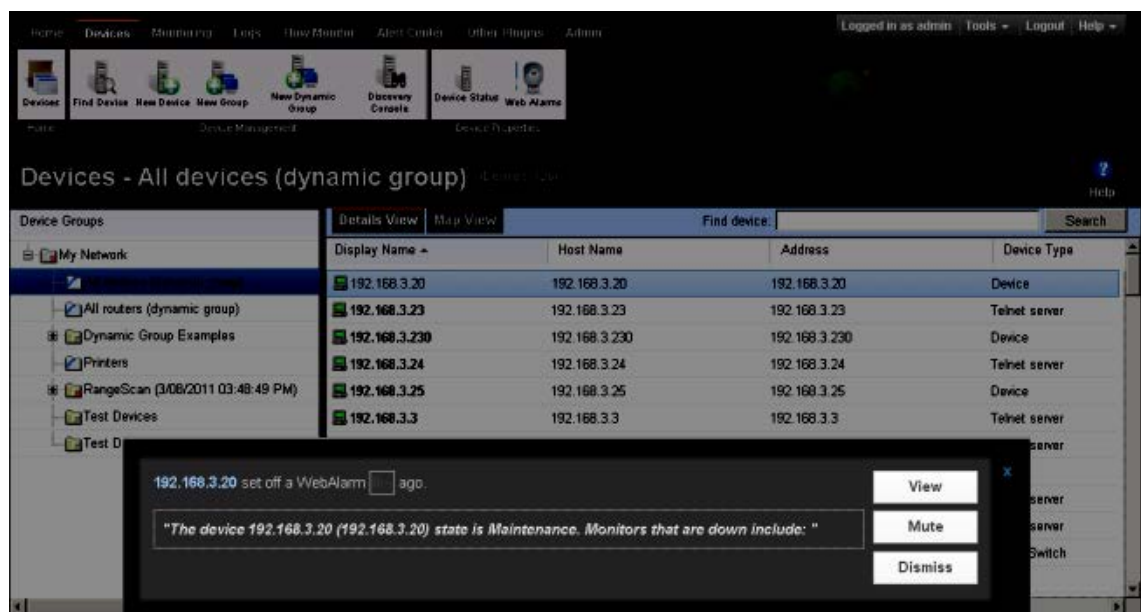
Databases

| Name | Edition | Current Size | Max Size | Percent Used |
|-----------|-----------------|--------------|----------|--------------|
| WhatsUp | Express Edition | 151.46 MB | 4 | 3.7 % |
| Netflow | Express Edition | 4.69 MB | 4 | 0.11 % |
| NFArchive | Express Edition | 6.23 MB | 4 | 0.15 % |

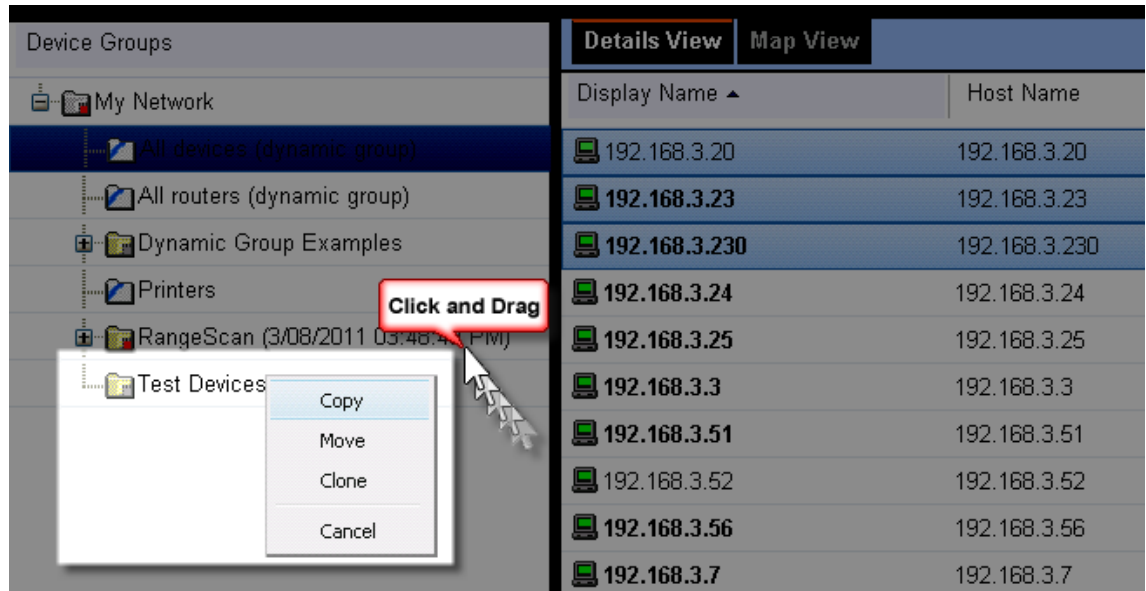
- **Improved charts and gauges.**



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

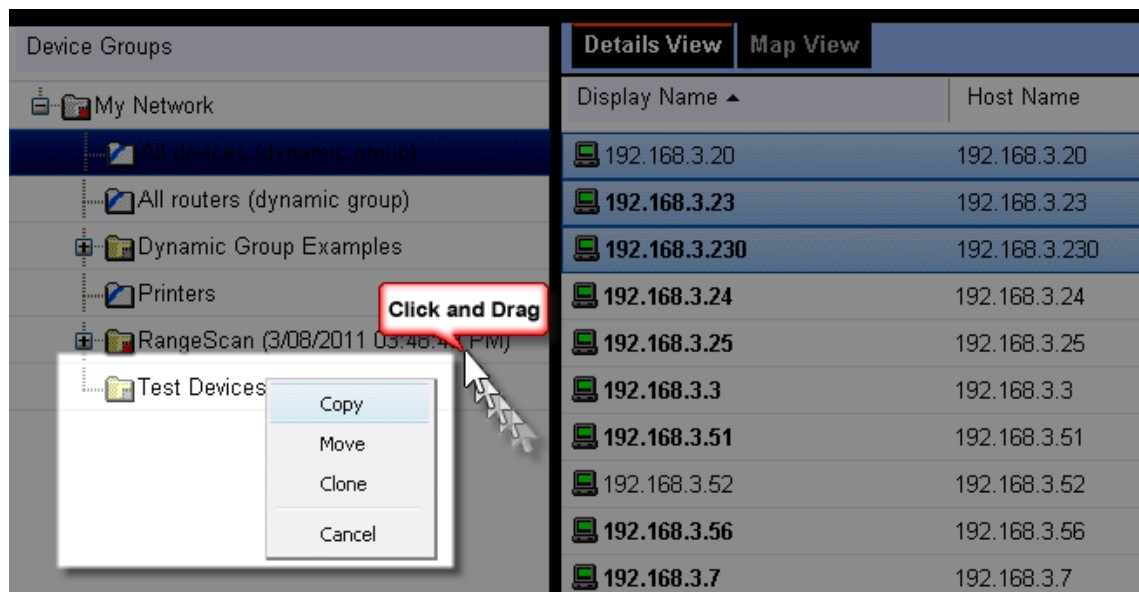


- **Improved drag-n-drop capabilities.** Drag devices to a new group, then confirm whether to Copy, Move, or Clone devices.



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

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





After you drop the icon or icons, a menu appears, asking if you want to move or copy the devices. If you move the devices, they are deleted from the previous device group. If you copy the devices, the devices appear in both device groups. For more information, see *Managing devices* (on page 97).



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

About the Task Tray and Desktop Actions icon

WhatsUp Gold installs two task bar icons on your computer.

- The Task Tray icon  alerts you to the status of the application as a whole.
- The Desktop Actions icon  displays to indicate that the application for Sound and Text-to-Speech actions is turned on.



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

WhatsUp Gold Icons

During normal operation, the Task Tray icon displays the worst state of all devices on your map.





Tip: You can enable tooltips to have the icon display any state change that occurs on the system. To do this, right-click on the icon and select or clear **Enable Tooltips**.



When the WhatsUp Gold service is stopped and the polling engine is not running, this icon appears:



In this case, you need to restart the WhatsUp Polling Engine service. If the polling engine is not running, WhatsUp Gold is not connected to the database, and nothing in the application functions properly.

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



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

Using the WhatsUp Gold Console

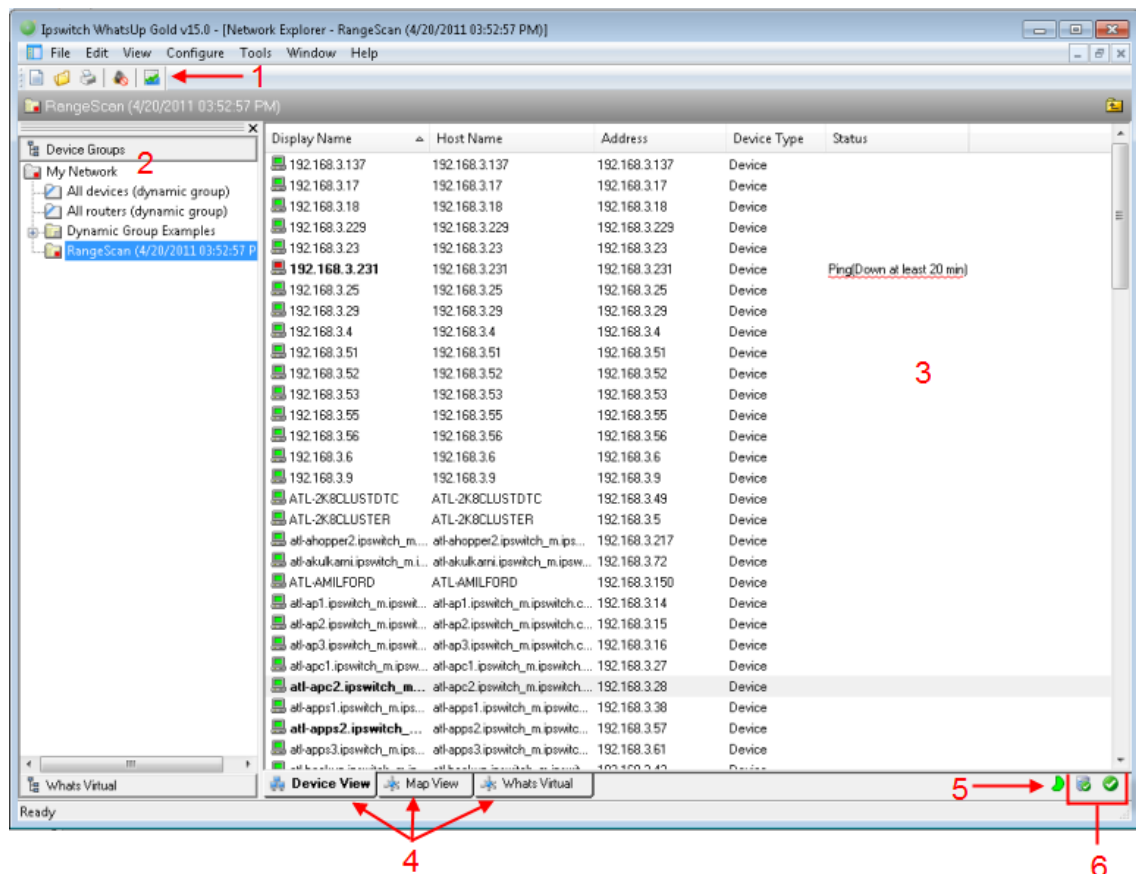
In This Chapter

About the console..... 34

About the Task Tray and Desktop Actions icon..... 35

About the console

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



- 1 WhatsUp Gold Toolbar.** The icons on this toolbar change according to the view you are currently using. Button functions are identified with mouse-over tooltips. Additional toolbar icons can be enabled for the Map view by selecting **View > Toolbars**.
- 2 Device Group Tree.** This is a list of all device groups created through WhatsUp Gold. When you perform a discovery scan, WhatsUp Gold creates a top level folder for that scan. All discovered subnetworks are created in subgroups, but can be organized, deleted, or renamed to fit your needs.
- 3 View pane.** This pane displays the selected device group based on the view from the tabs below (Device View or Map View).

- 4 View selectors.** Choose the way you want to view your device groups. Each of these views are explained in detail later in this chapter.
- **Device View.** This view provides an overview of each device and subgroup in a selected device group.
 - **Map View.** This view shows a graphical representation of the devices and subgroups in a selected device group.
 - **WhatsVirtual.** This tab displays the Whats Virtual plug-in. You must have WhatsVirtual licensed and enabled for this View to display. To upgrade your license to include WhatsVirtual, visit the *Ipswitch customer portal* (<http://www.myipswitch.com>).
- 5 Polling Indicator Icons.** These icons indicate the current state of the poll engine.



Poll engine is connected



Poll engine is not connected



Polling is enabled



Polling is disabled

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



49% and below





50% to 74%



75% and above

About the Task Tray and Desktop Actions icon

WhatsUp Gold installs two task bar icons on your computer.

- The Task Tray icon  alerts you to the status of the application as a whole.
- The Desktop Actions icon  displays to indicate that the application for Sound and Text-to-Speech actions is turned on.



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

WhatsUp Gold Icons

During normal operation, the Task Tray icon displays the worst state of all devices on your map.





Tip: You can enable tooltips to have the icon display any state change that occurs on the system. To do this, right-click on the icon and select or clear **Enable Tooltips**.



When the WhatsUp Gold service is stopped and the polling engine is not running, this icon appears:



In this case, you need to restart the WhatsUp Polling Engine service. If the polling engine is not running, WhatsUp Gold is not connected to the database, and nothing in the application functions properly.

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



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

Using WhatsUp Gold Mobile Access

In This Chapter

| | |
|---|----|
| About WhatsUp Gold Mobile Access..... | 37 |
| Managing WhatsUp Gold Mobile Access..... | 37 |
| Accessing WhatsUp Gold from a mobile device | 38 |
| Navigating and using the WhatsUp Gold Mobile Access home screen | 41 |
| Copyright notice | 46 |

About WhatsUp Gold Mobile Access

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

Mobile Access supported browsers

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



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

Browsers supported to access the WhatsUp Gold mobile interface

- Mobile Safari 2.2, Safari, 3.0, and Safari 4.0
- Microsoft Internet Explorer Mobile 6.1.x
- Opera Mini 4.2



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

Managing WhatsUp Gold Mobile Access

The WhatsUp Gold Mobile Access feature is enabled by default and the WhatsUp Gold Admin user rights are selected by default. You can provide access to other WhatsUp Gold users in the user rights options of the Edit User dialog. Use the following configuration options to manage Mobile Access.

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

- 1 From the WhatsUp Gold web interface, click the **Admin** tab, then click **Manage Server Options**. The Manage Server Options dialog appears.

- 2 Select the **Enable Mobile Access** option.

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

- 1 From the WhatsUp Gold web interface, click the **Admin** tab, then click **Manage Users**. The Manage Users dialog appears.
- 2 Select a user that you want to give rights to access to WhatsUp Gold mobile features, then click **Edit**. The Edit User dialog appears.
- 3 Under Account Administration, click **Mobile Access**.

Accessing WhatsUp Gold from a mobile device

You can access the WhatsUp Gold mobile interface from any supported mobile device browser. Enter the WhatsUp Gold web address which includes the hostname of the WhatsUp Gold host, the web server port number, followed by `/NmConsole/Mobile/Start`. The default port number is 80.

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

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

- or -

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

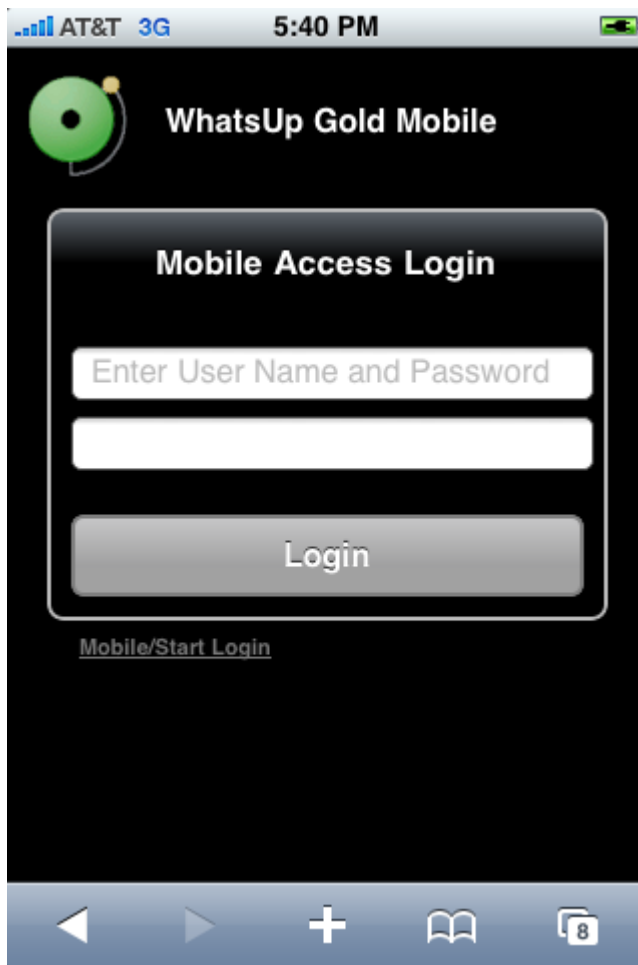


Note: When you use the default web server port (80), you do not have to include the port in the address, but all other ports require the port number following the url.



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

The mobile access login screen opens. Enter your **Username** and **Password**, then click **Login**.



Mobile/Start Login

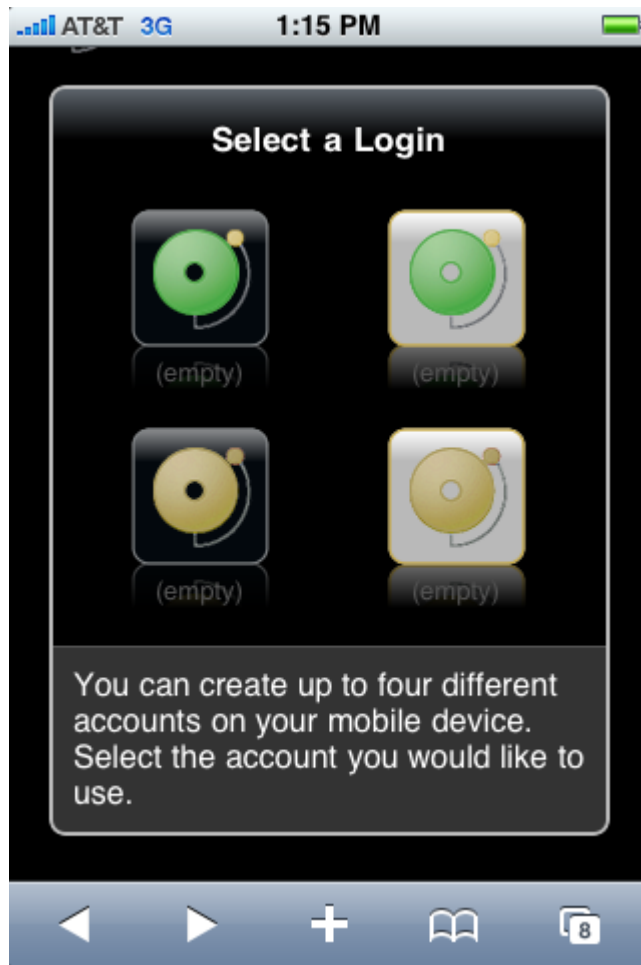
In addition to the standard login, WhatsUp Gold Mobile Access includes a one-click login feature. Because entering text in a mobile phone can be time consuming, WhatsUp Gold allows you to create up to four one-click logins per mobile device. You can bookmark each login or add to a mobile device Home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

To create a new Mobile/Start Login:

- 1 Navigate to `..NmConsole/Mobile/Start/`
- 2 Click **Create New Login**. The Mobile Start utility appears.
- 3 Click **Start**. The Select a Login dialog appears.



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



- 4 Select the login icon you want to use for the one-click login. The Create Login dialog appears.
- 5 Enter the Username and Password, then click **Create Mobile Login**. The Login Created dialog appears.
- 6 Click **Done**.

To login via the Mobile/Start Login:

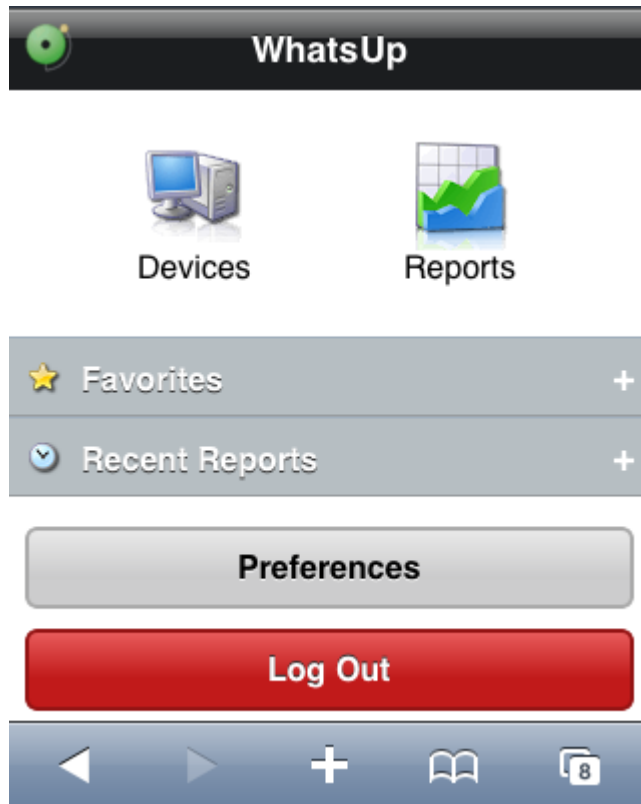


Note: If you want WhatsUp Gold Mobile Access to be accessible via the Internet (for example, via mobile phones using 3G or 4G), then make sure it is available on a server with a public IP.

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

Navigating and using the WhatsUp Gold Mobile Access home screen

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



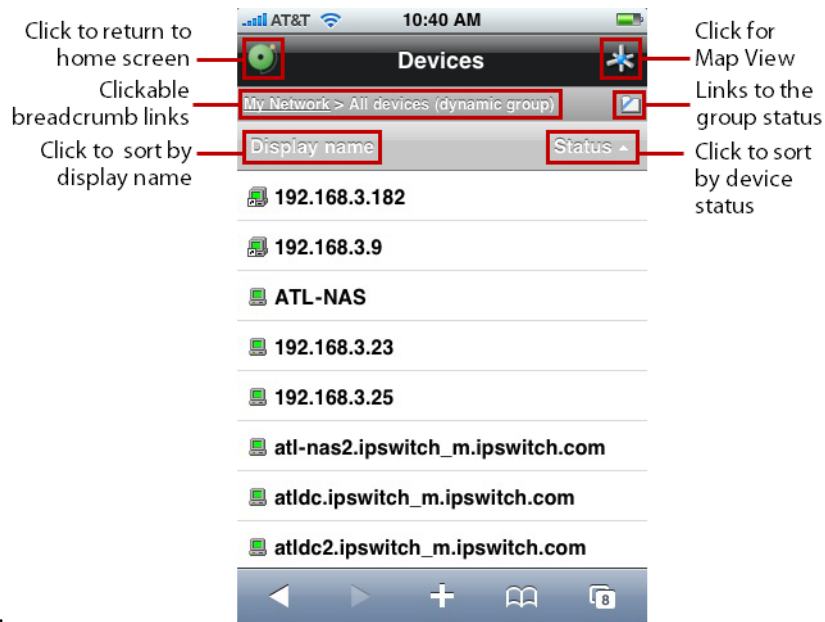
The home screen includes links to key WhatsUp Gold features so that you can view reports and monitor your network devices from remote locations:

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

Using Mobile Access Device List



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

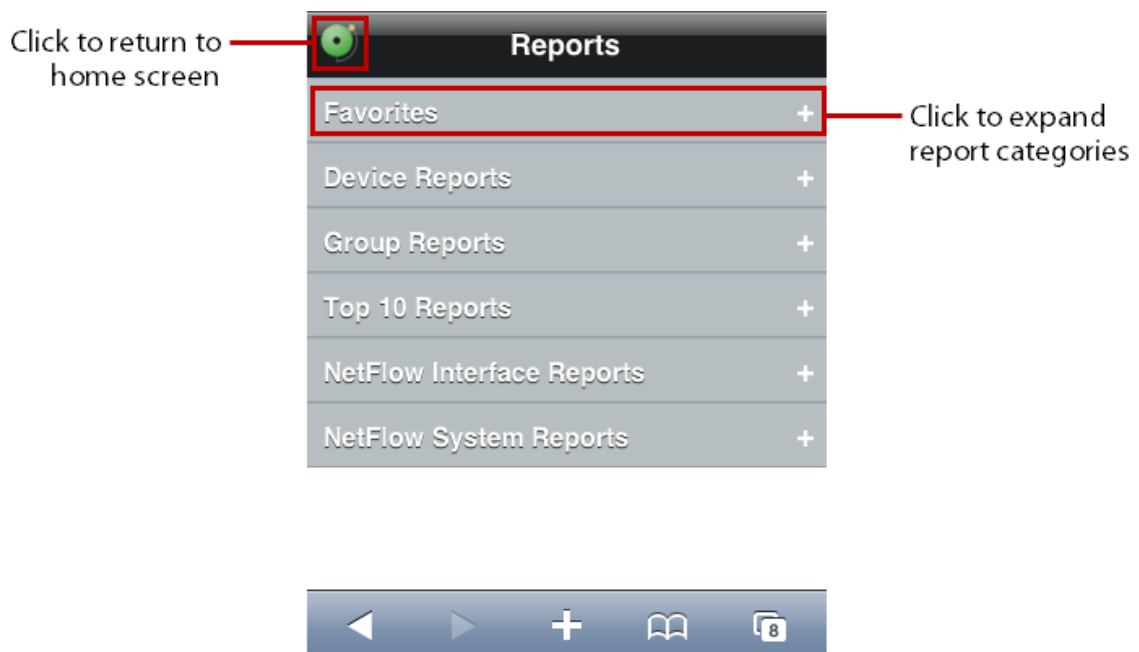


Click a device to view the device reports or click a device group to view devices within a group.

Using Mobile Access Reports



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



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

Configuring device Notes and Attributes

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

To add a phone number as a Note or Attribute:

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

To add an email address as a Note or Attribute:

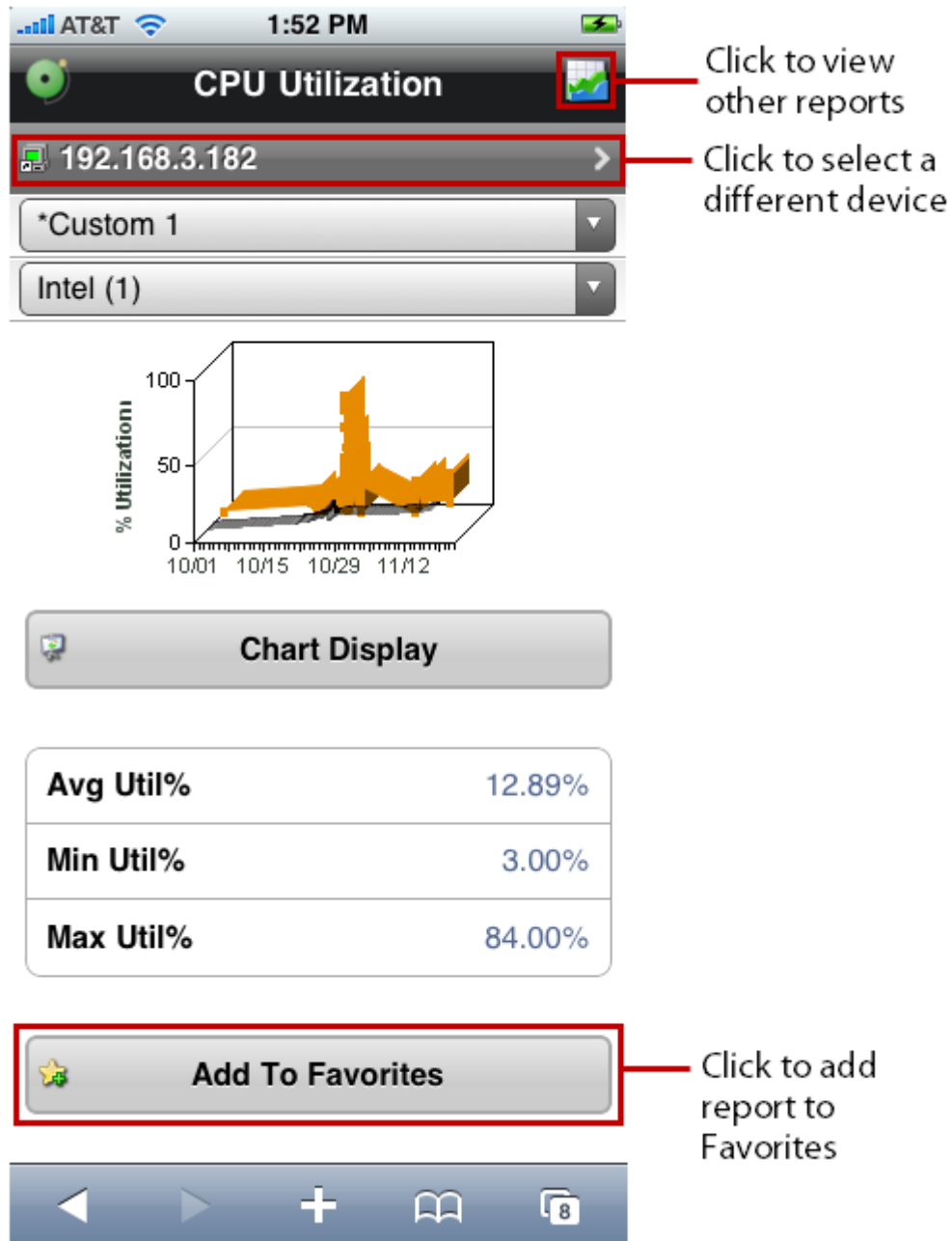
- 1 From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.
- 2 In the Attribute or Note field, use standard html code for an email link. For example:
`<a href="mailto:<John Doe>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

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

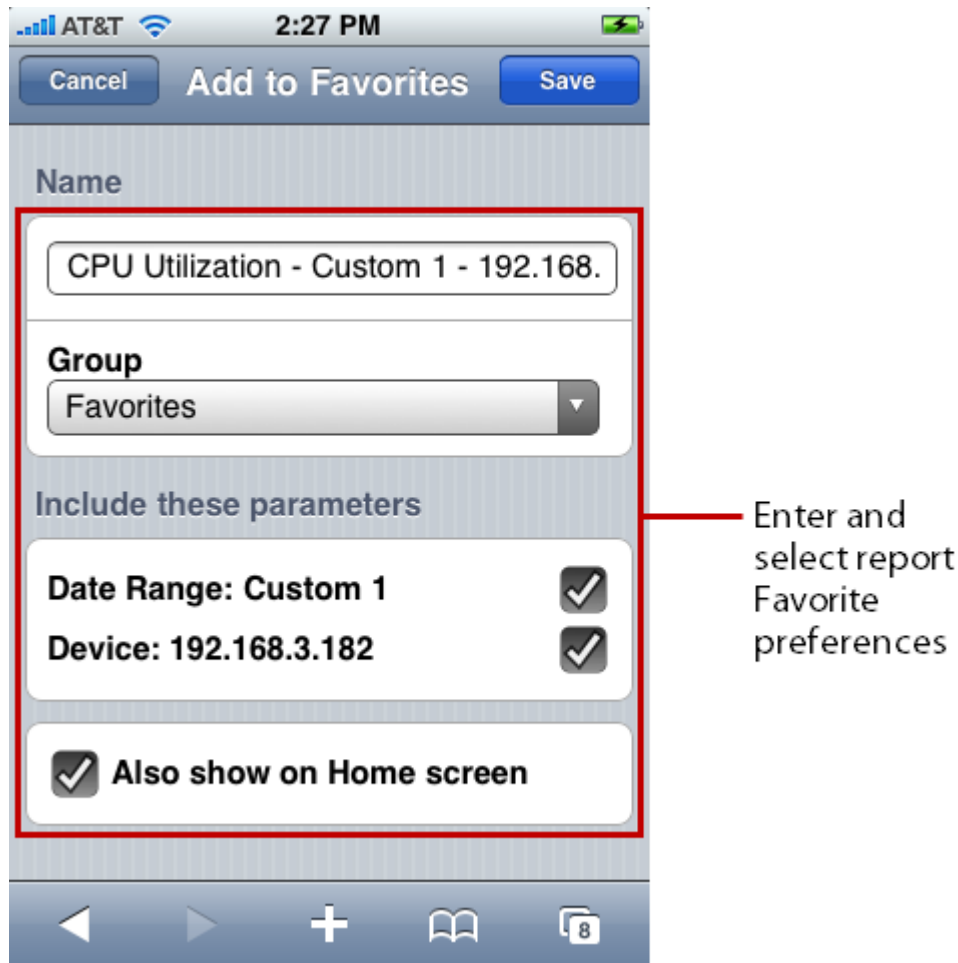
- 1 From the WhatsUp Gold console or web interface, in the Device View, right-click a device. In the right-click menu, select **Properties**, then select **Notes** or **Attributes**.
- 2 In the Attribute or Note field, use standard html code for a Google map link. Google map links can be copied from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

Using Mobile Access Favorites

WhatsUp Gold Mobile Access Favorites lets you view favorite reports that you mark with the **Add to Favorites** button at the bottom of each report.



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

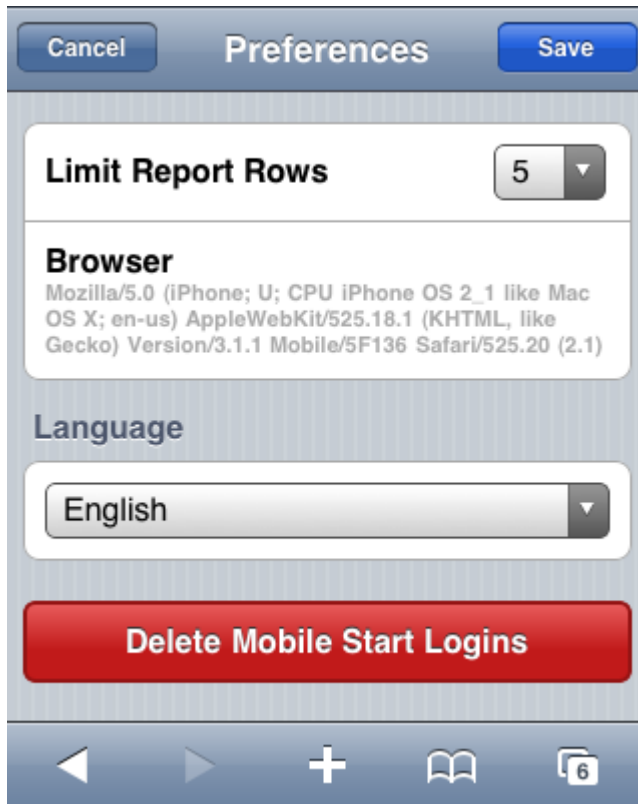


On the Home screen, click **Favorites** to expand and view your favorite reports. You can also click **Recent Reports** to view the ten most recent reports you have viewed.

Using Mobile Access Preferences

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

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



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

Devices

In This Chapter

| | |
|-------------------------------|-----|
| Discovery Console..... | 47 |
| Using Devices..... | 73 |
| Using Device Groups..... | 79 |
| Using Maps | 93 |
| Managing devices | 97 |
| Using Device Properties | 118 |
| Using Network Tools | 130 |

Discovery Console

In This Chapter

| | |
|--|----|
| Learning about the Discovery Console | 47 |
| Discovering network devices | 48 |
| Using Device Roles..... | 62 |
| Managing device roles | 70 |

Learning about the Discovery Console

The Discovery Console performs network scans to identify network devices and the *role* each device performs on the network. The WhatsUp Gold discovery is based on templates that are configured in the Device Roles, for more information see *Using Device Roles* (on page 62) in the WhatsUp Gold console application. The templates consists of:

- a set of criteria that a device must meet to match the discovery template. The criteria helps identify a device based on device role, brand/mode, OS, etc.
- a set of default configuration items to be applied to a device that matches this template.

Before you run a network discovery, you need to configure the discovery settings. You can configure the *discovery settings* (on page 51) in the Discovery Console in WhatsUp Gold web interface or console. The discovery settings are located in the Settings column on the left section of the Discovery Console.

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

- *Devices Discovered* (on page 56)
- *Progress Summary information* (on page 55)
- *Device Information tab* (on page 60)
- *Scheduled Discoveries tab* (on page 59)
- *Saved Results tab* (on page 61)

Discovering network devices

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

Before you discover the devices on your network, you need to prepare both your devices and WhatsUp Gold so that devices are discovered properly.

Preparing devices for discovery

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

Preparing devices to be discovered

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

- Ping (ICMP)
- Scanning for open TCP ports

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

Preparing devices to be identified

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

Enabling SNMP on devices

We recommend that important devices be configured to respond to SNMP requests. For information about how to enable SNMP on a specific device, see *Enabling SNMP on Windows devices* (on page 259) in the *WhatsUp Gold Online Help* (<http://www.whatsupgold.com/wug15webhelp>) or consult the device documentation. For information about configuring SNMP on network devices, you may also want to view the WUG Guru video *How to enable SNMP on a Windows server* (<http://www.whatsupgold.com/wug123snmpvideo>).

Enabling WMI on devices

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



Note: If a firewall exists between WhatsUp Gold and the devices to be discovered (or if the Windows Firewall is enabled on the computer where WhatsUp Gold is installed), make sure that the appropriate ports are open on the firewall to allow WhatsUp Gold to communicate via SNMP and WMI. For more information, see *Troubleshooting SNMP and WMI connections* (on page 957) in the help.

Preparing WhatsUp Gold for discovery

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

To apply appropriate action policies to discovered devices, we also recommend that you configure the policies in WhatsUp Gold prior to starting a discovery session, and then associate them with a device role. For more information, see *Using Device Roles* (on page 62) in the help.

Configuring credentials

To configure credentials:

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

For more information about credentials, see *Using Credentials* (on page 75) in the help.

Creating action policies

To create an action policy:

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

To associate an action policy with a device role:

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

For more information about action policies, see *About Action Policies* (on page 299) in the help.

Configuring and running discovery

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

- *Configuring discovery settings* (on page 51)
- *Running discovery* (on page 54)
- *Adding discovered devices to WhatsUp Gold* (on page 57)

To begin discovering devices on your network:

- From the WhatsUp Gold web interface, click **Devices > Discovery Console**. The Discovery Console appears.

Configure discovery settings

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

Select scan settings

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

- **SNMP Smart Scan.** This scan type uses one or more SNMP-enabled devices to identify the devices and sub-networks on your network. For more information, see *Using SNMP Smart Scan* (on page 52).
- **IP Range Scan.** Type the IP range that defines the addresses to include in the network scan. For example, **Start Address** 10.0.0.1 and **End Address** 10.0.0.100. For more information, see *Using IP Range Scan* (on page 53).
- **Hosts File Scan.** WhatsUp Gold imports devices from a hosts file. For more information, see *Using Hosts File Scan* (on page 53).



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

- **VMware Scan** (available for WhatsVirtual license). WhatsUp Gold connects to VMware servers and uses the VMware vSphere API to gather infrastructure information about your virtual environment. The VMware Scan uses a list of user provided VMware vCenter servers or VMware hosts as targets for the scan. For more information, see *Using VMware Scan* (on page 54).

Select SNMP, Windows, and VMware Credentials

To correctly identify devices, WhatsUp Gold needs to query the devices using SNMP, WMI, the VMware API or all of these methods. In these sections, select the credentials that you want WhatsUp Gold to use during discovery. You can select multiple credentials. The credentials list contains the credentials currently configured in the Credential Library. To use a credential that is not listed, you must first add the credential to the *Credential Library* (on page 836) in WhatsUp Gold. For more information, see *Using Credentials* (on page 75).



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

Configure Scan Method

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

- **Ping.** When using this method, WhatsUp Gold detects devices by issuing a ping request via ICMP and listening for a response.
- **Advanced.** When using this method, WhatsUp Gold first detects all devices that respond to ping. Then, if a device does not respond to ping, WhatsUp Gold scans common TCP ports for a response.
- **Ping Timeout (seconds).** Enter the time, in seconds, for a device to respond to a ping scan. If it does not respond to the scan within this time, the scan continues on to the next IP address. The default is 2 seconds.
- **Ping Retries.** Enter the number of times to attempt to ping a device before continuing on to the next device. The default is 1 retry.

Configure Layer 2 Scan Settings

Layer 2 discovery uses the WhatsConfigured discovery capabilities to perform ARP Cache and Ping Sweep discoveries of layer 2 networking information. This information is used to create graphical representations of network connections between discovered devices.

- **Use layer 2 discovery and generate layer 2 topology map.** Select this option to enable Layer 2 discovery using ARP Cache and Ping Sweep discovery methods.

Configure Advanced Settings

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

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

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

Using SNMP Smart Scan

To use **SNMP Smart Scan**, configure these settings:

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

Using IP Range Scan

To use **IP Range Scan**, configure these settings:

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

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

Using Hosts File Scan

To use **Hosts File Scan**:

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



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

Using Layer 2 Scan

Layer 2 discovery uses the WhatsConfigured discovery engine to perform ARP Cache and Ping Sweep discoveries of layer 2 networking information. This information is used to create graphical representations of the physical network connections between discovered devices.



Note: The Layer 2 discovery feature is available in WhatsUp Gold when you are licensed for WhatsConnected or when you are running the WhatsUp Gold product evaluation. To update or purchase a license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

- **Use layer 2 discovery and generate layer 2 topology map** (available for WhatsConnected license). Select this option to enable Layer 2 discovery using ARP Cache and Ping Sweep discovery methods.

Using VMware Scan



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

- **VMware Scan** (available for WhatsVirtual license). This scan connects to VMware servers and uses the VMware vSphere API to gather infrastructure information about your virtual environment. The VMware Scan uses a list of user provided VMware vCenter servers or VMware hosts as targets for the scan.
- **Rescan existing WUG VMware vCenter servers and hosts (recommended).** Use this option to rescan previously discovered vCenter servers and hosts. Choosing this option updates the device lists and maps provided in the Device View and Map View.
- **Add new VMware vCenter servers or hosts.** Enter the IP address of the managing vCenter or VMware hosts. Separate each host name or IP address with a comma.



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



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



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



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

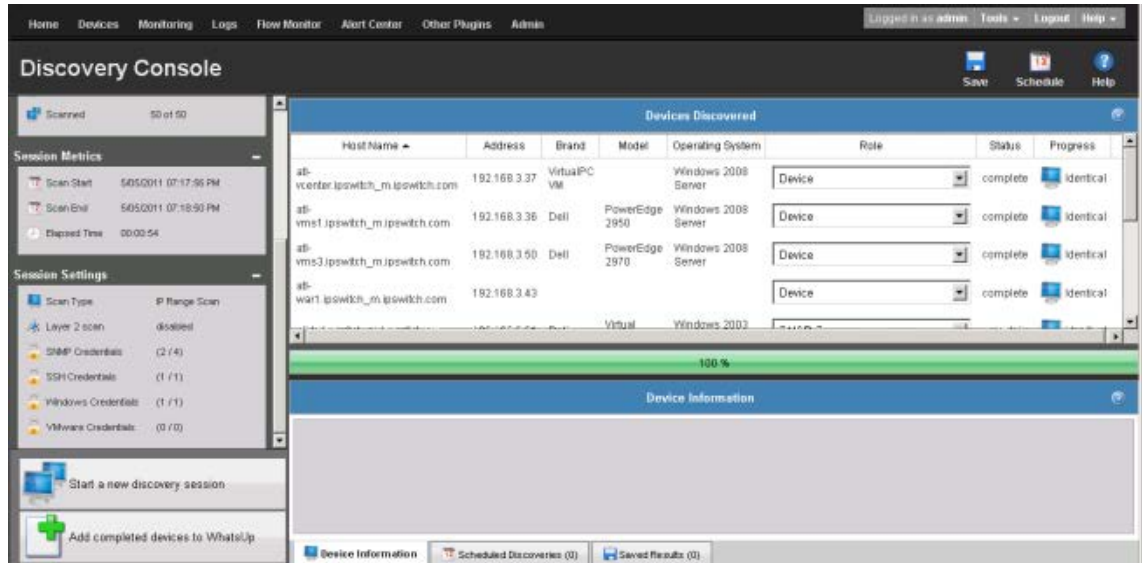
Running discovery

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

When you begin a new discovery session:

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

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



To view detailed information about a discovered device:

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

To stop a running discovery session:

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



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

Viewing progress summary information

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

Device Summary

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

Network Traffic

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

Session Metrics

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

Session Settings

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

Viewing device discovery information

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

- **Host Name.** Lists the the discovered device name by IP address or name.
- **Address.** Lists the discovered device IP address.
- **Brand.** Lists the device hardware manufacturer. The brand information helps narrow the discovery criteria to identify product model information.
- **Model.** Lists the device manufacturer model. The model information helps further refine the discovery criteria to help identify the device role.
- **Operating System.** Lists the operating system the device is running.

- **Role.** Based on the device brand, model, running applications, active ports, and other discovery criteria, a template or several template options are listed as device Role options (configurations). You can also create custom device role configurations so that device roles are identified more accurately, during discovery, for the devices on your network. For more information, see *Using Device Roles* (on page 62).
- **Status.** Lists the status of the discovery that is running.
- **Progress.** Lists the results of the discovery; whether the device found is a new or existing device. If the device is a new device, you can add it to the WhatsUp Gold database (device map) *OR* if the device is an existing device, the device has already been added to the WhatsUp Gold database.



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

Adding discovered devices to WhatsUp Gold

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



Tip: If a device identifies with an incorrect role or a role other than the one you want to use, you can change it in the drop down in the **Role** column. This field lists all of the roles for which the device met the criteria. If the role you want to use is not in this list, you must modify the device identification on the role. For more information, see *Using Device Roles* (on page 62) in the console application help.

To select a device role:

- In the Devices Discovered **Role** column, for each device listed, select the device role you want to use to define the device configuration. For more information about device role settings, see *Using Device Roles* (on page 62) in the console application help.

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

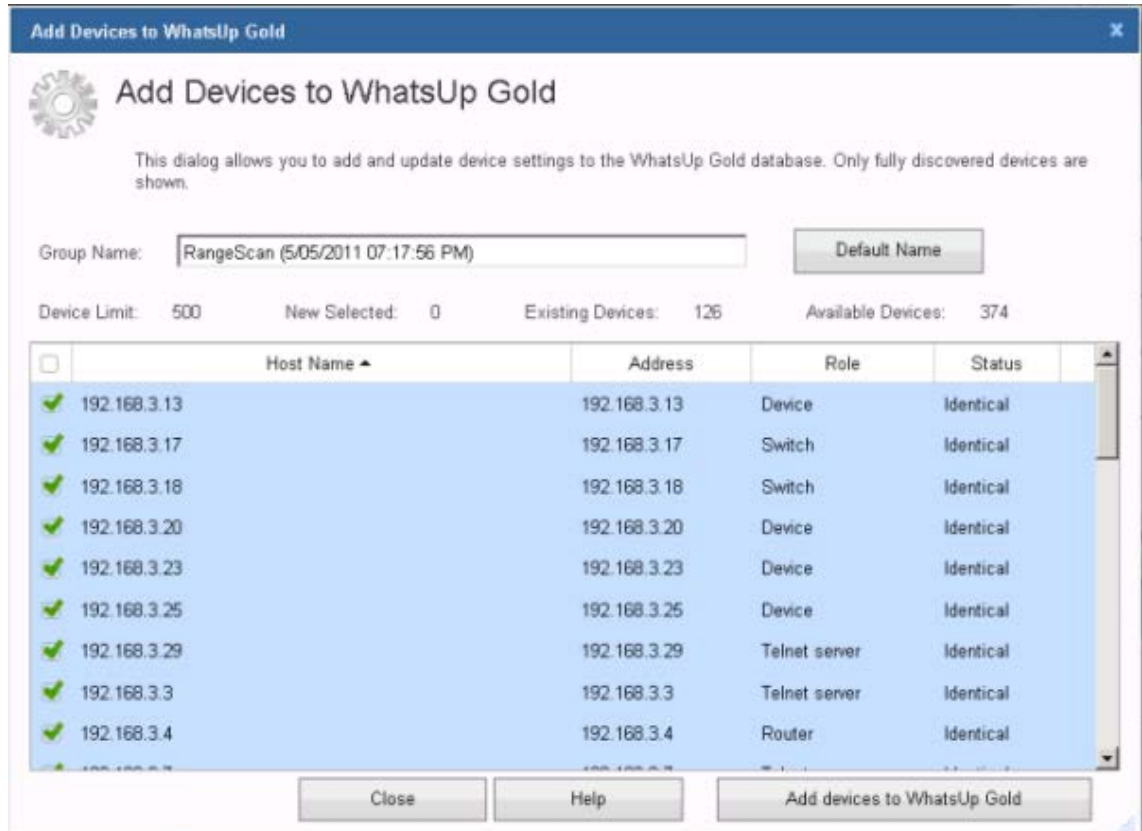
- **Device Limit.** Lists the total number of devices WhatsUp Gold is licensed to monitor.
- **New Selected.** Lists the number of devices you have selected to add to the WhatsUp Gold database.
- **Existing Devices.** Lists the number of devices WhatsUp Gold is currently monitoring.
- **Available Devices.**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

To add all completed devices to a device group:



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

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



- 2 In **Group name**, type the name of the device group to which you want to add devices. To use a device group that already exists in WhatsUp Gold, type the name exactly as it appears in WhatsUp Gold. If the name does not already exist in WhatsUp Gold, a device group with that name is created. To use a default name, which includes the type of scan and the time the scan started, click **Default name**.
- 3 Select each device you want to add to WhatsUp Gold. The check mark next to each device includes the device to be added to WhatsUp Gold.
- 4 Click **Add devices to WhatsUp Gold**. A progress dialog appears as the devices are added to the device group.
- 5 When you are finished adding devices, click **Close**. The Save Device Settings dialog closes.

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

Configuring scheduled discovery

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

To create a scheduled discovery:

- 1 Select **Devices > Discovery Console**. The Discovery console appears.
- 2 Click **Schedule**. The Scheduled Discovery Settings dialog appears.
- 3 Configure the settings for the discovery you want to schedule. For more information, see *Configure discovery settings* (on page 51).
- 4 Configure the discovery settings, schedule information, and schedule recurrence settings.
- 5 To have this discovery detect both new devices and new services on existing devices, click **Test for new monitors on existing devices**. If this option is not selected, WhatsUp Gold does not scan for new services on existing devices.
- 6 To receive an email notification of the discovery's results, click **Send email notification upon completion**.
 - a) Click **Email Settings** to configure the email notification. The Email Settings dialog appears.
 - b) Enter the information for the email. In **Body**, you can use HTML and *discovery percent variables* (on page 67).
 - c) After you have configured the email, click **OK**. The Email Settings dialog closes.
- 7 Verify that **Schedule enabled** is selected.
- 8 Click **OK** to save the scheduled discovery. The Scheduled Discovery Settings dialog closes.

To view and edit scheduled discoveries:

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

To delete a scheduled discovery:

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

Configuring discovery results email settings

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

A template email message has been created in the Body section of the dialog. You can use plain text or html code to style the message. You can also use other Discovery variables to customize the email message with additional information you want to include. For more information, see the *discovery percent variables* (on page 67) information in the console application help.

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

To configure global email settings:

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

Viewing Device Information tab

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



Note: Device Information varies, dependant upon on the device type and the SNMP information available on the device.

To view device details:

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

Viewing scheduled discoveries

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

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

- **Create.** Click to setup a new scheduled discovery.

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



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

For more information, see *Configuring scheduled discovery* (on page 59).

Saving discovery results

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

To save the results of a discovery session:



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

- 1 From the Discovery console, click **Save**. The Save Discovery Results dialog appears.
- 2 Enter a **Name** and **Description** for the saved discovery session, then click **OK**. The discovery session is saved under the Saved Results tab.

To open a saved discovery session:



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

- 1 From the Discovery console, select the **Saved Results** tab.
- 2 Select the saved discovery session that you want to open, then click **View**. The saved discovery session results appear in the Devices Discovered pane.

Using saved discovery results

The Saved Results tab lists all the discovery scans that have been saved for later use. Use the Saved Results tab to view the results of a previous discovery scan or delete the discovery scan from the list. When you view previous scans, you can select and add devices that you have not previously added to the WhatsUp Gold database. For more information, see *Adding discovered devices to WhatsUp Gold* (on page 57).

To access the Discovery Console Saved Results tab:

- 1 Click **Devices > Discovery Console**. The Discovery Console appears.
- 2 In the bottom section of the Discovery Console, click the **Saved Results** tab.

The following Saved Scan information is listed:

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

- **Description.** Lists descriptive information about the discovery.
- **Date Saved.** Lists the date and time the discovery was saved.
- **Scheduled.** Lists whether the scan is a scheduled scan or a discovery scan. A True value indicates that the scan is a scheduled scan, while False indicates that the scan is a discovery or unscheduled scan.

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

Using Device Roles

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

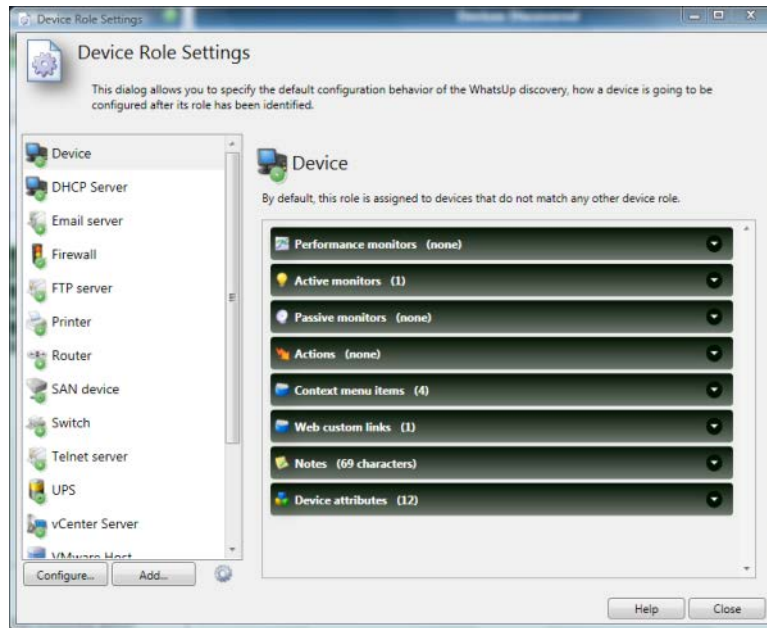
Device roles do two things:

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

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

Configuring device role settings

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



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

To configure device role settings:

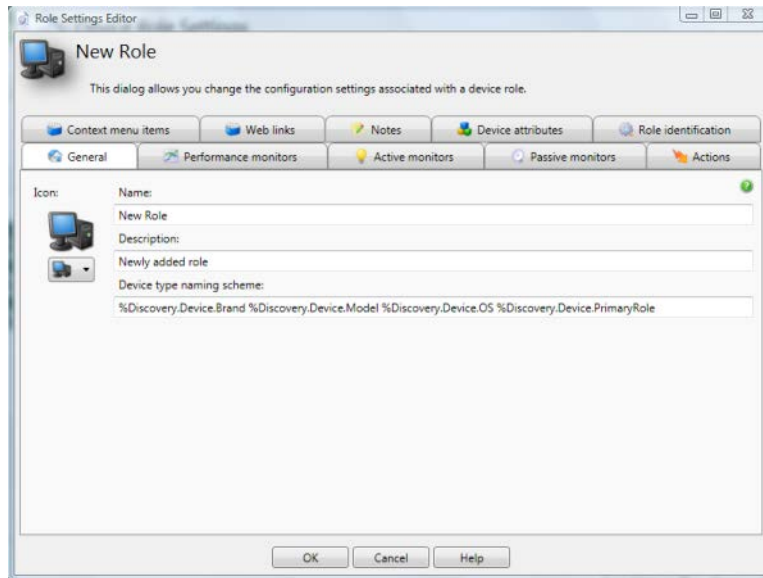
- 1 Open the Discovery console from the WhatsUp Gold console.
- 2 Select **Advanced > Device role settings**. The Device Role Settings dialog appears.
- 3 Select the device role you want to modify, then click **Configure**.

- or -

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



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



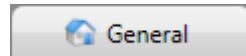
- 4 Configure the device properties. The following table lists the device properties that can be configured to be automatically added to discovered devices that match a device role.

To configure this property

Use this tab

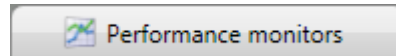
Notes

The device's icon and informational overlay text, as seen on the device map



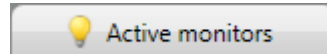
Supports *discovery percent variables* (on page 67). For more information, see the General tab console Help.

Performance monitors applied to the device



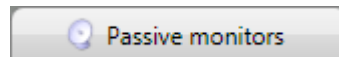
For more information, see the Performance monitors tab console Help.

Active monitors applied to the device, including which active monitors are critical



To make an active monitor critical, click the checkbox in the **Critical** column of that monitor. For more information, see *About critical active monitors* (on page 228) and the Active monitors tab console Help.

Passive monitors associated with the device



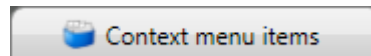
We do not recommend enabling the **Any** options. The **Any** options cause WhatsUp Gold to save a large volume of data and can lead to performance problems caused by a large database. For more information, see the Passive monitors tab console Help.

Action policy applied to the device



For more information, see the Actions tab console Help.

Context menu items available when right-clicking on the device



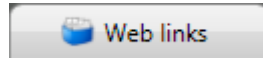
Supports *discovery percent variables* (on page 67). For

To configure this property
in the console

Use this tab

Notes

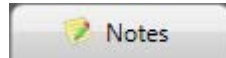
Web links available for the device
in the web interface



more information, see the
Context menu items tab
console Help.

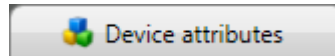
Supports *discovery percent variables* (on page 67). For
more information, see the
Web links tab console Help.

The initial content of the device's
Notes field



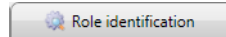
Supports *discovery percent variables* (on page 67). For
more information, see the
Notes tab console Help.

Attributes added to the device



Supports *discovery percent variables* (on page 67). For
more information, see the
Device attributes tab console Help.

The criteria a discovery scan uses
to determine whether a device
fits a specific role



For more information, see
*Configuring device role
identification settings* (on page
65).

Configuring device role identification settings

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

To configure how a role is identified:

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

- or -

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



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

- 4 Select the **Role identification** tab.
- 5 To add a new criterion, click **Add**. The **Select an identification criterion type** dialog appears.

- or -

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

- 6 Select a criterion from the list.

- **DNS hostname contains.** Select to set criteria that passes if the value of the polled SNMP object (OID) contains the specified hostname value. For example, you can check that a device name contains "ATL," the prefix used in the Atlanta office computer names.
- **SNMP object contains.** Select to set criteria that passes if the value of the polled SNMP object (OID) contains the specified value. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.1.0 (Microsoft branch) with "Version 5.1" system description information to determine the devices that are running Windows XP.
- **SNMP object has a child which contains.** Select to set criteria that passes if the value of the polled SNMP object (OID) includes a child object. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.17 (dot1dBridge, the root of the bridge MIB). If this OID has a child, it means the device supports the Bridge MIB, and therefore the device must be a switch.
- **SNMP object has a number of children greater than.** Select to set criteria that passes if the value of the polled SNMP object (OID) includes child objects greater than x number of children. For example, you can check the number of instances of a device interface by discovering instances of the interface table. This criterion could be used to identify "critical" network switches by identifying switches with 200 or more interface tables.
- **SNMP object has a value.** Select to set criteria that passes if the value of the polled SNMP object (OID) contains the specified value. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.1.6 (sysLocation) with "Server Room" system description information to determine the devices that are network servers.
- **SNMP object has at least one child.** Select to set criteria that passes if the value of the polled SNMP object (OID) includes at least one child object. For example, you can check that a printer OID includes at least one child printer OID. This criterion determines that the device is definitely a printer device. Printer OIDs must include a printer child OID.
- **SNMP object is.** Select to set criteria that passes if the value of the polled SNMP object (OID) is equal to the specified value. For example, you could poll the sysContact object to make sure the configured contact information is equal to "Jane Doe."
- **SNMP object matches regular expression.** Select to set criteria that passes if the value of the polled SNMP object (OID) matches the specified regular expression value. For example, you could check for devices that contain the OID value 1.3.6.1.2.1.1.0, the Catalyst switch sysDescr. If this system description matches the regular expression value (.Catalyst), the criteria is matched.
- **SNMP object starts with.** Select to set criteria that passes if the value of the polled SNMP object (OID) starts with the specified value. For example, you can check for devices that contain the OID value 1.3.6.1.2.1.1.2.0, an HP enterprise OID. If this OID starts with 1.3.6.1.4.1.11, the root of the HP Enterprise MIB space, it means the specified device is supported.
- **SNMP SysObjectID is.** Select to set criteria that passes if the value of the polled SysObjectID object the specified value. For example, the criterion could poll the

SysObjectID and check that it starts with 1.3.6.1.4.1.9.1.502, a Catalyst switch SysObjectID. This criteria will pass only if the polled device is a Catalyst machine.

- **SNMP SysObjectID starts with.** Select to set criteria that passes if the value of the polled SysObjectID object starts with the specified value. For example, the criterion could poll the system object ID and check that it starts with 1.3.6.1.4.1.9, the root of the Cisco Enterprise MIB space. This criteria will pass only if the polled device is a Cisco machine.
 - **NIC card brand name matches regular expression.** Select to set criteria that passes if the value of the device NIC card brand name matches the specified regular expression value. For example, SNMP is used to identify all NIC MAC addresses and they are converted to NIC vendor strings. The criterion could use the regular expression `.*intel` to check for a criteria match on all Intel NIC cards.
 - **TCP port is open.** Select to set criteria that passes if the value of the of the device port open is equal to the specified port open value. For example, if you want to find devices that have TCP ports 1234 open, then enter the port number "1234" for the port check criteria.
 - **Is always a successful match.** Select to set all criteria to always match when the option is selected.
 - **Device is a VMware host server (ESX/ESXi).** Select to set criteria that passes if the device type is a VMware host server.
 - **VMware server is hosting a number of VMs greater than.** Select to set criteria that passes if the number of VMs hosted is greater than the specified value.
 - **Name of VM hosted by VMware server is.** Select to set criteria that passes if the name of the VM hosted by the VMware server is the specified name.
 - **Name of VM hosted by VMware server contains.** Select to set criteria that passes if the name of the VM hosted by the VMware server contains the specified value.
 - **Device is a VMware vCenter Server.** Select to set criteria that passes if the device type is a VMware vCenter Server.
- 7 After selecting a criterion, click **OK**. The Edit Criterion dialog appears.
- 8 Configure the settings for the criterion, then click **OK**. For specific information about the criterion's settings, click **Help**.



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

Using the percent variables in the Discovery Console

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

| Device Discovery variables | Description |
|---|---|
| <code>%Discovery.Device.DeviceID</code> | Returns the device ID. |
| <code>%Discovery.Device.Description</code> | Returns the device description information. |
| <code>%Discovery.Device.Contact</code> | Returns the device contact information. |
| <code>%Discovery.Device.Location</code> | Returns the device location information. |
| <code>%Discovery.Device.Name</code> | Returns the device name information. |
| <code>%Discovery.Device.OID</code> | Returns the device OID information. |
| <code>%Discovery.Device.PrimaryRole</code> | Returns the device's primary role setting. |
| <code>%Discovery.Device.Model</code> | Returns the device product model information. |
| <code>%Discovery.Device.Brand</code> | Returns the device product brand information. |
| <code>%Discovery.Device.OS</code> | Returns the device operating system information. |
| <code>%Discovery.Device.OSVersion</code> | Returns the device operating system version. |
| <code>%Discovery.Device.PhysicalAddress</code> | Returns the device MAC address. |
| <code>%Discovery.Device.PhysicalAddressVendor</code> | Returns the device vendor name information. |
| <code>%Discovery.Device.VMware.Host.Name</code> | Returns the VMware host name. |
| <code>%Discovery.Device.VMware.Host.FullName</code> | Returns the full name of the VMware host. |
| <code>%Discovery.Device.VMware.Host.OSType</code> | Returns the VMware host operating system information. |
| <code>%Discovery.Device.VMware.Host.VIMVersion</code> | Returns the VMware virtual server version. |
| <code>%Discovery.Device.VMware.Host.APIVersion</code> | Returns the VMware virtual server API version. |
| <code>%Discovery.Device.VMware.Host.APIType</code> | Returns the VMware virtual server API type. |

| | |
|--|---|
| <code>%Discovery.Device.VMware.Host.Build</code> | Returns the VMware virtual server build number. |
| <code>%Discovery.Device.VMware.Host.BootTime</code> | Returns the VMware virtual server boot time. |
| <code>%Discovery.Device.VMware.Host.HardwareVendor</code> | Returns the hardware vendor name of the VMware host server. |
| <code>%Discovery.Device.VMware.Host.HardwareModel</code> | Returns the hardware model of the VMware host server. |
| <code>%Discovery.Device.VMware.Host.NumberCPUCores</code> | Returns the number of CPU cores on the VMware host server. |
| <code>%Discovery.Device.VMware.Host.NumberCPUPkgs</code> | Returns the number of CPU packages on the VMware host server. |
| <code>%Discovery.Device.VMware.Host.NumberCPUThreads</code> | Returns the number of CPU threads on the VMware host server. |
| <code>%Discovery.Device.VMware.Host.CPUFrequency</code> | Returns the CPU clock frequency of the VMware host server in Hz. |
| <code>%Discovery.Device.VMware.Host.CPUModel</code> | Returns the CPU model used by the VMware host server. |
| <code>%Discovery.Device.VMware.Host.MemorySize</code> | Returns the amount of memory in the VMware host server. |
| <code>%Discovery.Device.VMware.Host.NumberVMsTotal</code> | Returns the total number of virtual machines hosted by the VMware server. |
| <code>%Discovery.Device.VMware.Host.NumberVMsPoweredOn</code> | Returns the number of virtual machines hosted by the VMware server that are in the powered on state. |
| <code>%Discovery.Device.VMware.Host.NumberVMsSuspended</code> | Returns the number of virtual machines hosted by the VMware server that are in the suspended state. |
| <code>%Discovery.Device.VMware.Host.NumberVMsPoweredOff</code> | Returns the number of virtual machines hosted by the VMware server that are in the powered off state. |

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

Managing device roles



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

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

- *Create new device roles* (on page 71)
- *Duplicate existing device roles* (on page 71)
- *Modify device roles* (on page 71)
- *Enable or disable device roles* (on page 71)
- *Restore device roles to their original settings* (on page 72)
- *Delete device roles* (on page 72)

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


Creating new roles

To create a new device role:

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

Duplicating device roles

To duplicate an existing device role:

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


Modifying device roles

To modify an existing device role:

- 1 From the Discovery console, select **Advanced > Device role settings**. The Device Role Settings dialog appears.
- 2 Select a device role, then click **Configure**. The Role Settings Editor dialog appears.
- 3 Modify the device role.
- 4 When you are finished modifying the role, click **OK**. The Role Settings Editor dialog closes.

Enabling or disabling device roles

To enable/disable a device role:


- 1 From the Discovery console, select **Advanced > Device role settings**. The Device Role Settings dialog appears.
- 2 Select a device role, then click the gear icon (). A menu appears.
- 3 If the device role is disabled, select **Enable selected role**. If the device role is enabled, select **Disable selected role**. The device role's status is immediately updated in the list.

Restoring a device role to its original settings

To restore a default device role to its original settings:



Note: Only default device roles can be restored.


- 1 From the Discovery console, select **Advanced > Device role settings**. The Device Role Settings dialog appears.
- 2 Select a device role, then click the gear icon (). A menu appears.
- 3 Select **Restore selected role to factory defaults**. A confirmation dialog appears.
- 4 To restore the device role to its default settings, select **Yes**. The device role is restored to its original settings.

Deleting device roles

To delete a device role:



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

- 1 From the Discovery console, select Advanced > Device role settings. The Device Role Settings dialog appears.
- 2 Select a device role, then click the gear icon (). A menu appears.
- 3 Select Delete selected role. A confirmation dialog appears.
- 4 To delete the device role, select **Yes**. The device role is removed from the list.

Using Devices

In This Chapter

| | |
|--|----|
| Viewing devices in WhatsUp Gold | 73 |
| About device icons | 74 |
| Using Credentials..... | 75 |
| Searching for devices | 76 |
| Understanding group access and user rights for Find Device | 77 |
| Searching for devices with interface traffic..... | 77 |

Viewing devices in WhatsUp Gold

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

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

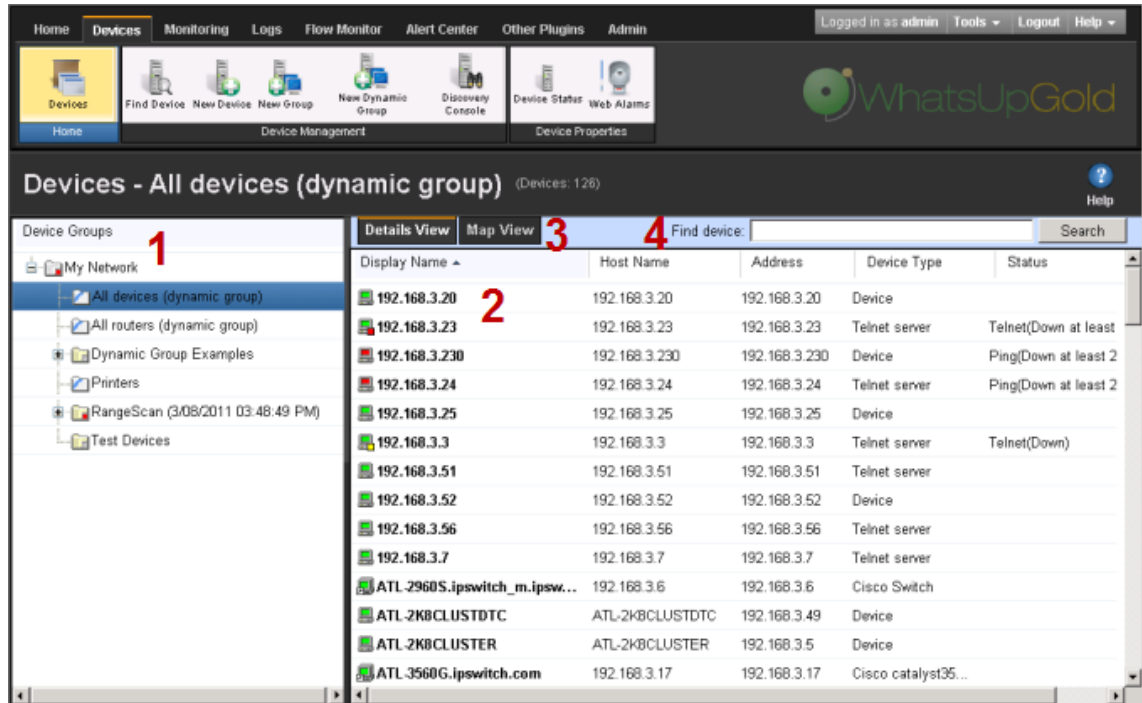
- After you associate active monitors with devices on your network, the monitors query the network services installed on a device and wait for a response, checking to make sure that the FTP server, web server, email server, etc., is up and responding. If a response is either not received or is not the expected response, the service is considered down. If the query is returned as expected, the service is considered up. Notifications or other actions can be setup in WhatsUp Gold to address the issue. For a more information about service monitors, see the *Active Monitors overview* (on page 155).

You can also configure passive monitors, which listen for specified events to occur on a device and when the event occurs, notifies you or takes other actions. For more information, see the *Passive Monitors overview* (on page 232).

Additionally, you can configure performance monitors to gather device performance information, such as CPU, disk, memory, and interface utilization. For more information, see the *Performance monitors overview* (on page 246).

To view network devices:

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







- Device Groups.** Lists network devices by categories. Select the device group you want to view. The selected device group appears in the right panel in the Details View or Map View. For more information, see *Using Device Groups* (on page 79).
- Details View** (shown). Lists network devices as a list of devices in a group.
- Map View** (not shown). Lists network devices as icon views of devices in a group. The map view provides visual information about the device status. For more information, see *Using the Map View* (on page 93).
- Find Device.** Use this search tool to find a device or device group(s) in WhatsUp Gold. For more information, see *Searching for devices* (on page 76).

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

About device icons

The following icons appear in the Device View (Console) or Details View (Web interface) when viewing the contents of a device group. For more information about device icons and status indicators, see *Using the Map View* (on page 93).

| Icon | Description |
|---|--|
|  | (Green) All monitors on the device are considered up. |
|  | Device entry appears in another device group. At least one monitor on the device is unresponsive, but at least one is considered up. |
|  | (Orange) The device is currently in maintenance mode. |
|  | A bold device name shows that the device has undergone a state change, and that state change has not been acknowledged. To acknowledge a device state, right-click the device and click Acknowledge . |

Using Credentials

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

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

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

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

VMware vCenter, and ESXi devices require VMware credentials to access system performance counters. WhatsConfigured plug-in requires either an SSH or Telnet connection to gather configuration data and to perform various task scripts.

For more information, see *Credentials Library* (on page 836).

Searching for devices

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

To search for a device:

- 1 Click the **Devices** tab, then click **Find Device**. The Find Device dialog appears.
- 2 Enter a device search in the **Find Device** box or click **Search** for advanced search options. Select the device aspect by which you would like to perform the device search; either *Device Display Name*, *Hostname*, *IP Address*, or *All*. If you select to perform a search by *All*, WhatsUp Gold searches for the matching criteria in the device's display name, hostname, and IP address.
- 3 In **For**, enter the device criteria for which WhatsUp Gold will search for a match.



Tip: Select **Exact match** to have WhatsUp Gold search for an exact match of the search criteria you enter in **For**.

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



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

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

- The device's **Display Name**.
- The device's **Hostname**.
- The device's **IP Address**.
- The **Device Group** to which the device belongs. If a device belongs to more than one device group, it is listed multiple times in the list of devices, one time for each group in which it belongs.



Note: Devices are displayed in this list according to a user's group access rights. You must have Group Read rights to at least one group to which a device belongs in order for it to appear in the results list. For more information, see *Group Access and User Rights for the Find feature* (on page 77).

To view a group to which the device belongs:

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

To edit a device configuration:

Select a device from the list, then click **Properties**. The device *Properties* (on page 119) dialog appears.

To delete a device from a group:

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

Understanding group access and user rights for Find Device

Find Device adheres to the group access and user rights assigned to a WhatsUp Gold user account.

User Rights are configured from the Manage Users dialog (click the **Admin** tab, then click **Manage Users**). Group access rights are enabled from the Manage Users dialog, but must be specified from a group's properties. For more information, see Assigning group access rights.

A user account must have Group Read rights to at least one group to which a device belongs in order for it to appear in the results list. Additionally, a user account must have the following rights to perform Find Device's functions:

- An account must have Device Read to edit a device via *Device Properties* (on page 119).
- An account must have both the Group Write and Manage Groups rights to remove a device from a group.
- An account must have both the Device Write and Manage Devices rights to remove a device from WhatsUp Gold.



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

Searching for devices with interface traffic

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

To search for device interface traffic:

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

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

- **Host name.** Displays the full host name of the device.
- **IP address.** Displays the IP address of the device.
- **Domain.** Displays the domain or group to which the device belongs.
- **Country.** Displays the country to which the public IP address of this device is assigned.
- **Last resolved.** Displays the date and time when the last record of the device was recorded on any interface.

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

To view data where the selected host generated the traffic:

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

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

Using Device Groups

In This Chapter

| | |
|--------------------------------------|----|
| Using device groups..... | 79 |
| Creating device groups | 80 |
| Configuring Dynamic Groups | 80 |
| Dynamic Group examples..... | 83 |
| Using the Dynamic Group builder..... | 91 |

Using device groups

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

Device group types

Two types of device groups exist in WhatsUp Gold:





- Non-dynamic groups
- Dynamic groups

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

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

Device group icons

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

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

Device group maps

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

Device group reports

Device groups are particularly important when you are viewing reports pertaining to a specific group, or *group reports* (on page 594). Viewing group reports requires you to select a device group and a monitor to view data for that group. When you create groups, consider ways of easily distinguishing them from one another for this reason. An easy way to distinguish groups is using group names that are meaningful, such as "Atlanta Developers" and "Atlanta Tech Support." As a result, you can easily tell what each device group is when choosing a group on which to view Group Report information.

Device Group Access Rights

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

Creating device groups

To create a new device group:



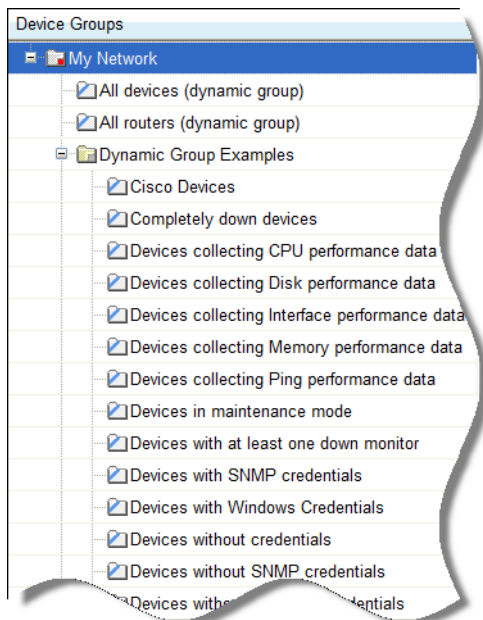
Note: You cannot create a new device group within a dynamic group.

- 1 Click **Devices** tab, then click **New Group**. The Create Group dialog appears.
- 2 Enter a title and short description for the group in the **Group Name** and **Description** fields.
- 3 Click **OK** to add the group to the My Network tree.

Configuring Dynamic Groups

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

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



All of the *Dynamic Group examples* (on page 83) are active, so if you have devices that meet the criteria, you will see the device displayed within the group. In the web interface, the dynamic group display is refreshed every 2 minutes. A group is also refreshed when you select it.

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



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

To configure Dynamic Groups:

- 1 Click the **Devices** tab, then click **New Dynamic Group**. The Create Dynamic Group dialog appears.
- 2 Select a method for configuring the new Dynamic Group. Select **Use the WhatsUp Gold Dynamic Group Builder**, **Use SQL dialog**, or **Create a predefined dynamic group**. If you are an advanced SQL user, select the second option. Otherwise, we recommend selecting the Dynamic Group Builder.

To use the Dynamic Group Builder:

- 1 Enter a name and description for the new dynamic group:
 - **Group Name.** Enter a name for the Dynamic Group as it will appear in the WhatsUp Gold Device List.
 - **Description** (Optional). Enter a short description for the new Dynamic Group. This description is visible to all users who can open the dynamic group.
- 2 In **Filter**, select which groups to search for devices that match the dynamic group criteria.
 - Select **All devices** to show all devices that match the criteria of the dynamic group.
 - Select **All devices in the parent group** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located.
 - Select **All devices in the parent group and its children groups** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located or any of that group's children groups.
- 3 Create and edit rules to form an SQL filter for the Dynamic Group.

To begin writing the rules for your SQL filter, click **Add**. The *Dynamic Group Rule Editor* (on page 315) appears.
- 4 In the Dynamic Group Editor, enter the appropriate information (for more information, see the help topic for this dialog). As you create rules, they are added to the Dynamic Group Builder dialog where you can add more rules, edit, or delete existing rules by clicking the **Add**, **Edit**, or **Delete** buttons.

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

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

Validating your filter code

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

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

Converting your filter code

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

To use the SQL Dynamic Group dialog:

- 1 Enter a **Display name** for the group, enter the group **Description**, and enter an SQL query in the **Filter** box that identifies the devices you want to appear in that group.
- 2 Click **OK** to add the group to the device list. SQL validation occurs as soon as you click **OK**. If the filter fails, an error message appears.

In addition to the pre-configured dynamic groups, we have provided several *sample filters* (on page 83) for you to create some very interesting dynamic groups.

Dynamic Group examples

WhatsUp Gold is pre-configured with dynamic group examples, which you can see in the Devices view, under Device Groups. For more information on these groups, see *Configuring Dynamic Groups* (on page 80).

The following examples show several dynamic group filters that you can use to create some interesting dynamic groups for your devices. To use these examples, select the text of the filter, and then copy and paste the text into the **Filter** box of the *Dynamic Group* (on page 312) dialog.



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

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

```
SELECT DISTINCT Device.nDeviceID
```



```
FROM Device

    JOIN PivotActiveMonitorTypeToDevice

        ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

    JOIN ActiveMonitorStateChangeLog

        ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

            ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

WHERE Device.bRemoved = 0

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

To show all devices with multiple interfaces:

```
SELECT DISTINCT NetworkInterface.nDeviceID

FROM Device

    JOIN NetworkInterface

        ON Device.nDeviceID = NetworkInterface.nDeviceID

WHERE Device.bRemoved = 0

GROUP BY NetworkInterface.nDeviceID

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

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

```
SELECT DISTINCT Device.nDeviceID

FROM Device

    JOIN PivotActiveMonitorTypeToDevice

        ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

    JOIN ActiveMonitorStateChangeLog

        ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

            ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

    JOIN MonitorState

        ON Device.nWorstStateID = MonitorState.nMonitorStateID
```

```
WHERE Device.bRemoved = 0

      AND PivotActiveMonitorTypeToDevice.bDisabled = 0

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

      AND MonitorState.nInternalMonitorState = 1
```

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN ActionActivityLog

      ON Device.nDeviceID = ActionActivityLog.nDeviceID

      JOIN PivotDeviceToGroup

      ON Device.nDeviceID = PivotDeviceToGroup.nDeviceID

      JOIN DeviceGroup

      ON PivotDeviceToGroup.nDeviceGroupID = DeviceGroup.nDeviceGroupID

WHERE  Device.bRemoved = 0

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

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

To show all devices that need acknowledgement:

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN PivotActiveMonitorTypeToDevice

      ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

      JOIN ActiveMonitorStateChangeLog

      ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

      ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

WHERE  Device.bRemoved = 0

      AND ActiveMonitorStateChangeLog.bAcknowledged = 0
```

```
AND PivotActiveMonitorTypeToDevice.bRemoved = 0
```

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

       JOIN PivotStatisticalMonitorTypeToDevice

       ON Device.nDeviceID = PivotStatisticalMonitorTypeToDevice.nDeviceID

       JOIN StatisticalDiskIdentification

       ON PivotStatisticalMonitorTypeToDevice.nPivotStatisticalMonitorTypeToDeviceID =

          StatisticalDiskIdentification.nPivotStatisticalMonitorTypeToDeviceID

       JOIN StatisticalDiskCache

       ON StatisticalDiskIdentification.nStatisticalDiskIdentificationID =

          StatisticalDiskCache.nStatisticalDiskIdentificationID

WHERE  Device.bRemoved = 0

       AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1

       AND StatisticalDiskCache.nDataType = 1

       AND (((nUsed_Avg / nSize) > 0.90)

           AND (NOT nSize = 0

               OR nSize IS

                   NULL))
```

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

       JOIN MonitorState

       ON Device.nWorstStateID = MonitorState.nMonitorStateID

WHERE  Device.bRemoved = 0

       AND MonitorState.nInternalMonitorState IN (1,2)
```

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

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN MonitorState

      ON Device.nWorstStateID = MonitorState.nMonitorStateID

WHERE  Device.bRemoved = 0

      AND MonitorState.nInternalMonitorState = 1

      AND Device.nWorstStateID = Device.nBestStateID
```

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN PivotActiveMonitorTypeToDevice

      ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

      JOIN ActiveMonitorStateChangeLog

      ON PivotActiveMonitorTypeToDevice.nPivotActiveMonitorTypeToDeviceID =

         ActiveMonitorStateChangeLog.nPivotActiveMonitorTypeToDeviceID

      JOIN MonitorState

      ON PivotActiveMonitorTypeToDevice.nMonitorStateID =

         MonitorState.nMonitorStateID

WHERE  Device.bRemoved = 0

      AND PivotActiveMonitorTypeToDevice.bRemoved = 0

      AND PivotActiveMonitorTypeToDevice.bDisabled = 0

      AND MonitorState.nInternalMonitorState = 1

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

      AND Device.nWorstStateId = Device.nBestStateId
```

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN PivotStatisticalMonitorTypeToDevice

      ON Device.nDeviceID = PivotStatisticalMonitorTypeToDevice.nDeviceID

      JOIN StatisticalMonitorType

      ON StatisticalMonitorType.nStatisticalMonitorTypeID =

      PivotStatisticalMonitorTypeToDevice.nStatisticalMonitorTypeID

WHERE  Device.bRemoved = 0

      AND PivotStatisticalMonitorTypeToDevice.bEnabled = 1

      AND StatisticalMonitorType.sStatisticalMonitorTypeName

      LIKE '%Interface Utilization%'
```

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN PivotPassiveMonitorTypeToDevice

      ON Device.nDeviceID = PivotPassiveMonitorTypeToDevice.nDeviceID

      JOIN PassiveMonitorType

      ON PassiveMonitorType.nPassiveMonitorTypeID =

      PivotPassiveMonitorTypeToDevice.nPassiveMonitorTypeID

WHERE  Device.bRemoved = 0

      AND PivotPassiveMonitorTypeToDevice.bRemoved = 0

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

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN PivotActiveMonitorTypeToDevice

      ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

      JOIN ActiveMonitorType

      ON ActiveMonitorType.nActiveMonitorTypeID =

          PivotActiveMonitorTypeToDevice.nActiveMonitorTypeID

WHERE  Device.bRemoved = 0

      AND PivotActiveMonitorTypeToDevice.bRemoved = 0

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

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

```
SELECT DISTINCT Device.nDeviceID

FROM   Device

      JOIN NetworkInterface

      ON Device.nDeviceID = NetworkInterface.nDeviceID

      AND Device.nDefaultNetworkInterfaceID =

          NetworkInterface.nNetworkInterfaceID

      JOIN DeviceType

      ON Device.nDeviceTypeID = DeviceType.nDeviceTypeID

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

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

      OR NetworkInterface.sNetworkAddress LIKE '%1.2.3.4%')

      AND Device.bRemoved = 0
```

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



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

```
SELECT DISTINCT Device.nDeviceID

FROM Device

JOIN ActionPolicy

ON Device.nActionPolicyID = ActionPolicy.nActionPolicyID

JOIN PivotActionTypeToActionPolicy

ON ActionPolicy.nActionPolicyID =

PivotActionTypeToActionPolicy.nActionPolicyID

JOIN ActionType

ON PivotActionTypeToActionPolicy.nActionTypeID =

ActionType.nActionTypeID

WHERE Device.bRemoved = 0

AND ActionType.sActionTypeName LIKE '%Critical%'

UNION

SELECT DISTINCT Device.nDeviceID

FROM Device

JOIN PivotActiveMonitorTypeToDevice

ON Device.nDeviceID = PivotActiveMonitorTypeToDevice.nDeviceID

JOIN ActionPolicy

ON PivotActiveMonitorTypeToDevice.nActionPolicyID =

ActionPolicy.nActionPolicyID

JOIN PivotActionTypeToActionPolicy

ON ActionPolicy.nActionPolicyID =

PivotActionTypeToActionPolicy.nActionPolicyID
```

```
JOIN ActionType

ON PivotActionTypeToActionPolicy.nActionTypeID =

ActionType.nActionTypeID

WHERE Device.bRemoved = 0

AND PivotActiveMonitorTypeToDevice.bRemoved = 0

AND ActionType.sActionTypeName LIKE '%Critical%'

UNION

SELECT DISTINCT Device.nDeviceID

FROM Device

JOIN ActionPolicy

ON ActionPolicy.nActionPolicyID=0 and bGlobalActionPolicy=1

JOIN PivotActionTypeToActionPolicy P

ON P.nActionPolicyID = ActionPolicy.nActionPolicyID

JOIN [ActionType]

ON P.nActionTypeID = ActionType.nActionTypeID

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

Using the Dynamic Group builder

To create a dynamic group using Dynamic Group Builder:

- 1 Click the **Devices** tab.
- 2 Click **New Dynamic Group**.
- 3 Select **Use the Dynamic Group builder**, and click **OK**.
- 4 Enter a name and description for the new dynamic group:
 - **Group Name.** Enter a name for the Dynamic Group as it will appear in the WhatsUp Gold Device List.
 - **Description** (Optional). Enter a short description for the new Dynamic Group. This description is visible to all users who can open the dynamic group.

- 5 In **Filter**, select which groups to search for devices that match the dynamic group criteria.
 - Select **All devices** to show all devices that match the criteria of the dynamic group.
 - Select **All devices in the parent group** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located.
 - Select **All devices in the parent group and its children groups** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located or any of that group's children groups.
- 6 Create and edit rules to form an SQL filter for the Dynamic Group.

To begin writing the rules for your SQL filter, click **Add**. The *Dynamic Group Editor* (on page 315) appears.
- 7 In the Dynamic Group Editor, enter the appropriate information (for more information, see the help topic for this dialog). As you create rules, they are added to the Dynamic Group Builder dialog where you can add more rules, edit, or delete existing rules by clicking the **Add**, **Edit**, or **Delete** buttons.

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

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

Validating your filter code

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

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

Converting your filter code

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

Using Maps

In This Chapter

| | |
|--|----|
| Using the Map View..... | 93 |
| About Map View device limitations..... | 95 |

Using the Map View

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

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

To access Map Views:

Access the WhatsUp Gold web interface Map View from the Devices tab > **Map View**.

- or -

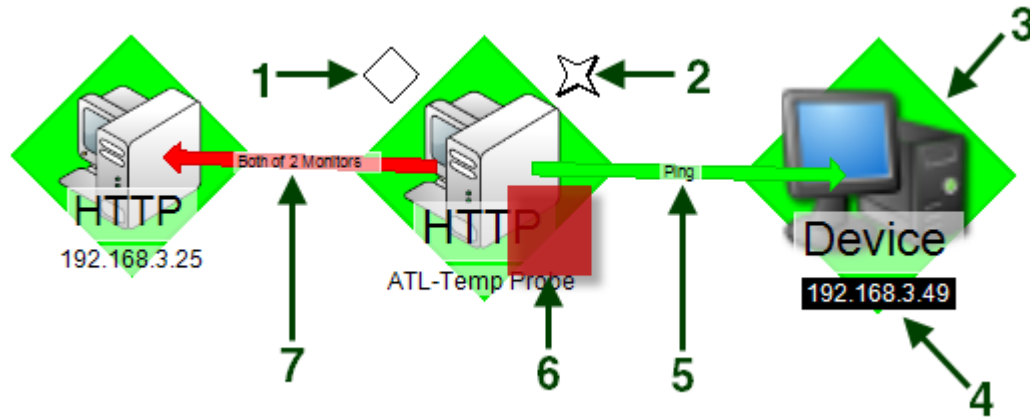
Access the WhatsUp Gold console Map View from **View > Map View**.

Interpreting the Map View

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

Graphical Indicators

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



- 1 **Passive monitor indicator.** A diamond shape at the upper left of the device icon, displays the state of the passive monitors associated with the device.
- 2 **SNMP indicator.** A four pointed star located at the upper right of the device icon, is present when the device has SNMP credentials stored in the Credentials Library.



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

- 3 **Device state indicator.** The background color and shape directly behind the device icon, provides an indication of the state of the device as determined by the active monitors monitoring the device.
- 4 **Device status change indicator.** A reverse of the normal background and foreground, indicates that the device has undergone a state change that has not yet been acknowledged.
- 5 **Up dependency indicator.** A green arrow that originates at the dependent device and terminates at the device on which it dependent. The active monitors on which the device is dependent are displayed on the arrow.
- 6 **Active monitor indicator.** A square located at the lower right of the device icon, indicates the state of the active monitors associated with the device. If the indicator is green, there is a recent Up state change in an active monitor. If the indicator is red, there is a recent Down state change in an active monitor.
- 7 **Down dependency indicator.** A red arrow that originates at the dependent device and terminates at the device on which it dependent. The active monitors on which the device is dependent are displayed on the arrow.

Annotations

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

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

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



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

About Map View device limitations

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



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

To change map device limitations:

- 1 Locate the registry key which controls this setting.
 - For 32-bit operating systems, open
HKEY_LOCAL_MACHINE\Software\Ipswitch\Network Monitor\WhatsUp Gold\Settings.
 - For 64-bit operating systems, open
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ipswitch\Network Monitor\WhatsUp Gold\Settings

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



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

Managing devices

In This Chapter

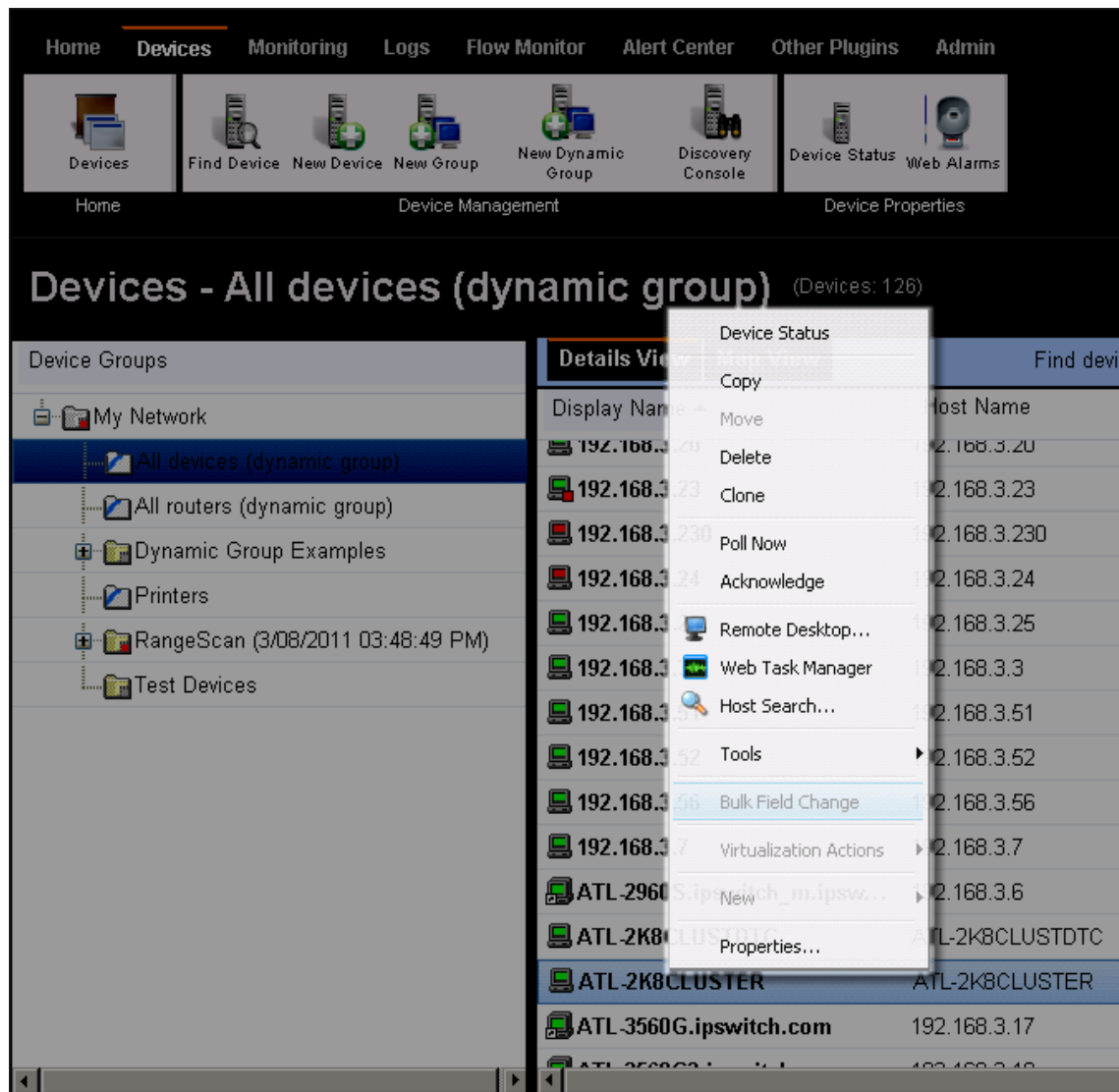
Learning about devices..... 97

Learning about devices

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

To view the Details View right-click menu:

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



Adding a single new device to WhatsUp Gold

There are two ways to add devices to WhatsUp Gold:

- Discover devices automatically. For more information, see *Learning about the Discovery Console* (on page 47)
- Manually add individual devices.

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

To add a single device to WhatsUp Gold:

- 1 Click **Devices > New Device**. The Add New Device dialog appears.
- 2 Type the **IP address or host name of the new device**.
- 3 If you want to add a device without scanning for additional device information, select **Add device immediately without scanning**. The new device is generically categorized as a workstation.
- 4 If you want to apply a device role to a new device, select **Force device role**. For more information, see *Using Device Roles* (on page 62).
- 5 Click **Advanced** to select a number of additional options for which to scan the device. You can select additional options to resolve the device host name, use advanced SNMP and ping timeout and retry settings. Additionally, select SNMP, SSH, WMI or VMware credentials for the new device. For more information, see *Setting Advanced single device discovery settings* (on page 99).
- 6 Click **OK** to save changes. WhatsUp Gold attempts to resolve the IP address or hostname, then scans that device for device roles (if selected). When the scan is complete, Device Properties dialog appears, allowing you to further configure the device as needed.



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

Setting Advanced device discovery settings

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

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



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

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



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

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



Tip: Click the browse (...) button in the console or the **Credentials** button in the web interface to open the WhatsUp Gold Credentials Library to configure a new set of credentials to use for discovery.



Tip: Credentials are configured in the Credentials Library. When a device is discovered using a credential, that credential is then associated to that device. You can change this on **Device Properties > Credentials**. If you select **All**, discovery uses all configured credentials in the Credentials Library. The credential that is successful is then associated with the device.

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

Changing a device name

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

To change a device name:

- 1 Click the **Devices** tab.
- 2 Click **Devices**.
- 3 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 4 Click **General**.
- 5 In the General section of Device Properties, enter the new name in the **Display Name** box.
- 6 Click **OK** to save changes.

Changing a device IP address

To change a device IP address:

- 1 Click the **Devices** tab.
- 2 Click **Devices**.
- 3 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 4 Click **General**.
- 5 Type the new IP address in the **Address** box.
- 6 Click **OK** to save changes.

Adding additional network interfaces to a device

To configure a network interface:

- 1 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- or -
From any page where a device is selected using the device picker, click **Properties** in the title bar.
- 2 Click **General**. The General dialog appears.
- 3 Click **Additional Network Interfaces**. The Network Interfaces dialog appears.
- 4 Click **Add**. The Add Network Interface dialog appears.
- 5 Enter the network information for the new interface.
- 6 Click **OK** to save the new interface information and return to the General section.

To change the default network interface on a device:

- 1 In the General section of Device Properties, click **Additional Network Interfaces**.
- 2 On the Network Interfaces dialog, select the interface you want to make the default.
- 3 Click **Set Default**.
- 4 Click **OK** to return to the General section.

Adding notes to a device

To add a note to a device:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
Click **Notes**. The Notes dialog opens.
- 2 Enter the note in the **Notes** box.
Use the Notes box to include information about the selected device. For example, you can record historical information about a device, physical location information, or notes relating to the actions configured for the device.



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

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

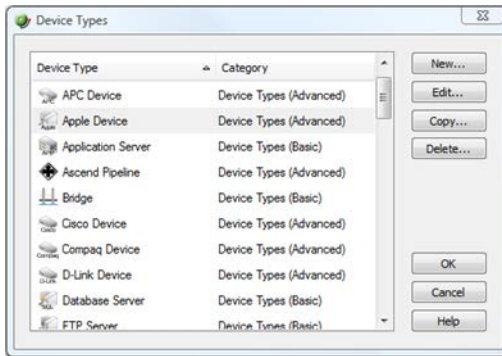
Using device types



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

The Device Types dialogs now have limited functionality. Active monitors, passive monitors, and action policies are no longer editable in the Device Type dialog. The device General and Menu Items information is editable. For more information, see *Discovering and Viewing Network Data* (on page 47).

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



To configure device types (WhatsUp Gold console only):

- 1 Open the Device Types Library:

In either Device View or Map View, select **Configure > Device Types**. The Device Types Library dialog appears.
- 2 In the Device Type Library, do one of the following:
 - Click **New** to configure a new device type.
 - Select a device type, then click **Edit** to reconfigure the selected device type.
 - Select a device type, then click **Copy** to make a duplicate of the selected device type.
 - Select a device type, then click **Delete** to remove it from the Device Type Library.
- 3 Click **OK** to save changes.

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

- 1 In Map View, right-click a device. The right-click menu appears.
- 2 Select a device in the device list, then right-click and select **Properties**. The Device Properties dialog appears.
- 3 Click General. The General Properties appear.

- 4 Select a new **Device Type** from the list on the right side of the dialog.
- 5 Click **OK** to save changes.
- 6 The device's type and coinciding icon updates on the map.

Copying a device

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

To copy a device:

- 1 From the WhatsUp Gold web interface, in the Details View or Map View, right-click the device for which you want to copy. The right-click menu appears.
- 2 Click **Copy**. The Select a Device Group dialog appears.
- 3 Select the group that you want to copy the device into, then click **OK**. The group that you copied the device to opens.



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

Moving a device

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

To move a device:

- 1 From the WhatsUp Gold web interface, in the Details View or Map View, right-click the device for which you want to move. The right-click menu appears.
- 2 Click **Move**. The Select a Device Group dialog appears.
- 3 Select the group that you want to move the device into, then click **OK**. The group that you copied the device to opens.



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

Deleting a device

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

To remove a device:

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

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

Cloning a device

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



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

Methods to clone a device

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

After you have cloned a device, you need to change the device host name and address in the Device Properties - General dialog settings so that WhatsUp Gold can monitor the new device and all of the active monitors, passive monitors, actions, and attributes that are applied to the new device. For more information, see *Changing the cloned Device Properties* (on page 105).

To clone a device:

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



Note: The new cloned device display name is as shown in the following device name example:

- Original name: Device-WHO
- First clone (in new group): Device-WHO
- Second clone: Device-WHO - Clone
- Third clone: Device-WHO - Clone (2)
- Subsequent clones: Device-WHO - Clone (nnn)



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

- 5 Change the cloned device properties as required. For more information, see *Changing the cloned Device Properties* (on page 105).

Cloning a device using drag-n-drop

To clone a device using drag-n-drop:

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



Note: The new cloned device display name is as shown in the following device name example:

- Original name: Device-WHO
- First clone (in new group): Device-WHO
- Second clone: Device-WHO - Clone
- Third clone: Device-WHO - Clone (2)
- Subsequent clones: Device-WHO - Clone (nm)



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

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

Changing the cloned Device Properties

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

To change the cloned Device Properties:

- 1 From the group where the new cloned device resides, right-click the device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **General**. The General dialog opens.
- 3 Enter the new device **Host name**, **Address**, and other information you want to change for this device, then click **OK**.

Polling overview

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

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

Changing how you poll devices

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

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

To change how you poll a device:

- 1 Click the **Devices** tab.
- 2 Click **Devices**. The device list appears.
- 3 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 4 Click **General**.
- 5 Select the protocol used to poll the device from the **Polling type** list.
- 6 Select **IP address** or **Host name** from the **Poll using** list.
- 7 If you selected Host name in the **Poll using** list, enter the device host name the **Host name** box.
- 8 Click **OK** to save changes.

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

Using Maintenance mode

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



Details View



Map View

To put a device into maintenance mode:

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

Changing the device polling frequency

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

To change the polling frequency for a device:

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

Stopping and starting monitor polling

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

- 1 Click the **Devices** tab.
- 2 Click **Devices**. The device list appears.

- 3 In the Details View or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 4 Click **Active Monitors**. The Active Monitors page appears.
- 5 Double-click the Active Monitor with the polling setting you want to change. The Active Monitor Properties dialog appears.
- 6 Change the polling status of the monitor:
Select **Enable polling for this active monitor** to start polling.
- or -
Clear **Enable polling for this active monitor** to stop polling.
- 7 Click **OK** to save changes.



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

Dependencies overview

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

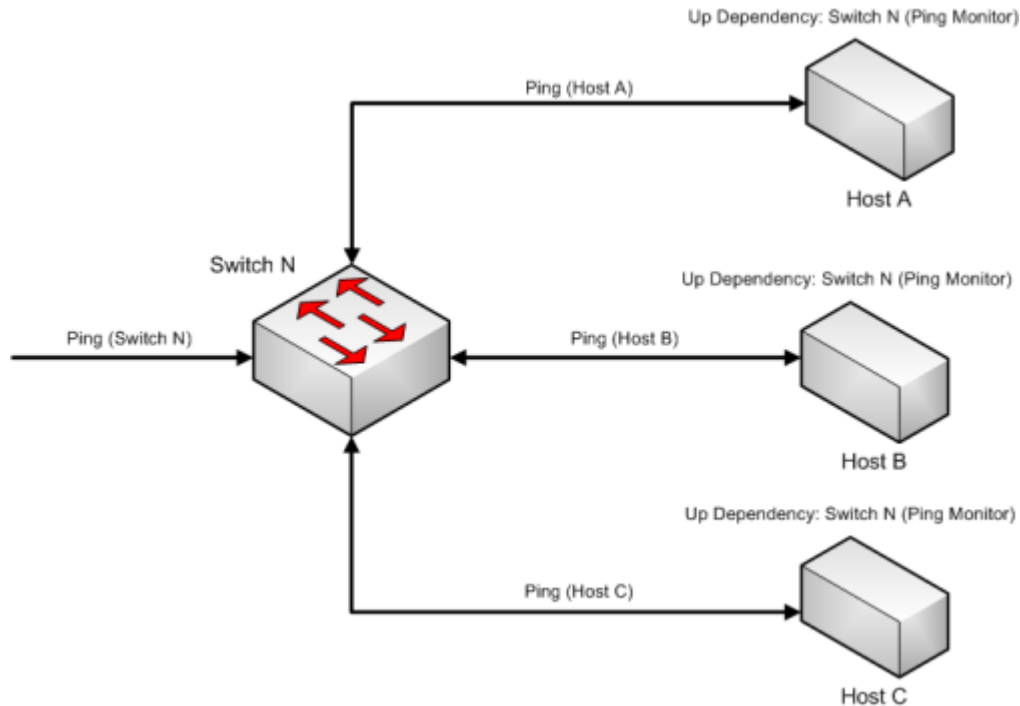
Up Dependencies

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

Example

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

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

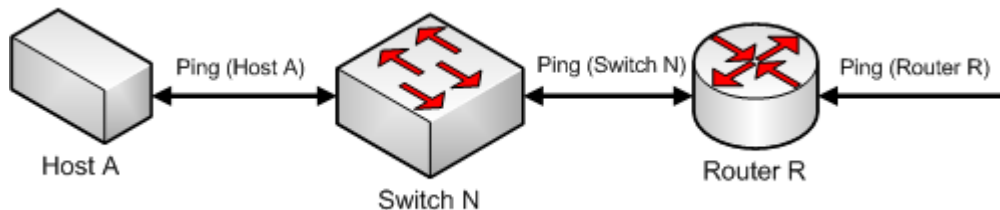


Down Dependencies

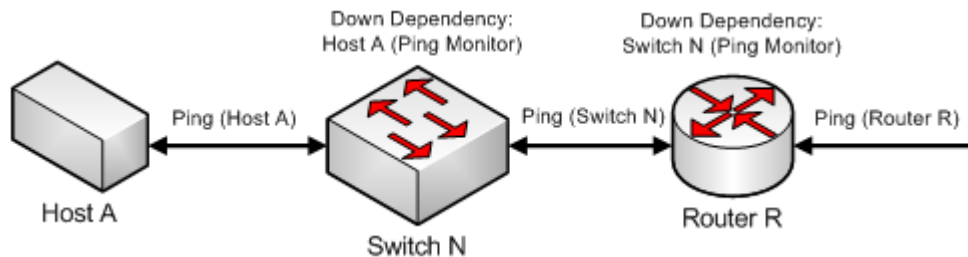
A down dependency establishes a rule so that a device is polled only if the selected active monitors on a second device are in the down state. The device can be thought of as something is "in front of" the device to which it has a dependency. The dependant devices in front will not be polled unless the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

Example

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



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



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

Down dependencies and the "assumed up" state

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

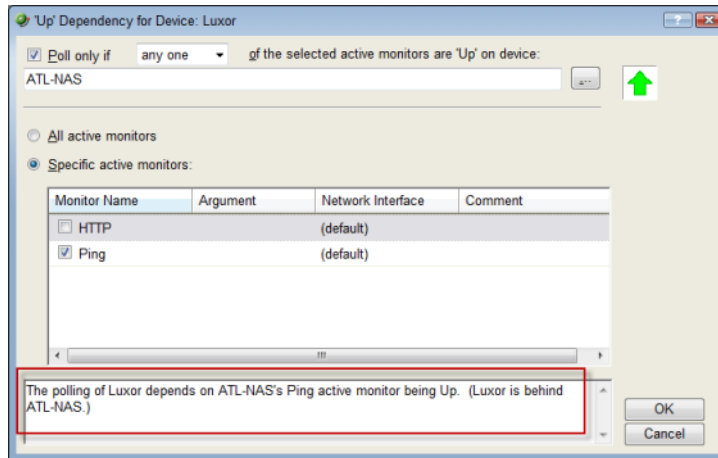
This condition occurs when the dependent device is in an inactive state, and is able to respond to an echo request from a ping of the device. Because of the down dependency, the dependent device is not being polled and is "assumed up", yet the actual state of the monitored service or process is unknown,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

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

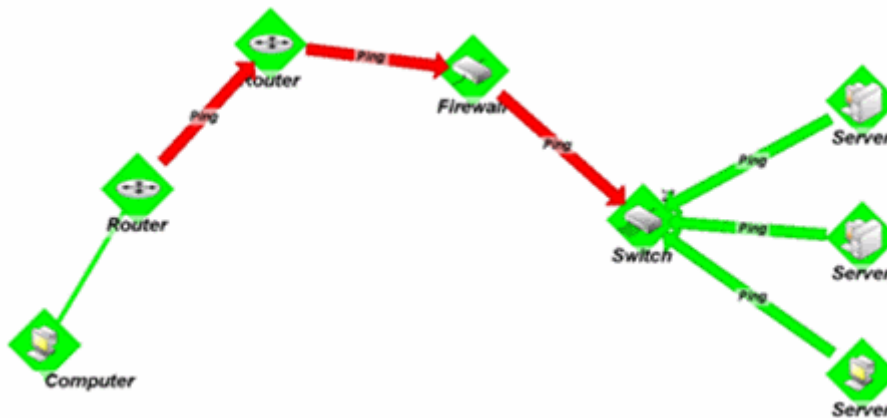
Reading dependencies

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

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



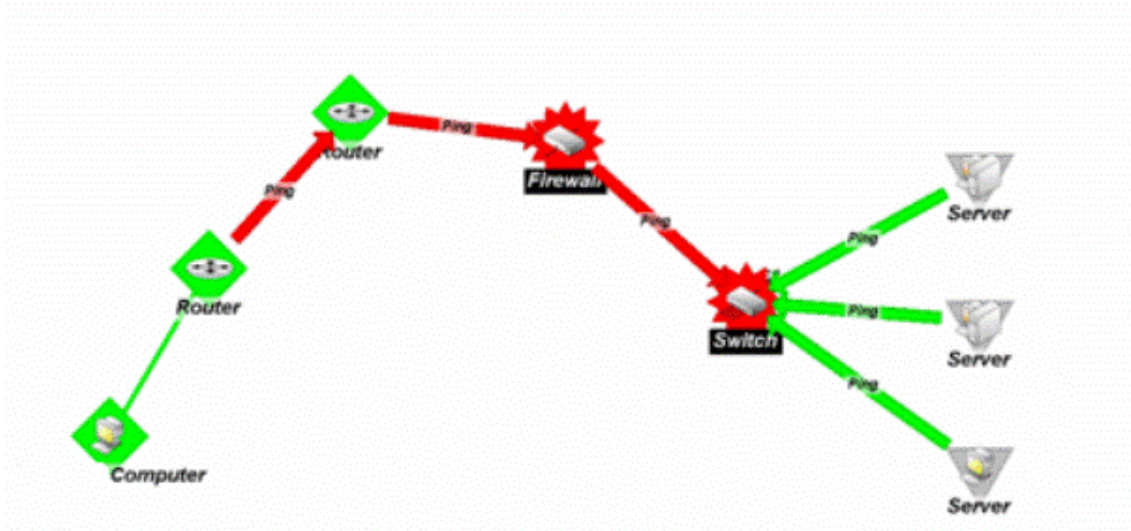
- 2 Read the dependency arrows in the Map View.



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

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

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



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

Setting Dependencies

There are two ways to set dependencies in WhatsUp Gold:

- Using Device Properties
- Using the Map View

To set dependencies in the Device Properties:

- 1 Go to the properties for a device:
 - On the console, from Device View, double-click a device.
 - On the web interface, click the **Devices** tab, then double-click a device. The Device Status Dashboard for that device appears. Click the **Properties** button. The Device Properties dialog appears.
- 2 Click **Polling**. The Polling, Maintenance, and Dependencies dialog appears.
- 3 Click either the **Up Dependency...** or the **Down Dependency...** button to bring up the appropriate Device Dependencies dialog, and to configure the up or down dependency.

To set dependencies in the Map View:

- 1 Go to Map View:
 - In the console, click the **Map View** tab. Map View appears.
- 2 Right-click a device, select **Set Dependencies**, then select either **Set Up Dependency on** or **Set Down Dependency on**. The cursor changes to the Set Dependency arrow.



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



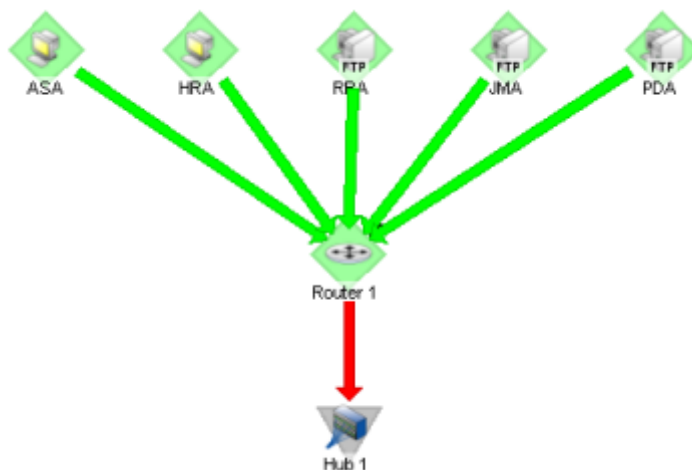
Note: You cannot set a dependency across groups. However, you can make shortcuts to the devices you want to set a dependency on in a group, then set the dependency to the shortcut.



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

Viewing Dependencies

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

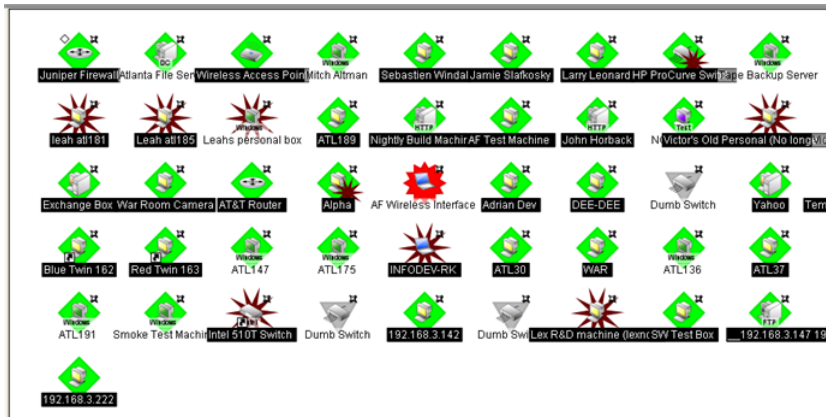


In the example above, the devices have an up dependency on the router, and the router has a down dependency on the hub. If the router's active monitors fail, the hub would be polled,

and the devices behind the router would not be polled. When the router's active monitors are successful, the hub is not polled, but the devices behind the router are.

Using Acknowledgements

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



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



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

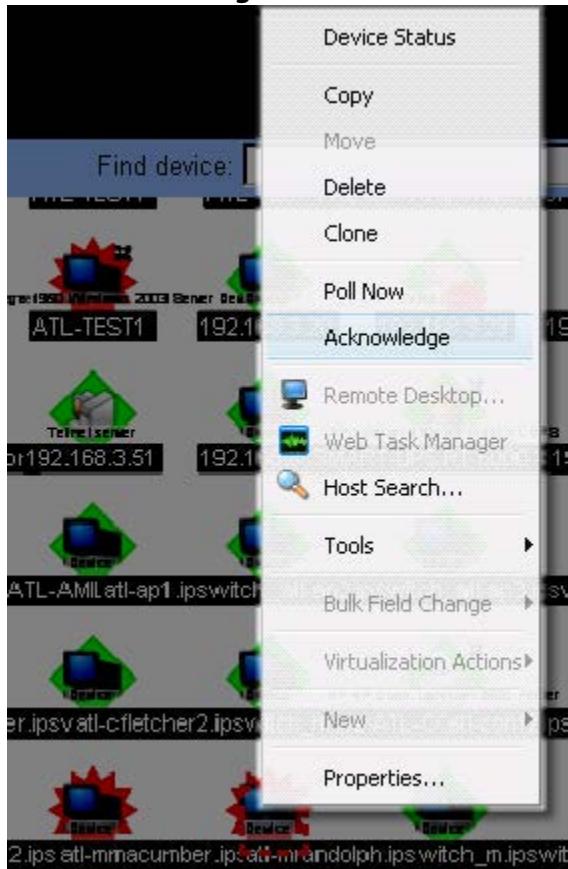
Acknowledging a State Change

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

To acknowledge a state change:

- 1 Click the **Devices** tab.
- 2 Click **Devices**. The device list appears.
- 3 In either the Details View or the Map View, right-click the device you want to acknowledge.

- 4 Select **Acknowledge** from the menu.



The device state change is acknowledged. The device is removed from the State Change Acknowledgement monitor report.

Accessing a remote desktop to view and manage devices

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

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



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

To connect to a remote desktop:

- 1 Click the **Device** tab, then click **Devices**. The Device page appears.
- 2 From the Details or Map View, right-click a device, then click **Remote Desktop**. The Remote Desktop Connection dialog appears.

- 3 Log in to the remote device to manage as needed.

Configuring multiple devices with the Bulk Field Change feature

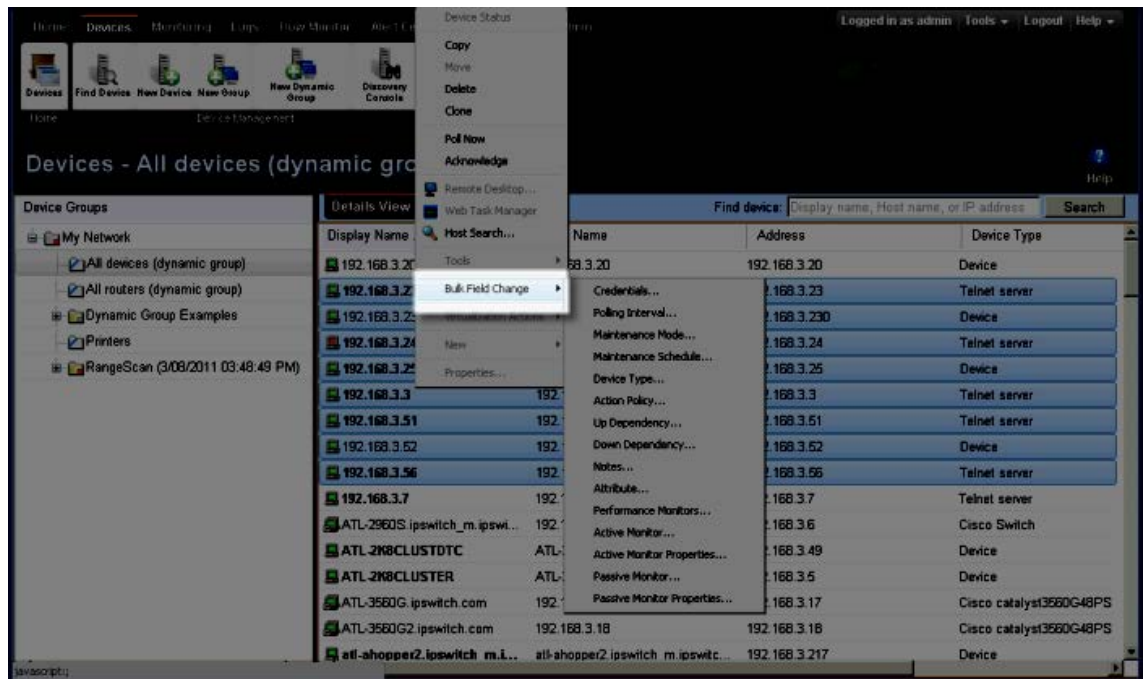
The Bulk Field Change feature gives you the ability to make changes to multiple devices and device groups. You must have administrative privileges to the devices or device groups that you want to make changes to.

To edit multiple devices:

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



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



- 2 Select the field you want to change. The following items can be modified through Bulk Field Change.
 - Credentials
 - Polling Interval
 - Maintenance Mode
 - Maintenance Schedule (web interface only)
 - Device Type
 - Action Policy
 - Up Dependency
 - Down Dependency

- Notes
 - Attribute
 - Performance Monitors
 - Active Monitor
 - Active Monitor Properties
 - Passive Monitor (web interface only)
 - Passive Monitor Properties (web interface only)
- 3 Enter the configuration information you want set. Refer to the help for more information on configuration options.
 - 4 Click **OK** to save changes.

Understanding Web Alarms

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

Managing a Web Alarm action:

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

Managing a Web Alarm:

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

To disable Web Alarms:

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



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



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



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

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

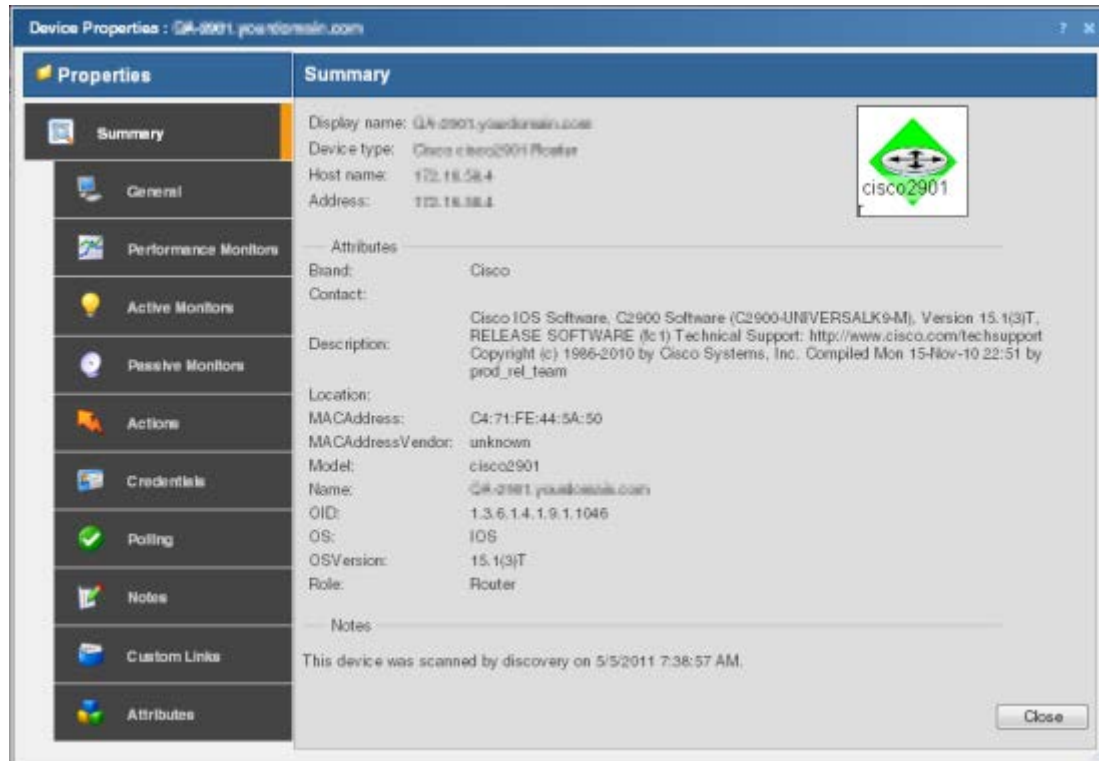
Using Device Properties

In This Chapter

| | |
|---|-----|
| Working with Device Properties | 119 |
| Using Device Properties - Summary | 120 |
| Using Device Properties - General..... | 121 |
| Device Properties - Performance Monitors | 121 |
| Using Device Properties - Active Monitors..... | 123 |
| Using Device Properties - Passive Monitors..... | 123 |
| Using Device Properties - Actions | 123 |
| Using Device Properties - Credentials..... | 124 |
| Using Device Properties - Polling | 125 |
| Using Device Properties - Virtualization..... | 126 |
| Using Device Properties - Notes..... | 127 |
| Using Device Properties - Custom Links..... | 127 |
| Using Device Properties - Attributes | 128 |
| Using the DeviceIdentifier attribute | 128 |
| Using Device Property - Menus | 129 |
| Using WhatsConfigured Device Properties - Tasks | 130 |

Working with Device Properties

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



To access device properties for a device:

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

The Device Properties dialog includes the following features:

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

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

Using Device Properties - Summary

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

The following Summary items are configured in the General tab:

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

The following items are gathered from MIBs on the device. If SNMP is not enabled on the device, then values for these items are not displayed.

- **Brand**
- **Contact**
- **Description**
- **Location**
- **MACAddress**
- **MACAddressVendor**
- **Model**
- **Name**
- **OID**
- **OS**
- **OSVersion**
- **Role**

Using Device Properties - General

The General section of the Device Properties dialog box provides, and lets you modify, basic information for the selected device.

- **Display name.** An identifying name for the current device. This name is populated during discovery, but can be changed by the user at any time. Changing the name will not change how the device is polled, only how it is displayed in WhatsUp Gold.
- **Polling type.** Select the type of polling you want WhatsUp Gold to use for this device.
 - ICMP (TCP/UDP)
 - IPX
 - NetBIOS



Note: If NetBIOS is selected, the Host Name box must contain a valid NetBIOS name. If IPX is selected, the Address box must contain a valid IPX address. If NetBIOS or IPX is selected, you cannot monitor TCP/IP services on this device.

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

Device Properties - Performance Monitors

Use Performance Monitors dialog to configure and manage performance monitors for the selected device. For more information, see *Using Performance Monitors* (on page 246).



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

- **Enable global performance monitors.** Select options in this list to enable monitors. The following monitors are populated by entries in the *Performance Monitor Library* (on page 247), but cannot be edited or changed from their default settings. These monitors are ready to be added to devices.
- **CPU Utilization.** Monitors the CPU utilization on the selected device.

- **Disk Utilization.** Monitors the available disk space for the selected device.
- **Interface Utilization.** Monitors all interfaces on the selected device.
- **Memory Utilization.** Monitors memory utilization on the selected device.
- **Ping Latency and Availability.** Monitors how often and quickly the device responds to a Ping check.

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

- CPU - All
- Disk - All
- Interface - All, Default, or Specific
- Memory - All
- Ping - All

For example, if you have multiple CPUs running on the device, WhatsUp Gold gathers statistics on all of them by default.

- **Configure.** Click to configure additional data stream options for the global performance monitor.



Note: If an error occurs, a warning message appears directing you to the problem. If it is a timeout error, you are prompted to open the Advanced dialog to change the **Timeout** value. For any other error, you are returned to this dialog.

- **Library.** Click for options to create (**New**), **Edit**, **Copy**, or **Delete** performance monitor library items to use on all devices.
- **Enable individual performance monitors (for this device only).** Use this section of the dialog to add customized APC UPS, Printer, Active Script, SNMP, or WMI performance monitors to only be used on this device. The monitors added here do not appear in the Performance Monitor Library, and cannot be used on other devices unless it is manually created for that device.
- Click **New** to configure a new monitor.
- Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.
- Select a performance monitor type, then click **Delete** to remove it from the list.

For information on the Active Script Performance Monitor, see *Adding and Editing an Active Script Monitor* (on page 226).



Note: If you are attempting to monitor a Cisco device with either the CPU or Memory Performance Monitors, the Cisco device must support Cisco IOS 12.2(3.5) or later.

Using Device Properties - Active Monitors

Use the Active Monitors dialog to display and manage Active Monitors for this device. For more information, see *Using Active Monitors* (on page 155).

To add an active monitor to this list:

- Click **Add** to configure a new active monitor. Use the wizard to select active monitor settings.
- Select an active monitor, then click **Edit** to change the configuration.
- or -
Double-click an active monitor to edit the configuration.
- Select an active monitor, then click **Disable** to disable the monitor on the device.
- Select an active monitor, then click **Enable** to enable the monitor on the device.
- Select an active monitor, then click **Remove** to remove the monitor from the device.
- Click **Configure** to select critical monitors for this device and set their polling order.

Using Device Properties - Passive Monitors

Some measurable network conditions occur at intervals instead of providing an up or down status. For example, an application may log a message to the system Event log (such as an antivirus application alerting when a virus is found). Because these types of messages or events can occur at any time, a Passive Monitor Listener listens for them, and notifies WhatsUp Gold when they occur. For more information, see *Using Passive Monitors* (on page 232).

This dialog displays all Passive Monitors configured for this device.

- Click **Add** to configure a new Passive Monitor.
- Select a Passive Monitor, then click **Edit** to change the configuration
- or -
Double-click a Passive Monitor to edit the configuration.
- Select a Passive Monitor, then click **Remove** to remove the monitor from the device.

Using Device Properties - Actions

You can select an Action Policy to use on this device or configure alerts specifically for this device. For more information, see *About actions* (on page 271).

Select a policy from the **Apply this Action policy** list. You can also create a new, or edit an existing action policy by clicking browse (...) next to the list.

Configured alerts appear in the **Apply individual actions** list, displaying the action type that is to be fired and the state change that will trigger the action. You may have multiple actions on a single device.

This dialog displays all Actions configured for this device.

- Click **Add** to configure a new Action.
- Select an Action, then click **Edit** to change the configuration
- or -
Double-click an Action to edit the configuration.
- Select an Action, then click **Remove** to remove the action from the device. Removing the action from the list also deletes all records for this action (on this device) from the Action Log.

Using Device Properties - Credentials

The Credentials dialog displays **SNMP, Windows, ADO, Telnet, SSH, and VMware credentials** information for the current device.

In the Device Dashboard Map View, devices that are SNMP-manageable devices appear on the map view with an icon with a white star in the top right corner.



Credentials

- **SNMP v1/v2/v3.** Select the SNMP credentials to connect to this device. If the Identify devices via SNMP option was selected during discovery (or if an SNMP discovery was performed) the correct SNMP credential was used during the discovery process, and if the device is an SNMP manageable device, then the correct credential is selected automatically. If any of these conditions are not met, None is selected.
- **Windows.** Select the Windows credential to connect to this device. Click browse (...) to browse the Credentials Library.
- **ADO.** Select the ADO credentials for database connection string information to be used when a database connection is required for WhatsUp Gold database monitors.
- **Telnet.** If you use WhatsConfigured, Telnet credentials may be used to connect and run command-line interface (CLI) commands with WhatsConfigured tasks.
- **SSH.** Select SSH credentials to connect with remote devices that WhatsUp Gold monitors with SSH monitors. Also, if you use WhatsConfigured, SSH credentials may be used to connect and run command-line interface (CLI) commands with WhatsConfigured tasks. WhatsConfigured uses SSH as default credentials, then will attempt to use Telnet credentials when SSH credentials are not available.
- **VMware.** Select the VMware credentials to be used when connecting to a VMware host or vCenter server.
- **Edit.** Click to open the Select Credentials dialog, then select the credential from the list or click browse (...) to browse the Credentials Library.

- **Device Object ID (OID).** Enter the SNMP object identifier for the device. This identifier is used to access a device and read SNMP data available for the device.

For more information, see *Using credentials* (on page 75).

Using Device Properties - Polling

About polling

Polling is the term used for monitoring discovered devices in WhatsUp Gold. Polling can occur in several ways, depending on the monitors configured for network devices. The default polling method uses Internet Control Message Protocol (ICMP). The default polling interval for WhatsUp Gold is 60 seconds.

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

The Polling dialog

The Polling dialog lets you configure polling options and/or schedule maintenance times for the selected device.

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



Note: Polling dependencies & blackouts only apply to the collection of device active monitors.

- **Up dependency.** Click to configure additional options, based on when another device is operational, that determine when the selected device is polled.
- **Down dependency.** Click to configure additional options, based on when the selected device is not operational, that determine when other devices are polled.

Maintenance

Use this section of the dialog to manually set the device Maintenance state, or schedule the maintenance state for a certain time period. Any device placed in Maintenance mode will not be polled, actions will not be triggered, and logging activity is disabled, but it remains in the device list with an identifying icon. By default, the maintenance state is represented by an orange background color.

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

- Select an entry, then click **Edit** to change a scheduled time.
- or -
Double-click a Schedule to edit its configuration.
- Select an entry, then click **Remove** to delete a scheduled time.

For more information, see *Polling overview* (on page 106) and *Dependencies overview* (on page 108).

Using Device Properties - Virtualization

The Virtualization dialog allows for the identification of vCenter servers, VMware hosts, and provides a list of the virtual devices associated with the VMware server. You can use this dialog to identify the virtualization component, and associate virtual devices with the component. Also, if the device is a vCenter server you can control event collection and select the event types you want to receive from the server.

Role selection

During discovery, the most likely role for the virtual device is determined and the result is displayed in the role selection area of the Virtualization tab. You can manually define the role of the VMware server by choosing one of the following options:

- **This device is not a VMware server.** Select this option if the device being configured is not a VMware host or vCenter server.
- **This device is a VMware host.** Select this option if the device being configured is a VMware host.
- **This device is a VMware vCenter.** Select this option if the device being configured is a vCenter server.

Event collection configuration

If the virtual device you are configuring is a vCenter server, a Configure event collection button appears in the dialog which provides the the option to configure event collection.



Note: To collect events, the WhatsVirtual event listener must be configured to listen for events from the vCenter. From the WhatsUp Gold console click **Configure > Program Options > General** dialog to configure WhatsVirtual to listen for events.

Click **Configure event collection** to open the **Configure VMware event listener** dialog and select the event types you want to collect for the vCenter server.



Note: The current status of the Virtualization event listener is displayed beside the **Configure event collection** button.

Virtual devices managed by this VMware server

The virtual devices managed by VMware server list provides the following information about each virtual device.

- **Device name.** The name of the device as it appears in the **Display name** box of the General dialog of the Device Properties menu.
- **Device IP address.** The IP address of the virtual machine.
- **Virtual machine VMware name.** The name of the virtual machine within the VMware system.

Click **Add** to manually add a virtual machine to the list of virtual devices hosted on the VMware server. The Associate WUG device to a virtual machine dialog appears.

Select a virtual device from the list and click **Remove** to remove the device from the list of virtual devices managed by the VMware server.

Click **OK** to accept the virtualization settings, otherwise click **Cancel** to discard any changes you have made.

Using Device Properties - Notes

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

Notes. The first line of the Notes box displays the time and date when WhatsUp Gold added the device to the database.

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

Using Device Properties - Custom Links

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

To view custom links created for a device, you need to add the Device Custom Links dashboard report to its Device Status dashboard view. For more information, see *Adding dashboard reports to a dashboard view* (on page 342).

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

- or -

Double-click a custom link to edit its configuration.

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

Using Device Properties - Attributes

The Attributes dialog lists information about the associated device, such as contact person, location, serial number, etc. The first three attributes in the list (Contact, Description, and Location) are added by WhatsUp Gold when the device is added to the database, either by the Device Discovery wizard, or through another means.

To add attributes to a device:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- or -
From any page where a device is selected using the device picker, click **Properties** in the title bar.
- 2 Click **Attributes**. The Attributes dialog appears.
- 3 Use the following options:
 - Click **Add** to add a new device attribute. The Add Attribute dialog appears.



Note: When you add or edit an attribute, ensure **Attribute name** does not contain a space. For example, use Phone_Number as an attribute name, instead of Phone Number. WhatsUp Gold returns an 'No Such Attribute' error when an attribute variable such as `%Device.attribute.[attribute_name]` is used in a message and the attribute name contains a space.

- Select a device attribute in the list, then click **Edit** to change the settings.
 - Select a device attribute in the list, then click **Remove** to remove it from the list.
- 4 Enter information in the **Attribute name** and **Attribute value** boxes.
 - 5 Click **OK** to save changes.

Using the DeviceIdentifier attribute

When a Beeper Action fires, it looks for and returns a device attribute called DeviceIdentifier. You can add this attribute to a device via its Properties (**Device Properties > Attributes**).

If the Beeper Action does not find the DeviceIdentifier in a device's attributes, WhatsUp Gold uses the last two octets of the IP address to identify the device. For example, a numeric message is sent to a beeper when a device returns to the up state after being down:

0-149-238

The first digit is the number configured in the Up, Down, or passive monitor code, the second two sets of numbers identify the device using the last two octets of the device's IP address.

To configure a DeviceIdentifier attribute for a device:

- 1 Open the device's Properties:
 - Right-click a device, then click **Properties**. The Device Properties dialog appears.
 - Click **Attributes**. The Attributes dialog appears.
- 2 Click **Add**. The Add Attribute dialog appears.
- 3 In **Attribute name**, enter DeviceIdentifier.
- 4 In **Attribute value**, enter the desired numeric value.



Note: The DeviceIdentifier attribute value should contain only numeric characters or the asterisk (*); alphabet characters, spaces, and other special characters are not recognized by the Beeper Action.

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

Using Device Property - Menus

In the WhatsUp Gold console, you can use the Menu dialog to create a custom context menu for a device. Context menus are custom menu items that appear when you right-click a device; they serve as *shortcuts* to launch applications.

The menu item can launch programs based on the command line you enter. You can also append command line arguments, including *WhatsUp Gold percent variable arguments* (on page 293) to include device IP address, device host name, and other types of percent variable arguments. When you select the new menu item, the associated command is launched with the arguments that were included in the device's custom menu configuration.

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



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

Using WhatsConfigured Device Properties - Tasks

The Tasks section of the Device Properties dialog displays, and lets you modify and run WhatsConfigured scheduled tasks, and modify and compare WhatsConfigured configuration archives assigned to this device.



Note: To add tasks to a device and/or view configuration information, WhatsConfigured must be activated. To update your license to purchase WhatsConfigured plug-in, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

Tasks attached to this device

Each scheduled task is listed by **Name**, **Description**, and the time it was **Last Run**.

- Click **Add** to add a scheduled task to this device.
- Select a task, then click **Remove** to delete a scheduled task from this device.
- Select a task, then click **Run Now** to perform the selected task immediately. The task will run only for the currently selected device. To run a task for all devices to which it is assigned, use the **Run Now** option in the WhatsConfigured Task Library.

Configuration archives saved for this device

Each archived configuration is listed by its **Time Created** and **Activity**.

- Select a configuration, then click **Restore** to restore the device to the selected configuration.
- Select a configuration, then click **Delete** to remove the configuration from the device's list of archives.
- Select a configuration, then click **View** to see the configuration details.
- Select two configurations, then click **Compare** to view the two configuration files side-by-side.

Using Network Tools

WhatsUp Gold includes several network troubleshooting tools. These tools allow you to take a closer look at the status of your network devices.



Note: Network Tools are only available on the WhatsUp Gold web interface.

The following tools help you check the connectivity of networked devices:

- *Ping Tool* (on page 132)
- *Traceroute Tool* (on page 133)
- *Lookup Tool* (on page 133)
- *Telnet Tool* (on page 134)

The following tools help you identify information about MIB objects that network devices support:

- *SNMP MIB Walker Tool* (on page 135)
- *SNMP MIB File Explorer Tool* (on page 138)

The following tools help you identify problems with network devices so you can take corrective action to resolve issues:

- *MAC Address Tool* (on page 139)
- *Diagnostic Tool* (on page 326)
- *Web Performance Monitor* (on page 141)
- *Web Task Manager* (on page 143)



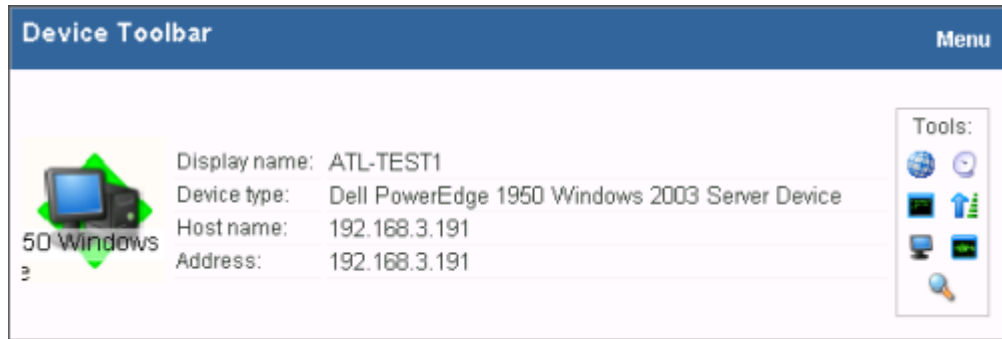
Note: The Web Performance Monitor and Web Task Manager tools are not available in WhatsUp Gold Standard Edition.

Accessing Network Tools

There are multiple ways to access the network tools.

- **Web interface Tools menu**
 - From the web interface, select **Tools**. The Tools menu appears.
- **Details View and Map View**
 - From either the Details View or Map View, right-click on a device, then select **Tools**.
- **Device Toolbar Dashboard Report**
 - 1 From either the Details View or Map View, double-click on a device. The Device Status dashboard view appears.

- 2 Locate the *Device Toolbar* dashboard report for the selected device. On the right side of report, small icons are linked to some of the network tools.



- 3 Click an icon to launch the network tool in the context of the selected device.

Using the Ping tool

The Ping tool sends out an ICMP (Internet Control Message Protocol) echo request to the networked device identified in **Address/Hostname**.

Tool results

The results of this request appears after the request has been made.

- **Destination.** The address specified in Address/Hostname.
- **Packets.** The number of data packets sent, received, and lost during the device ping.
- **RTT.** Round trip time in milliseconds; the amount of time it takes for the ping request to be returned from the remote device.
- **Status.** Success or failure. If failure, a reason is stated for the failure. For example, "Failure: Request timed out."

To use the Ping Tool:

- 1 Enter or select the appropriate information in the following fields.
 - **Address/Hostname.** The target of the Ping echo request. Enter the host name or IP address of the device you want to check.



Note: The Ping tool supports IPv6 addresses.

- **Timeout.** Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The Ping fails if this time limit is exceeded.
 - **Count.** Enter the number of data packets sent by the Ping tool.
 - **Packet size.** Enter the size (in bytes) of the packets you want the Ping tool to send. 32 bytes is the default.
- 2 Click **Ping** to run the tool.

Using the Traceroute tool

This tool sends out echo requests to a specific device, then traces the path it takes to get to that IP address or host name. This tool is often used to determine where, on the network, a data transmission interruption occurs.

Tool results

The results of this request appear in the bottom of the page after the tool has run:

- **Result.** Success or Failure. This is the general result of each hop in the Trace Route process.
- **Ping 1/2/3.** The tool sends out three ping requests to each hop in the route to the device. These columns show the round trip time for each of the requests.
- **Address.** The IP address of each device encountered on the path.
- **Host name.** The host name of each device encountered on the path.

To use the Traceroute Tool:

- 1 Enter or select the appropriate information in the following fields.
 - **Address/Host name.** Enter the host name or IP address of the device you want to trace the route to.



Note: The Trace Route tool supports IPv6 addresses.

- **Timeout.** Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The Trace Route fails if this time limit is exceeded.
 - **Max hops.** Enter the maximum number of hops you want to limit the route to. It is generally felt that 32 hops should be enough to find any device on the internet.
- 2 Click **Traceroute** to run the test.

Using the Lookup tool

This is a debugging tool that lets you query your Internet domain name system (DNS) server for information about a domain and its registered hosts. Lookup can show you what happens when an application on your network uses your DNS server to find the address of a remote host.

To use the Lookup Tool:

- 1 Enter or select the appropriate information in the following fields.
 - **Address/Host name.** Enter the host name or IP address of the device you want to trace the route to.
 - **Lookup Type.** Select the lookup type from the drop-down list:
 - **A.** Look up the host's Internet address from the hostname.

- **AAAA.** Look up for the host IPv6 address from a hostname.
- **All.** Display all available information about the host.
- **CNAME.** Display alias names for the host.
- **HINFO.** Display the CPU type and operating system type of the host.
- **MX.** Display the hostname of the mail exchanger for the domain.
- **NS.** Display the hostnames of name servers for the named zone.
- **PTR.** Look up the hostname from the Internet address.
- **SOA.** Display the domain's Start of Authority information, which indicates the primary name server for the domain and additional administrative information.
- **SRV.** Look up any SRV record configured on this DNS server. SRV records specify the location of services on the network.
- **TXT.** Look up any arbitrary text information the DNS server may have for this domain name or host.
- **ZONE.** Display the zone listing for the domain. The zone listing describes the domains for which the name server is the primary name server) and lists all registered hosts in the domain.
- **Timeout.** Enter the amount of time (in milliseconds) for the tool to wait on a response from the device. The Trace Route fails if this time limit is exceeded.
- **DNS.** Select the method of the look up:
 - **Stack.** Use the OS TCP/IP stack look up routines.
 - **Default.** Use the default DNS server configured on the computer WhatsUp Gold is running on.
 - **Custom.** Query a custom DNS server. You must then enter the hostname or IP address of the domain name server you want to use.

- 2 Click **Lookup** to run the tool.

Using the Telnet tool

Telnet is a simple service monitor that checks for a Telnet server on port 23. If no telnet service responds on this port, then the service is considered down.

To begin the service check, click the **Telnet** button. Refer to the Telnet application Help for more information.



Important: The Telnet protocol handler is disabled by default in Microsoft Internet Explorer 7. To re-enable it, see *Re-enabling the Telnet protocol handler* (on page 326).

Using the SNMP MIB Walker

This network tool lets you discover, or explore in detail, the SNMP objects that a device supports and that can be monitored with WhatsUp Gold. The SNMP MIB Walker actively polls for objects. It does not require MIB files for the polled objects to be loaded.

An SNMP walk is a succession of SNMP getnext reads starting with the configured Object ID (the root of the subtree walked) until there are no next objects in the MIB subtree or until the specified number of lines in the MIB have been walked. As results return from the MIB Walker, you can click an object (node) for more detailed information about the SNMP object and to walk further down the list of objects. You can also hover the mouse cursor over a node to display SNMP object details.

To use the SNMP MIB Walker:

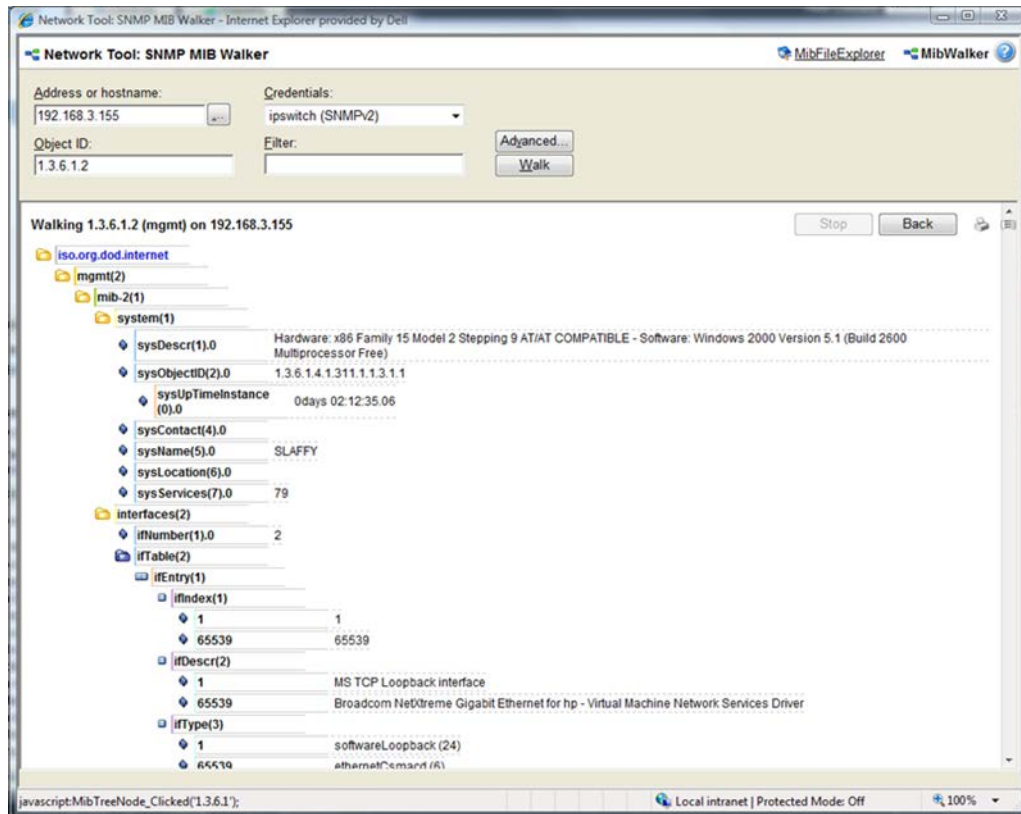
- 1 Enter or select the appropriate information in the following fields.
 - **Address or hostname.** Enter an IP address hostname for the device.
 - **Credentials.** Select the appropriate credentials for the device from the list. For more information, see *Using Credentials* (on page 75).
 - **Object ID.** Enter the numeric or label ID for the object for which you want information. A default OID is displayed in the box.
 - **Filter.** (Optional) Enter a filter to narrow down the search by returning only OIDs whose values match the filter criteria.



Tip: This is a regular expression, non-case-sensitive filter. For more information, see *Regular Expression Syntax* (on page 172).

- Click the **Advanced** button to change the value for the search timeout and retries, output types (tree, list-numeric OIDs, list-labels), and the maximum number of lines displayed.

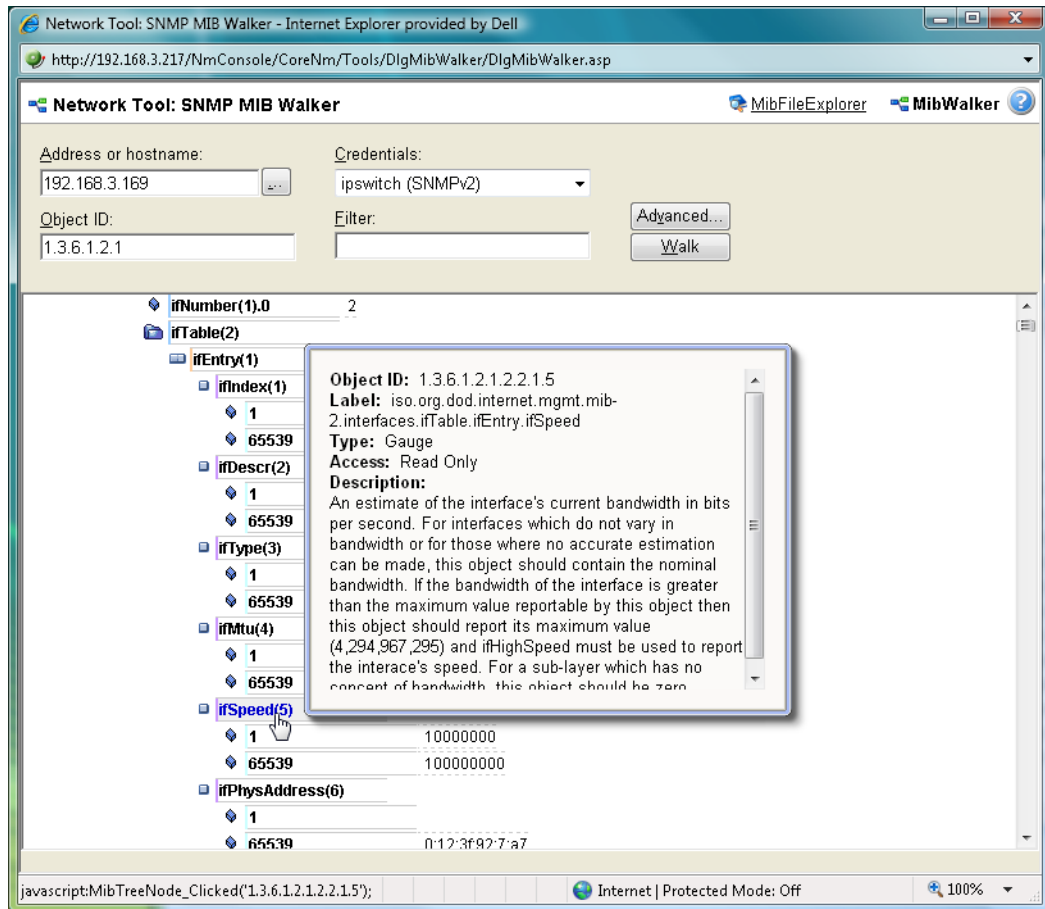
- 2 After you have entered all of the information, click **Walk** to perform the search. The SNMP MIB Walker returns a list of SNMP objects that are available on the selected device.



To cease the walk, click **Stop**. If you are performing multiple walks, click **Back** to view the previous walk.

After the SNMP Walker returns a list of the supported SNMP objects, you can use this information to create custom performance monitors and active script performance monitors for devices. For more information, see *Creating custom performance monitors* (on page 260).

To view detailed information about a specific MIB object, mouse over the object for which you need more information. The information displays in a popup bubble.



About MIB Output Types

You can change the format for the way MIB objects are displayed in the *Advanced Parameters* (on page 317) dialog. Whether the OID information is output as numeric OIDs or descriptive labels, each node may have additional sub-nodes that can be drilled down (walked) for more information. Each time you click a node, if there are child nodes, the node you clicked becomes the root node for the drill-down. The child nodes are expanded and attributes are displayed. MIB objects can be listed in one of three format options:

- **Tree.** Lists the MIB object in a tree structure format. This format is most useful in showing the OID hierarchy.
- **List - Numeric OIDs.** Lists the objects in a tabular format showing OIDs in a row numeric format. This format is especially helpful if you do not have the MIB file for the device objects. It provides the raw OID information that you can use in Custom Performance Monitors and Active Script Performance Monitors. Also, you can click the individual OID digits to display more or less MIB object information. As you click OID digits, the digits further to the left expand the sub-node information of the respective digits. As you click OID digits further to the right, the sub-node information expands for the respective digit and therefore more granular sub-node information.
- **List - Labels.** Lists the objects in a tabular format with user friendly labels. If the MIB for the object is not loaded, labels will default to numeric OIDs. Click an OID label name to expand the sub-nodes and view more information.



Note: You can switch to the WhatsUp Gold MIB Explorer by clicking on the MIB Explorer link on the upper-right side of this dialog.

Using the SNMP MIB Explorer

This network tool lets you search for, or explore through, SNMP objects defined in MIB files. The MIB File Explorer has three search/explore options.

As results return from the MIB File Explorer you can click an object (node) for more detailed information about the SNMP object. You can also hover the mouse cursor over a node to display SNMP object details.

To search by object ID:

Enter an object label or object ID in the **Object ID** field, then click **Detail**.

To search by MIB module:

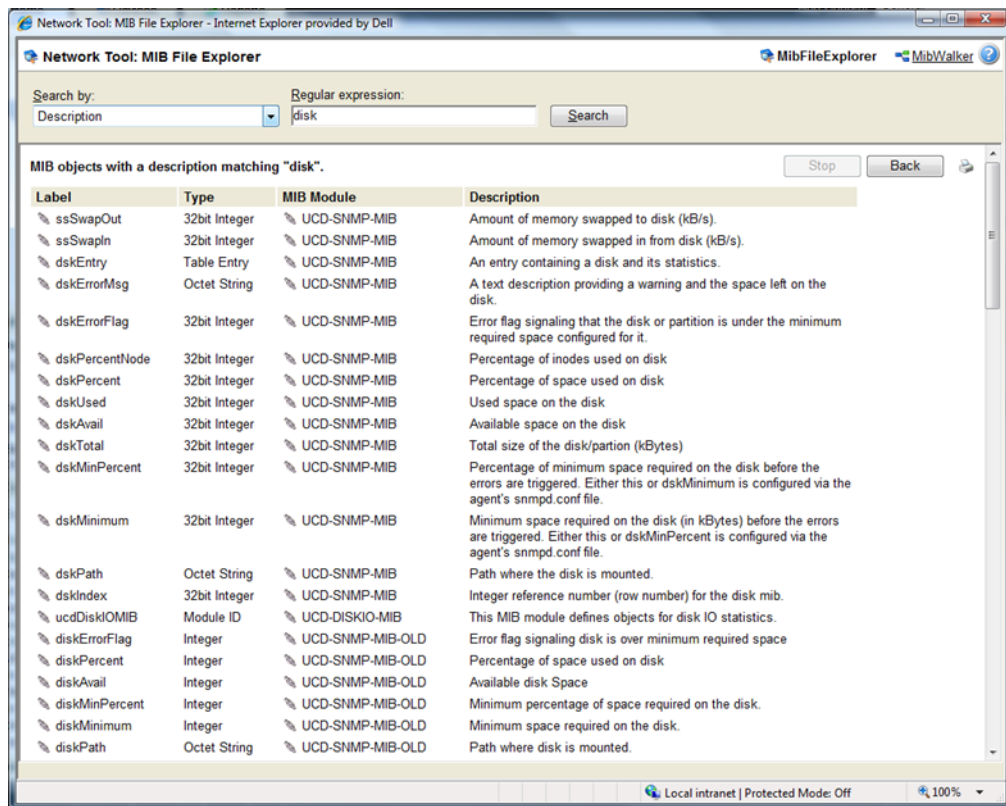
Select a module from the **MIB Module** list, then click **Display**.

To search objects by type or description:

First, select **Type** or **Description** from the **Search Object** list, then proceed appropriately:

- To search by object **Type**:
- Select a type from the list, then click **Find**.
- To search by object **Description**:

- Enter a regular expression in the **Description** field. This is a regular expression, non-case-sensitive filter. For more information, see *Regular Expression Syntax* (on page 172). After entering the description in the field, click **Find**.



- After the MIB File Explorer returns a list of the supported MIB objects, you can use this information to create custom performance monitors and active script performance monitors for devices. For more information, see *Creating custom performance monitors* (on page 260).



Note: You can switch to the WhatsUp Gold MIB Walker by clicking on the MIB Walker link on the upper-right side of this dialog.

Using the MAC Address Tool

The MAC Address tool enables you to discover what MAC addresses are present on your network and gives you the opportunity to obtain physical connectivity information for devices on your network. This tool is useful to solve IP address conflicts within your network by providing you with specific switch information.

Tool results

After running the tool, the results of the test are displayed at the bottom of the page.

If **Get connectivity information using SNMP** is not selected when the tool is run, the results include the following columns:

- **IP Address.** The IP addresses of devices on your network.
- **MAC Address.** The MAC addresses of devices on your network.
- **Hostname.** The hostnames of devices on your network.

If **Get connectivity information using SNMP** is selected when the tool is run, the results include the following columns:

- **IP Address.** The IP addresses of devices on your network.
- **MAC Address.** The MAC addresses of devices on your network.
- **Hostname.** The hostnames of devices on your network.
- **Port.** The port numbers of the switch ports that are connected to the devices that own the listed MAC addresses.
- **Index.** The unique value assigned to each interface. This number typically corresponds with the interface port number.



Note: If **Port** and **Index** report values of -1, WhatsUp Gold did not understand the response from the switch or the request timed out. Verify that credentials are correct and that you can view other SNMP information from the switch, and then run the MAC Address tool again.

- **Description.** The interface description of the interface to which a device is connected. Listed as a letter and a numeral, such as "B4". The interface description allows you to identify the physical connector on the switch.

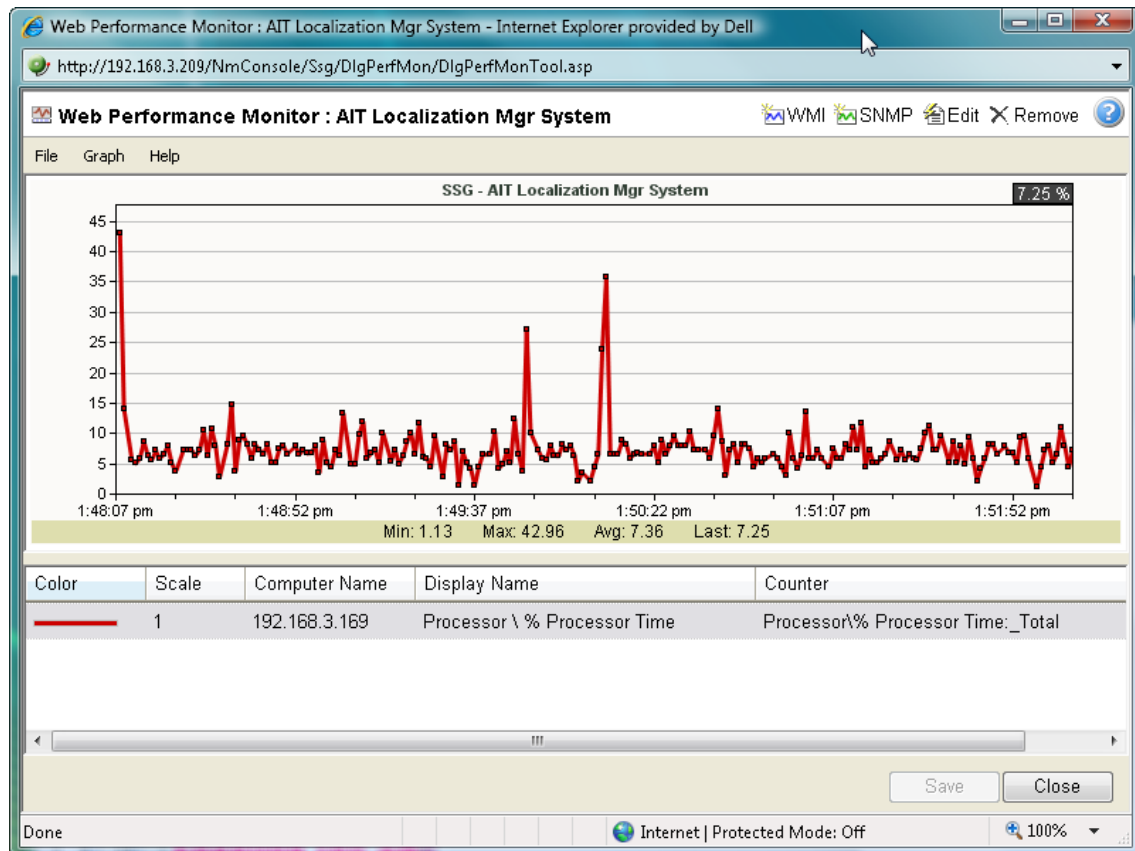
To use the MAC Address Tool:

- 1 Enter or select the appropriate information in the following fields.
 - **Local subnet.** Enter the subnet on which you would like to find MAC addresses.
 - **Get connectivity information using SNMP.** If you would like switch-specific connectivity information for a device in the network, select this option. If this option is selected, the following options are enabled. If this option is cleared, the following options are disabled.
 - **Switch IP address.** Enter the switch IP address.
 - **SNMP credential.** Select the SNMP credential that you use to poll this device. If the credential you want to use is not listed, you can add it using the Credential Library.
 - **Timeout (seconds).** Enter the amount of time for the tool to wait on a response from the switch. The MAC address discovery fails if this time limit is exceeded.

- **Retries.** Enter the maximum number of retries when polling the switch using SNMP.
- 2 Click **Discover** to discover the MAC addresses present on your network.

Using the Web Performance Monitor

The Web Performance Monitor extends the functionality of the Microsoft Windows Performance Monitor to the Web. It is a data collecting and graphing utility designed specifically for the WhatsUp Gold Web interface that graphs and displays real-time information on user-specified SNMP and WMI performance counters. It can be used for a quick inspection of a specific network device.



The graphs can be saved to the database and displayed on dashboard views using the Split Second Graph - Performance Monitor dashboard report or on the Web Performance Monitor tool. Multiple SNMP and WMI counters can be displayed on a single graph, and the color and scale of each graphed item can be individually configured.

Graphs created with the Web Performance Monitor are saved on a per-user account basis, meaning, graphs are only accessible by the user account that created and saved them.

The Web Performance Monitor has two purposes:

- To provide a Web enabled WMI and SNMP performance counter poller and grapher. It supports WMI for Windows servers, and SNMP for network devices such as switches, routers, and UNIX devices.
- To build and edit graphs for use by the Performance Monitor dashboard report. You can use this dashboard report to display any saved graph.

To add a WMI performance counter to the Web Performance Monitor:

- 1 Click **Tools > Web Performance Monitor**. The Web Performance Monitor appears.
- 2 Click **Graph > Add WMI Counter**.

- or -

Click the WMI button in the upper right corner of the dialog (see the Toolbar buttons table below). The *Add WMI Performance Counter* (on page 320) dialog appears.

- 3 Enter the appropriate information into the dialog fields.
- 4 Click **OK** to save changes.

To add an SNMP performance counter to the Web Performance Monitor:

- 1 Click **Tools > Web Performance Monitor**. The Web Performance Monitor appears.
- 2 Click **Graph > Add SNMP Performance Monitor**.

- or -

Click the SNMP button in the upper right corner of the dialog (see the Toolbar buttons table below). The *Add SNMP Performance Counter* dialog appears.

- 3 Enter the appropriate information into the dialog fields.
- 4 Click **OK** to save changes.

Web Performance Monitor menu items

The Web Performance Monitor menu is located at the top left corner of the window.

File menu

- **File > New Graph**. This menu item resets the graph back to a blank graph.
- **File > Edit Graph Name**. This menu item lets you change the name of the selected graph.
- **File > Load Graph**. This opens the Load Graph dialog, which displays a list of saved graph files on the Web server.
- **File > Save Graph**. This saves the current graph to the database. If no filename is specified, it launches the Save Graph dialog, which allows a filename to be specified. All files are saved to the WhatsUp database.
- **File > Save Graph As**. This opens the Save Graph dialog which prompts you for a filename, and then saves the current graph to disk.
- **Windows Properties**. This opens the Configure Window Properties dialog. Use this dialog to configure the graph and window properties for the Web Performance Monitor.

Graph menu






- **Graph > Add WMI Performance Counter.** This launches the Add WMI Performance Counter dialog.
- **Graph > Add SNMP Performance Counter.** This launches the Add SNMP Performance Counter dialog.
- **Graph > Edit Selected Counter.** This launches the appropriate dialog for editing the selected WMI or SNMP performance counter.
- **Graph > Remove Selected Counter.** This removes the selected counter from the list and graph. No changes are saved to disk until the OK button is clicked or the graph is manually saved (**File > Save Graph** - or - **Save Graph As**).

Help menu

- **Help > Help.** This launches help for the Web Performance Monitor.

Web Performance Monitor Toolbar buttons

The Web Performance Monitor Toolbar is located at the top right corner of the window.

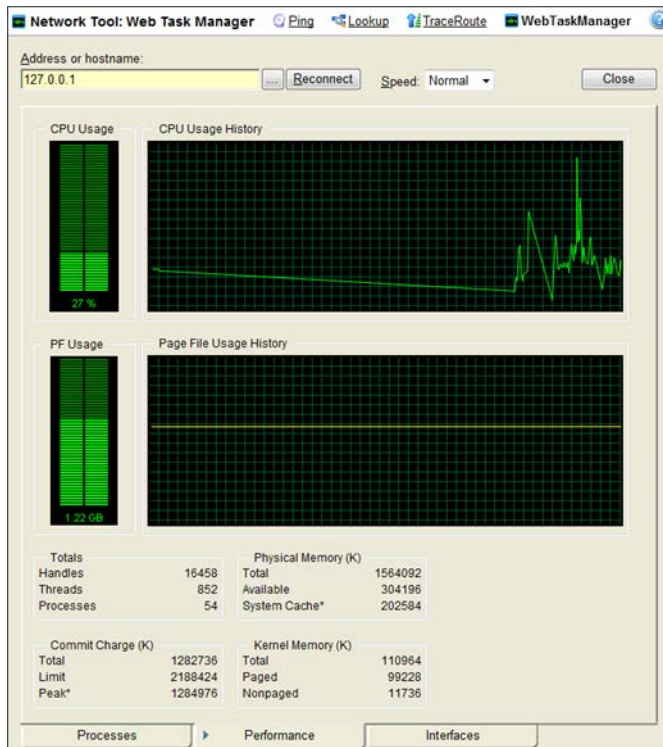
| Button | Function |
|--|--|
|  WMI | Opens the Add WMI Performance Counter dialog. |
|  SNMP | Opens the Add SNMP Performance Counter dialog. |
|  Edit | Opens the appropriate dialog for editing the selected WMI or SNMP performance counter. |
|  Remove | Removes the selected graph item from the list and graph. |
|  | Opens the help topic for the Web Performance Monitor |

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 957).

Using the Web Task Manager

The Web Task Manager extends the functionality of the Microsoft Windows Task Manager to provide network device overview information about processes occurring on a device, device performance, and device interface activity. The Web Task Manager graphs and displays real-time information using SNMP or WMI device connections.

You can use the Web Task Manager to identify device issues and take corrective action on a device.



There are three tabs that provide device information:

- **Processes** (on page 147). Provides key indicator process information for a selected device that WhatsUp Gold is monitoring. For example, you can view a list of .exe files that are running and the amount of CPU and memory used by each program.
- **Performance** (on page 149). Provides dynamic performance information for a selected device that WhatsUp Gold is monitoring. For example, you can view details about the CPU and memory usage.
- **Interfaces** (on page 152). Provides information about a selected device's interfaces that WhatsUp Gold is monitoring. For example, you can view a list of interfaces that the device uses to learn about how much data is transmitted and received via each interface.

To use the Web Task Manager:

- 1 Click the **Devices** tab, then click **Devices**. The Device page appears.
- 2 From the Details View or Map View, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.
- 3 Enter or select the appropriate information for the following fields:
 - **Address or hostname.** Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.
 - **Browse (...).** Click to open the *Web Task Manager Credentials dialog* (on page 145) and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the Credentials Library.
 - **Speed.** Select the speed at which you want to monitor the device performance.
 - **Normal.** Updates device information every one second.
 - **Medium.** Updates device information every five seconds.
 - **Slow.** Updates device information every ten seconds.
 - **Paused.** Stops updating device information.
 - **Connect using** (Processes tab). Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the Credentials Library are used to connect and read information on the selected device.



Note: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

- 4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 957).



Note: Some differences exist in column names between the Web Task Manager and Windows Task Manager in Windows Vista and Windows 2008. The **Mem Usage** column in Web Task Manager is named **Working Set (Memory)** in Windows Task Manager on Windows Vista and Windows 2008. The **VM Size** column in Web Task Manager has no corresponding column in Windows Task Manager on Windows Vista and Windows 2008.

Setting up Web Task Manager device credentials

Use the Web Task Manager Credentials dialog to select credentials for the device you want to monitor with the Web Tools Task Manager.

- **Address or hostname.** Enter a device IP address to select a device for which you want to view process, performance, or interface information. Click the Browse (...) button to select a device.
- **Windows.** Select the Windows credential to connect to this device. Click the browse (...) button to browse the Credentials Library.
- **SNMP v1/v2/v3.** Select the SNMP credentials to connect to this device. If the Identify devices via SNMP option was selected during discovery (or if an SNMP discovery was performed) the correct SNMP credential was used during the discovery process, and if the device is an SNMP manageable device, then the correct credential is selected automatically. If any of these conditions are not met, None is selected.
- **ADO.** Select the ADO credentials for database connection string information to be used when a database connection is required for WhatsUp Gold database monitors.
- **Edit.** Click to open the Select Credentials dialog, then select the credential from the list or click the browse ... button to browse the Credentials Library.

How To example: Using the Web Task Manager - Process tab

The Web Task Manager Processes tab provides key indicator process information for a selected device that WhatsUp Gold is monitoring. This information helps you learn about device processes and identify trends and issues that occur on a particular network device. You can use the Web Task Manager Process tab to view the processes running on WMI- or SNMP-enabled network devices.

| Image Name | User Name | CPU | Mem Usage | VM Size |
|---------------------|-----------------|-----|-----------|----------|
| System Idle Process | SYSTEM | 100 | 16 K | 0 K |
| svchost.exe | SYSTEM | 3 | 33,632 K | 22,508 K |
| System | SYSTEM | 1 | 256 K | 0 K |
| smss.exe | SYSTEM | 0 | 372 K | 148 K |
| csrss.exe | SYSTEM | 0 | 5,452 K | 2,152 K |
| winlogon.exe | SYSTEM | 0 | 10,108 K | 10,248 K |
| services.exe | SYSTEM | 0 | 5,280 K | 4,340 K |
| lsass.exe | SYSTEM | 0 | 1,964 K | 4,216 K |
| svchost.exe | SYSTEM | 0 | 6,472 K | 3,232 K |
| svchost.exe | NETWORK SERVICE | 0 | 5,640 K | 2,280 K |
| svchost.exe | NETWORK SERVICE | 0 | 3,816 K | 1,520 K |
| svchost.exe | LOCAL SERVICE | 0 | 5,000 K | 2,036 K |
| ccSetMgr.exe | SYSTEM | 0 | 3,632 K | 4,116 K |
| ccExtMgr.exe | SYSTEM | 0 | 3,580 K | 4,116 K |

After you have identified a process that is causing device performance issues, such as an application executable like `Outlook.exe` running multiple instances of the program, you can correct the problem to bring the device performance back to normal.



Note: Unlike the Windows Task Manager, you cannot terminate processes using the Web Task Manager. To terminate a task, you must log in to the computer where the task is running and use the Windows Task Manager to end the process.

To use the Web Task Manager:

- 1 Click the **Devices** tab, then click **Devices**. The Device page appears.
- 2 From the Details View or Map View, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.
- 3 Enter or select the appropriate information for the following fields:
 - **Address or hostname.** Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.

- **Browse (...).** Click to open the Web Task Manager Credentials dialog and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the Credentials Library.
- **Speed.** Select the speed at which you want to monitor the device performance.
 - **Normal.** Updates device information every one second.
 - **Medium.** Updates device information every five seconds.
 - **Slow.** Updates device information every ten seconds.
 - **Paused.** Stops updating device information.
- **Connect using.** Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the Credentials Library are used to connect and read information on the selected device.



Note: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

- 4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).

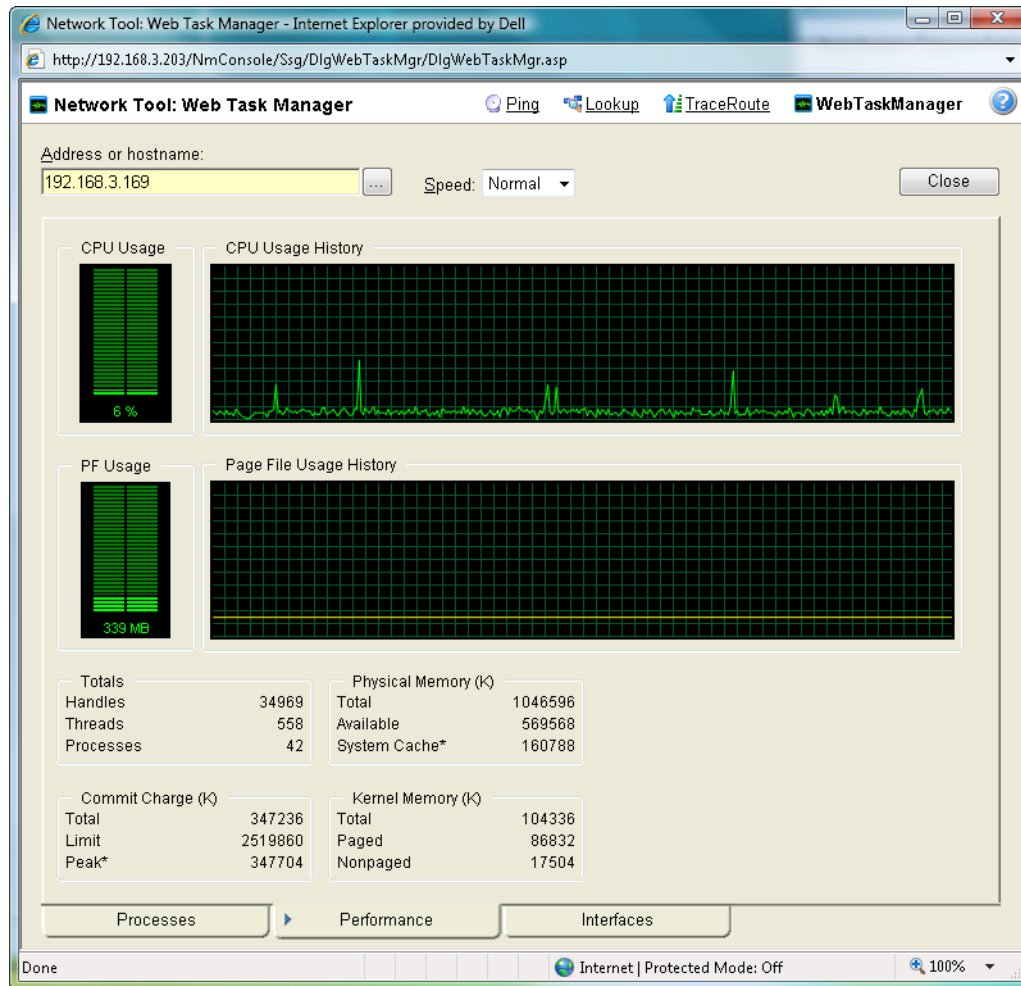
For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 957).



Note: Some differences exist in column names between the Web Task Manager and Windows Task Manager in Windows Vista and Windows 2008. The `Mem Usage` column in Web Task Manager is named `Working Set (Memory)` in Windows Task Manager on Windows Vista and Windows 2008. The `VM Size` column in Web Task Manager has no corresponding column in Windows Task Manager on Windows Vista and Windows 2008.

Using the Web Task Manager - Performance tab

The Performance tab provides dynamic performance information for a selected device that WhatsUp Gold is monitoring. This information helps you learn about device performance and identify trends, spikes, or other issues that occur on a particular network device. You can use the Web Task Manager to view device performance for devices that are WMI or SNMP enabled network devices.



After you have identified a performance issue that is causing device performance issues, such as the Page File Usage indicating that the system memory is nearly at full capacity, you can correct the problem to bring the device performance back to normal.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To use the Web Task Manager:

- 1 Click the **Devices** tab, then click **Devices**. The Devices page appears.
- 2 From the details or icon view, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.
- 3 Enter or select the appropriate information for the following fields:
 - **Address or hostname.** Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.
 - **Browse (...).** Click to open the *Web Task Manager Credentials dialog* (on page 145) and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the *Credentials Library* (on page 836).
 - **Speed.** Select the speed at which you want to monitor the device performance.
 - **Normal.** Updates device information every one second.
 - **Medium.** Updates device information every five seconds.
 - **Slow.** Updates device information every ten seconds.
 - **Paused.** Stops updating device information.
 - **Connect using** (Processes tab). Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the *Credentials Library* (on page 836) are used to connect and read information on the selected device.



Note: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed of Medium or Slow** when using SNMP to view interface information about a device running Microsoft Windows.

- 4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).
- 5 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 957).

The following are examples of information that is provided when you connect to and view a WMI enabled device. Note, this information varies by operating system:

- **CPU Usage.** This graph indicates the percentage of time the processor is operating. Use this graph to view how much the processor is operating.
- **CPU Usage History.** This graph indicates how much the processor has operated over time. You can change the Speed option (High, Normal, Slow, Paused). The Speed option determines how often updates occur to the CPU Usage History.
- **PF Usage.** This graph indicates how much page file memory is used.

- **Page File Usage History.** This graph indicates how much the page file memory is used over time. If page file memory usage is high, you may want to increase the available page file memory.
- **Totals.** This provides the total number of Handles, Threads, and Processes occurring on the selected device.
- **Commit Charge (K).** Provides information about the memory (Total, Limit, and Peak) allocated to the operating system and applications running on the device.
- **Physical Memory (K).** Provides information about the amount of physical memory (Total, Available, and System Cache) installed on the device.
- **Kernel Memory (K).** Provides information about how much memory (Total, Paged, and Nonpaged) the operating system kernel and device drivers are using.



Note: Values reported for Peak and System Cache will differ from values reported by the Windows Task Manager on the actual device. In the Web Task Manager, Peak reflects the peak value for the time that the Web Task Manager has been open only, and System Cache does not include the size of the free page list.

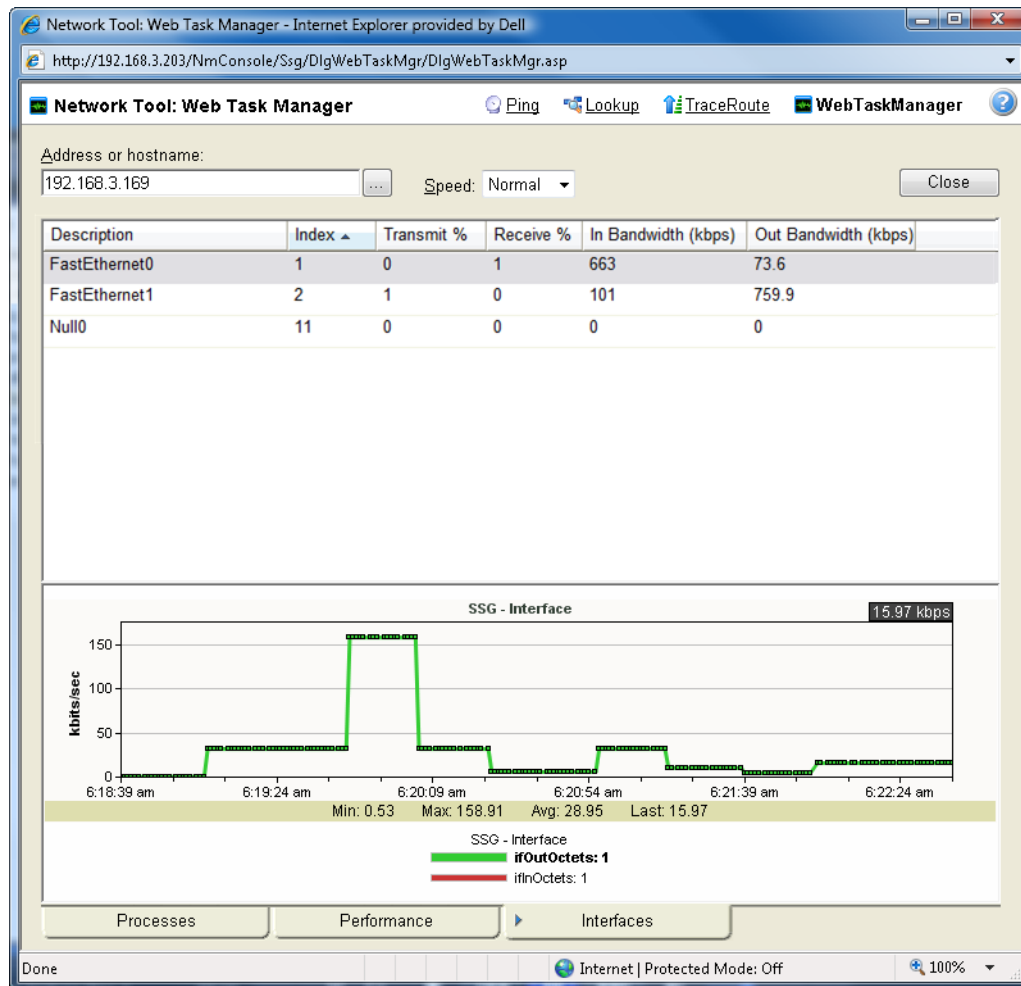
The following information are examples of the information that is provided when you connect to and view a SNMP enabled device. Note, this information varies by operating system:

- **In (PKTS).** Provides detailed information about the network packets that this device receives.
- **Out (PKTS).** Provides detailed information about the network packets that this device sends.
- **System.** Provides general system information about CPU performance, the number of interfaces that are running on the device, the total amount of time the device has been operating in the up mode, and the version number of Cisco software running on the device (if applicable).

For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 957).

Using the Web Task Manager - Interfaces tab

The Interfaces tab provides information about the interfaces available on a selected device that WhatsUp Gold is monitoring. This information helps you determine how much data is transmitted and received via each interface, and therefore may help you locate an interface that using an unexpected amount of bandwidth.



After you have identified the interface that is causing bandwidth performance issues, such as a file sharing application exposing shared files on a computer for others on the Internet to access and download, you can correct the problem to bring the device performance back to normal.

The Web Task Manager includes the following columns:

- **Description.** This column is the text description of the interface as configured on the device.
- **Index.** This column is the unique numerical identifier of the interface as defined on the device.
- **Transmit %.** This column indicates what percentage of the interface's capacity is currently being used to transmit data.

- **Receive %.** This column indicates what percentage of the interface's capacity is currently being used to receive data.
- **In Bandwidth (kbps).** This column shows the amount of data received by the device in kilobits per second.
- **Out Bandwidth (kbps).** This column shows the amount of data transmitted by the device in kilobits per second.

To use the Web Task Manager:

- 1 Click the **Devices** tab, then click **Devices**. The Devices page appears.
- 2 From the details or icon view, right-click a device, then click **Web Task Manager**. The Web Task Manager dialog appears.
- 3 Enter or select the appropriate information for the following fields:
 - **Address or hostname.** Enter a device IP address to select a device for which you want to view process information. Click **Reconnect** to connect with a device that has disconnected from the Web Task Manager.
 - **Browse (...).** Click to open the *Web Task Manager Credentials dialog* (on page 145) and set a WMI user name and password or an SNMP read community. The credential options are provided from the credentials stored in the *Credentials Library* (on page 836).
 - **Speed.** Select the speed at which you want to monitor the device performance.
 - **Normal.** Updates device information every one second.
 - **Medium.** Updates device information every five seconds.
 - **Slow.** Updates device information every ten seconds.
 - **Paused.** Stops updating device information.
 - **Connect using** (Processes tab). Select the device protocol (WMI or SNMP) used to monitor and manage the device. The credentials stored in the *Credentials Library* (on page 836) are used to connect and read information on the selected device.



Note: When viewing information for devices running Microsoft Windows, information gathered by SNMP may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values. For this reason, we recommend using a **Speed** of **Medium** or **Slow** when using SNMP to view interface information about a device running Microsoft Windows.

- 4 At the bottom of the Task Manager page, select the tab that you want to use (**Processes**, **Performance**, or **Interfaces**).
- 5 For troubleshooting information, see *Troubleshooting SNMP and WMI connections* (on page 957).

Monitoring Devices

In This Chapter

| | |
|---|-----|
| Using Active Monitors..... | 155 |
| Passive Monitor Library | 232 |
| Using Performance Monitors | 246 |
| Enabling global performance monitors | 254 |
| Configuring the CPU monitor collection settings | 255 |
| Configuring the disk monitor collection settings | 255 |
| Configuring the interface monitor collection settings | 256 |
| Configuring the memory monitor collection settings | 258 |
| Configuring the ping monitor collection settings..... | 258 |
| Enabling SNMP on Windows devices..... | 259 |
| Using the Active Script Performance Monitor | 269 |

Using Active Monitors

In This Chapter

| | |
|--|-----|
| Active Monitors overview | 155 |
| About the Active Monitor Library | 156 |
| Selecting an Active Monitor Type | 157 |
| Configuring Active Monitors | 157 |
| Adding and editing a Temperature Monitor | 176 |
| Adding and editing a WAP Radio Monitor | 177 |
| Using Premium Active Monitors | 178 |

Active Monitors overview

Active monitors poll target devices for information such as ping accessibility, device services, such as Web or email servers, and more. Active monitors regularly query or poll the device services for which they are configured and wait for responses. If a query is returned with an expected response, the queried service is considered "up." If a response is not received, or if the response is not expected, the queried service is considered "down" and a state change is issued on the device.

In an effort to help you manage your network after you install the application, WhatsUp Gold includes a number of pre-configured active monitors. These pre-configured monitors display in the Active Monitor Library. As you configure new active monitor types, they are added to the library.

Use the Active Monitor Library to configure new or existing Active Monitor Types. The Active Monitors list displays active monitors configured and available to apply to network devices. For more information, see *Configuring Active Monitors* (on page 157).

To manage active monitors in the Active Monitor Library:

- 1 Click **Admin**, then click **Monitor Library**. The Monitor Library dialog opens.
- 2 Configure new or existing active monitor types:
 - To configure a new Active Monitor Type, click **New**.
 - To change an Active Monitor Type, select an existing type from the list, then click **Edit**.
 - To make a copy of an Active Monitor Type, select an active monitor type from the list, then click **Copy**.
 - To remove an Active Monitor Type, select an active monitor type from the list, then click **Delete**.



Caution: When you delete an active monitor from the Active Monitor Library, any instance of that active monitor is also deleted, and all related report data is lost.

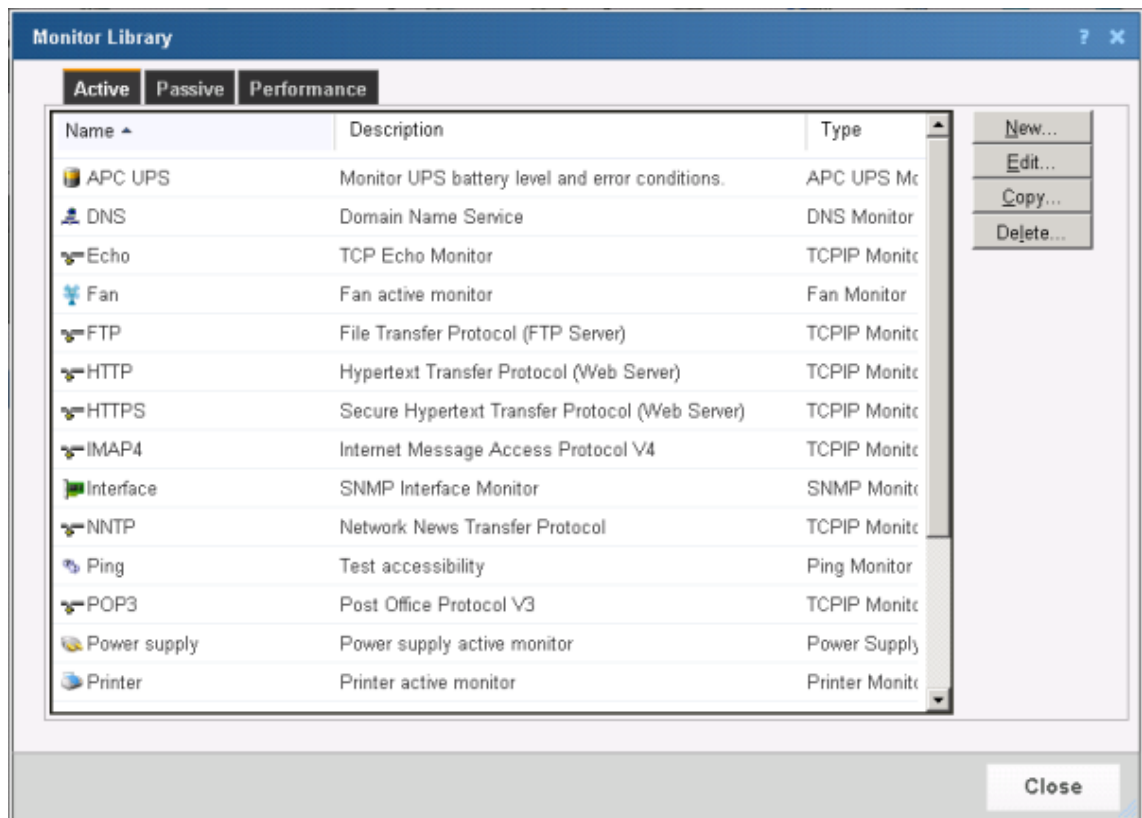
About the Active Monitor Library

The Active Monitor Library displays all active monitors currently configured for use in WhatsUp Gold.

To help you manage your network easily after your initial installation of the application, WhatsUp Gold includes a number of pre-configured active monitors. These pre-configured monitors display in the Active Monitor Library. As you configure new active monitor types, they are added to the library.

To access the Active Monitor Library:

- 1 From the **Admin** panel, select **Monitor Library**. The Monitor Library dialog opens.
- 2 If not already selected, click the **Active** tab to open the Active Monitor Library.



From the Active Monitor Library you can configure new or existing active monitor types:

- Click **New** to configure a new active monitor type.
- Select an active monitor type, then click **Edit** to modify its configuration.
- Select an active monitor type, then click **Copy** to make a copy of that type.
- Select an active monitor type, then click **Delete** to remove it from the list.



Caution: When you delete an active monitor from the Active Monitor Library, any instance of that active monitor is also deleted, and all related report data is lost.

Selecting an Active Monitor Type

Use the list to select one of the following active monitor types; after selecting the monitor type, click **OK**.

- *Active Script Monitor* (on page 226)
- *APC UPS Monitor* (on page 178)
- *DNS Monitor* (on page 157)
- *Email Monitor* (on page 180)
- *Exchange 2003 Monitor* (on page 190)
- *Exchange Monitor* (on page 185)
- *Fan Monitor* (on page 194)
- *File Properties Monitor* (on page 195)
- *Folder Monitor* (on page 196)
- *FTP Monitor* (on page 199)
- *Network Statistics Monitor* (on page 204)
- *NT Service Monitor* (on page 158)
- *Ping Monitor* (on page 159)
- *Power Supply Monitor*
- *Printer Monitor*
- *Process Monitor* (on page 209)
- *SNMP Monitor* (on page 160)
- *SQL Query Monitor* (on page 218)
- *SQL Server Monitor* (on page 213)
- *SSH Monitor* (on page 163)
- *TCP/IP Monitor* (on page 164)
- *Telnet Monitor* (on page 175)
- *Temperature Monitor* (on page 176)
- *VoIP Monitor* (on page 225) (available with the VoIP Monitor plug-in)
- *WAP Radio Monitor* (on page 177)
- *WMI Monitor* (on page 177)

Configuring Active Monitors

All active monitor types are stored in and configured from the Active Monitor Library. In order to function as designed, active monitors must be assigned to devices. When an active monitor is assigned, an individual instance of the monitor is placed on the device to which it is assigned. Subsequent changes made to the active monitor in the Active Monitor Library affect all instances of the monitor.

Adding and editing a Domain Service (DNS) Monitor

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

To add or edit a DNS active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **DNS Monitor** from the list to create a new DNS monitor. Click **OK**.
- or -
Select the DNS monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Timeout.** Type a timeout value. This is the length of time in which the service is given a chance to respond. If there is no response in this amount of time, the service is considered down.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
- 5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing an NT Service Monitor

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



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

To add or edit an NT service active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New**, then select **NT Service Monitor** from the list to create a new NT service monitor. Click **OK**.
- or -
From the list of current monitors, select the NT service monitor you want to change, and then click **Edit**.

- 4 Complete the appropriate information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Service name.** Click the **Browse (...)** button next to the Service Name text box to open the Browse for Service dialog, allowing you to locate *any* server/workstation running the service.
 - **Restart on failure.** Select this option to have the monitor attempt to restart the service when it enters a down state.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.



Note: WhatsUp Gold uses Windows Management Instrumentation (WMI) to verify the status of the NT Service Active Monitors you have configured. WhatsUp Gold currently only supports monitoring on Windows 2000 Service Pack 2 or higher, Windows XP Professional, and Windows 2003 or higher.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Troubleshooting

Having problems with your WMI monitor returning false negatives?

Adding and editing a Ping Monitor

Configure an active ping monitor for WhatsUp Gold to send an ICMP (ping) command to the device. This is the default monitor added to all devices during discovery. If the device does not respond, the monitor is considered down.

To add or edit a ping monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New**, then select **Ping Monitor** from the list to create a new ping monitor. Click **OK**.
 - or -Select the ping monitor you want to change from the list of current monitors, and then click **Edit**.

- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Timeout.** The ping fails if the device does not respond after this number of seconds.
 - **Retries.** The number of times WhatsUp Gold attempts to send the command before the device is considered down.
 - **Payload size.** The length in bytes of each packet sent by the ping command.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
- 5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing a SNMP Active Monitor

The Simple Network Management Protocol is the protocol governing network management and monitoring of network devices and their functions. In this monitor, WhatsUp Gold utilizes SNMP to gather specific information about the functions of SNMP-enabled network devices by querying a device to verify that it returns an expected value. Depending on the state you choose, the monitor is considered either Up or Down according to the returned value.

To add or edit a SNMP active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New**, then select **SNMP Monitor** from the list to create a new SNMP monitor. Click **OK**.
- or -
Select the SNMP monitor you want to change from the list of monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Object ID.** Click the **Browse (...)** button, then locate and select the appropriate SNMP object in the MIB object tree. For more information, see **Selecting an Object in the MIB Tree** below.
 - **Check type.** Select **Constant Value**, **Range of Values**, or **Rate of Change in Value**.

5 Complete the check type information.

When **Constant Value** is selected:

- **Value.** Depending on the Object ID you selected, type the appropriate value.
- **If the value matches, then the monitor is:** select **Up** or **Down**.

When **Range of Values** is selected:

- **Low Value.** Depending on the Object ID you selected, type the appropriate value.
- **High Value.** Depending on the Object ID you selected, type the appropriate value.

When **Rate of Change in Value** is selected:

- **Rate of Change** (in variable units per second). Type the desired value.
- **If the value is above the rate, then the monitor is:** select **Up** or **Down**.

6 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Selecting an Object in the MIB Tree

In order to select the appropriate object in the MIB tree, you need to be familiar with the MIB names for the SNMP objects you want to monitor. For more information, see RFC 1213.

Example A. Suppose you want to monitor the volume of data going out through your router, select `ifOutOctets` in the MIB object tree, thus inserting 1.3.6.1.2.1.2.2.1.16 in the MIB box.

Example B. Suppose you are interested in the operating status value of a port on your router, select `ifOperStatus`, thus inserting 1.3.6.1.2.1.2.2.1.8 in the MIB box.

Example C. Suppose you are interested in the errors on a port on your router, select `ifInErrors`, thus inserting 1.3.6.1.2.1.2.2.1.14 in the MIB box.

i) Selecting an object in the MIB Tree

In order to select the appropriate object in the MIB tree, you need to be familiar with the MIB names for the SNMP objects for which you want to monitor. For more information, see RFC 1213.

Example A.

If you want to monitor the volume of data traveling from your router, you select `ifOutOctets` in the MIB object tree and insert 1.3.6.1.2.1.2.2.1.16 in the MIB box.

Example B.

If you are interested in the operating status value of a port on your router, you select `ifOperStatus` and insert 1.3.6.1.2.1.2.2.1.8 in the MIB box.

Example C.

If you are interested in errors from a specific port on your router, you select `ifInErrors`, and inserting `1.3.6.1.2.1.2.2.1.14` in the MIB box.

For more information, see *Extending WhatsUp Gold with scripting* (on page 909).

ii) Example: Monitoring Network Printer Toner Levels

To avoid running out of printer ink in the middle of print jobs, or wasting toner by switching toner cartridges before they are empty, through WhatsUp Gold you can create a custom SNMP active monitor that notifies you when toner levels are low.

To configure a printer monitor:

- 1 Access the Monitor Library.
- 2 Click **New**, select **SNMP Monitor**, then click **OK**. The Add SNMP Monitor dialog appears. You need to create an active monitor for each printer type in use. It may be that the office uses the same printer type in each office. In this example, we are using a Hewlett Packard LaserJet 4050N. Check your network printers for their specific maximum capacity toner levels.
- 3 Type a **Name** and **Description** for the monitor. For example, TonerMonitor and Toner monitor for the Hewlett Packard LaserJet 4050N.
- 4 For the **Object ID** and **Instance**, click the browse (...) button, then locate the **prtMarkerSuppliesLevel** (OID 1.3.6.1.2.1.43.11.1.1.9) **SNMP** object in the MIB object tree. This SNMP object is found in the MIB tree at:
mgmt > mib 2 > printmib > prtMarkerSupplies > prtMarkerSuppliesEntry > prtMarkerSuppliesLevel
- 5 Select **Range of Values** from the type drop down menu and enter 4600 (the maximum capacity toner level) as the **High value** and 100 as the **Low Value**, then click **OK**. The action fails when the printer toner level reaches 99.
- 6 Test the newly created active monitor and make appropriate changes if needed.
- 7 Assign the active monitor to the printer device, select **Properties > Active Monitors**. The Device Properties Active Monitor dialog appears.
- 8 Click **Add**.
- 9 During the configuration wizard, create or select an action to notify you when the printer's toner levels are low.

Repeat steps 4-6 for each network printer that requires monitoring.

iii) Example: Monitoring TCP Connections Established for a Device

Too many TCP connections can signal that a device is being maliciously used, in the case of a workstation, or that your web server is close to maxing out, indicating the need to initiate a backup server. You can create an SNMP active monitor to watch a range of established TCP connections for a particular device. If the number of connections goes above the range you specify, you can be notified by an associated action.

To configure a TCP monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click **New**, select **SNMP Monitor**, then click **OK**. The Add SNMP Monitor dialog appears.
- 3 Enter a **Name** and **Description** for the monitor. For example, Number of TCP connections less than 2000.
- 4 For the **Object ID** and **Instance**, click the browse (...) button, then locate the **TcpCurrEstab** (1.3.6.1.2.1.6.9) SNMP object in the MIB object tree.
- 5 Select **Range of Values** from the Check type list and enter 1999 (the maximum number of established TCP connections) as the **High value** and 0 as the **Low Value**, then click **OK**. Any associated actions fail when the number of established TCP connections reaches 2000.
- 6 Test the newly created active monitor and make appropriate changes if needed.
- 7 Assign the active monitor to the web server:
 - a) Right-click on the device on the appropriate device, then select **Properties > Active Monitors**. The Device Properties Active Monitor dialog appears.
 - b) Click **Add**.
 - c) Using the configuration wizard, create or select an action to notify you when the number of established TCP connections reaches 2000.

Adding and editing an SSH Active Monitor

The SSH Monitor connects to a remote device using SSH to execute commands or scripts. The success or failure of the monitor is dependant upon values returned by the commands or scripts that can be interpreted by WhatsUp Gold as Up or Down.

To add or edit a SSH active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **SSH Monitor** from the list to create a new SSH monitor. Click **OK**.
- or -
Select the SSH monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name**. Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description**. Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Command to run**. Type the command you want to run and execute on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.



Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- **The monitor is considered Up if the following output ____.** Either Contains or Does not contain. Select the appropriate output criteria. For example, if you are checking to see that a specific network connection is present on the remote device, you would select that the output contains that specific connection. If the network connection you specify is not present when the monitor checks, the monitor is considered down.
 - **Use regular expression.** Select this option to have WhatsUp Gold use regular expression when searching for the output of command or script. If you do not choose to use regular expression, WhatsUp Gold looks for specific text outputs, rather than outputs including a regular expression.
 - **SSH credential.** Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.
- 5 Click **OK** to return to the monitor properties dialog.
 - 6 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing a TCPIP Monitor

The TCPIP monitor is used to monitor a TCP/IP service that either does not appear in the list of standard services, or uses a non-standard port number.

To add or edit a TCPIP monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **TCPIP Monitor** to create a new TCPIP monitor. Click **OK**.
- or -
Select the TCPIP monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Network type.** Select either TCP, UDP, or SSL from the Network type list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
 - **Port number.** Type the TCP or UDP port that you want to monitor.
 - **Timeout.** Amount of time (in seconds) WhatsUp Gold should wait for a response to a poll.

- **Script.** Write your script using as many Send, Expect, SimpleExpect, and Flow Control keywords as you would like. For more information, see Script Syntax.
- **Expect.** Opens the Rules Expression editor. Whatever is placed in the Expression box appends to the end of the script as an Expect expression.
- **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.

5 Click **OK** to save changes.

Types of TCPIP Monitors

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

WhatsUp Gold is installed with the following types of TCP/IP monitors already configured.

- **Echo.** Checks to make sure an Echo server is running on the assigned port.
- **FTP.** Checks to make sure an FTP server is running on the assigned port.
- **HTTP.** Checks to make sure an HTTP server is running on the assigned port.
- **HTTPS.** Checks to make sure the Secure HTTP server is running on the assigned port, and that WhatsUp Gold can negotiate a connection using SSL protocols. This monitor does not check on the validity of SSL certificates.
- **HTTP Content Scan.** Performs advanced monitoring of a specific web page to make sure specific content appears in the page's code. Supports advanced HTTP processes such as form submission and non-standard HTTP headers. For information on creating a basic HTTP Content Scan monitor, see New/Edit HTTP Content Monitor.
- **IMAP4.** Checks to make sure a IMAP4 server is running on the assigned port.
- **NNTP.** Checks to make sure a NNTP server is running on the assigned port.
- **POP3.** Checks to make sure a POP3 mail server is running on the assigned port.
- **Radius.** Checks to make sure a Radius server is running on the assigned port.
- **SMTP.** Checks to make sure a SMTP mail server is running on the assigned port.
- **Time.** Checks to make sure a Time server is running on the assigned port.

iv) Types of TCP/IP monitors

WhatsUp Gold is installed with the following types of TCP/IP monitors already configured.

- **Echo.** Checks to make sure an Echo server is running on the assigned port.
- **FTP.** Checks to make sure an FTP server is running on the assigned port.
- **HTTP.** Checks to make sure an HTTP server is running on the assigned port.
- **HTTPS.** Checks to make sure that the Secure HTTP server is running on the assigned port, and that WhatsUp Gold can negotiate a connection using SSL protocols. This monitor does not check on the validity of SSL certificates.

- **HTTP Content Scan.** Monitors a specific web page to make sure that specific content appears in the code for the page.
- **IMAP4.** Checks to make sure a IMAP4 server is running on the assigned port.
- **NNTP.** Checks to make sure a NNTP server is running on the assigned port.
- **POP3.** Checks to make sure a POP3 mail server is running on the assigned port.
- **Radius.** Checks to make sure a Radius server is running on the assigned port.
- **SMTP.** Checks to make sure a SMTP mail server is running on the assigned port.
- **Time.** Checks to make sure a Time server is running on the assigned port.

v) Using the Rules Expression Editor

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

You can use a rule expression to test a string of text for particular patterns.

- Enter an expression in the **Expression** box. Use the **>**, **Match case**, and **Invert result** options to the right of the Expression box to help build the expression.
- In the **Comparison text** box, enter text to test compare against the expression you built in the Expression box.
- Click **Test** to compare the expression against potential payloads you can receive.

After creating and testing the expression, click **OK** to insert the string into the Match on box.



Note: If you have multiple payload "match on" expressions, they are linked by "OR" logic - not "AND" logic. Example: If you have two expressions, one set to "AB" and the other to "BA", it will match against a trap containing any of the following: "AB" or "BA" or "ABBA".

a. Script Syntax

You create a script using keywords. In general, Script Syntax is `Command=String`. The command is either `Send`, `Expect`, `SimpleExpect`, or `Flow Control`.



Note: A script can have as many send and receive lines as needed. However, the more you have, the slower the service check.

Keywords



Note: To comment out a line, use the # symbol as the first character of the line.

- To send a string to a port, use the *Send* (on page 168)= keyword.
- To expect a string from a port, use the *SimpleExpect* (on page 167)= or the *Expect* (on page 167)= keyword.
- To receive a conditional response for an error or success, use *Flow Control Keywords* (on page 171).

Examples

If you have a TCP service to check, you need to do the following:

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

b. Script Syntax: Expect=Keyword

Expect=Keyword gives you flexibility to accept variable responses and pick out crucial information using special control characters and regular expressions. If you do not need flexibility, or are new to writing your own custom TCP/UDP scripts, you may want to use the *SimpleExpect* (on page 167) keyword.

There are 4 variations of the Expect Keyword:

- **Expect.** Returns true when the expected value is matched.
- **Expect(MatchCase).** Only returns true when the case matches the expected value.
- **DontExpect.** Returns true when the value is not found.
- **DontExpect(MatchCase).** Returns true when the value is not found.

The Expect syntax is *Expect=Response*, where the Response is either specified as an exact text string, or a mixture of *regular expression rules* (on page 172) and text. The **Add/Edit Expect Rule** button helps you construct and test a regular expression response string. It automatically chooses the variation of Expect for you based on options you select.



Note: **Add/Edit Expect Rule** does not aid in the generation of SimpleExpect keywords.

WhatsUp Gold v7 or v8 users: The ~, ^, ! and = = codes have been replaced with variations on the Expect keyword itself. Migrated definitions are automatically converted.

Example 1:

```
#
# Note: script comments start with a # character
#
# Send a simple text command
#
Send = Hello There
#
# Expect a nice response that begins with, "Hi, How are you"
#
Expect=^Hi, How are you
```

Example 2:

```
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
#
# Expect a large response, but we only care to check that somewhere
# in the response John Doe is mentioned
#
Expect=John Doe
```

Example 3:

```
#
# Send a binary escape (27) and an x y and z and then a nak (21)
#
Send=\x1Bxyz\x15
#
# Expect something that does *not* contain 123 escape (27)
#
DontExpect=123\x1B
```

c. Script Syntax: Send=Keyword

To Send command on a connection, use a `Send=keyword`. The script syntax is `Send=Command`. The Command is exactly the message you want to send. You may use a combination of literal characters and binary representations.

WhatsUp Gold understands the C0 set of ANSI 7-bit control characters. A Binary can be represented as `\\x##`, where the ## is a hexadecimal value. Those familiar with the table may also choose to use shorthand such as `\A` (`\x01`) or `\W` (`\x17`)

You can also use `\r` and `\n` as the conventions for sending the carriage return and line feed control characters to terminate a line.

The following table shows the keywords you can use.

| Keyword | Description |
|--------------------|--|
| <code>\\x##</code> | Binary value in Hexadecimal. For example, <code>\\x1B</code> is escape |
| <code>\\</code> | The "\" character |
| <code>\t</code> | The tab character (<code>\x09</code>) |
| <code>\r</code> | The return character (<code>\x0D</code>) |
| <code>\n</code> | The new line character <code>\x0A</code>) |

WhatsUp Gold versions 7 and 8 users: The `%###` decimal syntax for specifying binary octets has been replaced with the `\x##` hexadecimal syntax.

Example 1:

```
#
# Note: script comments start with a # character
#
# Send a simple text command
#
Send=Hello There
```

Example 2:

```
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
```

Example 3:

```
#
# Send a binary escape (27) an x y and z and then a nak (21)
#
Send=\\x1Bxyz\\x15
```

d. Script Syntax: SimpleExpect Keyword

The SimpleExpect Keyword lets you specify expected responses from a service. Responses can even be binary (i.e. non-printable ASCII character) responses. If you know exactly (or even approximately) what to expect you can construct a simple expect response string to match against.

This keyword allows you some flexibility in accepting variable responses and picking out only crucial information. If you need additional flexibility you may want to consider using the regular expression syntax available in the *Expect* (on page 167) keyword.

The SimpleExpect script syntax is `SimpleExpect=Response`, where the response is a series of characters you expect back from the service. The following table displays keywords that match logic and wildcards to compare responses byte-by-byte expanding escape codes as you go.

Command Options:

| Keyword | Description |
|---------|--|
| \x## | Binary value (in Hexadecimal) for example \x00 is null |
| . | Matches any character |
| \% | The "%" character |
| \. | The "." character |
| \\ | The "\" character |



Note: Only the number of characters specified in the expect string are used to match the response. The response is expected to start with these characters. Any extra trailing characters received are just ignored.

Example 1:

```
#
# Note: script comments start with a # character
#
# Send=Hello There
#
# Expect a nice response
#
SimpleExpect=Hi, how are you?
```

Example 2:

```
#
# Send a command followed by CR/LF
#
Send=Select * from Accounts\r\n
#
# Expect a large response, be we only care to check that first word
# received is "Customer"
#
SimpleExpect=Customer
```

Example 3:

```
#
# Send a binary escape (27) an x y and z and then a nak (21)
#
Send=\x1B\x15
#
# Expect any byte (we don't care) then an abc and an ack (6)
#
SimpleExpect=.abc\x06
```

e. Script Syntax: Flow Control Keywords

The following Flow Control keywords are used in a script to return "error" or "success" responses of steps within that script.

- **IfState.** This checks for the current state (ok or error) and jumps to a label if true.
Valid syntax: `IfState {ERR|OK} label`

Example:

```
IfState ERR End
IfState OK Bye
```

- **Goto.** This immediately jumps to a label.
Valid syntax: `Goto End`

Example:

```
Goto End
```

- **Exit.** This immediately ends the script with an optional state (ok or error). The optional state overrides the current state.
Valid syntax: `Exit {ERR|OK}`

Example:

```
Exit ERR
Exit OK
```


- **:Label.** This defines a label that can be the target of a jump. A label is defined by a single word beginning with the ":" character.
Valid syntax: :(with a name following)

Example:

Bye

- **OnError.** This allows for a global handling of an error situation
Valid Syntax: OnError {EXIT|CONTINUE|GOTO} label

Example:

OnError EXIT (Default behavior)

OnError CONTINUE

OnError GOTO Logoff

f. Send to Disconnect Examples

For a service like FTP, to disconnect would be QUIT/*r*/*n*. If a command string is not specified, the connection is closed by sending a FIN packet and then an RST packet.

The /*r* (carriage return) and /*n* (line feed) are the conventions for sending these control characters to terminate a string. You can use:

- /*r* = 0x0a
- /*n* = 0x0d
- /*t* = 0x09 or /*xnn* where *nn* is any hexadecimal value from 00 to FF

The disconnect string is:

Send=QUIT/*r*/*n*

g. Regular Expression Syntax

This table lists the meta-characters understood by the WhatsUp Gold Regex Engine.

Matching a Single Character

| Meta-character | Matches |
|----------------|--|
| . | Matches any one character |
| [...] | Matches any character inside the brackets. Example, [abc] matches "a", "b", and "c" |
| [^...] | Matches any character except those inside the brackets. Example, [^abc] matches all characters except "a", "b", and "c". See below for alternate use - the way ^ is used controls its meaning. |
| - | Used within a character class. Indicates a range of characters. Example: [2-7] matches any of the digits "2" through "7". Example: [0-3a-d] is equivalent to [0123abcd] |
| \ | Interpret the next character literally. Example: 3\.14 matches only "3.14". whereas 3.14 matches "3214", "3.14", "3z14", etc. |

| Meta-character | Matches |
|-------------------------------------|--|
| <code>\\xnn</code> binary character | Match a single binary character. nn is a hexadecimal value between 00 and FF. Example: <code>\\x41</code> matches "A" Example: <code>\\x0B</code> matches Vertical Tab |

Quantifiers

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

Matching Position

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

Other

| Meta-character | Matches |
|----------------------------|--|
| <code> </code> alternation | Matches either expression it separates. Example: <code>H Cat</code> matches either "Hat" or "Cat" |

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

Abbreviations

Abbreviations are shorthand Meta-characters.

| Abbreviation | Matches |
|--------------|--|
| \a | Any alphanumeric character: ([a-zA-Z0-9]) |
| \b | White space (blank): ([\t]) |
| \c | Any alphabetic character: ([a-zA-Z]) |
| \d | Any decimal digit: [0-9] |
| \D | Any non decimal digit: [^0-9] |
| \h | Any hexadecimal digit: ([0-9a-fA-F]) |
| \n | Newline: (\r \r?\n) |
| \p | Any punctuation character: ,./\':;"!~?@\$%^&*(){}- _=+ <>!\~ |
| \P | Any non-punctuation character |
| \q | A quoted string: (\["^\\"]*\") (\['^\\']*\') |
| \s | WhatsUp Gold style white space character: [\t\n\r\f\v] |
| \S | WhatsUp Gold style non-white space character: [^ \t\n\r\f\v] |
| \w | Any word characters (letters and digits): ([a-zA-Z0-9_]) |
| \W | Non-word character: ([^a-zA-Z0-9_]) |
| \z | An integer: ([0-9]+) |

h. Text String Example

Example 1

To check an IRC (Internet Relay Chat) service, you can send the command `Version/r/n` and the expected response from the IRC service is: `irc`.

Name: IRC; Port: 6667; TCP.

Send=Version/r/n

Expect=irc

Send=QUIT/r/n



Note: You can use *Telnet* (on page 176) to find the proper value for **SimpleExpect**, or an **Expect** string for a particular service. Packet Capture tools can also be very useful.

Adding and editing a Telnet Monitor

Telnet is a simple service monitor that checks for a Telnet server on port 23. If no telnet service responds on this port, then the service is considered down.

To add or edit a Telnet monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **Telnet Monitor** from the list to create a new Telnet monitor. Click **OK**.
- or -
Select the Telnet monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Timeout.** Enter a timeout value. This is the length of time in which the service is given a chance to respond. If there is no response in this amount of time, the service is considered down.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
- 5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

vi) Using telnet to determine "Expect on Connect" string

Telnet to the desired port on the host when you are certain it is working properly, and note the host response. You can enter just an identifying portion of a `SimpleExpect` or `Expect` keyword.

For example, if you expect to get "220 hostname.domain.com lmail v1.3" back from the host, you could use "220 host" as a response string (i.e. `SimpleExpect=220 host`, or `Expect=^220 host`).



Note: Some services are based on binary protocols (such as DNS) and do not provide you with a simple response string to use. You can use a packet capture tool to view these types of responses.

Adding and editing a Temperature Monitor

The Temperature Monitor checks select Cisco switches/routers, Dell servers, HP ProCurve switches/routers, and Ravica temperature probes to see that they return a value that signals they are in an up state. The monitor first checks to see if a device is a Cisco, Dell, HP, or Ravica device, then checks any enabled temperature monitor devices. If a temperature probe is disabled, the monitor ignores it; if a temperature probe does not return a value of 1 - Normal (for Cisco switches/routers), 3 - OK (for Dell server devices), 4 - Good (for HP ProCurve switches and routers), 2 - OK (for HP ProLiant servers), or 2 - normal (for Ravica temperature probes) the monitor is considered down.

This monitor is pre-configured and exists in the Active Monitor Library upon installation of WhatsUp Gold. Unlike many pre-configured active monitors, the Temperature Monitor's default configuration cannot be modified. However, you can modify the monitor name and description, as well as the SNMP timeout and number of retries used while attempting to connect to devices.

To add or edit a temperature monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **Temperature Monitor** to create a new temperature monitor. Click **OK**.
- or -
Select the temperature monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.



Tip: Click **Advanced** to set the SNMP timeout and number of retries.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing a WAP Radio Monitor

The Wireless Access Point (WAP) Radio Active Monitor, included in the WhatsUp Gold Premium, Distributed, and MSP Editions, uses Simple Network Management Protocol (SNMP) to query WAP devices and report the status of the wireless access point. This monitor indicates that the wireless radio is in either an up or down state. Currently, the WAP Radio Active Monitor supports Cisco Aironet WAPs.



Important: The Cisco WAP you want to monitor must support Cisco Dot 11 and IEEE 802.11 MIBs for WhatsUp Gold WAP Monitor features to operate.

To determine the monitor status, the monitor first looks at the ifType (OID 1.3.6.1.2.1.2.2.1.3) value. The ifType value of 71 - IEEE 80211 must be present for the monitor to continue checking the WAP radio device status. If the ifType value is true, then the ifAdminStatus (OID: 1.3.6.1.2.1.2.2.1.7) value is checked. Finally, if the ifAdminStatus value for the interface is in the down or testing state, the active monitor is considered down and the ifOperStatus (OID: 1.3.6.1.2.1.2.2.1.8) value is checked. If the ifOperStatus value is 1 - up or 5 - dormant, the WAP radio is determined to be in the up state; otherwise the device is considered to be in the down state.

This monitor is pre-configured and exists in the Active Monitor Library upon installation of WhatsUp Gold. Unlike many pre-configured active monitors, the WAP Radio Monitor's default configuration cannot be modified. However, you can modify the monitor name and description, as well as the SNMP timeout and number of retries used while attempting to connect to devices.

To add or edit a WAP radio monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **WAP Radio Monitor** to create a new WAP radio monitor
- or -
Select the WAP radio monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.



Tip: Click **Advanced** to set the SNMP timeout and number of retries.

5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Using Premium Active Monitors

WhatsUp Gold Premium Edition provides all of the network monitoring capabilities of WhatsUp Gold and extends the product to allow additional monitoring capabilities, including:

- APC UPS monitor watches your American Power Conversion Uninterruptible Power Supply (APC UPS) device and alerts you when selected thresholds are met or exceeded, output states are reached, and/or abnormal conditions are met.
- Email monitor lets you periodically verify that mail servers are not only up, but are receiving and delivering messages properly.
- Microsoft® Exchange™ and Microsoft SQL Server monitors let you manage the availability of key application services, rather than just the network visibility of the host server.
- Fan monitor checks select Cisco, Dell, and HP device fans and cooling devices, such as active and passive cooling components, to see that they are enabled and return a values that signal they are working properly.
- File Properties monitor
- Folder monitor
- FTP monitor
- HTTP Content monitor
- Network Statistics monitor
- Power Supply monitor
- Printer monitor
- Process monitor
- SQL Query monitor
- General application monitoring using Microsoft's WMI lets you monitor any performance counter value and trigger an alarm if the value changes, goes out of range, or experiences an unexpected rate of change.

Adding and editing an APC UPS Monitor

An APC UPS monitor watches your American Power Conversion Uninterruptible Power Supply (APC UPS) device and alerts you when selected thresholds are met or exceeded, output states are reached, and/or abnormal conditions are met. For example, an alert can be sent when the UPS battery capacity is below 20%, when the battery temperature is high, when the battery is in bypass mode due to a battery overload state, and many other UPS alert conditions.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit an APC UPS active monitor:

- 1** Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2** Click the **Active** tab. The Active Monitor list appears.
- 3** Click **New** and select **APC UPS Monitor** to create a new APC UPS monitor. Click **OK**.
- or -
Select the APC UPS monitor you want to change from the list of current monitors, and then click **Edit**.
- 4** Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor name in the Active Monitor Library.
 - **Thresholds.** Select the threshold(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the thresholds. By default, all of the thresholds are selected for use in the monitor.



Tip: Select a threshold, then click **Configure** to set its individual threshold settings.

- **Monitor the following output states.** Select the output state(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the output states. By default, the following output states are selected for use in the monitor:
 - Abnormal Condition Present
 - Bad Output Voltage
 - Battery Charger Failure
 - Battery Communication Lost
 - High Battery Temperature
 - In Bypass due to Fan Failure
 - In Bypass due to Internal Fault
 - Low Battery
 - No Batteries Attached
 - Overload
 - Replace Battery
 - Software Bypass



Tip: Use the list's vertical scroll bar to browse the output states.

- **Monitor the following abnormal conditions.** Select the abnormal condition(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the abnormal conditions. By default, all of the abnormal conditions are selected for use in the monitor.



Tip: Use the vertical scroll bar to browse the list of abnormal conditions.



Tip: Click **Advanced** to set the SNMP timeout and number of retries.

5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Monitoring mail servers

The Email Monitor lets you monitor that a mail server is available and functioning correctly. This monitor checks a mail server by first sending the server an email via SMTP. The monitor then attempts to delete previously sent emails using either POP3 or IMAP. If no emails from the monitor are present in the inbox to delete, the mail server is considered down.

The email active monitor supports encryption with SSL/TLS and SMTP Authentication which ensures that the monitor sends emails to a secure email account.

The Email Monitor's email delivery check is done across two polls. Therefore, it is important that you pick a meaningful polling interval. For example, if you want to be notified when your mail server is taking more than two minutes to send and receive email, use a two-minute polling interval.



Note: WhatsUp Gold can monitor any POP3 server that supports these commands: USER, PASS, LIST, TOP, QUIT, RETR, and DELE. WhatsUp Gold can monitor any IMAP server that supports these commands: LOGIN, SELECT, SEARCH, STORE, CLOSE, and LOGOUT.

vii) Adding and editing an Email Monitor

Email monitors check a mail server by first sending the server an email via SMTP. The monitor then attempts to delete previously sent emails using either POP3 or IMAP. If no emails from the monitor are present in the inbox to delete, the mail server is considered down.

The email active monitor supports encryption with SSL/TLS and SMTP Authentication which ensures that the monitor sends emails to a secure email account.



Important: You must use a separate email account for every Email Active Monitor that you create. Failure to do so will result in false negatives. For example, if you want to check both IMAP and POP3 on the same server, and create two instances of the Email Monitor, one configured with POP3 and one with IMAP, you must use two separate email accounts. Otherwise, one monitor will delete all emails previously sent from both instances of the monitor and will incorrectly report the mail server as down.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit an Email Active Monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **Email Monitor** from the list to create a new Email monitor. Click **OK**.
- or -
Select the Email monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.

Outgoing mail

- **SMTP server.** Type the address of the server on which SMTP is running. Use the default, %Device.Address, to use the device IP address on which the monitor is attached.
- **Port.** Type the port on which the SMTP service is listening. The standard SMTP port is 25.
- **Mail to.** Type the address to which the Email Monitor sends email.
- **Mail from.** Type the address you want listed as "From" in the email sent by the Email Monitor.

Incoming mail

- **Mail server.** Type the address of the server on which the POP3 or IMAP service is running.
 - **Account type.** Type the protocol (POP3 or IMAP) you want the monitor to use to check for correct email delivery.
 - **Username.** Type the username of the account in which the monitor uses to log in.
 - **Password.** Type the password for the account in which the monitor uses to log in.
- 5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).



Note: You can configure additional options, including authentication and encryption options by *Setting Advanced Properties for an Email Active Monitor*. To access this dialog, click **Advanced**.

viii) Example: Email Monitor

This example creates an Email Monitor that checks to see if an account on Google's Gmail service is working properly. To test and use the Email Monitor created in this example properly, you need a working Gmail account configured to allow POP3 and SMTP access.

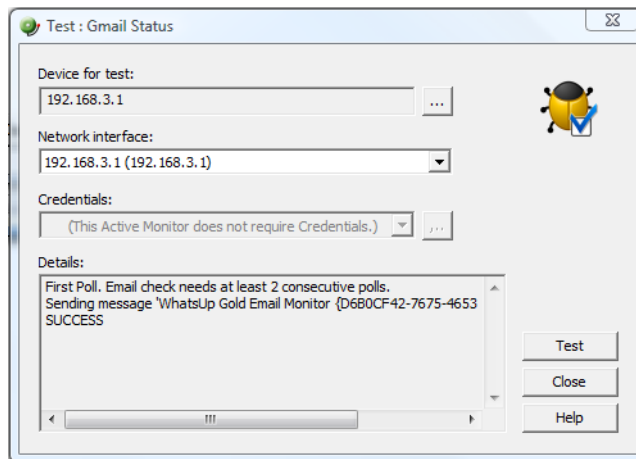
To create an Email Monitor for a Gmail account:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab inside the dialog.
- 3 Click **New**. The Select Active Monitor Type dialog appears.
- 4 Select the Email Monitor, then click **OK**. The Add Email Monitor dialog appears.

- 5 Enter or select the appropriate information in the dialog fields:
 - a) Enter Gmail Status in **Name**.
 - b) In **Description**, enter Checks Gmail status.
In the **Outgoing mail** section of the dialog:
 - c) Enter smtp.gmail.com in **SMTP server**.
 - d) Enter 587 for the Port.

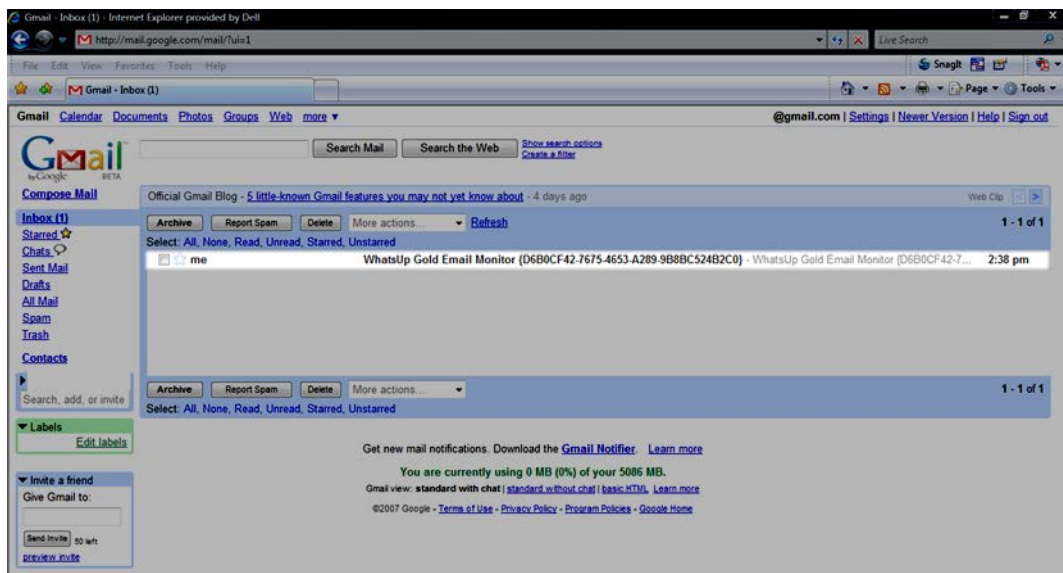
- e) If you have a Gmail account, enter it in **Mail to**, in the following format:
youraccount@gmail.com. If you do not have a Gmail account, create one on the Gmail site.
- f) Enter the same Gmail account in **Mail from**.
In the **Incoming mail** section of the dialog:
- g) Enter pop.gmail.com in the **Mail server** box.
- h) Choose **POP3** from the **Account type** list.
- i) Again, enter your Gmail account in **Username**.
- j) Enter the password for your Gmail account in **Password**.
- 6** Click **Advanced**. The Advance Monitor Properties dialog appears.
- 7** Enter or select the appropriate information in the dialog fields:
In the **SMTP advanced properties** section of the dialog:
 - a) Select **Use SMTP authentication**.
 - b) Enter your Gmail account in **Username**.
 - c) Enter the password for your Gmail account in **Password**.
 - d) Select **Use an encrypted connection (SSL/TLS)**.
 - e) Use the default **Timeout** of 5 seconds.
In the **POP3 advanced properties** section of the dialog:
 - f) Enter **995** for the Port
 - g) Select **Use an encrypted connection (Use SSL with TLS)**.
 - h) Use the default **Timeout** of 5 seconds.
 - i) Click **OK** to save changes and return to the Add Email Monitor dialog.
 - j) Click **OK** on the Add Email Monitor dialog to add the Gmail Monitor to the Active Monitor Library.
- 8** Test the Gmail Status monitor.
 - a) From the WhatsUp Gold console, go to **Configure > Active Monitor Library**. The Active Monitor Library dialog appears.

b) Select the Gmail Status monitor, then click **Test**.



The Test dialog will list the test as either SUCCESS or FAILED.

You can log in to the Gmail account used for the Gmail Status monitor and actually see the email sent by WhatsUp Gold via the Email Monitor.



Monitoring a Microsoft Exchange 2007 Server

The Exchange Monitor lets you monitor the Microsoft® Exchange™ Server application. The Exchange Monitor provides real-time information about the state and health of Microsoft Exchange servers on your network.

The Exchange Monitor supports monitoring of Microsoft Exchange Server version 2007 and later, which can be installed on any machine in your network.



Important: Do not use the Exchange Monitor to monitor Exchange 2003 servers.

To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.

Why use it?

WhatsUp Gold can monitor and report the status of the standard services associated with any mail server, such as SMTP, POP3, and IMAP. If any of these services fail, your users are unable to get mail. It is a good idea to set up monitoring on these services so that you are the first to know if they fail. The Exchange Monitor extends monitoring to parameters reported by Microsoft Exchange, allowing you to get an early warning of a degradation in performance. For example, you can monitor the SMTP queues to see if performance is within an expected range, and if not, you can intervene before the SMTP service fails.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

Getting Started with Exchange Monitors

This topic describes the overall process of configuring an Exchange Monitor, assigning it to a device, and getting feedback from the monitor.

A basic approach to using the Exchange Monitor:

- 1 Determine which *Exchange roles and performance thresholds* (on page 186) to monitor.
- 2 Determine which *Exchange services* (on page 187) to monitor.
- 3 Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination.

To start, it may be simpler to create one monitor for each parameter or service that you want to monitor. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions.

- 4 *Configure an Exchange Monitor* (on page 185) with your selected parameters and/or services.
- 5 Add the Exchange Monitor to the device that represents your Microsoft Exchange server.
- 6 Set up an Action to tell you when the monitor goes down or comes back up.



Note: The monitor will be reported down if any of the parameters or services in that monitor are down.

Adding and Editing an Exchange Monitor

The Exchange Monitor lets you monitor the Microsoft® Exchange™ Server application. The Exchange Monitor provides real-time information about the state and health of Microsoft Exchange servers on your network. The Exchange Monitor supports monitoring of Microsoft Exchange Server version 2007 and later, which can be on any machine in your network. To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.



Important: Do not use the Exchange Monitor to monitor Exchange 2003 servers.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit an Exchange active monitor:

- 1** Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2** Click the **Active** tab. The Active Monitor list appears.
- 3** Click **New** and select **Exchange Monitor** from the list to create a new Exchange monitor. Click **OK**.
- or -
Select the Exchange monitor you want to change from the list of current monitors, and then click **Edit**.
- 4** Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Performance aspects to monitor.** Select the Category that matches the Exchange server role(s). Highlight the category and click **Configure** to set the individual thresholds. The threshold configuration dialog for the highlighted category opens.
 - **Services to monitor.** Select the services you want to monitor.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.
- 5** Click **OK** to save your changes.

For more information on configuring an Exchange Monitor, go to *Getting Started with Exchange Monitors*.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

ix) Exchange Roles and Performance Monitoring

Exchange Server Roles are used to group the performance monitoring parameters used by WhatsUp Gold to indicate the state of the Exchange server. A server role is a unit that logically groups the required features and components needed to perform a specific function in the messaging environment. By mirroring these roles in the Exchange Server monitor, the configuration of the monitor becomes a simple exercise of setting the threshold values associated with each Exchange Server Role you want to monitor.

- Hub Transport Server Role thresholds
- Mailbox Server Role thresholds
- Outlook Web Access Server Role thresholds

x) Exchange Services

You can monitor the following critical Exchange services to determine if the service is available (Up) or is disabled (Down).

| Select this process: | If you want to: |
|-----------------------------------|--|
| Active Directory Topology Service | Monitor the Active Directory Topology service (<code>MSExchangeADTopology</code>). This service provides Active Directory topology information to several Exchange Server components. |
| Anti-spam Update | Monitor the Anti-Spam Update service (<code>MSExchangeAntispamUpdate</code>). Used to automatically download anti-spam filter updates from Microsoft Update. |
| Edge Sync | Monitor the Edge Sync service (<code>MSExchangeEdgeSync</code>). Connects to ADAM instance on subscribed Edge Transport servers over secure Lightweight Directory Access Protocol (LDAP) channel to synchronize data between a Hub Transport server and an Edge Transport server. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| File Distribution | Monitor the File Distribution service (<code>MSExchangeFDS</code>). Used to distribute offline address book and custom Unified Messaging prompts. This service is dependent upon the Microsoft Exchange Active Directory Topology and Workstation services. |
| IMAP4 | Monitor the IMAP4 service (<code>MSExchangeIMAP4</code>). Provides IMAP4 services to IMAP clients. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| Information Store | Monitor the MAPI Information Store service (<code>MSExchangeIS</code>). Manages Exchange Server databases. Provides data storage for messaging clients. This service is dependent upon the following services: Event Log, NT LM Security Support Provider, Remote Procedure Call (RPC), Server, and Workstation. |
| Mailbox Assistants | Monitor the Mailbox Assistants service (<code>MSExchangeMailboxAssistants</code>). This service provides functionality for Calendar Attendant, Resource Booking Attendant, Out of Office Assistant, and Managed Folder Mailbox Assistant. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |

| Select this process: | If you want to: |
|-----------------------|---|
| Mail Submission | Monitor the Mail Submission service (MSExchangeMailSubmission). Submits messages from a Mailbox server to a Hub Transport server. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| Monitoring | Monitor the Monitoring service (MSExchangeMonitoring). Provides a remote procedure call (RPC) server that can be used to invoke diagnostic cmdlets. This service does not have any dependencies. |
| POP3 | Monitor the POP3 service (MSExchangePOP3). Provides POP3 services to POP3 clients. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| Replication Service | Monitor the Replication service (MSExchangeRepl). Provides log shipping functionality for local continuous replication (LCR) and cluster continuous replication (CCR). This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| System Attendant | Monitor the System Attendant service (MSExchangeSA). Provides monitoring, maintenance, and directory lookup services for Exchange Server. This service is dependent upon the following services: Event Log, NT LM Security Support Provider, Remote Procedure Call (RPC), Server, and Workstation. |
| Search Indexer | Monitor the Search Indexer service (MSExchangeSearch). Provides content to the Microsoft Search (Exchange Server) service for indexing. This service is dependent upon the Microsoft Exchange Active Directory Topology service and the Microsoft Search (Exchange Server) service. |
| Service Host | Monitor the Service Host service (MSExchangeServiceHost). Configures the RPC virtual directory in Internet Information Services (IIS), and registry data for ValidPorts, NSPI Interface Protocol Sequences, and AllowAnonymous for Outlook Anywhere. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| Transport | Monitor the Transport service (MSExchangeTransport). Provides Simple Message Transfer Protocol (SMTP) server and transport stack. This service is dependent upon the Microsoft Exchange Active Directory Topology service. |
| Transport Log Search | Monitor the Transport Log Search service (MSExchangeTransportLogSearch). Provides message tracking and transport log searching. This service has no dependencies. |
| Speech Engine Service | Monitor the Speech Engine service (MSSpeechService). Provides speech processing services for Unified Messaging. This service is dependent upon the Windows Management Instrumentation service. |
| Unified Messaging | Monitor the Unified Messaging service (MSExchangeUM). Provides Unified Messaging features, such as the storing of inbound faxes and voice mail messages in a user's mailbox, and access to that mailbox via Outlook Voice Access. This service is dependent upon the Microsoft Exchange Active Directory Topology service and the Microsoft Exchange Speech Engine service. |

Example: Exchange Server monitor

To monitor the operating system on the Exchange server, you can create a monitor called `ExchangeMailServer` to monitor an Exchange server operating in the Mailbox Server role. The purpose of this monitor is to give an indication of the performance of the Exchange server in regards to the threshold values and services associated with the Mailbox Server role. To this end, you can configure the monitor to monitor the thresholds associated with the Mailbox Server role, as well as to monitor the Information Store, Mailbox Assistants and Mail Submission services.

- 1 From the **Admin** panel, select **Monitor Library**. The Monitor Library dialog appears.
- 2 If not already selected, click the **Active** tab.
- 3 Click **New**. The Select Active Monitor Type dialog appears.
- 4 Select **Exchange Monitor** and click **OK**. The New Exchange Server Monitor dialog appears.
 - a) In the **Name** box, type `ExchangeMailServer` to identify that this monitor checks system parameters.
 - b) In the **Category** field, select **Mailbox Server**.
 - c) Highlight the Mailbox Server role, then click **Configure**. The Configure Mailbox Server Thresholds menu appears.
 - d) In the **RPC Averaged Latency must not exceed:** field, type an appropriate threshold for the average latency for Remote Procedure Calls, and click **OK**. The New Exchange Monitor screen appears.
 - e) Under **Services to monitor**, select the System Attendant service. Make sure these items have a check in the box to the left. You need to clear the selections for the other parameters and also for the other processes.
 - f) Click **OK** to add the `ExchangeMailServer` monitor to the Active Monitor library.
- 5 Add the `ExchangeMailServer` monitor to your Exchange server device.
 - a) In your device list, find the device that represents the Exchange server. Right-click the device, then select **Properties**. Select **Active Monitors**.
 - b) Click **Add**. The Active Monitor wizard appears.
 - c) Select the `ExchangeMailServer` monitor, and continue with the wizard to configure any actions for the monitor.

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

Monitoring Microsoft Exchange 2003 Servers

The Exchange 2003 Monitor lets you monitor the Microsoft® Exchange™ 2003 Server applications. The Exchange 2003 Monitor provides real-time information about the state and health of Microsoft Exchange servers on your network.

The Exchange 2003 Monitor supports monitoring of Microsoft Exchange Server versions 2000 and 2003, which can be on any machine in your network.

To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.

Why use it?

WhatsUp Gold can monitor and report the status of the standard services associated with any mail server, such as SMTP, POP3, and IMAP. If any of these services fail, your users are unable to get mail. It is a good idea to set up monitoring on these services so that you are the first to know if they fail. The Exchange Monitor extends monitoring to parameters reported by Microsoft Exchange, allowing you to get an early warning of a degradation in performance. For example, you can monitor the SMTP queues to see if performance is within an expected range, and if not, you can intervene before the SMTP service fails.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

xi) Getting Started with Exchange 2003 Monitors

This topic describes the overall process for configuring an Exchange 2003 Monitor, assigning it to a device, and getting feedback from the monitor.

A basic approach to using the Exchange 2003 Monitor:

- 1 Determine which *Exchange 2003 parameters* (on page 191) to monitor.
- 2 Determine which *Exchange 2003 services* (on page 192) to monitor.
- 3 Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination.

To start, it may be easier to create one monitor for each parameter or service that you want to monitor. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions. For example, a single monitor to check disk space, named Exchange2003Disk, is reported in logs with this name. If Exchange2003Disk is reported down, you know it's a disk space problem.

- 4 *Adding and Editing an Exchange 2003 Monitor* (on page 190) with your selected parameters and/or services.
- 5 Add the Exchange 2003 Monitor to the device that represents your Microsoft Exchange 2003 server.
- 6 Set up an Action to tell you when the monitor goes down or comes back up.



Note: The monitor is reported down if any of the parameters or services in that monitor are down.

xii) Adding and Editing an Exchange 2003 Monitor

The Exchange Monitor lets you monitor the Microsoft® Exchange™ 2003 Server application. The Exchange 2003 Monitor provides real-time information about the state and health of Microsoft 2003 Exchange servers on your network. The Exchange 2003 Monitor supports monitoring of Microsoft Exchange Server version 2003 only, which can be on any machine in your network. To create custom parameters to monitor, the Exchange Server host must be WMI-enabled.



Important: Use the Exchange 2003 Monitor to monitor Exchange 2003 servers only.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit an Exchange 2003 active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **Exchange 2003 Monitor** from the list to create a new Exchange 2003 monitor.
- or -
Select the Exchange 2003 monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Thresholds to monitor.** Select the thresholds you want to monitor. To configure the setting for a threshold, highlight the parameter, and click **Configure**.
 - **Services to monitor.** Select the services you want to monitor. By default, all services are selected.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
- 5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

a. Exchange 2003 parameters

You can set thresholds on the following parameters:

| Select this parameter: | If you want to: |
|------------------------|---|
| CPU (on page 892) | Monitor CPU state on the Exchange host. |
| Memory | Monitor free memory on the Exchange host. |
| Disk | Monitor available disk space on the Exchange host. |
| System | Monitor operating system performance on the Exchange host, including context switches, CPU queue length, and system calls. |
| Links | Monitor message-handling links between mail servers. A link can contain zero or more ExchangeQueue objects, depending on the current message traffic along the link. In the Exchange System Manager, these links are called queues. |
| Queues (on page 887) | Monitor the dynamic queues created to transfer individual messages between mail servers. An ExchangeQueue is part of an ExchangeLink. ExchangeQueue objects are not the same as the queues listed in the Exchange System Manager. |
| Cluster | Monitor the state of the clustered resources on the Exchange server. This parameter will return a value of Unknown - 0; OK - 1; Warning - 2; Error - 3. |
| Custom Thresholds | Browse and select from the large number of additional parameters that Microsoft Exchange reports. |

b. Exchange 2003 services

You can monitor the following critical Exchange services to determine whether the service is available (Up) or is disabled (Down).

| Select this process: | If you want to: |
|--------------------------|---|
| Information Store | Monitor the MAPI message store service. The information store can contain messages, forms, documents, and other information created by users and applications. It provides each user with a server-based mailbox and stores public folder contents. |
| Site Replication Service | Monitor the Site Replication service. |
| Management | Monitor the Management service. |
| MTA Stacks | Monitor the Mail Transport Agent (MTA) service. The MTA service provides the engine for sending messages and distributing information between Microsoft Exchange Server systems or between Microsoft Exchange Server and a foreign system. Each MTA is associated with one information store. It is accessed using MAPI calls only and has no direct programmer interface with Microsoft Exchange Server. The MTA conforms to the 1988 X.400 specification. |
| System Attendant | Monitor the System Attendant service. |
| Routing Engine | Monitor the Routing Engine, which determines the routes for delivering messages to remote addresses. It forwards the message to remote Exchange |

| Select this process: | If you want to: |
|----------------------|---|
| | addresses using SMTP. If some addresses are on a foreign messaging system, the routing engine assigns the message to a gateway that handles the address type of the recipient and passes the message to the message transfer agent (MTA). |
| Event | Monitor the Event service, which reports warnings and errors. |
| POP3 | Monitor the POP3 service, which lets a mail client access mail on the server. |
| IMAP4 | Monitor the IMAP4 service, which lets a mail client access mail on the server. |

xiii) Example: Exchange Server 2003 Monitor

To monitor the condition of the operating system on the Exchange server, you can create a monitor called `ExchangeSystemCheck` and add several parameters. The purpose of this monitor is to give an indication of the general state of the system on which your Exchange server is running. To this end, you can configure the monitor to check thresholds for the CPU, Memory, and System parameters. The monitor will also check the state of the System Attendant service.

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab inside the dialog.
- 3 Click **New**. The Select Active Monitor Type dialog appears.
- 4 Select **Exchange 2003 Monitor** and click **OK**. The New Exchange Server 2003 Monitor dialog appears.
 - a) In the **Name** box, enter `ExchangeSystemCheck` to indicate that this monitor performs a check on system parameters.
 - b) Under **Thresholds to monitor**, select the CPU, Memory, and System parameters; then under **Services to monitor**, select the System Attendant service. Make sure these items have a check in the box to the left. Clear the selections for the other parameters and services.
 - c) Highlight the **CPU** parameter, then click **Configure**. The CPU Threshold dialog opens. Enter an appropriate threshold and click **OK**.
 - d) Highlight the **Memory** parameter, then click **Configure**. The Memory Threshold dialog disappears. Enter an appropriate threshold for the amount of free memory and click **OK**.
 - e) Highlight the **System** parameter, then click **Configure**. The System Threshold dialog appears. Enter an appropriate threshold and click **OK**.
 - f) Click **OK** to add the `ExchangeSystemCheck` monitor to the Active Monitor library.
- 5 Add the `ExchangeSystemCheck` monitor to your Exchange server device.
 - a) In your device list, find the device that represents the Exchange server. Right-click the device, then select **Properties**. Select **Active Monitors**.
 - b) Click **Add**. The Active Monitor wizard appears.

- c) Select the ExchangeSystemCheck monitor, and continue with the wizard to configure any actions for the monitor. For more information on setting up an action, see *Configuring an action* (on page 273).

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

xiv) Adding and editing a Fan Monitor

The Fan Monitor checks select Cisco, Dell, and HP device fans and cooling devices, such as active and passive cooling components, to see that they are enabled and returning values that signal they are working properly. The monitor first checks to see if a device is a Dell, Cisco, or HP device, then checks any enabled fans and other cooling devices. If a fan is disabled, the monitor ignores it; if a fan does not return a value of 1 - Normal (for Cisco devices), 3 - OK (for Dell Servers), 1 - Normal (for Dell PowerConnect switches and routers), 4 - OK (for HP ProCurve Servers), 2 - OK (for ProLiant switches and routers) the monitor is considered down.



Note: Not all types of device fans and cooling components can be monitored using the Fan Monitor. Check the make and model of your device fan or cooling component before attempting to monitor.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a fan active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New**, then select **Fan Monitor** to create a new fan monitor. Click **OK**.
- or -
Select the fan monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the appropriate information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.



Tip: Click **Advanced** to change the SNMP timeout and number of retries.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing a File Properties Monitor

This monitor checks to see if a file in a local folder, or on a network share, meets the conditions specified in the monitor's configuration.



Note: The File Properties Monitor only checks files in folders local to a device on which WhatsUp Gold is installed, or files in network shares accessible from the WhatsUp Gold device.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To configure a file properties active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **File Properties Monitor** to create a new file properties monitor. Click **OK**.
- or -
Select the file properties monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Path of the file to monitor.** Type the Universal Naming Convention (UNC) file path that WhatsUp Gold uses to access the file. For example:
`\\192.168.3.1\website\product\index.htm`



Note: Mapped drive paths are not permitted for the File Properties Monitor

- 5 Complete the information in the **Monitor is up if** section:
 - **File.** Select the appropriate option: exists or does not exist. If you select exists, the monitor is up if the selected file is found in the folder on the local directory. If you select does not exist, the monitor is up if the file is not found in the folder on the local directory.



Note: The following options are not required for the monitor scan:

- **File size is.** Select this option, then select the appropriate variable to determine the success or failure of the monitor scan:
 - less than
 - less than or equal to

- greater than
- greater than or equal to
- equal to
- not equal to

Then enter a numerical value for the file size. The default unit used for the file size is bytes. Optionally, you can change the unit to either KB, MB, or GB.

Click the file properties button to obtain the file's current size. This current value populate the file size value field and is used to set the file size threshold. The File size option must be selected for the file properties button to appear.

- **Last modified date is.** Select this option make the monitor dependent on the date on which the file is last modified. This field is populated using the file properties button; click this button to populate the field with the most recent date and time on which the file was modified. This option must be selected for the file properties button to appear.
- **File checksum using ____ is ____.** Select this option to make the monitor dependent on the file's checksum. Select the option, then select the algorithm (SHA1, SHA224, SHA256, SHA384, SHA512) WhatsUp Goldl uses to calculate the checksum. This field is populated using the file properties button; click this button to populate the field with the file's current checksum. This option must be selected for the file properties button to appear.



Warning: Selecting this option can greatly increase the amount of time it takes to complete the monitor scan and can possibly have an adverse affect on WhatsUp Gold performance. The probability of lengthy monitor scans and slower performance increases when you use algorithms other than SHA1 when you are scanning large files, or when you scan files located on network shares.

6 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

xv) About file checksum

File checksums are fingerprint-like fixed data strings assigned to files when they are saved. Checksum algorithms, such as *SHA1* and *SHA512*, are used to monitor checksum files to detect accidental modification of a file, such as corruption during the storage or transmission process. These algorithms match checksums against each other to look for discrepancies; if any exist, the file is known to have been modified.

The File Properties Monitor can monitor current checksum for a file to ensure that it has not been modified by matching the checksum specified in the monitor-configuration to the current checksum. If the monitor finds mismatched checksums, the file is corrupted.

Adding and editing a Folder Monitor

The Folder Monitor checks to see if a local or network share folder meets the conditions specified in the monitor configuration.



Note: The Folder Monitor only checks folders local to a machine on which WhatsUp Gold is installed, or folders on a network share accessible from the WhatsUp Gold device.



Note: This monitor uses the Windows credentials assigned to the device.



Note: If folder or directory contents change during a poll, the change is ignored and is not counted toward folder/file size.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a folder monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **Folder Monitor** from the list to create a new folder monitor. Click **OK**.
- or -
Select the folder monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Path of the folder to monitor.** Type the Universal Naming Convention (UNC) file path that WhatsUp Gold uses to access the file. For example:
\\192.168.3.1\website\product\
 - **Include sub-folders.** Select this option to include all folders within the parent folder in the monitor scan.



Important: Selecting this option can greatly increase the amount of time it takes to complete the monitor scan and possibly have an adverse affect on WhatsUp Gold performance.

- 5 Complete the information for the **Files to include** section.
 - **Include all files.** Select this option to include all files within the parent folder in the monitor scan.

- **Include files with names matching following wildcard expression.** Select this option, then type a wildcard expression. Files that match the wildcard expression are included in the monitor scan. For example, enter *.exe to check for executable (.exe) files in the selected folder.



Note: This option only works for a single wildcard expression at a time. If you enter more than one expression, the monitor reads the entry as one wildcard expression.



Important: When enabled, this option has the probability to greatly slow WhatsUp Gold performance, dependent on the wildcard expression specified. The probability of slower performance increases when this option is used in conjunction with the Include sub-folders option.

6 Complete the information in the **Monitor is up if** section.

- **Folder.** Select the appropriate option: **exists** or **does not exist**. If you select exists, the monitor is up if the selected folder is found. If you select does not exist, the monitor is up if the folder is not found.



Note: The following options are not required for the monitor scan.

- For the following options, select the appropriate variables to determine the success or failure of the monitor scan:
 - **less than**
 - **less than or equal to**
 - **greater than**
 - **greater than or equal to**
 - **equal to**
 - **not equal to**
- **Actual folder size is.** Select this option to make the monitor dependent on the actual folder size. The default unit used for the folder size is bytes. Optionally, you can change the unit to either KB, MB, or GB.
- **Folder size on disk is.** Select this option to make the monitor dependent on the folder size on the disk. The default unit used for the folder size on disk is bytes. Optionally, you can change the unit to either KB, MB, or GB.
- **Number of files is.** Select this option to make the monitor dependent on the number of files in the folder.



Tip: To obtain the current actual folder size, folder size on disk, and number of files, first select the appropriate option, then click the folder properties button. These current values populate the option value field and can be used to set the monitor threshold.

7 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing an FTP Monitor

The FTP active monitor performs upload, download, and delete tasks on designated FTP servers to ensure that the FTP servers are functioning properly. You can configure a single monitor to perform all three tasks, but note that if any one of the tasks fails, the entire monitor is considered down.



Note: We recommend that you create a separate FTP monitor for each FTP server you are monitoring, unless the same username and password are used for each of the servers.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **FTP Monitor** from the list to create a new FTP monitor. Click **OK**.
- or -
Select the FTP monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
- 5 Complete the information in the **Server Settings** section:
 - **FTP Server.** Type the device address of the FTP server for which the FTP monitor is configured. The monitor performs tasks on this FTP server.
 - **Port.** Type the port over which the monitor should use to connect to the FTP server. The default port is 21.
 - **Username.** Type the username used to log in to the FTP server for which the monitor is configured.
 - **Password.** Type the password used to log in to the FTP server for which the monitor is configured.



Important: You must specify an account with the appropriate user permissions for the file actions you select. For more information, see *FTP user permissions* (on page 883).

- **Use Passive Mode.** Select this option to instruct WhatsUp Gold to use passive (PASV) mode as it attempts to connect to the FTP server and then to perform the selected tasks. If you do not select this option, the monitor uses Active mode. This option is selected by default. For more information, see Active and Passive modes.
- 6 Make the appropriate selections in the **File Actions** section:
- **Upload.** Select this option to have the active monitor upload a file to the designated FTP server. This option is selected by default.
 - **Download.** Select this option to have the active monitor download a file from the designated FTP server. This option is selected by default.
 - **Delete.** Select this option to have the active monitor delete a file from the designated FTP server. This option is selected by default.



Note: You cannot select the Download or Delete options if you have not selected the Upload option.

- **Timeout (sec).** Type a timeout (in seconds) for the amount of time WhatsUp Gold should wait for each attempted task to complete. The default timeout is 3 seconds.
 - **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.
- 7 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing an HTTP Content Monitor

This monitor requests a URL and checks the HTTP response against the expected content. If the response does not return the expected content, the monitor fails. You can use this monitor to ensure that your web pages are available for viewing or that they are rendering on certain browsers. For example, you can check to see that a web page contains specific content that is to be listed after a certain date, such as "Ipswitch introduces its newest release, WhatsUp Gold v15." If the monitor does not find the content that you request it to find, the monitor fails and you know to update your web page.



Note: You can access some HTTPS sites, such as Gmail's login screen, using the HTTP content monitor.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit an HTTP content active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **HTTP Content Monitor** from the list to create a new HTTP content monitor. Click **OK**.
- or -
Select the HTTP content monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
- 5 Complete the information in the **HTTP server settings** section.
 - **URL.** Type the URL address that you want to check using the monitor. The URL must begin with a proper URI, such as http:// or https://.



Note: The URL can include the full path to the document, including the document's file name and any query string parameters. For example, `http://www.domain.com/nmconsole/reports.htm?ReportID=100`.

- **Authentication username.** If required, type the username the web site uses for authentication.
- **Authentication password.** Type the password that coincides with the username that the web site uses for authentication.



Note: The HTTP Content Monitor only supports basic authentication.

- **Proxy server.** If the content that you want WhatsUp Gold to check is behind a proxy server, type the IP address of the proxy server.
 - **Proxy port.** Type the port on which the proxy server listens.
 - **Timeout (seconds).** Type the number of seconds WhatsUp Gold should attempt the connection (min timeout is 1 second / max timeout is 30 seconds)
- 6 Complete the information in the **Web page content** section.
 - **Web page content to find.** Type the content you want WhatsUp Gold to look for on the web page it checks. Type either plain text or a regular expression.
 - **Use regular expression.** Select this option to use regular expression in Web page content search.



Note: The HTTP Content Monitor uses standard regular expression processing as supported by the .NET framework.

- 7 Complete one or more of the following actions:
 - Click **Request URL contents** to populate the dialog box with the Web page contents of the URL you entered above.
 - Click **Advanced** to configure the user agent and custom headers.
 - Check **Use in Rescan** to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the **Rescan** button on the Device Properties dialog, if the protocol or service is active on the device.
- 8 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

xvi) Example: Monitoring and alerting on web page content

The HTTP Content monitor checks a specified web page to make sure that content appears on the page. If the results of the web page content are not what is expected, you can be notified through an associated action.

For example, to check whether a page is up and available, you can look for a text string contained in the web page. The following script checks for the words "WhatsUp Gold Tech Support" on the WhatsUp Gold main Support page. If this HTTP Content monitor shows as UP, the web page is displaying as expected. If this HTTP Content monitor shows as DOWN, the web page is down, missing, or has been changed:

```
Send=GET /support/index.aspx HTTP/1.0\r\nAccept:
*/*\r\nHost:www.whatsupgold.com\r\nUser-Agent: WhatsUp/1.0\r\n\r\n
```

```
Expect=WhatsUp Gold Tech Support
```

To configure a web page monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab inside the dialog.
- 3 Click **New**. The Select Active Monitor Type dialog appears.
- 4 Select **HTTP Content Monitor**, then click **OK**. The Add HTTP Content Monitor dialog appears.
- 5 Complete the following information for the monitor:
 - **Name.** Enter a name for the monitor as it will appear in the Active Monitor Library.
 - **Description.** Enter a short description for the monitor as it will appear in the Active Monitor Library.

HTTP server settings

- **URL.** Enter the URL address that you want to check using the monitor. The URL must begin with a proper URI, such as `http://` or `https://`.



Note: The URL can include the full path to the document, including the document's file name and any query string parameters. For example, `http://www.domain.com/nmconsole/reports.htm?ReportID=100` .

- **Authentication username.** If required, enter the username the web site uses for authentication.
- **Authentication password.** Enter the password that coincides with the username that the web site uses for authentication.



Note: The HTTP Content Monitor only supports basic authentication.

- **Timeout (seconds).** Enter the number of seconds WhatsUp Gold should attempt the connection (min timeout is 1 second / max timeout is 30 seconds).
- **Proxy server.** If the content that you want WhatsUp Gold to check is behind a proxy server, enter the proxy server's IP address.
- **Proxy port.** Enter the port on which the proxy server listens.

Web page content

- **Web page content to find.** Enter the content that you would like WhatsUp Gold to look for on the web page it checks. Enter either plain text or a regular expression.
- **Use regular expression.** Select this option to use regular expression in **Web page content to find**.



Note: The HTTP Content Monitor uses standard regular expression processing as supported by the .NET framework.



Note: Refer to the script above as an example for setting up a check for expected content on a specific web page URL.

To configure a web page monitor and email alert for a device:

- 1 Right-click the device (web server) that hosts the web page content for which you want to monitor. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Active Monitors dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.
- 4 Select the monitor to add to the device from the list. Look for the monitor name that you assigned to the monitor created in the previous steps. This is your HTTP Content Monitor.

- 5 Complete the settings for the monitor:
 - a) Leave the default settings selected (**Enable polling for this Active Monitor** and **Use default network interface**), then click **Next**. The Setup Actions for Monitor State Changes dialog appears.
 - b) Select **Apply individual actions**, then click **Add**. The Select or Create Action dialog appears.
 - c) Select **Select an action from the Action Library**, then click **Next**. The Select Action and State dialog appears.
 - d) In the **Select an action from the Action Library** list, select an existing email action or click browse (...) to create a new email action. Refer to the Help for creating a new email action.
 - e) In the **Execute the actions on the following state change** list, select **Down**, and then click **Finish** to save the changes and return to the Setup Actions for State screen.
 - f) Click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.
 - g) Click **Finish**. The Device Properties dialog appears.
 - h) Click **OK**.

The active monitor and resulting E-mail Action are now enabled. When the web page cannot return the web content, the page is triggered as down and the HTTP Content Monitor fails, triggering the E-mail Action that tells you that the page is down the Web server cannot return web content.

Adding and editing a Network Statistics Monitor

This monitor uses Simple Network Management Protocol (SNMP) to query a device to collect data on three device protocols, Internet Protocol (IP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP), and alerts you when the thresholds you specify are met or exceeded. For example, you can use the IP received discarded threshold monitor to watch for situations where a router with Quality of Service (QoS) has priorities set for Voice over IP (VoIP).

For more information, see Example - Using a Network Statistic Monitor to check for IP data received and discarded.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a network statistics monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.

- 3 Click **New** and select Network Statistics Monitor to create a new network statistics monitor. Click **OK**.
- or -
Select the network statistics monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Thresholds to monitor.** Select the IP, TCP, and/or UDP thresholds you want to monitor.



Tip: To configure individual settings, highlight a selected threshold, then click **Configure**.



Note: You can only configure one threshold at a time.

- **Object ID.** The OID of the most recently selected parameter.
 - **Description.** The description of the most recently selected parameter.
- 5 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

xvii) Example: Using a Network Statistics Monitor to check for IP data received and discarded

You can use the Network Statistics Monitor to verify that various types of packet and connection statistic information for network protocols, such as IP, TCP, and UDP, are within the thresholds that you define as acceptable. By doing so, you can ensure that devices handle specific types of network data as expected.

For example, you can use the *IP received discarded* threshold monitor to watch for situations where a router with Quality of Service (QOS) has priorities set for Voice over IP (VoIP). In these situations, other IP datagrams that a router receives are buffered for delayed processing to give processing priority to the VoIP data. If the buffer space is overrun, lower priority IP datagrams are discarded even though the router initially received them. This example describes configuring and assigning a network statistic monitor that monitors thresholds set for IP data received by a router but discarded from the buffer. It also configures and assigns an Email Action to notify you if the monitor fails.

To configure a Network Statistics Monitor:

- 1 From the **Admin** panel, select **Monitor Library**. The Monitor Library dialog appears.
- 2 If not already selected, select the **Active** tab.
- 3 In the Active Monitor Library, click **New**. The Select Active Monitor Type dialog appears.
- 4 Select **Network Statistics Monitor** from the list, and then click **OK**.

- 5 Type a **Name** for the monitor, such as `Cisco Router Buffer Overflow Monitor`.
- 6 Type a **Description** for the monitor. This description displays next to the monitor name in the Active Monitor Library.
- 7 In the **Thresholds to monitor** section of the dialog, select **IP received discarded**.
- 8 Click **OK** to save changes.

After configuring the *IP received discarded* monitor, you need to assign it to the device(s) that you want to check using the monitor. In the next steps of this example, you will assign the monitor to a single device, then using the Action Builder, configure and assign an Email Action that will notify you when the monitor goes down.



Tip: You can also assign the monitor to multiple devices at one time via Bulk Field Change. For more information, see *Assigning a monitor to multiple devices* (on page 227).

To assign the IP Received Discarded monitor, and configure and assign an Email Action:

- 1 Go to the properties for the device to which you want to assign the monitor.
 - a) From either the Device View or Map View, right-click the device. The right-click menu appears.
 - b) Select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Click **Add**. The Active Monitor Properties dialog appears.
- 4 Select the **Cisco Router Buffer Overflow Monitor**, then click **Next**.
- 5 Set the monitor polling properties, then click **Next**.
- 6 Select **Apply individual actions**, then click **Add**. The Action Builder appears.
- 7 Select **Create a new action**, then click **Next**.
- 8 Select the **Email Action**, then click **Next**.
- 9 Under **Execute the action on the following state change**, select **Down**; this option specifies that WhatsUp Gold issues a state change after the monitor has detected that the router has received IP data, but the buffer has been overrun with too much data. Click **Finish**. The New Email Action dialog appears.
- 10 Type a **Name** for the monitor, such as `Cisco Router Buffer Overflow Monitor`.
- 11 Optionally, edit the description.
- 12 In the **SMTP Server** box, type the IP address or Host (DNS) name of your email server (SMTP mail host).
- 13 Type the **Port** on which the SMTP Server is installed. The default SMTP port is 25.
- 14 Optionally, change the **Timeout** from the default of 5 seconds.
- 15 In the **Mail To** box, type the email addresses which will receive the notification. You can enter two addresses, separated by commas (with no spaces). The address should not contain brackets, spaces, quotation marks, or parentheses.
- 16 Optionally, edit the address in the **Mail from** box. The address appearing here appears as the notification sender.
- 17 Select **SMTP server requires authentication** if your SMTP server uses authentication. This enables the Username and Password options.

- 18 Type a **Username** and **Password** for authentication, if necessary.
- 19 Select **Use an encrypted connection (SSL/TLS)** if your SMTP server requires data encryption over a TLS connection.
- 20 Click **Mail Content** to enter the notification content.
- 21 In **Subject**, type `%ActiveMonitor.Name has failed (%Device.HostName)`. This message indicates the device type, its down state, and the hostname of the device on which the monitor has failed.
- 22 In **Message body**, type

`This %ActiveMonitor.Name has failed on %Device.Address.`

`Please check or restart the %Device.HostName.`

`This mail was sent on %System.Date at %System.Time
Ipswitch WhatsUp Gold`

This message indicates that the device, such as a router, has reached the threshold where IP data has overrun the buffer and should be checked or restarted.



Tip: Optionally, you can add a link to the **Device Status** or **Mobile Device Status** report for the device to which the monitor is assigned.

- 23 Click **OK** to save changes.
- 24 On the Active Monitor Properties dialog, click **Finish**.

Adding and editing a Power Supply Monitor

The Power Supply Monitor checks Cisco switches/routers, Dell servers, Dell Power Connect switches/routers, and HP ProCurve and switches/routers, HP ProLiant servers, and other device power supplies to see that they are enabled and return a value that signals they are in an up state. The monitor first checks to see if a device is a Cisco, Dell, or HP device, then checks any enabled power supply devices. If a power supply is disabled, the monitor ignores it; if a power supply does not return a value of 1 - Normal (for Cisco switches/routers), 3 - OK (for Dell server devices), 1 - OK (for Dell switches/routers), 4 - Good (for HP ProCurve switches/routers), or 2 - OK (for HP ProLiant servers), the monitor is considered down.



Note: Not all types of device power supplies may be monitorable using the Power Supply Monitor. Check the make and model of your device power supply before attempting to monitor.

This monitor is pre-configured and exists in the Active Monitor Library upon installation of WhatsUp Gold. Unlike many pre-configured active monitors, the Power Supply Monitor default configuration cannot be modified. However, you can modify the monitor name and description, as well as the SNMP timeout and number of retries used while attempting to connect to devices.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a power supply monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **Power Supply Monitor** from the list to create a new power supply monitor. Click **OK**.
- or -
Select the supply monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.



Tip: Click **Advanced** to set the SNMP timeout and number of retries.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing a Printer Monitor

This monitor uses SNMP to collect data on SNMP-enabled network printers. If a failure criteria is met, any associated actions fire. For example, you can monitor for printer ink levels, for a paper jam, for low input media (paper), for a fuse that is over temperature, and more.



Important: In order for the Printer Active Monitor to work, in addition to being SNMP-enabled, the printer you are attempting to monitor must also support the Standard Printer MIB.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a printer monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.

- 3 Click **New** and select **Printer Monitor** from the list to create a new printer monitor. Click **OK**.
- or -
Select the printer monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
- 5 Complete the information in the **Failure Criteria** section:
 - **If the ink level in any of the cartridges falls below ___%.** Type a numerical value for the threshold. If the ink level of any printer ink cartridge falls below this percentage, the monitor is considered down. By default, this option is not selected.
 - **If the printer registers any of the following alerts.** By default, the monitor watches for all of the listed printer alerts. If you do not want to monitor a particular alert, clear its selection in the list. If the printer registers one of the selected alerts, the monitor is considered down.



Note: Your printer may not support all of the SNMP objects associated with the available monitor alert checks.



Tip: Click **Advanced** to set the SNMP timeout and number of retries.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing a Process Monitor

This monitor uses SNMP to monitor the status of device processes and issues state changes as needed. The Process Monitor can detect whether a process is running. You can use this monitor to verify that anti-spyware or antivirus software is running on a device. If the monitor does not find the specified program running, an associated action notifies you of this potentially harmful vulnerability.

For more information, see the example *Using the Process Monitor to Check for Antivirus Software*.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a process monitor:

- 1** Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2** Click the **Active** tab. The Active Monitor list appears.
- 3** Click **New** and select **Process Monitor** from the list to create a new process monitor. Click **OK**.
- or -
Select the process monitor you want to change from the list of current monitors, and then click **Edit**.
- 4** Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Process name.** Type or browse (...) to the process name you want to use in the monitor.
- 5** Completed the information for the **Thresholds to monitor** section.
 - **Down if the process is.** Select this option to instruct the monitor to verify that the selected process is either not loaded, or is running, on a device, and issue a down state change accordingly.



Tip: Click **Advanced** to set the SNMP timeout and number of retries, and to decide if the monitor is used in Discovery.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

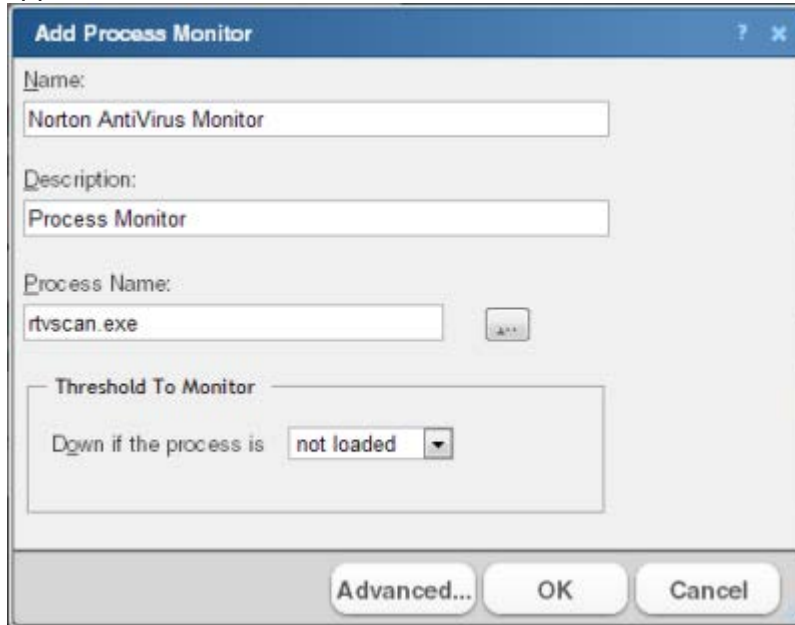
xviii) Example: Using the Process Monitor to check for antivirus software

You can use the Process Monitor to verify that antivirus or anti-spyware software is a running on a device. If the monitor does not find the specified program running, an associated action notifies you of this potentially harmful vulnerability.

For this example, you will configure and assign a Process Monitor that checks to see if Norton AntiVirus™ is running on a device. You will also configure and assign an Email Action to notify you if the monitor fails.

To configure the Process Monitor:

- 1 In the Active Monitor Library, click **New**. The Select Active Monitor Type dialog appears.
- 2 Select **Process Monitor** from the list, then click **OK**. The Add Process Monitor dialog appears.



- 3 Enter a **Name** for the monitor, such as Norton AntiVirus Monitor.
- 4 Enter a **Description** for the monitor. This description is displayed next to the monitor name in the Active Monitor Library.
- 5 Type or browse (...) to the **Process name** that the monitor will check. To monitor Norton AntiVirus software, enter `rtvscan.exe`.
- 6 Under the **Thresholds to monitor** section of the dialog, select **Down if the process is** and **not loaded**. If the monitor does not find the `rtvscan.exe` process running on the device to which the monitor is assigned, the monitor is considered down.



Tip: Click **Advanced** to set the SNMP timeout and number of retries, and to decide if the monitor is used in Discovery.

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

After configuring the Norton AntiVirus Monitor, you need to assign it to the device(s) that you want to check are running the monitor. In the next steps of this example, you will assign the monitor to a single device, and then, using the Action Builder, configure and assign an Email Action that will notify you when the monitor goes down.



Tip: You can also assign the monitor to multiple devices at one time via Bulk Field Change. For more information, see *Assigning a monitor to multiple devices* (on page 227).

To assign the Norton AntiVirus Monitor, and configure and assign an Email Action:

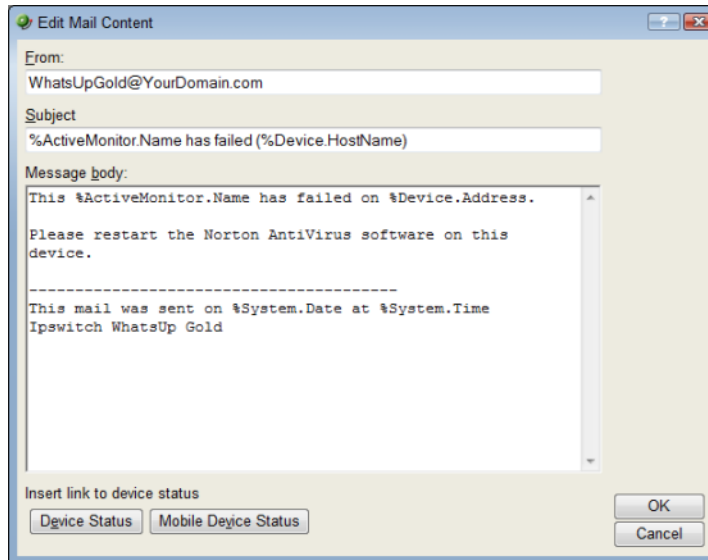
- 1** Go to the properties for the device to which you want to assign the monitor.
 - From either the Device View or Map View, right-click the device. The right-click menu appears.
 - Select **Properties**. The Device Properties dialog appears.
- 2** Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3** Click **Add**. The Active Monitor Properties dialog appears.
- 4** Select the **Norton AntiVirus Monitor**, then click **Next**.
- 5** Set the monitor polling properties, then click **Next**.
- 6** Select **Apply individual actions**, then click **Add**. The Action Builder appears.
- 7** Select **Create a new action**, then click **Next**.
- 8** Select the **Email Action**, then click **Next**.
- 9** Under **Execute the action on the following state change**, select **20 minutes (Down at least 20 min)**. This option specifies that WhatsUp Gold will issue a state change after the monitor has been unable to find `rtvscan.exe` on the device for 20 minutes.
- 10** Click **Finish**. The New Email Action dialog appears.



Note: On the console, ensure that the Mail Destination tab is selected.

- 11** Enter a **Name** for the monitor, such as `Norton AntiVirus Email Notification`.
- 12** In **SMTP Mail Server**, enter the IP address or Host (DNS) name of your email server (SMTP mail host).
- 13** Enter the **Port** on which the SMTP Server is installed. The default SMTP port is 25.
- 14** Optionally, change the **Timeout** from the default of 5 seconds.
- 15** In **Mail To**, enter the email addresses to which you want send the notification. You can enter two addresses, separated by commas (with no spaces). The address should not contain brackets, spaces, quotation marks, or parentheses.
- 16** Select **SMTP server requires authentication** if your SMTP server uses authentication. This enables the Username and Password options.
- 17** Enter a **Username** and **Password** to be used with authentication.
- 18** Select **Use an encrypted connection (SSL/TLS)** if your SMTP server requires data encryption over a TLS connection.

- 19 Click **Mail Content** to enter the notification content.



- 20 In **From**, enter the email address that will appear in the From field of the email that is sent from WhatsUp Gold.
- 21 In **Subject**, enter `%ActiveMonitor.Name has failed (%Device.HostName)`. This message indicates the monitor's name, its failed state, and the hostname of the device on which the monitor has failed.
- 22 In **Message body**, enter

```
This %ActiveMonitor.Name has failed on %Device.Address.  
Please restart the Norton AntiVirus software on this device.  
-----  
This mail was sent on %System.Date at %System.Time  
Ipswitch WhatsUp Gold
```

This message indicates that the Norton AntiVirus software has stopped on the specified device and that it should be restarted.



Tip: Optionally, you can add a link to the **Device Status** or **Mobile Device Status** report for the device to which the monitor is assigned.

- 23 Click **OK** to save changes.
- 24 On the Active Monitor Properties dialog, click **Finish**.

Adding and editing a SQL Server Monitor

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 installed on any machine in your network.

To create custom parameters to monitor, the SQL Server host must be WMI-enabled.

WhatsUp Gold can monitor and report the status of the standard services associated with TCP/IP servers, such as SMTP, POP3, and IMAP, FTP, HTTP. If any of these services fail, users are unable to get mail, transfer files, or use the web. It is a good practice to set up monitoring on these services so you are the first to know if they fail. The SQL Server 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.

To configure an instance of the SQL Server Monitor:



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.



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

- 3 Add a SQL monitor:
 - a) Click **New**. The Select Active Monitor Type dialog appears.

- b) Select **SQL Server Monitor** from the list and click **OK**. The New SQL Server Monitor dialog appears.

New SQL Server Monitor

Name:

Description:

SQL Server instance name:

Thresholds to monitor:

| Parameters | Down If |
|---|---|
| <input type="checkbox"/> CPU | Percent CPU > 95% |
| <input type="checkbox"/> Memory | Free memory < 1000 KB |
| <input type="checkbox"/> Disk Performance | Read > 5120 KB/Sec, Write > 5120 KB/sec |
| <input type="checkbox"/> Disk Space | Disk Drive (C:) free space < 50 MBytes |
| <input type="checkbox"/> System | Number of Processes > 200 |

Configure...

Services to monitor:

| Service |
|---|
| <input checked="" type="checkbox"/> MSSQLSERVER |
| <input checked="" type="checkbox"/> SQLSERVERAGENT |
| <input type="checkbox"/> Microsoft Search |
| <input checked="" type="checkbox"/> Distributed Transaction Coordinator |

☒ Use in rescan

OK Cancel

- c) In the **Name** box, type the name you want to use to identify this instance of the SQL Server monitor. For example, if you are configuring a monitor to check disk space, you might enter `SQLServerDisk`.
- d) In the **Description** box, type any text information to further describe the monitor.
- e) In the **SQL Server Instance Name** box, type the name of the database you want to monitor.
- f) Select the thresholds to add to the monitor. For more information about specific thresholds, see *SQL Server Parameters*.
- g) Select the services to add to the monitor. For more information about specific services, see *SQL Server Services* (on page 217).
- h) Click **OK** to save the monitor in the Active Monitor Library.
- 4** Add the monitor to your SQL Server device.

- a) In your device list, find the device that represents the SQL Server.
- b) Right-click the device, then select **Properties**.
- c) Select **Active Monitors**.
- d) Click **Add**. The Active Monitor wizard appears.
- e) Select the monitor from the list, and continue with the wizard to configure any actions for the monitor.

For more information on setting up an action, see *Configuring an action* (on page 273).



Note: If you select **Use in rescan**, WhatsUp Gold adds the monitor to the Active Monitors list. From that list, you can select to scan for that service on all applications found during discovery.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

xix) Getting Started with SQL Server Monitors

- 1 Determine which SQL parameters to monitor.



Note: To use some parameters, configure your System Data Source (ODBC) name for the SQL Server. This is done in the Windows Data Sources (ODBC) administrator.

- 2 Determine which SQL services to monitor.
- 3 Decide whether to create a single monitor with multiple parameters and services, several monitors with one parameter or service, or some combination. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions. For example, if you create a single monitor to check disk usage, you can name it `SQLDisk` and it will be reported in logs with this name.
- 4 Configure an SQL Server Monitor with your selected parameters and/or services.
- 5 Add the SQL Monitor to the device that represents your SQL server.
- 6 Set up an action to tell you when the monitor goes down or comes back up.



Note: The monitor is reported down if any of the parameters or services in that monitor are down.

a. SQL Server Parameters

You can set thresholds on the following parameters:

| Select this parameter: | If you want to: |
|------------------------|--|
| CPU | Monitor the CPU state on the SQL host. |
| Memory | Monitor free memory on the SQL host. |
| Disk | Monitor disk usage on the SQL host by the SQL server. |
| Disk space | Monitor free disk space on the SQL host. |
| System | Monitor system processes on the SQL host. |
| Buffers | Monitors SQL page buffers. |
| Cache | Monitors cache usage on the SQL server. |
| Locks | Monitors wait locks on the SQL server. |
| Transactions | Monitors the transactions on the SQL server. |
| Users | Monitors the users on the SQL server. |
| Alerts | Monitors SQL alerts and severity of alerts. |
| Custom Thresholds | Browse and select from the large number of additional parameters that SQL reports. |

b. SQL Server Services

You can monitor the following critical SQL services to determine whether the service is available (Up) or is disabled (Down).

| Select this process: | To monitor this function: |
|-------------------------------------|--|
| MSSQLSERVER | This is the database engine. It controls processes all SQL functions and manages all files that comprise the databases on the server. |
| SQLSERVERAGENT | This service works with the SQL Server service to create and manage local server jobs, alerts and operators, or items from multiple servers. |
| Microsoft Search | A full-text indexing and search engine. |
| Distributed Transaction Coordinator | The MS DTC service allows for several sources of data to be processed in one transaction. It also coordinates the proper completion of all transactions to make sure all updates and errors are processed and ended correctly. |
| SQL Server Analysis Services | Implements a highly scalable service for data storage, processing, and security. |
| SQL Server Reporting Services | Used to create/manage tabular, matrix, graphical, and free-form reports. |
| SQL Server Integration Services | A platform for building high performance data integration solutions. |
| SQL Server FullText Search | Issues full-text queries against plain character-based data in SQL Server tables. |

| Select this process: | To monitor this function: |
|------------------------------------|---|
| SQL Server Browser | Listens for incoming requests for SQL Server resources and provides information about SQL Server instances installed on the computer. |
| SQL Server Active Directory Helper | View replication objects, such as a publication, and, if allowed, subscribe to that publication. |
| SQL Server VSS Writer | Added functionality for backup and restore of SQL Server 2005. |

xx) Example: SQL Server Monitor

To monitor user activity on an SQL Server, you can create a monitor called `SQLUser`, then select **Users** as the only parameter to monitor.

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library appears.
- 2 If not already selected, select the **Active** tab.
- 3 Click **New**. The Select Active Monitor Type dialog appears.
- 4 Select SQL Server Monitor and click **OK**. The New SQL Server Monitor dialog appears.
 - a) In the **Name** box, enter `SQLUser`.
 - b) In the **SQL Server Instance Name** box, enter the name of your database.
 - c) Make sure that **Users** is the only parameter selected.
 - d) Clear the selections for all other parameters and for the services as well.
 - e) Highlight the **Users** parameter, 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.
 - f) When finished, click **OK** to add the `SQLUser` monitor to the Active Monitor Library.
- 5 Add the `SQLUser` monitor to your SQL server device.
 - a) In the device list, select the device that represents the SQL server. Right-click the device, then select **Properties**. Select **Active Monitors**.
 - b) Click **Add**. The Active Monitor wizard appears.
 - 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 *Configuring an action* (on page 273).

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

Adding and editing a SQL Query Monitor

This monitor lets you check that certain conditions exist in a Microsoft SQL or MySQL database, based on a database query. You can define the criteria you want to exist in the database, and as long as the specified conditions are present, the SQL Query Monitor is in an up state. If the database data changes outside the boundaries of the query criteria, the monitor triggers to a down state.

After the monitor is configured, you must assign the monitor to a device through the **Device Properties > Active Monitors** dialog.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).



Important: To use the SQL Query Monitor to monitor a MySQL database, you must first download and install the MySQL .NET connector. Because of compatibility issues with later versions, only MySQL version 5.2.5 .NET connector is supported. This connector is located on the *WhatsUp Gold website* (<http://www.whatsupgold.com/MySQL525connector>). This link downloads the `mysql-connector-net-5.2.5.zip` file. Once downloaded, extract the `MySQL.Data.msi` and run the MySQL Connector Setup utility by double-clicking on the `MySQL.Data.msi` icon. On the **Choose Setup Type** screen, select **Typical** and click **Install**. The MySQL .NET connector is installed at the following location: `C:\Program Files\MySQL\MySQL Connector Net 5.2.5\`. After the .NET connector has been installed, restart WhatsUp Gold.



Note: The SQL Query monitor does not support Windows authentication. Make sure that ADO credentials are set up in the Credentials Library for the database for which you want to query. The Credentials system stores ADO database credentials information in your WhatsUp Gold database to be used when a database connection is required. For more information, see *Using Credentials*.



Note: When connecting to a remote SQL instance, WhatsUp Gold only supports the TCP/IP network library.

To add or edit a SQL Query monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **SQL Query Monitor** from the list to create a new SQL Query monitor. Click **OK**.
- or -
Select the SQL Query monitor you want to change from the list of current monitors, and then click **Edit**.

- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
- 5 Complete the information for the **Server Properties** section.
 - **Server Type.** Select the database server type.



Note: MySQL database is supported and listed as a Server Type option if the MySQL 5.2 or later .NET connector is installed. You can download the connector on the MySQL Connectors Download site.

- **Server Address.** Type the server address in the ServerName\Instance format.



Note: The ServerName\Instance format is only required for SQL Server. MySQL only requires the ServerName.

- **Port (optional).** Type the database server port number if other than the standard database port number.
- **SQL Query to Run.** Type a query you want to run against a database to monitor and check for certain database conditions. Only SELECT queries are allowed.



Important: Ensure that you include the full database name in your query. For query help, click **Build**. The SQL Query Builder assists in developing proper query syntax.

- **Build.** Click to open the SQL Query Builder dialog for assistance building queries.
- **Verify.** Click to check that the query is valid. If there is a syntax error with the SQL query, a message appears with tips about the syntax issue.

- 6 Complete the information for the **Monitor is up if** section.



Important: All database rows must match the criteria settings in the Monitor is up if section for the monitor to be considered up. If multiple threshold criteria is used in the Content of each retrieved row matches the following criteria, all thresholds must match the criteria in each row.

- **Number of rows returned is.** Select this option to determine the success or failure of the monitor scan based on rows returned by the SQL query.
For the following options, select the appropriate variables to determine the success or failure of the monitor scan:
 - **less than**
 - **less than or equal to**

- **greater than**
- **greater than or equal to**
- **equal to**
- **not equal to**

Enter a numeric value for number of rows in the box to the right of the conditions list.

- **Content of each retrieved row matches the following criteria.** Select to set criteria that each database row must match to determine the success or failure of the monitor scan.
- **Add.** Click to open the New Row Content Threshold dialog. This dialog lets you set the database column values and conditions that must be matched for each table row.
- **Edit.** Click to modify existing row criteria.
- **Delete.** Click to remove existing row criteria.

As you specify the desired monitor criteria settings, this description updates to illustrate the monitor you have configured.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and Editing a WMI Monitor

The WMI active monitor watches for specific values on WMI enabled devices. Windows Management Instrumentation (WMI) is a Microsoft Windows standard for retrieving information from computer systems running Windows. WMI is installed by default on Windows 2000, Windows 2003, Windows XP, and Windows Vista systems.

WhatsUp Gold can monitor and report the status of the standard services associated with TCP/IP servers, such as SMTP, POP3, IMAP, FTP, HTTP. If any of these services fail, network users cannot send mail, transfer files, or use the web. It is good practice to set up monitoring on these services so you are the first to know if they fail. The WMI Monitor extends monitoring to parameters reported by Windows-based applications and servers, allowing you to get an early warning of a degradation in performance. For example, you can monitor system parameters on your Oracle® database server to see if performance is within an expected range, and if not, you can intervene before the Oracle server fails. In other words, you can detect a looming problem before it causes an application or service failure.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a WMI active monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select **WMI Monitor** from the list to create a new WMI monitor. Click **OK**.
- or -
Select the WMI monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Performance counter/Instance.** Click the browse (...) button next to this box to select a performance counter and instance for the monitor.



Note: When WhatsUp Gold is run on Windows 2000, the performance counters are not supported and are not displayed.

- **Check type.** Select the type of check you want the WhatsUp Gold WMI monitor to make on the performance counter selected above.
 - **Constant Value.** Monitors the performance counter/instance for a specific value. If that value changes, the monitor triggers a device state change.
 - **Range of Values.** Monitors the performance counter/instance to make sure the returned value falls within a range of values. If the value falls outside of the range, the monitor triggers a device state change.
 - **Rate of Change.** Monitors the performance counter/instance to make sure the change in value matches the rate you enter in the check values section. If that rate changes, the monitor triggers a device state change.
- **Check values.** Enter the values for the check type selected above. For **Constant Value** and **Rate of Change**, select the state of the device when the check value is met.



Note: You can also click **Advanced** to access Advanced Monitor Properties.

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

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Troubleshooting

Having problems with your WMI monitor returning false negatives?

xxi) How to use WMI Monitors

This topic describes the overall process for configuring a WMI monitor, assigning it to a device, and getting feedback from the monitor.

- 1 Determine which WMI object you want to monitor.
- 2 Decide whether to create a single monitor with multiple WMI objects, several monitors with one object, or some combination.

To start, it may be simpler to create one monitor for each WMI object that you want to monitor. Whether you set up one monitor or many has a bearing on how the information is reported in WhatsUp Gold logs and by actions. For example, a single monitor to check errors on logon, named LogonErrors, is reported in logs with this name. If LogonErrors is reported down, you know it's a specific problem.

- 3 Configure a WMI Monitor with your objects.
- 4 Add the WMI Monitor to the device that represents your application host or server.
- 5 Set up an action to inform you when the monitor goes down or comes back up.



Note: The monitor is reported down if any of the objects that you select to monitor are down.

xxii) Example: WMI Monitor

Imagine that a device on your network has been illegally logged into through a brute force attack (an attack where an intruder runs a script to try random usernames and passwords on a range of IP addresses on your network). These types of attacks are extremely dangerous if the device in peril is on your domain or is storing sensitive information.

You can use a custom WMI Active Monitor to check the appropriate performance counters on a Windows device and notify you when this type of attack occurs, so you can do something about it before a potential intruder gains access to your network.

To configure this type of active monitor:

- 1 Using the WhatsUp Gold web interface, create the WMI monitor.
 - a) Click the **Admin** tab, then click **Monitor Library**. The Active Monitor Library appears.
 - b) Click the **Active** tab inside the dialog.
 - c) Click **New**. The Select Active Monitor Type dialog appears.
 - d) Select **WMI Monitor** and click **OK**. The Add WMI Monitor dialog appears.
 - e) In the **Name** box, enter "ErrorsLogon" to identify that this monitor checks for logon errors.
 - f) Click the **Browse (...)** button next to **Instance** to access the Performance Counters dialog.

- g) Enter the computer name or IP address of the computer in which you want to connect.
 - h) Select a credential from a list of Windows credentials (pulled from the Credentials Library), then click **OK** to connect to the computer.
 - i) Select **Server** from the **Performance object** list.
 - j) Under **Performance Counters**, select the **ErrorsLogon**.
 - k) Click **OK** to add the Performance counter to the New WMI Monitor dialog.
 - l) Select **Rate of Change** from the **Check type** list.
 - m) In the **Rate of Change** box, enter the number of logon errors you feel is acceptable. This is the number of failed logon attempts between polls.
 - n) In the **If the value is above the rate, then the monitor is** box, select **Down**.
 - o) Click **OK** to add the active monitor to the library.
- 2** Enter the credentials for logging on to the device to which you will add this monitor.
- a) In the Device Properties dialog for the device, select **Credentials**.
 - b) Select **Windows**, then click **Edit**.
 - c) Click the browse (...) button next to **Windows credentials** to access the Credentials Library.
 - d) Create a Windows credential using the administration login and password for the device you want to create the monitor for. When you have configured the credential, click **Close**.
 - e) On the Credentials page, select the new **Windows credential**, then click **OK**.
- 3** Add the **ErrorsLogon** monitor to the device.
- a) In your device list, find the device. Double-click the device to display its properties, then select Active Monitors.
 - b) Click **Add**. The Active Monitor wizard appears.
 - c) Select the ErrorsLogon monitor, and continue working through the wizard to configure any actions for the monitor.
- For more information on setting up an action, see *Configuring an Action* (on page 273).

Consider creating several levels of the active monitor, each with a higher threshold than the other, and with more severe actions associated with it.

For example, create a monitor with 30 as the threshold that simply sends you an email, letting you know that at least 31 attempts have been made. Next, create another monitor that uses 60 as the threshold. This monitor may have an SMS action associated with it that sends a text message to you when at least 61 attempts are made. For the most severe level you could create a 100 threshold and have the action send messages to several people who could block the IP or take the device off the network while the attack is addressed.

Adding and editing a VoIP Monitor

The VoIP Active Monitor lets you set the acceptable Mean Opinion Score (MOS) threshold for an IP SLA device. If the threshold is exceeded, an alert can be sent specifically to notify the appropriate network manager about the issue. For more information, see Using the WhatsUp Gold VoIP Monitor on the WhatsUp Gold web site.



Note: The WhatsUp Gold VoIP Monitor must be activated to use the VoIP Active Monitor.



Note: This feature is only available in WhatsUp Gold Premium Edition. To update your license, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

To add or edit a VoIP monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Active** tab. The Active Monitor list appears.
- 3 Click **New** and select VoIP to create a new VoIP monitor. Click **OK**.
- or -
Select the VoIP monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the active monitor. This name displays in the Active Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Active Monitor Library.
 - **Acceptable MOS threshold.** Use the slide bar to adjust the acceptable MOS (Mean Opinion Score) threshold.
 - **Check MOS values of all jitters configured on the device.** Select this option to include all of the device RTT entries to check MOS performance thresholds. For example, if the following tags define the source and destination devices:
 - SLA 1 (Atlanta to Augusta Sat Office)
 - SLA 200 (Atlanta to Lexington)
 - SLA 300 (Atlanta to Florida Sat Office)then all entries are monitored for the acceptable MOS threshold compliance.
 - **Only check MOS if tag contains.** Select this option to limit the device RTT entries that use this MOS performance threshold. Enter all, or a portion, of the tag used to identify the source and destination devices. For example, if the following tags define the source and destination devices:
 - SLA 1 (Atlanta to Augusta Sat Office)
 - SLA 200 (Atlanta to Lexington)

- SLA 300 (Atlanta to Florida Sat Office)
then if you include `Sat Office` in this box, only the source/destination devices with `Sat Office` as part of the tag entry is monitored for the acceptable MOS threshold compliance.

5 Click **Advanced** to configure the active monitor SNMP timeout and number of retries.

6 Click **OK** to save changes.

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Adding and editing an Active Script Active Monitor

The Active Script monitor lets you write either VBScript or JScript code to perform specific customized checks on a device. If the script returns an error code, the monitor is considered down. A variety of active script resources are available on the *Active Scripts Resource page* (http://www.whatsupgold.com/script_library).



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

For more information, see *Extending WhatsUp Gold with scripting* (on page 909).

After configuring an active monitor in the Active Monitor Library, *add the monitor to devices* (on page 226).

Assigning active monitors

After you configure an active monitor in the Active Monitor Library, you must add it to the individual devices for which you want to monitor services.



Note: When you assign an active monitor to a device, an instance of the monitor is added to the device. Changes that you make to the monitor configuration via the Active Monitor Library affect all instances of the monitor. For example, if you assign a monitor to four separate devices and then make changes to the monitor from the Active Monitor Library, all four instances of the monitor adopt the changes.

To assign an active monitor to a device:



Note: If you are assigning an active monitor to a device that uses WMI or SNMP credentials, before assigning an active monitor, make sure that the device has the proper credentials assigned. For more information, see *Using Credentials* (on page 75).

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

To manually assign an active monitor to the device:

- 1 In the Device Properties Active Monitor dialog, click **Add**. The Active Monitor Properties dialog appears.
- 2 Select the active monitor type you want to assign to the device, then click **Next**.
- 3 Set the polling properties for the monitor, then click **Next**.
- 4 Set up *actions* (on page 297) for the monitor state changes.
- 5 Click **Finish** to add the monitor to the device.

To use Bulk Field Change to add an active monitor to multiple devices:

- 1 Select the devices in the device list, then right-click on one of the selected items.
- 2 From the right-click menu, select **Bulk Field Change > Active Monitor**.
- 3 Select the active monitor type you want to add.
- 4 Click **OK**.

xxiii) Assigning a monitor from Device Properties

To assign an active monitor to a device from its properties:

- 1 Go to the properties for the device to which you want to assign the monitor.
 - a) From either the Details View or Map View, right-click the device. The right-click menu appears.
 - b) Select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Active Monitors dialog appears.
- 3 Click **Add**. The Active Monitor Properties dialog appears.
- 4 Select the active monitor type you want to assign to the device, then click **Next**.
- 5 Set the monitor polling properties, then click **Next**.
- 6 Set up the actions for the monitor state changes, then click **Finish**. The active monitor is assigned to the device.

xxiv) Assigning a monitor to multiple devices

To assign an active monitor to multiple devices through Bulk Field Change:

- 1 From Details View, select multiple devices or a group to which you want to assign an active monitor, then right-click the selected devices or group. The right-click menu appears.
- 2 Select **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog appears.
- 3 Select the active monitor type that you want to assign, then click **OK**. The active monitor is assigned to the selected devices.

Removing and deleting active monitors

Because active monitors are assigned to devices on an individual basis, active monitors can only be removed from devices, and must be deleted from the Active Monitor Library. You also have the option to disable a monitor on the device-level, rather than completely removing it from a device. If you want to stop monitoring a particular device, but would like to keep the device-specific historical data associated with the active monitor, you should disable the monitor rather than removing it from the device.

xxv) Disabling an active monitor

To disable an active monitor from monitoring a device:

- 1 In the Details or Map View, right-click the device from which you want to disable polling for the active monitor. The right-click menu appears.
- 2 Select **Properties**. The Device Properties dialog appears.
- 3 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 4 Select the monitor you want to disable, then click **Edit**. The Active Monitor Properties dialog appears.
- 5 Clear **Enable polling for this active monitor**, then click **Next**.
- 6 On the following dialog, click **Finish**.

When you return to the Device Properties - Active Monitors dialog, you will see that the monitor is disabled for the device.

xxvi) Removing an active monitor

To remove an active monitor from a device:

- 1 From Device or Map View, right-click the device from which you want to remove the active monitor, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Select the monitor you want to remove.
- 4 Click **Remove**. A warning dialog appears that states all data for that instance of the monitor is deleted when the monitor is removed.
- 5 Click **Yes** to remove the monitor.

To remove an active monitor from multiple devices:

- 1 Select the appropriate devices in Device View or Map View, then right-click on one of the selected items. The right-click menu appears.
- 2 Select **Bulk Field Change > Active Monitor**. The Bulk Field Change: Active Monitor dialog appears.
- 3 Under **Operation**, select **Remove**.
- 4 Under **Active Monitor type**, select the active monitor that you want to remove.
- 5 Click **OK** to remove the monitor from the selected devices.

About critical active monitors

Critical active monitors allow you to define a specific polling order for a device's active monitors; you can make one monitor dependent on another monitor on the same device, such as making an HTTP monitor dependent on the Ping monitor, so that you are not flooded with multiple alerts on the same device if network connectivity is lost.

In a critical monitor polling path, critical monitors are polled first. If you specify more than one critical monitor, you also specify the order in which they are polled. Critical monitors are "up" dependent on one another; if critical monitors return successful results, non-critical monitors are polled. If any of the critical monitors go down, all monitors behind it in the critical polling order are no longer polled and are placed in an unknown state for the duration of the polling cycle. If at the start of the next polling cycle, the critical monitor returns successful results, polling of successive critical monitors and non-critical monitors resumes.



Note: Up and Down device dependencies take precedence over critical monitor polling; if WhatsUp Gold detects device dependencies, the configured dependencies are respected.

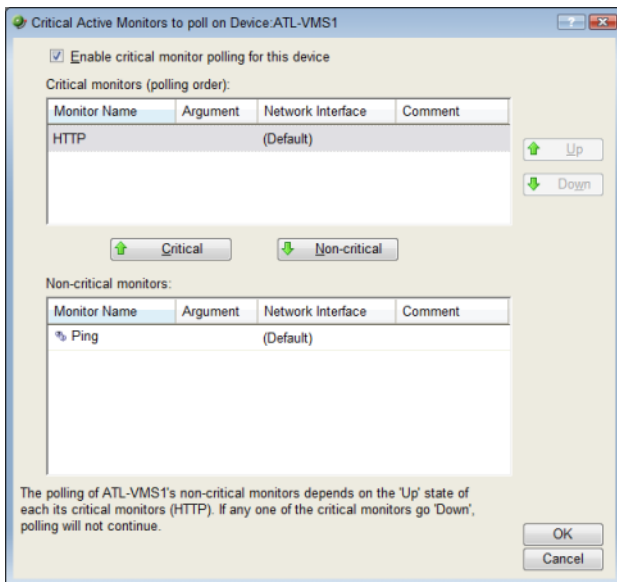
When critical monitoring is enabled, and you specify a critical polling order, you now receive only one alert when a device loses its network connectivity.



Note: When a monitor is placed in the unknown state, assigned actions are not fired. Likewise, when a monitor comes out of the unknown state into an up state, assigned actions are not fired.

Only monitors that you specify as critical follow a specific polling order; non-critical monitors are not polled in any specific order. Additionally, if multiple non-critical monitors fail, all associated actions fire.

Critical active monitors can be viewed and configured from the *Device Properties - Active Monitors* (on page 123) dialog.



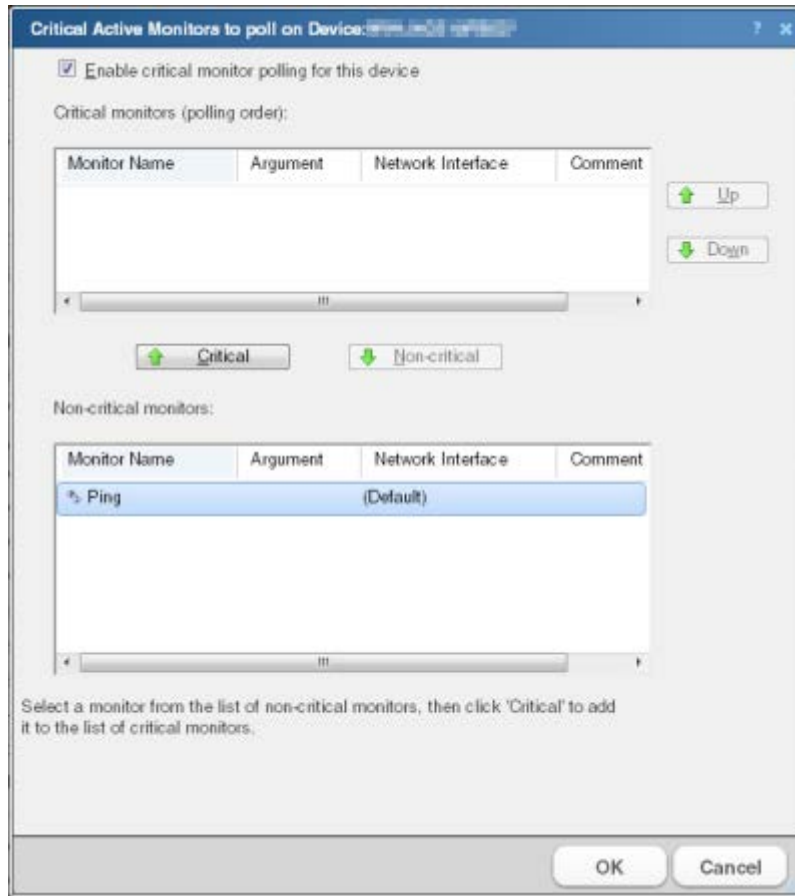
Note: Independent poll frequency for all monitors is ignored when a monitor is specified as critical.

xxvii) Configuring a critical polling path

To configure a critical polling path for device active monitors:

- 1 Right-click the device for which you want to configure a critical polling path in the Details or Map View and select **Properties**. The Device Properties dialog appears.
- 2 Select **Active Monitors**. The Device Properties - Active Monitors dialog appears.

- 3 Select an active monitor, then click **Critical**. The Critical Active Monitor properties appear.



- 4 Select **Enable critical monitor polling for this device**.
- 5 Under the **Non-critical monitors** list, select the monitor(s) that you would like polled first in the critical polling path, then click **Critical**.



Tip: To remove a monitor from the **Critical monitors** list, select the monitor in the **Critical monitors (polling order)** list, then click **Non-critical**.

- 6 Under the **Critical monitors** list, use the **Up** and **Down** buttons to place critical monitors in the order that you want the monitors polled. The first monitor is the first polled in the critical polling path. If the first monitor goes down, all monitors below it are not polled until the first monitor returns to an up state. If you select only one critical monitor, this is the first and only critical monitor in the critical polling path; all non-critical monitors are not polled unless the critical monitor is in the up state. Additionally, if a critical monitor fails, all subsequent critical and non-critical monitors are forced into an unknown state until the critical monitor returns to an up state.



Tip: The paragraph at the bottom of the dialog describes the critical monitor path as it is configured.

7 Click **OK** to save changes.

Group and Device active monitor reports

The following reports display information for devices and device groups that have active monitors configured and enabled. Access these reports from the WhatsUp Gold web interface's Reports tab.

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

Passive Monitor Library

In This Chapter

| | |
|---|-----|
| Passive monitors overview..... | 232 |
| Passive Monitor Icon | 233 |
| Using the Passive Monitor Library..... | 233 |
| Understanding Passive Monitor Listeners..... | 235 |
| Configuring passive monitors..... | 238 |
| Assigning passive monitors | 243 |
| Group and device passive monitor reports..... | 245 |

Passive monitors overview

Passive monitors are the WhatsUp Gold feature responsible for listening for device events. As active monitors actively query or poll devices for data, passive monitors passively listen for device events. Because passive monitors do not poll devices, they use less network bandwidth than active monitors.

Passive monitors are useful because they gather information that goes beyond simple Up or Down service and device states by listening for a variety of events. For example, if you want to know when someone with improper credentials tries to access one of your SNMP-enabled devices, you can assign the default Authentication Failure passive monitor. The monitor listens for an authentication failure trap on the SNMP device, and logs these events to the SNMP Trap Log. If you assign an action to the monitor, every time the authentication failure trap is received, you are notified as soon as it happens.

Although passive monitors are useful, you should not rely on them solely to monitor a device or service—passive monitors should be used in conjunction with active monitors. When used together, active and passive monitors make up a powerful and crucial component of 360-degree network management.

Passive monitor types are specific configurations of SNMP traps, Windows Log Events, and Syslog Events. After the monitor types are configured, you can associate them to devices on the Passive Monitors section of Device Properties dialog.

Using the Passive Monitor Library, you can:

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

Successful passive monitors

Creating a successful passive monitor requires that you take several steps:



Important: Before you attempt to create a passive monitor, you should know the specific traps (and coinciding MIBs) for which you want WhatsUp Gold to listen —this makes the process much easier.

- 1 Turn on traps on the device from which you want to receive logs, entries, and/or alerts.
- 2 Point the traps on that device to the WhatsUp Gold machine.
- 3 Enable the WhatsUp Gold *Passive Monitor Listeners* (on page 235).
- 4 Create a passive monitor for each of the traps for which you want WhatsUp Gold to listen.
- 5 Assign the passive monitor to the device on which you want to listen for traps.

Additionally, after you create a passive monitor, you can configure alerts to notify you when a particular trap is received.

Passive Monitor Icon

Passive Monitors Icon



When a passive monitor is configured on a device, the device icon displays a diamond shape on the upper left side.



This shape changes color when an unacknowledged state change occurs on the monitor. After the device has been acknowledged, the icon returns to the above appearance.

Using the Passive Monitor Library

The Passive Monitor Library stores all passive monitor types that have been created for WhatsUp Gold. The library includes a variety of pre-configured SNMP passive monitors, as well as a generic "Any" passive monitor for SNMP, Syslog, and Windows Event Log types. The Any passive monitor listens and receives *all* traps and events that occur on the device to which it is assigned.

Though you can create three types of passive monitors, SNMP passive monitors are the type most widely used.

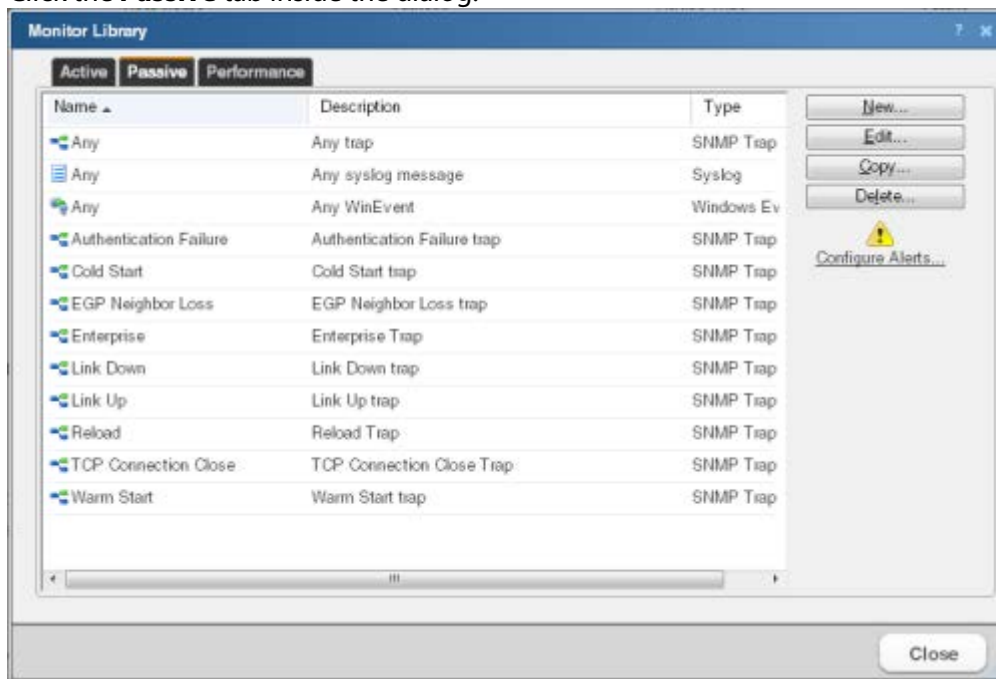
SNMP Trap passive monitors in the library

The SNMP Trap monitors listed in the Passive Monitor Library are based on one of three things:

- **Passive monitors already in the database.** By default, the passive monitor database comes with a few of the most Common SNMP traps already in it.
- **Passive monitors automatically created by WhatsUp Gold Trap Definition Import Tool.** Use the Trap Definition Import Tool to create SNMP Traps from MIB files stored in the \Program Files\Ipswitch\WhatsUp\Data\Mibs folder.
- **Passive monitors that you define yourself.** This can be done either by copying and pasting actual trap information directly from your existing logs, or by browsing the MIB for OID values that you are interested in, and adding the **Generic type (Major)** and **Specific type (Minor)** information if required.

To access and use the Passive Monitor Library:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Passive** tab inside the dialog.



Use the Passive Monitor Library dialog to configure new or existing passive monitor types:

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

Understanding Passive Monitor Listeners

A Passive Monitor Listener is the component in passive monitors that listens for events to occur. When an event occurs, the listener notifies WhatsUp Gold and associated actions are fired.

WhatsUp Gold is installed with three Passive Monitor Listeners:

- **SNMP Trap Listener.** This listens for SNMP traps, or unsolicited SNMP messages, that are sent from a device to indicate a change in status.
- **Syslog Trap Listener.** This listens for Syslog messages forwarded from devices regarding a specific record and/or text within a record.
- **Windows Event Log Listener.** This listens for any WinEvent; for example a service start or stop, or logon failures.



Important: Before you can configure passive monitors, you must configure the coinciding Passive Monitor Listener(s) on the WhatsUp Gold console via Program Options. For more information, see *Enabling the SNMP Trap listener* (on page 873), *Enabling the Syslog listener* (on page 875), and *Enabling the Windows Event Log listener* (on page 874).

Configuring the SNMP Trap Listener

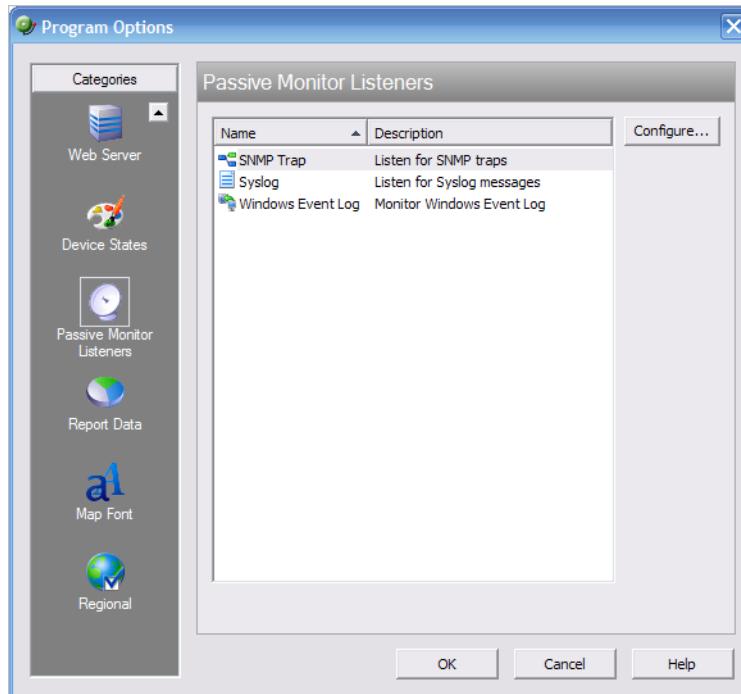
To configure the SNMP Trap Listener:

- 1 From the WhatsUp Gold console main menu, select **Configure > Program Options**. The Program Options dialog appears.



Note: If the Windows SNMP Trap Service (**Control Panel > Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

- 2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.



- 3 Select the SNMP Trap listener, then click **Configure**. The SNMP Listener Configuration dialog appears.
- 4 Enter or select the appropriate information in the following fields:
 - **Listen for messages on port.** Select this option if you want WhatsUp Gold to listen for SNMP traps. The standard SNMP trap port is 162, but you can change this port to a non-standard port number.



Note: When you change the port number, the change takes place as soon as you save the change; you do not have to re-start WhatsUp Gold for the change to take effect.

- **Accept unsolicited SNMP traps.** Select this option to receive and log all incoming SNMP traps, including those not assigned to devices as passive monitors. By default, SNMP traps assigned to devices as passive monitors are logged and can trigger actions. Incoming traps received as unsolicited traps are logged to the System SNMP Trap Log.



Caution: When this option is selected, every SNMP trap that is received by WhatsUp Gold is logged to the database. Enabling this option can result in a large database that impacts performance; we strongly advise that you leave this option disabled, except when you are troubleshooting.



Note: To configure SNMP traps initially, we recommend enabling the **Any** SNMP trap on the source device; you can then see all incoming traps sent from that device in the Device SNMP Trap Log. After you configure the trap successfully, you should disable the **Any** trap, as it may also log large amounts of data.

- **Forward traps.** Select this option to forward traps to the IP address(es) you specify in **Forward traps to**.
- **Forward unsolicited traps.** Select this option to forward all traps, including unsolicited traps.
- **Forward traps to.** Click Add to add in IP address and port to which to forward traps.



Note: You can forward traps to multiple IP addresses.



Tip: You can **Edit** and/or **Remove** IP addresses from this list.

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

Configuring the Syslog Listener

WhatsUp Gold has an internal SNMP trap handler, which when enabled, listens for and accepts SNMP traps. WhatsUp Gold records the trap in the device's **SNMP Trap Log**.

To configure WhatsUp Gold to receive traps:

- 1 On the devices that are to be monitored, set the SNMP agent to send traps to WhatsUp Gold. Trap manager addresses must be set on each physical device. This cannot be done from WhatsUp Gold.
- 2 Set up the MIB entries for traps by placing the MIB text file in the `C:\Program Files\Ipswitch\WhatsUp\Data\Mibs` directory.
- 3 Enable the SNMP Trap Handler.

To configure the Syslog Passive Monitor Listener:

- 1 From the WhatsUp Gold console main menu, select **Configure > Program Options**. The Program Options dialog appears.



Note: If the Windows SNMP Trap Service (**Control Panel > Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

- 2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.
- 3 Select the Syslog Trap listener, then click **Configure**. The Syslog Listener Configuration dialog appears.

- 4 Enter or select the appropriate information in the following fields:
 - Listen for messages on port. Select this option if you want WhatsUp Gold to listen for Syslog messages. The Syslog Listener runs on port 514 by default, but can be changed if necessary.
 - **Accept unsolicited passive monitors.** If option this is cleared, ONLY Syslog entries which are specifically added to devices as passive monitors are logged to the System Syslog report. If you select this option, ALL incoming Syslog messages are detected and logged to the System Syslog report.



Note: Regardless of this filter setting, only Syslog messages that are solicited are logged to the devices' Syslog reports and are able to trigger actions.

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

Configuring the Windows Event Log Listener

To configure the Windows Event Log Listener:

- 1 From the WhatsUp Gold console main menu, select **Configure > Program Options**. The Program Options dialog appears.



Note: If the Windows SNMP Trap Service (**Control Panel > Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

- 2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.
- 3 Select the Windows Event Log Listener, then click **Configure**. The Windows Event Log Listener Configuration dialog appears.
- 4 Enter or select the appropriate information in the following fields:
 - **Start Server.** Select this option if you would like WhatsUp Gold to listen for Windows Event logs.
 - **Do not generate payload.** Select this option to only add the event time and message to the Windows Event Log; the payload is withheld from the entry.
 - **Check connections interval.** Select this option to have WhatsUp Gold check for and close inactive connections at the interval you specify. The default interval is 60 seconds.
- 5 Click **OK** to save changes.

Configuring passive monitors

You can configure passive monitors two ways:

- 1 Automatically using the Trap Definition Import Tool.
- 2 Manually using the Passive Monitor Library.

The Trap Definition Import Tool allows you to search for the specific SNMP trap for which you want WhatsUp Gold to listen, and then import that trap into the Passive Monitor Library. After you import the trap, you can make specifications to the passive monitor in the Passive Monitor Library using the Rules Expression Editor dialog. For example, if you want WhatsUp Gold to monitor when a specific IP address causes an authentication failure on your SNMP-enabled device, you would create a rule that tells WhatsUp Gold to log an event only when that particular IP address attempts to access the SNMP-enabled device.

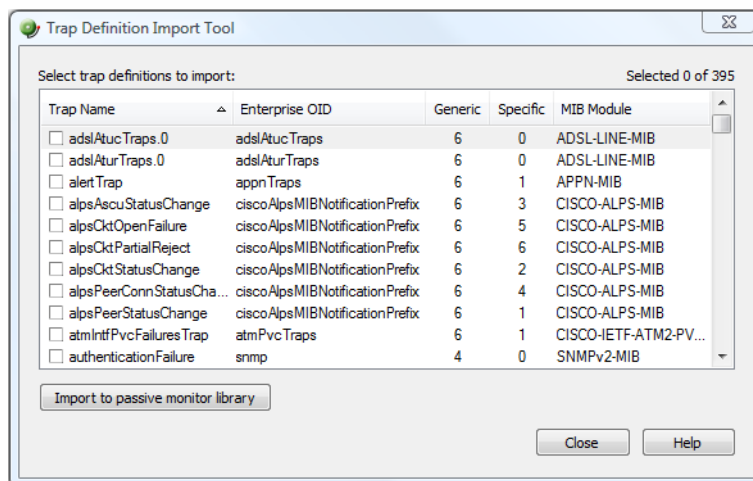
While using the Trap Definition Import Tool or any of the pre-configured passive monitors are two easy ways to configure SNMP Trap passive monitors, you still have the option to manually configure all passive monitor types via the Passive Monitor Library.

Using the Trap Definition Import Tool

The Trap Definition Import tool is used to import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your WhatsUp Gold MIB folder (\Program Files\Ipswitch\WhatsUp\Data\Mibs).

To import SNMP trap definitions into the Passive Monitor Library:

- 1 In the WhatsUp Gold console, select **Tools > Import Trap Definitions**. The Trap Definition Import Tool dialog appears.



- 2 Select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog appears and provides a message about the import results.



Note: Traps that already exist in the database are not imported.



Tip: Use the dialog's scroll bar to scan available traps.

Using the Passive Monitor Library

You can use the Passive Monitor Library to manually create new instances of a passive monitor type, or to edit the configuration of monitors you import using the Trap Definition Import Tool.

xxviii) Adding and Editing a SNMP Trap Monitor

To add or edit a SNMP trap passive monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Passive** tab. The Passive Monitor list appears.
- 3 Click **New** and select **SNMP Trap** from the list to create a new SNMP trap passive monitor.
- or -
Select the SNMP trap passive monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the monitor. This name displays in the Passive Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Passive Monitor Library.
 - **Enterprise/OID.** Use the browse button to select the desired object identifier (OID) from the Enterprise section of the MIB. This is the SNMP enterprise identifier in the trap, which is used for unique identification of traps for a particular application. If you specify the OID in this field, then an incoming trap matches this rule only if the trap enterprise field begins with the OID that you have specified. If you are unsure of the OID to use, or you do not need to be specific, you can leave this field blank and it is ignored.



Note: This option is only available if **Generic Type** is set to **6-EnterpriseSpecific**.

- **Generic Type (Major).** Each trap has a generic type number. This number is part of the rule that determines the matching criteria for an incoming trap. For more information, see Common SNMP Traps.



Note: The definitions of 0 through 6 are not WhatsUp Gold definitions, but come from the SNMP specifications.

- **Specific Type (Minor).** This can have an integer value from 0 to 4294967296. To use this option, **Generic Type** must be always enterprise-specific. If you want to ignore this field, select **Any**.
- **Payload.** Click **Add** to view the Expression Editor where you can create an expression, test it, and compare it to potential payloads. After creating an expression, click **OK** to insert that string into the list under **Match On**.

- 5 Click the **Add** button to view the Expression Editor where you can create an expression, test it, and compare it against potential payloads you can receive. After creating the expression, click **OK** to insert that string into the **Match on** box.



Note: If you have multiple payload "match on" expressions, they are linked by "OR" logic—not "AND" logic. If you have two expressions, one set to "AB" and the other to "BA", it matches against a trap containing any of the following: "AB" or "BA" or "ABBA".

- 6 Click **OK** to add the monitor to the Passive Monitor Library.

After configuring a passive monitor in the Passive Monitor Library, *add the monitor to devices* (on page 243).

xxix) Adding and Editing a Syslog Monitor

To add or edit a Syslog monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Passive** tab. The Passive Monitor list appears.
- 3 Click **New** and select **Syslog** from the list to create a new Syslog monitor. Click **OK**.
- or -
Select the Syslog monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the monitor. This name displays in the Passive Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Passive Monitor Library.
 - **Match On.** You can click the **Add** button to access the *expression editor* (on page 166), where you can create your expression, test it, and compare it against potential payloads you can receive. After creating the expression, click **OK** to insert that string into the Match on box.



Note: If you have multiple payload "match on" expressions, they are linked by "OR" logic - not "AND" logic. Example: If you have two expressions, one set to "AB" and the other to "BA", it will match against a trap containing any of the following: "AB" or "BA" or "ABBA".

- 5 Click **OK** to list this event in the Passive Monitor Library as a Syslog Passive Monitor.

After configuring a passive monitor in the Passive Monitor Library, *add the monitor to devices* (on page 243).

For an example of why you might create a Syslog Event, see *Sample of a Syslog Monitor Event*.

xxx) Adding and Editing a Windows Event Log Monitor

When assigning a Windows Event Log passive monitor to a device, make sure the device has credentials assigned to it before creating the passive monitor. To use multiple Windows Event Log passive monitors, assign a unique Windows Event Log passive monitor for each device.

The upgrade process to WhatsUp Gold from previous versions automatically migrates Windows Event Log passive monitor credentials into the Credentials Library. If you experience upgrade problems with Windows Event Log passive monitors, look in the Credentials Library for the Windows (WMI) credentials that work for the device. If the device credentials do not exist, create new credentials for the device.

To add or edit a Windows Event Log monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Passive** tab. The Passive Monitor list appears.
- 3 Click **New** and select **Windows Event Log** to create a new Windows Event Log monitor. Click **OK**.
- or -
Select the Windows Event Log monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the monitor. This name displays in the Passive Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Passive Monitor Library.
 - **Condition.** Enter a list of conditions to match. Only log entries matching these expressions are converted to events. Conditions are processed sequentially from top to bottom. As each condition is evaluated, its results are applied to the next condition until all conditions are evaluated. For complex sets of conditions involving both ANDs and ORs, this serial logic may produce different results than intended. As a best practice, we recommend keeping conditions simple by opting for multiple Passive Monitors over complex sets of conditions. When complex conditions are unavoidable, we recommend grouping all OR conditions together at the beginning of the set of conditions, followed by the ANDs.
 - Click **Edit** to add or edit a condition or **Clear** to remove a condition from the box.
 - **Match On.** You can click the **Add** button to access the *expression editor* (on page 166), where you can create your expression, test it, and compare it against potential payloads you can receive. After creating the expression, click **OK** to insert that string into the **Match On** list.



Note: If you have multiple payload **Match On** expressions, they are linked by OR logic, not AND logic. For example, if you have two expressions, one set to "AB" and the other to "BA", it is matched against any log entry that includes either of the two strings.

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

After configuring a passive monitor in the Passive Monitor Library, *add the monitor to devices* (on page 243).

xxxxi) Using the Any Passive Monitor

The Any passive monitor receives *all* type-specific (SNMP, Syslog, Windows Event Log) traps and events sent from the device to which it is assigned. This monitor can be useful when you are trying to pinpoint the specific trap and coinciding MIB for which you want to WhatsUp Gold to listen and monitor. As the monitor gathers traps and events, this data is added to the respective log (SNMP Trap Log, Syslog Entries, Windows Event Log). You can scan the report entries to find the specific trap that you would like to monitor, and create a passive monitor for that specific trap.

If, after running the monitor for some time, you do not notice the trap for which you are looking, the MIB may not be loaded in the WhatsUp Gold MIB directory. If this is the case, import the MIB. For more information, see *Using the SNMP MIB Manager*.



Important: Because of the volume of data gathered when this monitor is enabled, we strongly advise that this monitor only be used for troubleshooting purposes. If this monitor is enabled for more than short periods of time, you run the risk of flooding your database and compromising the performance of WhatsUp Gold.

As the monitor has been pre-configured for you, to use it, you are required only to assign it to the device for which you researching traps and events. For more information, see *Assigning passive monitors* (on page 243).

It is important that you remember to remove the monitor when you have completed troubleshooting because of the monitor's potential to fill up the WhatsUp Gold database.

Assigning passive monitors

After you configure a passive monitor in the Passive Monitor Library, you must add it to the individual devices for which you want to monitor services.



Note: If you are assigning a Windows Event Log passive monitor type to a device, make sure that the device has credentials assigned before creating a passive monitor for it. For more information, see *Using Credentials* (on page 75).

If want to use multiple Windows Event Log passive monitors, you must assign a unique Windows Event Log passive monitor for each device.



Note: The upgrade process to WhatsUp Gold from previous versions, automatically migrates Windows Event Log passive monitor credentials into the Credentials Library. If you experience upgrade problems with Windows Event Log passive monitors, look in the credentials library for the Windows (WMI) credentials that will work for the device. If the device credentials do not exist, create new credentials for the device. For more information, see *Using Credentials* (on page 75).



Note: When you assign a passive monitor to a device, an instance of the monitor is added to the device. Changes that you make to the monitor's configuration via the Passive Monitor Library affect all instances of the monitor. For example, if you assign a monitor to four separate devices and then make changes to the monitor from the Passive Monitor Library, all four instances of the monitor adopt the changes.

To assign a passive monitor to a device:

- 1 From the Details or Map View, right-click a device and select **Properties**. The Device Properties dialog appears.
- 2 Click **Passive Monitors**. The Device Properties Passive Monitor dialog appears.
- 3 Click **Add**. The Passive Monitor Properties dialog appears.

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

Select an action from the Action Library

- or -

Create a new action

Follow the remaining Wizard dialog screens for the selection you made.

- 7 Click **Finish** to add the passive monitor to the device.



Note: You can view the monitor logs by selecting an option on the Logs tab.

Group and device passive monitor reports

The following reports display information for devices or device groups that have passive monitors configured and enabled. Access these reports from the WhatsUp Gold web interface's Reports tab.

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

Using Performance Monitors

In This Chapter

| | |
|--|-----|
| Performance monitors overview | 246 |
| Using the Performance Monitor Library..... | 247 |
| Working with Performance Monitors..... | 248 |
| Adding and editing an SNMP Performance Monitor..... | 249 |
| Adding and editing an SSH Performance Monitor..... | 250 |
| Adding and editing an Active Script Performance Monitor..... | 250 |
| Adding and editing a WMI Performance Monitor | 254 |

Performance monitors overview

Performance monitors are the WhatsUp Gold feature responsible for gathering data about the performance components of the devices running on your network; for example, CPU and memory utilization. The data is then used to create reports that trend utilization and availability of these device components.

WhatsUp Gold performance monitors gather data from the following components:

- CPU utilization
- Disk utilization
- Interface utilization
- Interface traffic
- Memory utilization
- Ping availability
- Ping response time

Additionally, you can create custom performance monitors to track specific performance monitors for APC UPS, Printer, Active Script, SNMP, SSH, and WMI performance counters.

Performance Monitors are configured in the *Performance Monitor Library* (on page 247) and are added to individual devices through a the Device Properties dialog. From the Device Properties Performance Monitor dialog, you can add:

- Pre-configured (standard) Performance Monitors
- Device-specific (custom) Performance Monitors



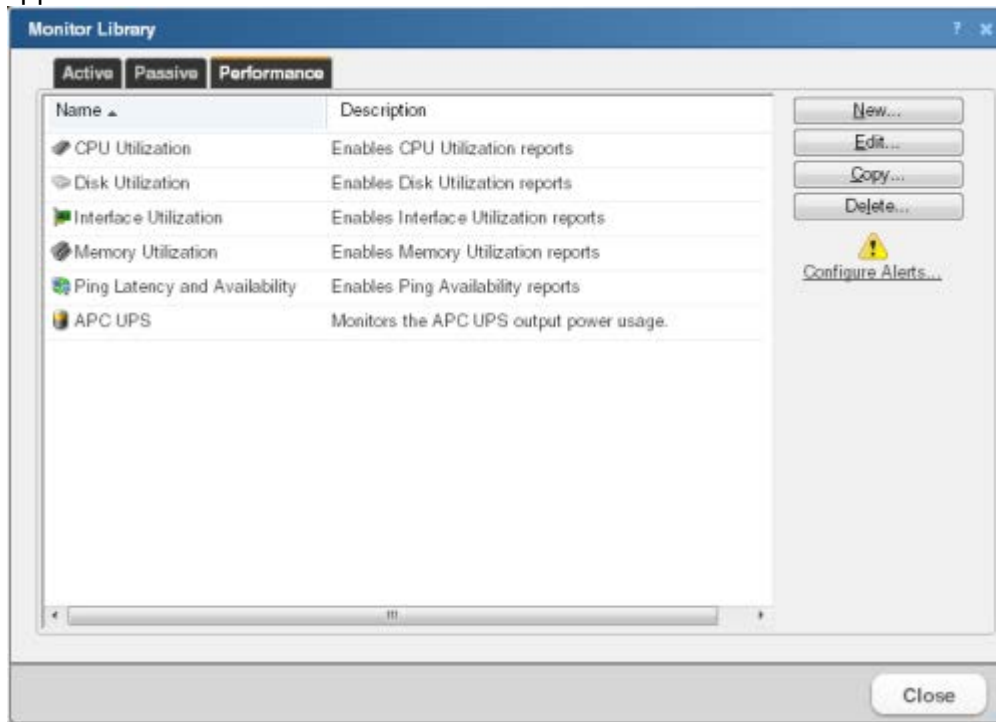
Note: Unlike the other performance monitors, because a printer monitor is specific to an individual printer device, the Printer Performance Monitor can only be added as an individual performance monitor in the Device Properties Performance Monitor dialog.

Using the Performance Monitor Library

The Performance Monitor Library stores and displays the Performance Monitors that have been created for WhatsUp Gold. Performance monitors gather information about specific WMI and SNMP values from network devices. There are several default performance monitors, such as CPU and Disk Utilization, available in the library and you can add new monitors to the library. Performance monitors can be applied to devices from the Device Properties dialog for that device.

To access the Performance Monitor Library:

- 1 Click the **Admin** tab, and then click **Monitor Library**. The Monitor Library dialog appears.



- 2 If it is not already selected, click the **Performance** tab.
- 3 Use the Performance Monitor Library dialog to configure new or existing performance monitor types:
 - Click **New** to configure a custom performance monitor.
 - Select an existing performance monitor, then click **Edit** to modify its configuration.
 - Click **Copy** to create a duplicate of a monitor. You can use the Copy option to create new monitors based on existing monitors.



Note: The five default global monitors cannot be edited, copied or deleted: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

- Select an existing performance monitor, then click **Delete** to remove it from the list.



Caution: When you delete a performance monitor from the Performance Monitor Library, any instance of that monitor is also deleted, and all related report data is also lost.

- Click **Configure Alerts** to view the Alert Center Threshold Library.

For more information on Performance Monitors, see *Enabling performance monitors* (on page 622).

Working with Performance Monitors

The Performance Monitor Library is a central storehouse of all global performance monitors configured for your network. *Performance monitors* (on page 630) gather information about specific WMI and SNMP values from the network devices.



Note: Default monitors in the library cannot be edited or removed: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

You can use the Performance Monitor Library to configure and manage performance monitors.

Use the Performance Monitor Library dialog to configure new or existing performance monitor types:

- Click **New** to configure a custom performance monitor.
 - Select an existing performance monitor, then click **Edit** to modify its configuration.
- 1 **Note:** The five default global monitors cannot be edited or deleted: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.
 - 2 Select an existing performance monitor, then click **Delete** to remove it from the list.



Caution: When you delete a performance monitor from the Performance Monitor Library, any instance of that monitor is also deleted, and all related report data is lost.



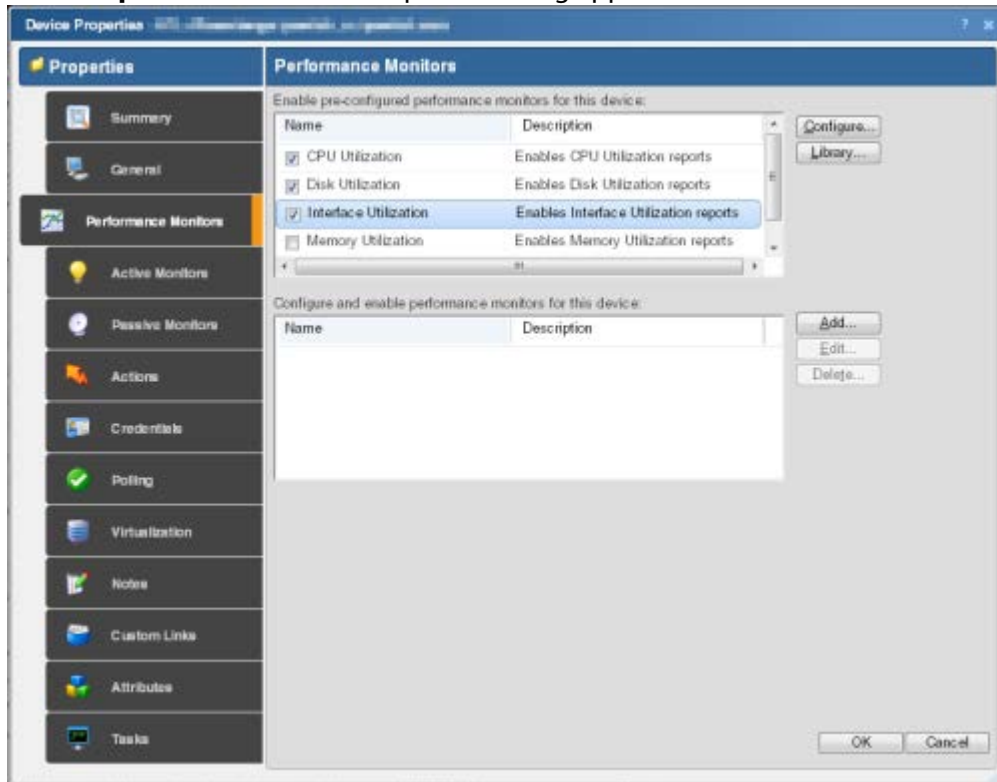
Tip: Click **Configure Alerts** to view the Alert Center Threshold Library.



Caution: When custom Performance Monitors are changed, the changes affect each instance of that particular monitor across device groups.

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

- 1 From the Device Properties page, right-click a device you want to configure. The right-click menu appears.
- 2 Click **Properties**. The Device Properties dialog appears.



- 3 Select the monitor from the list and click **Configure** to enable a pre-configured monitor for this device.
 - or -
 - Click **Add** and create a device-specific monitor.
 - or -
 - Double-click an existing monitor to change its configuration.
 - or -
 - Select a performance monitor type, then click **Delete** to remove it from the list.
- 4 Click **OK** to save changes.

Adding and editing an SNMP Performance Monitor

To add or edit an SNMP Performance Monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab. The Performance Monitor list appears.
- 3 Click **New** and select **SNMP Performance Monitor** from the list to create a new SSH performance monitor. Click **OK**.
 - or -
 - Select the SNMP performance monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type a **Name** and **Description** for the monitor as you want it to appear in the Performance Monitor Library.

- 5 Either type the OID and instance or click the browse (...) button next to the **Instance** box to access the SNMP MIB Walker dialog.
- 6 Click **OK** to save the changes.

Adding and editing an SSH Performance Monitor

To add or edit a SSH performance monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab. The Performance Monitor list appears.
- 3 Click **New** and select **SSH Performance Monitor** from the list to create a new SSH performance monitor. Click **OK**.
- or -
Select the SSH performance monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the monitor. This name displays in the Performance Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Performance Monitor Library.
 - **Command to run.** Type the command you want to run and execute on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a Perl script.



Important: The command or script must return a single numeric value.



Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- **SSH Credential.** Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select **Use the device SSH credential**, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, click browse (...) to open the WhatsUp Gold Credentials Library and configure a set of credentials.
- 5 Click **OK** to save changes.

Adding and editing an Active Script Performance Monitor



Warning: Modifying the configuration of any of the VoIP Active Script Performance monitors is not recommended; doing so prevents the VoIP setup utility from detecting pre-existing VoIP configuration.

For more information on the Active Script Performance Monitor, see Scripting Performance Monitors.

This script performance monitor has a context object used to poll for specific information about the device in context.

We have provided several code samples to help you in creating useful Active Script Performance Monitors for your devices.

To add or edit an active script performance monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab. The Performance Monitor list appears.
- 3 Click **New** and select **Active Script Performance Monitor** from the list to create a new active script performance monitor. Click **OK**.
- or -
Select the active script performance monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Complete the information for the following fields.
 - **Name.** Type a name for the monitor. This name displays in the Performance Monitor Library.
 - **Script type.** VBScript or JScript.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Performance Monitor Library.
 - **Timeout.** The length of time (in seconds) WhatsUp Gold waits for a response to the poll.



Note: Though the maximum timeout allowed is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

- **Collection interval.** (For the device-specific Active Script Performance Monitor only). The length of time, in minutes, for the monitor polling interval.
- **Reference variable.** Add, Edit, or Remove SNMP and WMI reference variables using the respective buttons on the right of the dialog.
- **Script text.** Write or paste your monitor code here.

- 5 Add a new variable to the Reference Variables list by clicking **Add**.



Important: You can add up to 100 reference variables.

Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms you would normally have manage to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable` (variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script.



Important: The use of reference variables in the Active Script Performance Monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed.

- 6 On the Add reference variables dialog, type a name and description for the variable.
- 7 Select the type of object (SNMP) from the **Object type** list.
- 8 If needed, adjust the **Timeout** and **Retries** count for connection to the device.
- 9 Click the browse (...) button next to the Instance box. The SNMP MIB Browser appears.
- 10 Type the share name or IP address of the computer to which you are trying to connect.
- 11 Type the SNMP credential used to connect to the device (or click the browse (...) button to access the Credentials Library to create a new credential.)
- 12 If needed, adjust the **Timeout** and **Number of retries** for the computer to which you are trying to connect.
- 13 Click **OK**. The SNMP MIB Browser appears.
- 14 Use the navigation tree in the left panel to select the specific MIB you want to monitor. You can view more information about the property/value at the bottom of the dialog.
- 15 Click **OK** to add the OID to the **Performance counter** and **Instance box** in the Add new reference variable dialog.
- 16 Verify the configuration and click **OK** to add the variable to the **Reference variable** list on the Add active script performance monitor dialog.
- 17 Write or paste your monitor code in the **Script text** box.
- 18 Click **OK** to save changes and add the monitor to the Performance Monitor Library.



Tip: The SNMP API is useful for writing Active Script Performance Monitors using SNMP. For more information, see Using the SNMP API.

To configure a WMI active script performance monitor:

- 1 On the Add Active Script Performance Monitor dialog, type a **Name** and **Description** for the monitor as you want it to appear in the Performance Monitor Library.
- 2 Type a number for the timeout (in seconds), and for the device-specific Active Script Performance Monitor, type a number (in minutes) for the Collection interval.
- 3 Choose the type of script (JScript or VBScript) you are using to write the monitor from the **Script type** drop down menu.
- 4 Add a new variable to the Reference Variables list by clicking **Add**.



Important: You can add up to 10 reference variables.

Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They manage the underlying SNMP or WMI mechanisms that you would normally manage to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable` (variable name), you only need to specify the name of a pre-defined variable. WhatsUp Gold uses device credentials and connects to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable you can use later in your script.



Important: The use of reference variables in the Active Script Performance Monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed.

- 5 On the Add reference variables dialog, type a name and description for the variable.
- 6 Select the type of object (WMI) from the **Object type** drop-down menu.
- 7 Click the browse (...) button next to the Instance box. The Performance Counters dialog appears.
- 8 Type the computer name or IP address of the computer to which you want to connect.
- 9 Select a credential from a list of Windows credentials (pulled from the Credentials Library), then click **OK** to connect to the computer.
- 10 Use the Performance counter tree to navigate to the performance counter you want to monitor.
- 11 Once you select the performance counter, select the specific instance you want to monitor.
- 12 Click **OK** to add the variable to the **Reference variable** list on the Add active script performance monitor dialog.
- 13 Write or paste your monitor code in the **Script text** box.
- 14 Click **OK** to save changes and to add the monitor to the Performance Monitor Library.



Warning: The first time that you poll a WMI reference variable that requires two polls in order to calculate an average (such as "Processor\% Processor Time"), it returns "Null."

Troubleshooting

Having problems with your WMI monitor returning false negatives?

Adding and editing a WMI Performance Monitor

From here you can update the name and description of the performance monitor and open the WMI Performance Counter tree.

To add or edit a WMI performance monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab. The Performance Monitor list appears.
- 3 Click **New** and select **WMI Performance Monitor** from the list to create a new WMI performance monitor. Click **OK**.
or
Select the WMI performance monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the monitor. This name displays in the Performance Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Performance Monitor Library.
 - **Browse (...).** Connects to the WMI Performance Counter tree.
 - **Performance counter/Instance.** Click the browse (...) button next to this box to *select a performance counter* (on page 322) for the monitor.
- 5 Click **OK** to save changes.

Enabling global performance monitors

In order for a performance monitor to gather performance data from a device, it must be enabled on that device. You can *enable a monitor on a single device* (on page 254) through the Device Properties dialog, or *enable a monitor on multiple devices* (on page 255) through the Bulk Field Change feature.

Enabling a global performance monitor on a single device

To enable a global performance monitor for a single device:

- 1 In Device or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 Under **Enable pre-configured performance monitors for this device**, select the global monitor you would like to enable.

- 4 Click **Configure** to complete the settings for the selected performance monitor.



Important: To enable a CPU, disk, interface, or memory global performance monitor, you must first select an SNMP credential for the device from the Credentials Library. For more information, see *Using credentials* (on page 75).

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

Enabling a global performance monitor on multiple devices

To enable multiple a performance monitor on multiple devices:

- 1 In Details or Map View, select the devices or group for which you would like to enable the monitor, then right-click. Select **Bulk Field Change > Performance Monitors**. The Bulk Field Change: Performance Monitors dialog appears.
- 2 Under **Collect data for**, select the desired option for the appropriate performance monitor. After you have selected the monitor for which you want to collect data, you also have the option to modify the monitor **Data collection interval**.
- 3 Click **OK** to save changes.

Configuring the CPU monitor collection settings

To configure the CPU utilization monitor collection settings for a device:

- 1 On the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 Under **Enable pre-configured performance monitors for this device**, select **CPU Utilization**, then click **Configure**. The Configure CPU Utilization dialog appears.
- 4 Enter or select the appropriate information in the following fields.
 - **Collect data for.** Select the CPU(s) for which you want to gather data. You can choose to track all CPUs or a specific CPU. If you select All CPUs, all CPUs in the list are automatically selected.
 - **Data collection interval.** Enter how often (in minutes) you want data to be collected for the selected CPUs. This number represents the number of minutes between each collection.



Tip: Click **Advanced** to specify the timeout and number of retries, and how WhatsUp Gold is to determine uniqueness when the monitor is tracking more than one CPU.

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

Configuring the disk monitor collection settings

To configure the disk utilization monitor collection settings for a device:

- 1 On the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 Under **Enable pre-configured performance monitors for this device**, select **Disk Utilization**, then click **Configure**. The Configure Disk Utilization dialog appears.
- 4 Enter or select the appropriate information in the following fields.
 - **Collect data for.** Select the disk(s) for which you want to gather data. You can choose to track all disks, one disk, or a combination of disks. If you select **All disks**, all disks in the list are automatically selected.
 - **Data collection interval.** Enter how often (in minutes) you want data to be collected for the selected disks. This number represents the number of minutes between each collection.



Tip: Click **Advanced** to specify the timeout and number of retries, and how WhatsUp Gold is to determine uniqueness when the monitor is tracking more than one disk.

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

Configuring the interface monitor collection settings

To configure the interface utilization monitor collection settings for a device:

- 1 From the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 Under **Enable pre-configured performance monitors for this device**, select **Interface Utilization**, then click **Configure**. The Configure Interface Utilization dialog appears.
- 4 Enter or select the appropriate information in the following fields.
 - **Collect data for.** Select the interface(s) for which you want to gather data. You can select all interfaces, active interfaces, specific interfaces, or custom active interfaces. If you select custom active interface, you can specify to track high speed interfaces, interfaces whose name contain a certain variable, or interfaces that match a certain type. Additionally, if you chose to track a specific interface, you can override the interface **Speed**.



Important: Be aware when you use the **Collect errors and discards data for selected interfaces** feature, it has potential to increase the database size quickly because there is potential for a significant amount of errors and discards data. You can set WhatsUp Health thresholds in the Alert Center to stay informed when the database size exceeds specified thresholds. For more information, see *Configuring system thresholds* (on page 790).



Tip: To disable the errors and discards data collection, you can disable for the individual device (**Device Properties > Performance Monitor**) or disable for multiple devices with the bulk field change option:

1. Select multiple devices that have the Interface Utilization performance monitor enabled, right-click, then select **Bulk Field Change > Performance Monitors**. The Bulk Field Change dialog appears.
2. In the Interface section of the dialog, under the **Collect errors and discards data for enabled interfaces** list, click **Yes**.

For more information, see *Editing multiple devices with the Bulk Field Change feature* (on page 116).

- **Collect errors and discards data for all selected interfaces.** Select this option to collect the following device interface data:
 - **ifInErrors.** Lists the number of inbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.14.
 - **ifOutErrors.** Lists the number of outbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.20.
 - **ifInDiscards.** List the number of inbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.13.
 - **ifOutDiscards.** List the number of outbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.19.



Note: All of the above OIDs point to values of type "counter," and therefore their raw value by itself is not meaningful. The difference between the values obtained from two consecutive polls provides meaningful data.

- **Speed.** Click to specify the speed for the currently selected interface.
- **Data collection interval.** Enter how often (in minutes) you want data to be collected for the selected interfaces. This number represents the number of minutes between each collection.



Tip: Click **Advanced** to specify the timeout and number of retries, how WhatsUp Gold is to determine uniqueness when the monitor is tracking more than one disk, and which interface traffic counters to poll.

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

Configuring the memory monitor collection settings

To configure the memory utilization monitor collection settings for a device:

- 1 On the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 Under **Enable pre-configured performance monitors for this device**, select **Memory Utilization**, then click **Configure**. The Configure Memory Utilization dialog appears.
- 4 Complete the information for the following fields.
 - **Collect data for.** Select the memory item(s) for which you want to gather data. You can choose to track all memory items, or specific memory items. If you select **All memory items**, all memory items in the list are automatically selected.
 - **Data collection interval.** Enter how often (in minutes) you want data to be collected for the selected CPUs. This number represents the number of minutes between each collection.



Tip: Click **Advanced** to specify the timeout and number of retries, and how WhatsUp Gold determines uniqueness when the monitor is tracking more than one memory item.

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

Configuring the ping monitor collection settings

To configure the ping latency and availability monitor collection settings for a device:

- 1 On the Device or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 Under **Enable pre-configured performance monitors for this device**, select **Ping Latency and Availability**, then click **Configure**. The Configure Ping Latency and Availability dialog appears.
- 4 Enter or select the appropriate information in the following fields.
 - **Collect data for.** Select the interface(s) for which you want to gather data. You can choose to track the default interface, all interfaces, or a specific interface. If you select **All interfaces**, all interfaces in the list are automatically selected.
 - **Data collection interval.** Enter how often (in minutes) you want data to be collected for the selected CPUs. This number represents the number of minutes between each collection.



Tip: Click **Advanced** to specify the timeout and number of iterations.

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

Enabling SNMP on Windows devices

Before you can collect performance data on a Windows computer using SNMP, you must first install and enable the Microsoft SNMP Agent on the device itself. For more information, see *Using SNMP Features* (on page 898).

To install SNMP Monitoring :

- 1 From the Windows Control Panel, do one of the following:
 - Click **Add or Remove Programs**.
- or -
 - Click **Programs**.
- 2 Do one of the following:
 - Click **Add/Remove Windows Components**.
- or -
 - Click **Turn Windows features on or off**.
- 3 Do one of the following:
 - From the Components list, select **Management and Monitoring Tools**, then click **Details** to view the list of Subcomponents.
- or -
 - Locate **Simple Network Management Protocol (SNMP)** in the list.
- 4 Make sure Simple Network Management Protocol is selected.
- 5 Click **OK**.
- 6 Click **Next** to install the components.
- 7 After the install wizard is complete, click **Finish** to close the window.

To enable SNMP Monitoring:

- 1 Click the Start button and type `services.msc` in the box.
- 2 In the Services (Local) list, double-click **SNMP Service** to view the Properties.
- 3 On the **Agent** tab, enter the **Contact** name for the person responsible for the upkeep and administration of the computer, then enter the **Location** of the computer. These items are returned during some SNMP queries.
- 4 On the **Security** tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like WhatsUp Gold to read information about the computer. This community string will be later used to *create credentials* (on page 75) 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.

In addition to the five default performance monitors, WhatsUp Gold gives you the option to create custom performance monitors to track specific APC UPS, Printer, Active Script, SNMP, and WMI performance counters.

You can *create global monitors* (on page 260) for system-wide use through the Performance Monitor Library, or *create device-specific monitors* (on page 264) through device Properties.

Creating global custom performance monitors

Global custom performance monitors are stored in the Performance Monitor Library and can be enabled on any device with the proper credentials that supports the performance counters utilized in the monitor.

You can create global custom monitors for APC UPS, Active Script, SNMP, and WMI performance counters.

Creating global SNMP performance monitors

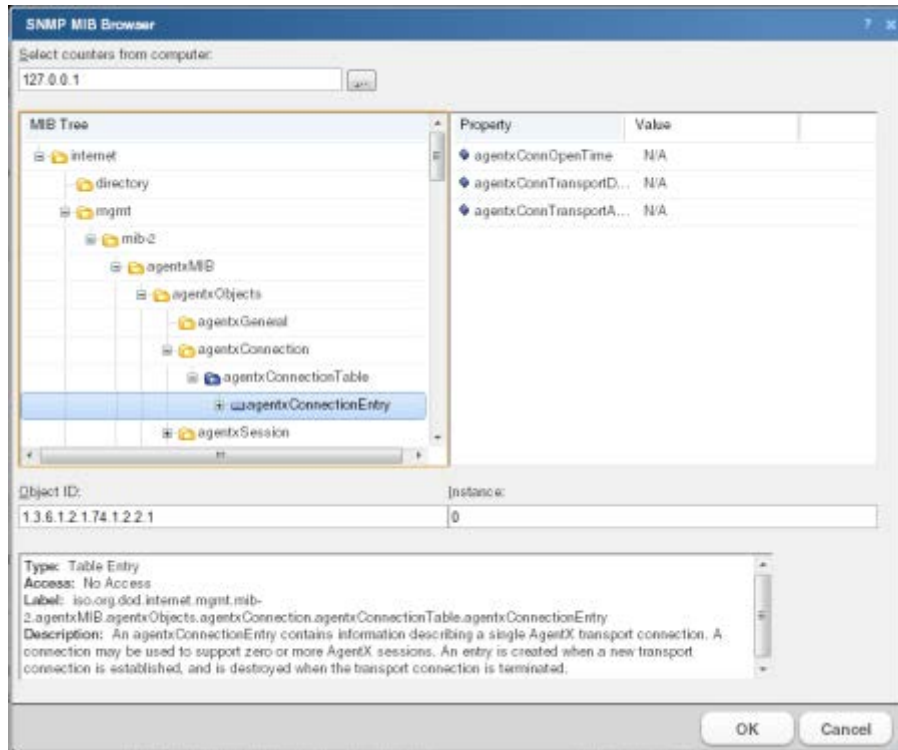
To create an SNMP performance monitor for system-wide use:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab inside the dialog.
- 3 Click **New**. The Select Performance Monitor Type dialog appears.
- 4 Select **SNMP Performance Monitor**, then click **OK**. The Add SNMP Performance Monitor dialog appears.
- 5 Enter a **Name** and short **Description** for the monitor, as it will appear in the Performance Monitor Library.
- 6 Click the browse (...) button next to Instance to access the SNMP MIB Browser. The MIB Browse dialog appears.
- 7 Enter the or select (using the browse (...) button) the IP address of the computer to which you want to connect to browse MIBs.
- 8 Select the SNMP credential set used to connect to the device to which you are attempting to connect.



Tip: If you do not see the appropriate credential set listed, click the browse (...) button to access the Credentials Library where you can create a new set of SNMP credentials.

- 9 Optionally, adjust the values for the **Timeout** and **Number of retries**, then click **OK**. The SNMP MIB Browser appears.



- 10 Use the navigation tree in the left panel to select the MIB for which you want to monitor.
- 11 In the right pane, select the specific property of the selected MIB for which you want to monitor.



Tip: The bottom of the dialog displays any available information about the property/value pair.

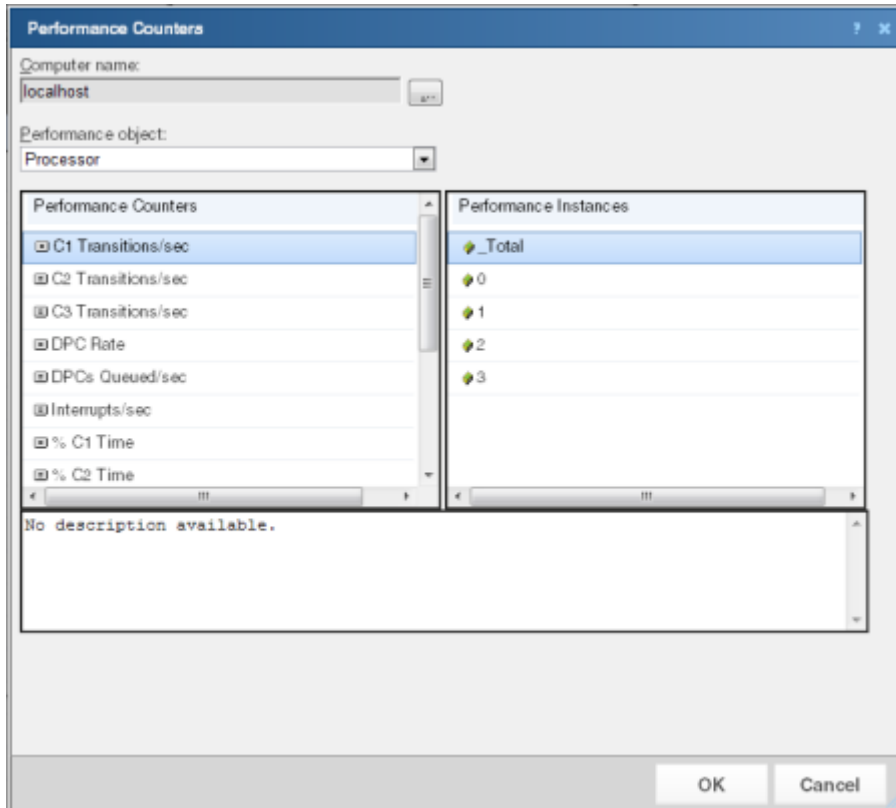
- 12 Click **OK** to add the OID to the **Performance counter** and **Instance** fields of the Add SNMP Performance Monitor dialog.
- 13 Verify the configuration of the monitor, then click **OK** to add the monitor to the Performance Monitor Library.
- 14 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling global performance monitors* (on page 254).

Creating global WMI performance monitors

To create a WMI performance monitor for system-wide use:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab inside the dialog.
- 3 Click **New**. The Select Performance Monitor Type dialog appears.
- 4 Select **WMI Performance Monitor**, then click **OK**. The Add WMI Performance Monitor dialog appears.

- 5 Enter a **Name** and short **Description** for the monitor. This information appears in the Performance Monitor Library and helps you identify the monitor.
- 6 Click the browse (...) button next to **Instance** to connect to the WMI Performance Counter tree.
- 7 Enter the computer name, or use the browse (...) button to locate the computer you want to monitor. In the following window, enter the coinciding Windows Credentials for the computer to which you are attempting to connect, then click **OK**. The Performance Counters dialog appears.



- 8 Use the **Performance Object** list to select an object to monitor in the left pane.
- 9 Use the navigation tree in the left pane to select the counter you want to monitor.
- 10 In the right pane, select the specific instance of the selected counter you want to monitor.



Tip: The bottom of the dialog displays any available information about the counter/instance pair.

- 11 Click **OK** to add the appropriate values to the **Performance counter** and **Instance** fields on the Add WMI Performance Monitor dialog.
- 12 Verify the configuration of the monitor, then click **OK** to add the monitor to the Performance Monitor Library.
- 13 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling global performance monitors* (on page 254).

Adding and Editing an APC UPS Performance Monitor

Global performance monitors are configured in the Performance Monitor Library and can be applied to a device via its Device Properties dialog.

This monitor collects statistical output power usage information and graphs APC UPS power utilization over time.

This monitor detects when UPS devices are close to maximum performance level, and what time of day networking devices connected to UPS devices are using the most power--both indicating the need to equally distribute the load across several UPS devices.

To add or edit an APC UPS performance monitor:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab. The Performance Monitor list appears.
- 3 Click **New** and select **APC UPS Performance Monitor** to create a new APC UPS performance monitor. Click **OK**.
- or -
Select the APC UPS performance monitor you want to change from the list of current monitors, and then click **Edit**.
- 4 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the performance monitor. This name displays in the Performance Monitor Library.
 - **Description.** Type a short description for the monitor. This description displays next to the monitor in the Performance Monitor Library.
- 5 Click **OK** to save changes.
- 6 After the monitor has been added to the library, you can enable the monitor through **Device Properties > Performance Monitors**. For more information, see *Enabling global performance monitors* (on page 254).

Creating global SSH performance monitors

To create an SSH performance monitor for system-wide use:

- 1 Click the **Admin** tab, then click **Monitor Library**. The Monitor Library dialog appears.
- 2 Click the **Performance** tab inside the dialog.
- 3 Click **New**. The Select Performance Monitor Type dialog appears.
- 4 Select **SSH Performance Monitor** and click **OK**. The New SSH Performance Monitor dialog appears.
- 5 Complete the information for the following fields.
 - **Name.** Enter a name for the monitor. This name is displayed in the Performance Monitor Library.
 - **Description.** Enter a short description for the monitor. This description is displayed next to the monitor name in the Performance Monitor Library.
 - **Command to run.** Enter the command that is to be ran and executed on the remote device. This command can be anything that the device can interpret and run; for example, a basic Unix command or a Perl script.



Important: The command or script must return a single numeric value.



Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- **SSH Credential.** Select the appropriate SSH credential that WhatsUp Gold will use to connect to the remote device. If you select *Use the device SSH credential*, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.

6 Click **OK**.

7 Click **Close** to close the Monitor Library.

Creating device-specific custom performance monitors

Device-specific custom performance monitors are configured for use only on the devices for which they are configured.

You can create device-specific custom monitors for APC UPS, Printer, Active Script, SNMP, and WMI performance counters.

Creating device-specific SNMP performance monitors

To create a device-specific SNMP performance monitor:

- 1 In Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 In the **Configure and enable performance monitors for this device** section, click **Add**. The Select Performance Monitor Type dialog appears.
- 4 Select **SNMP**, then click **OK**. The Add SNMP Performance Monitor dialog appears.
- 5 Enter a **Name** and short **Description** for the monitor. This information helps you to identify the monitor later.
- 6 Click the browse (...) button next to Instance to access the SNMP MIB Browser. The MIB Browse dialog appears.
- 7 Enter the or select (using the browse (...) button) the IP address of the computer to which you want to connect to browse MIBs.
- 8 Select the SNMP credential set used to connect to the device to which you are attempting to connect.



Tip: If you do not see the appropriate credential set listed, click the browse (...) button to access the Credentials Library where you may create a new set of SNMP credentials.

- 9 Optionally, adjust the values for the **Timeout** and number **Number of retries**, then click **OK**. The SNMP MIB Browser appears.

- 10 Use the navigation tree in the left pane to select the MIB for which you want to monitor.
- 11 In the right pane, select the specific property of the selected MIB for which you want to monitor.



Tip: The bottom of the dialog displays any available information about the property/value pair.

- 12 Click **OK** to add the OID to the **Performance counter** and **Instance** fields of the Add SNMP Performance Monitor dialog.
- 13 Verify the configuration of the monitor, then click **OK** to add the monitor to the device Properties.

Creating device-specific WMI performance monitors

To create a device-specific WMI performance monitor:

- 1 In Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 In the **Configure and enable performance monitors for this device** section, click **Add**. The Select Performance Monitor Type dialog appears.
- 4 Select **WMI Performance Monitor** from the list, then click **OK**. The Add WMI Performance Monitor dialog appears.
- 5 Enter a **Name** and short **Description** for the monitor. This information helps you to identify the monitor later.
- 6 Click the browse (...) button next to **Instance** to connect to the WMI Performance Counter tree.
- 7 Enter or select (using the browse (...) button) the computer name, and coinciding Windows Credentials for the computer to which you are attempting to connect, then click **OK**. The Performance Counters dialog appears.
- 8 Use the navigation tree in the left pane to select the counter for which you want to monitor.
- 9 In the right pane, select the specific instance of the selected counter for which you want to monitor.



Tip: The bottom of the dialog displays any available information about the counter/instance pair.

- 10 Click **OK** to add the appropriate values to the **Performance counter** and **Instance** fields on the Add WMI Performance Monitor dialog.
- 11 Verify the configuration of the monitor, then click **OK** to add the monitor to the device Properties.

Creating device-specific APC UPS performance monitors

To create a device-specific APC UPS performance monitor:

- 1 In Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 In the **Configure and enable performance monitors for this device** section, click **Add**. The Select Performance Monitor Type dialog appears.
- 4 Select **APC UPS Performance Monitor** from the list, and then click **OK**.
- 5 Enter a **Name** and short **Description** for the monitor. This information helps you to identify the monitor later.
- 6 Enter or select the appropriate information in the following fields.
 - **Collection interval**. Enter how often (in minutes) you want data to be collected for the selected APC UPS. This number represents the number of minutes between each collection.
 - **Timeout**. The length of time (in seconds) WhatsUp Gold attempts to connect to the selected device.
 - **Retries**. Enter the number of times you want to attempt to make the connection to the selected device.
- 7 Verify the configuration of the monitor, then click **OK** to add the monitor to the device Properties.

Creating device-specific Printer performance monitors

To create a device-specific Printer performance monitor:

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



Important: In order for the Printer Performance Monitor to work, in addition to being SNMP-enabled, the printer you are attempting to monitor must also support the Standard Printer MIB. Make sure that you select a device that supports the Standard Printer MIB.

- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 In the **Configure and enable performance monitors for this device** section, click **Add**. The Select Performance Monitor Type dialog appears.
- 4 Select **Printer Performance Monitor**, then click **OK**. The New Printer Performance Monitor dialog appears.
- 5 Enter the **Name** and short **Description** for the monitor. This information helps you to identify the monitor later.
- 6 Select the ink/toner cartridge from which you want to collect ink/toner level data.



Note: You must set up a Printer performance monitor for each color ink/toner cartridge you want to monitor.

- 7 Select the **Collection interval** (in minutes) for how often you want data to be collected for the selected toner cartridge. This number represents the number of minutes between each collection.
- 8 You can click the **Advanced** button to select Advanced options:
 - **Timeout.** Enter the timeout in seconds. If a device does not respond to within this time, the monitor is considered down.
 - **Retries.** Enter the number of attempts to communicate with the device over the network. After this number is exceeded, the monitor is considered down.
- 9 Verify the configuration of the monitor, then click **OK** to add the monitor to the device Properties.

Creating device-specific SSH performance monitors

To create a device-specific SSH performance monitor:

- 1 In Device or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Device Properties - Performance Monitors dialog appears.
- 3 In the **Configure and enable performance monitors for this device** section, click **Add**. The Select Performance Monitor Type dialog appears.
- 4 Select **SSH Performance Monitor**, then click **OK**. The New SSH Performance Monitor dialog appears.
- 5 Enter the **Name** and short **Description** for the monitor, as it will appear in the Performance Monitor Library.
- 6 Enter the **Command to run**, or the command that is to be executed on the remote device. This command can be anything that the device can interpret and run; for example, a basic Unix command or Perl script.



Important: The command or script must return a single numeric value.



Note: If you create a script to run on the remote device, the script must be developed, tested and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- 7 Select the appropriate **SSH credential** that WhatsUp Gold will use to connect to the remote device. If you select **Use the device SSH credential**, WhatsUp Gold uses the SSH credential assigned to the device to which the monitor is assigned. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.
- 8 Enter how often (in minutes) you want data to be collected for the selected APC UPS in the **Collection interval** box. This number represents the number of minutes between each collection.
- 9 Verify the configuration of the monitor, then click **OK** to add the monitor to the device Properties.

Example: monitoring router bandwidth

You can configure WhatsUp Gold to gather bandwidth usage on your SNMP enabled devices (routers, switches, etc.) and then track that usage through performance logs. For bandwidth monitoring, the Interface Utilization monitor is the most useful as it illustrates percent utilization and throughput.

The Interface Utilization monitor gathers statistics on the volume of bytes traveling to and from the active interfaces on a device. You can collect data on all interfaces, active interfaces, or specific interfaces. This monitor is configured and enabled through **Device Properties > Performance Monitors**.



Note: Before you can configure the monitor for a device, you must enable SNMP and assign the proper credentials via the *Credentials Library* (on page 836). The Performance Monitoring system uses these credentials to connect to the device during the configuration process, and during normal performance gathering. For more information, see *Enabling SNMP on Windows devices* (on page 259).

Configuring the monitor

The Interface Utilization Performance Monitor is one of the default performance monitors installed with WhatsUp Gold, and needs no global configuration to configure the monitor for a single device.

To configure the Bandwidth Monitor:

- 1 In either the Details or Map View, right-click on a device, then select **Properties** from the right-click menu.
- 2 Select **Performance Monitors** on the Device Properties dialog.
- 3 Select the Interface Utilization monitor from the list.
- 4 Click **Configure** to set up the monitor for the device. WhatsUp Gold scans the device and discovers the interfaces on the device.

When the scan completes, the Configure Interface Data Collection dialog appears. If the credentials for the device are not configured properly, the scan fails (return to the Credentials Library to fix it). If the device is not SNMP-enabled, the scan fails.

- 5 Select the interfaces you want to collect data for. From the **Collect data for** list, select **All**, **Active**, **Specific**, or **Custom active**. If you select **Specific**, select just the interfaces you want to monitor in the list below. By default, active interfaces are measured.
- 6 On the Configure Interface Data Collection dialog, enter a time interval (in minutes) for how long you want the application to wait between polls in the **Data collection interval** box. The default is 10 minutes. See *Program Options - Report Data* (on page 815) for more information on data collection and roll-up.
- 7 Select **Collect errors and discards data for selected interfaces** to record this data.
- 8 Optionally, click **Advanced** to change the retry and timeout settings for the SNMP connection to the device. Click **OK** to save the changes to the Advanced Settings.
- 9 Click **OK** to save the Interface Utilization configuration.

Viewing data

WhatsUp Gold takes several polling cycles to produce meaningful graphs (with a 10 minute poll interval, this may mean a few hours). After enough data is gathered, several reports display this data.

- **By Device.** Click the Monitoring tab, click the Interface or Interface Errors & Discards monitor report, and then select a device.
- **By Group.** Click the Monitoring tab, click the Interface or Interface Errors & Discards monitor report, and then select a group.
- **System Wide.** Use the Top 10 Dashboard to view the top performers in terms of bandwidth utilization across your network.

Example: troubleshooting a slow network connection

The real-time reporting provided by performance monitors can provide both the raw data and the data trend analysis that can help you isolate network problems. For example, we recently experienced a problem with a network connection between two of our Ipswitch office sites. This example shows how we used Performance Monitors to troubleshoot the slow network connection.

Scenario:

A developer working in Augusta, GA on an Atlanta-based project complained of a slow network connection between the Augusta and Atlanta offices. He stated it took 40 minutes to check in files to the source library over the T1 connection.

The Atlanta office network administrator reacted by completing the following steps:

- 1 On the WhatsUp Gold web interface, he accessed the Monitoring tab to select the Ping Response Time report.
- 2 From the Ping Response Time report, he checked the connection from the Atlanta WhatsUp Gold application to the Augusta primary server. The report showed an increased response time beginning at 11:45 a.m.

This connection was previously configured with the appropriate Performance Monitors and had accumulated data for several weeks. This data enabled the administrator to accurately narrow down the possible cause of the problem to the primary server connection. He was then able to troubleshoot that specific connection and take steps to fix the slowness issue.

To set up this type of monitor for a connection, configure the Ping Latency and Availability monitor on a device located on the other end of the connection. For more information, see *Learning about network monitors* (on page 641).

Using the Active Script Performance Monitor

Active Script Performance Monitors let you write VBScript and JScript to easily poll one or more SNMP or WMI values, perform math or other operations on those values, and graph a single output value. You should only use the Active Script Performance Monitor when you need to perform calculations on the polled values. A variety of Active Script resources are available on the *Active Scripts resources page*. (http://www.whatsupgold.com/script_library)



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

For more information, see *Extending WhatsUp Gold with scripting* (on page 909).

Using Actions

In This Chapter

| | |
|---------------------------------|-----|
| Actions overview | 271 |
| About the Action Library | 272 |
| Selecting an Action Type | 273 |
| Configuring an action | 273 |
| About Percent Variables | 293 |
| Testing an action | 296 |
| Assigning an action | 296 |
| Removing an action..... | 298 |
| Creating a Blackout Period..... | 299 |
| Action Policies | 299 |

Actions overview

WhatsUp Gold actions are designed to perform a task as a device or monitor state change occurs.

As you configure an action, you choose the task it is to perform. Actions can try to correct the problem, notify someone of the state change, or launch an external application. Also, when you configure an action, you choose whether to assign it to a device, or to an active or passive monitor.

When assigned to an active monitor, actions fire according to the state changes it issues. For example, you can configure an Email Action to send an email alert when the active monitor for a Web server issues a down state change.

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

Managing Action Strategies

As you configure and assign actions, you should take several things into consideration.

- Assigning an external notification action (email, SMS, beeper) to a large list of devices greatly increases the chance of numerous notifications being sent at one time.

For example, an email action assigned to a router and each of the devices that depend on that router for their Internet connectivity, would send email notifications not only from the router, but also from every single connected device, should the router go down.

In a situation like this, it considers using dependencies allowing you to restrict email notifications to only the router and the critical devices to which it is connected. For more information, see *Dependencies overview* (on page 108).

- An action can be assigned to a device or to an active or passive monitor.

If you want to be notified if and when any or all of the monitors on a device go down, assign the action to the device. If you are concerned with specific monitors on a device, assign the action to the monitor itself. If you assign to both the device and a specific monitor, both actions fire when the monitor goes down.

- *Action policies* (on page 299) are easier to manage than lists of actions built on a device.

Whenever possible, use action policies in lieu of configuring multiple actions for one device.

- If the existing WhatsUp Gold device states do not fit your monitoring needs, you can modify them, or configure new ones.

Consider adding device states for longer periods of downtime, such as creating a **Down at least 60 mins** state, and sending an escalated message to show that the device is still down after an hour.

- Web Alarms are only useful if someone is able to hear the notifications.

While Web Alarms are useful in many situations, they are not the most efficient way to monitor devices and services overnight.

- Visual notifications are usually ample enough for most of the devices on your network.

Unless the device is vital to the daily-operation of your network or business, the color and shape of each device state easily informs you of current network device status.

- You can check on the status of firing alerts via Running Actions. From here, you can cancel single alerts, or all currently firing alerts.

About the Action Library

The Action Library displays all actions currently configured for use in WhatsUp Gold.

WhatsUp Gold includes five pre-configured actions. These actions display in the Action Library. As you create new actions, they are added to the Action Library.

To access the Action Library:

- From the web interface, click **Admin**, then click **Action Library**.

Use the Action Library to configure new or existing action types:

- Click **New** to configure a new action type.
- Select an action type, then click **Edit** to change its configuration.



Note: If the action you are editing was previously created in the Alert Center, any changes that you make here are made to the version of the action in the Alert Center Notification Library.

- Select an action type, then click **Copy** to make a duplicate of the selected action type.
- Select an action type, then click **Delete** to remove it from the library.



Caution: When you delete an action from the Action Library, all instances of that action are also deleted, and all related report data is lost.

Selecting an Action Type

Select the type of action you want to create for this device. The list menu lists all possible actions that can occur through the WhatsUp Gold action system.

- **Active Script Action.** Write code to perform a customized action.
- **Beeper Action.** Activate a beeper with this type of action.
- **Email Action.** Send an Email to a specific address.
- **Log to Text File.** Write a message to a text file.
- **Pager Action.** Send a message to a pager.
- **Program Action.** Execute an external application.
- **Service Restart Action.** Start or stop a Windows service.
- **SMS Action.** Send a text message to a specific target.
- **SMS Direct.** Send a text message to a wireless phone or other wireless device.
- **SNMP Set.** Use SNMP to set the value of an attribute of a managed object.
- **Sound Action.** Play a specific sound.
- **SSH Action.** Connect to remote devices via SSH to execute commands or scripts.
- **Syslog Action.** Write a message to a log in the Syslog system.
- **Text to Speech Action.** Plays a voice message on your computer.
- **VMware Action.** Use the VMware API to perform an action on a virtual machine.
- **Web Alarm Action.** Activate a Web Alarm in the WhatsUp Gold Web Interface
- **Windows Event Log Action.** Write an event in the Windows Event Log.
- **Winpopup Action.** Send a Winpopup to a user or specific computer.

All Action Types are executed based on a state change specified in the next dialog.

Configuring an action

There are two aspects of fully configuring an action. First, you create the action itself in the Action Library dialog or through the Action Builder wizard. The setup consists of:

- Defining the target of the action (for example, a pager or email address)
- Entering the notification variables or program arguments (that specify what information to report in the action message, or to pass to another program).

Next, you assign the action or action policy to a device or active monitor and to link it to a state change (action policies are already linked to a state change during the policy definition). For more information see:

- *Assigning an action to a device* (on page 296)
- *Assigning an action to an active monitor* (on page 297)
- *Creating a custom action policy* (on page 299)

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

Adding and editing an Active Script Action

This action allows you to write either VBScript or JScript code to perform a customized action. If the script returns an error code, the action failed.

To add or edit an active script action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** to create a new active script action, and then select **Active Script Action** from the list. Click **OK**.
- or -
From the list of current actions, select the action you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Timeout.** The amount of time (in seconds) WhatsUp Gold should wait for the action script to run.



Note: Though the maximum timeout is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

- **Script type.** Select the scripting language that you want to use to write this active script (either VBScript or JScript).
- **Script text.** Write or insert your action code here.



Note: It is not recommended that you use percent variables in script text, because they may resolve to text containing special characters (' ' (quotes), " " (double-quotes), % (percent), new line characters, and the like) that may break your script.

This script action has a context object you can use to get specific information about the context of the action.

We have provided several code samples for you to create useful script actions for your devices.

All script features in WhatsUp Gold utilize the SNMP API.



Tip: To check the status of an action, or to cancel an action, on the console go to **Tools > Running Actions**.

Adding and editing a Beeper Action

You can define beeper actions to activate a beeper when a device reaches a certain state change. The settings below are used to automatically build a dial string for use by the modem sending the beeper action.

To add or edit a beeper action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** and select **Beeper Action** to create a new beeper action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Complete the information for the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Beeper number.** Type the phone number to dial. You can use parentheses to delimit the area code and a dash to separate the exchange from the extension numbers, for example: (617) 555-5555.
 - **Pause after answer.** Type a number of seconds the modem should pause before sending the signal codes once a connection is made.
 - **End transmission.** By default, # is the correct symbol for the end transmission command. Some international systems require other or additional symbols.
 - **Modem setup.** Select either Primary, or one of the Alternate setups. Click **Port Settings** to further define your selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your beeper notifications. There could also be times you want to change your settings to meet a specific service provider requirements for a specific notification (for example, a

lower baud rate). To do this, set up an alternate Modem Setup and associate this to the notification instead of using your Primary setting.



Note: Changing the Port Settings for the desired Modem Setup affects all uses of that setting.

- **Up code.** Specifies the characters sent to the beeper to indicate that the device is up after being down (the default value is 0*).
- **Down Code.** Specifies the code sent to indicate the device is down (the default value is 1*).
- **On passive monitor code.** Specifies the code sent to indicate that an active monitor has been received for the device. (Default value is 2*) You can use the asterisk (*) character to separate codes from a subsequent message.
- **Recurring action code.** The percent variables for the action. The default action code is:
 - %System.NumberofUpDevices*%System.NumberofDownDevices

4 Click **OK** to save changes.



Tip: The Beeper Action can identify network devices through a specific device attribute, for more information.



Tip: To check the status of an action, or to cancel an action, on the console go to Tools > Running Actions.

Adding and editing a Log to Text File Action

This action logs custom messages to specified text files.

To add or edit a log to text file action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** and select **Log to Text File** to create a new log to text file action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library. Specify a Name for the action as it will appear in the Action Library.



Tip: On the console, click the Browse _ button to browse to the log file.

- **Log file.** Type the full path to the location where the log file will be written.

- Select the **Log file write mode**. Select **Append** to have log messages appended to the Log file. Select **Overwrite** to have log messages overwrite existing log messages.
- Type the **Log Message** that will be written to the log file. This message supports percent variables. The default log message is:

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

Details:

Monitors that are down include: %Device.ActiveMonitorDownNames

Monitors that are up include: %Device.ActiveMonitorUpNames

Notes on this device (from device property page):

```
%Device.Notes
```

This message was logged on %System.Date at %System.Time

Ipswitch WhatsUp Gold



Tip: Right-click in the Log Message box to select the percent variables you would like to use in the action.

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

Adding and editing a Pager Action

To add or edit an Email action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** and select **Pager Action** from the list to create a new Pager action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Terminal number.** Type the pager number to dial. Your service provider can provide you with this number.
 - **Terminal password.** If required, type the pager password here. This is a password that is required to log in to some paging services.

- **Modem Setup.** Select either Primary, or one of the Alternate setups.
 - **Port Settings.** Click to further define your modem setup selection. Modem Setup is used specifically to support different service providers in case you use more than one provider for sending your pager notifications. There could also be times you want to change your settings to meet a specific service provider's requirements for a specific notification (for example: a lower baud rate). To do this, you can set up an alternate Modem Setup and associate this to the notification instead of using your Primary setting.



Note: Changing the Port Settings for the desired Modem Setup affects ALL uses of that setting.

- **Protocol.** Select the type of protocol used by your pager service.
- **Pager ID.** Type the pager identification number.
- **Message.** Type a text message plus any of the percent variable codes used to deliver WhatsUp Gold information with the page.

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



Tip: To check the status of an action, or to cancel an action, on the console go to Tools > Running Actions.

Adding and editing a Program Action

You can define Program actions to launch an external application when a state change occurs.

To add or edit a program action:

- 1** Click the **Admin** tab, then click **Action Library**.
- 2** Click **New** and select **Program Action** from the list to create a new program action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3** Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Program filename.** Type or browse to the executable of the application you want to launch.
 - **Working path.** Type or browse to the directory where the working files for the application are stored. The working path is located on the server where WhatsUp Gold is running.
 - **Program arguments.** Type any percent variables you want to pass to the specified program.

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



Tip: To check the status of an action, or to cancel an action, on the console go to Tools > Running Actions.

Adding and editing a SMS Action

The SMS Action sends a Short Message Service (SMS) notification to a pager or cell phone using an email gateway or dial-up modem. An SMS Action can also be used as an SMS notification in the WhatsUp Gold Alert Center.

To add or edit an SMS action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** and select **SMS Action** from the list to create a new program action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Country.** Using the list box, select the country for the SMS provider.
 - **Provider.** Using the list box, select the desired provider.



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

- **Mode.** Either Email or Dialup, depending on how the Provider was created in the system.
- **Email to.** If the connection setting is Email, type the email address of the SMS device.
- **Phone Number.** If the connection setting is Dialup, type the phone number to call with the message. You can enter multiple phone numbers, separated by a comma. There is a 2,000 character limit in this field, so you can enter many numbers.



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

- 4 The New/Edit SMS Action dialog contains two tabs. Select a tab to configure message settings.
 - The **Message** tab contains options pertaining to the message sent as the result of an active or passive monitor.
 - **Message.** Type a text message plus any desired percent variable codes. If you use percent variables, character count is greatly increased.



Note: If the message exceeds 140 characters, the message is broken into up to 3 parts and is sent as separate messages. ("1 of 3", "1 of 2", etc.)



Tip: Click **Mobile Device Status** to insert a link to the device status in the message.

- The Alert Center Message tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.
 - **Alert Center Message.** Type a text message plus any desired percent variable codes. If you use percent variables, character count is greatly increased.



Note: If the message exceeds 140 characters, the message is broken into up to 3 parts and is sent as separate messages. ("1 of 3", "1 of 2", etc.)



Tip: To enter Alert Center Percent variables, right-click inside the message box.

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

Configuring an SMS Action on the web

To configure an SMS Action on the web interface:

- 1 Go to **Admin > Action Library**. The Action Library appears.
- 2 In the Action Library, do one of the following:
 - Click **New**, then select **SMS Action**.
 - or -
 - Select an existing SMS Action, then click **Edit**.The action properties page appears.
- 3 Enter or select the appropriate information in the following fields.
 - **Name.** Enter a unique display name to identify the SMS notification.
 - **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
 - **Country.** Using the list box, select the country for the SMS provider.
 - **Provider.** Using the list box, select the desired provider.



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

- **Mode.** Either *Email* or *Dialup*, depending on how the Provider was created in the system.
- **Email to.** If the connection setting is *Email*, enter the email address of the SMS device.

- **Phone Number.** If the connection setting is *Dialup*, enter the phone number to call with the message. You can enter multiple phone numbers, separated by a comma. There is a 2,000 character limit in this field, so you can enter many numbers.



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

- 4 The New/Edit SMS Action dialog contains two tabs. Select a tab to configure message settings.

The **Message** tab contains options pertaining to the message sent as the result of an active or passive monitor.

Enter a text message plus any desired percent variable codes. Keep in mind that if you use percent variables, this will greatly increase the character count.



Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).



Tip: Click **Mobile Device Status** to insert a link to the device status in the message

The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

Enter a text message plus any desired percent variable codes. Keep in mind that if you use percent variables, this will greatly increase the character count.



Tip: To enter Alert Center percent variables, right click inside the message box.



Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

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

Adding and editing a SMS Direct Action

SMS direct messages are similar to SMS messages, except a phone line is not required. Instead, messages are sent directly to a cell phone, or other texting capable device, via a GSM modem. If the receiving phone is not active or is out of range when a SMS message is sent, messages are received when the phone is turned on. SMS messages are listed in the WhatsUp Gold Action log.

Required for SMS Direct Actions

You need several items in order to use the SMS Direct Action:

- GSM modem to connect to the WhatsUp machine
- SIM card for the GSM modem
- Cell service/signal in the room in which the WhatsUp machine and GSM modem reside

To add or edit a SMS direct action:

- 1 Access the Action Library.
- 2 Click **New** to create a new SMS direct action or from the list of current actions, select the action you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Phone number.** Type the cell phone number(s) of the intended SMS message recipients. You can enter multiple phone numbers, separated by a comma. For example: 555-555-5555, 55 555 55 55 55, (555) 555 5555



Note: All non-numeric characters, other than the comma, such as "-" and ".", are ignored.

There is a 2,000 character limit in this field, so you can enter many numbers.

- **COM Port.** Select the COM port you want to use with this notification.



Note: The list displays all ports associated with the GSM modem, including virtual and hard-wired, serial ports. You must select the port that is assigned to the modem in the Windows Device Manager.

The New/Edit SMS Direct Action dialog contains two tabs. Select a tab to configure message settings.

- The **Message** tab contains options pertaining to the message sent as the result of an active or passive monitor.

Type a text message, plus any desired percent variable codes. If you use percent variables, the character count is greatly increased.



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

- The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

Type a text message, plus any desired percent variable codes. If you use percent variables, the character count is greatly increased.



Tip: To enter Alert Center percent variables, right click inside the message box.



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

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

Adding and editing a SSH Action

This action connects to remote devices via SSH to execute commands or scripts.

To add or edit an SSH action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** and select **SSH Action** from the list to create a new SSH action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **IP address.** Type the IP address of the device to which you want to connect using SSH.



Note: You can enter %Device.Address into the IP Address field; however, an SSH action that does not specify a specific IP address in this field is not available in the Recurring Actions wizard.

- **Command to run.** Type the command to be run and executed on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.



Note: If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- **SSH credential.** Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device for which the IP address is listed above. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.

4 Click **OK** to save changes.

Adding and editing a Syslog Action

When a device does not respond to polling, you can send a Syslog message to a host that is running a Syslog server.

To add or edit a Syslog action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** and select **Syslog Action** from the list to create a new Syslog action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Syslog Server.** Type the IP address of the machine that is running the Syslog server.
 - **Port.** Type the UDP port that the Syslog listener is listening on. The default port is 514.
 - **Message.** Type a text message to send to the Syslog server. This message may include notification variables. The Syslog message box limits input to 511 characters. If notification variables are used, then the message that actually gets sent is limited to 1023 bytes, in order to comply with the Syslog protocol. Non-visible ASCII characters such as tabs and line feeds are replaced by space characters.
- 4 Click **OK** to save changes.



Note: If you attempt to run another application on the same system that also listens on the same Syslog port as WhatsUp Gold, the error message *Unable to Open Socket* displays.



The WhatsUp Gold Syslog listener runs on Port 514 by default. This port can be configured in the console at **Configure > Program Options > Passive Monitor Listeners > Syslog**.



Tip: To check the status of an action, or to cancel an action, on the console go to **Tools > Running Actions**.

Using the Email Action

The Email Action sends an SMTP mail message to a specific email account. An Email Action can also be used as an email notification in the WhatsUp Gold Alert Center. While you can configure this action on both the console and web interface, you can only configure the Alert Center notification message on the web. For more information, see *Configuring an Alert Center email notification* (on page 736).

Adding and editing an Email Action

The Email Action sends an SMTP mail message to a specific email account. An Email Action can also be used as an email notification in the WhatsUp Gold Alert Center.

To add or edit an Email action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New**, then select **E-mail Action** from the list to create a new E-mail action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Complete the appropriate information for the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
- 4 Complete the information on the Configuration tab. This tab contains options pertaining to the action email destination.
 - **SMTP Mail Server.** Type the IP address or Host (DNS) name of your email server (SMTP mail host).
 - **Port.** Type the port number on which the SMTP server is installed.
 - **Timeout.** Type the amount of time (in seconds) to wait for user authentication on the SMTP server. The authentication fails if this time limit is exceeded.
 - **Mail To.** Type the email addresses to which you want to send the alert. Email addresses must be fully qualified. You can enter two addresses, separated by commas (but no spaces). The address should not contain brackets, braces, quotes, or parentheses.
 - **Mail From.** Type the email address you want to appear in the From field of the email that is sent by the Email action.
 - **SMTP server requires authentication.** Check this option if your SMTP server uses authentication. This enables the Username and Password fields.

The Email action supports three authentication types:

- CRAM-MD5
- login
- plain

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

- **Username.** Type the username for SMTP authentication.
- **Password.** Type the password of the username for authentication.
- **Use an encrypted connection (SSL/TLS).** Check this option if your SMTP server requires the data to be encrypted over a TLS connection (formerly known as SSL).

5 Complete the information on the **Mail Content** tab. This tab contains options pertaining to the action email message content.

- **Subject.** Type a text message or edit the default message. You can use percent variable codes to display specific information in the subject.
- **Message body.** Type a text message or edit the default message. You can use percent variable codes to display specific information in the message body.



Tip: You can add a link to either or both the Device Status and Mobile Device Status reports by clicking the appropriate button.

6 Complete the information on the **Alert Center Settings** tab. This tab contains options pertaining to the message sent from WhatsUp Gold Alert Center.

- **Alert Center email subject.** Type a subject for the message. This text appears as the subject in the email that is sent by the Alert Center notification. This subject can include percent variables.



Tip: To include Alert Center percent variables, right click inside the above field.

- **Alert Center Link.** Select **Include hyperlink to Alert Center in the email content** to include a link to the Alert Center home page in the email message sent by the Alert Center notification.
 - Select to use either **HTTP** or **HTTPS** in the link address.
 - Select to either **Use dynamic address** or **Use static hostname or IP address**. If you select to use the dynamic address, WhatsUp Gold automatically generates the URL using the current IP address or hostname at the time the action runs.
 - When static hostname or IP address is selected, specify the **Hostname** or **IP address** to include in the link address.
 - Specify the **Port** to include in the link address.



Important: The address you enter here must be the exact address of the Alert Center home page to which you want to connect. Verify the address and enter its exact contents in the above options.

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

Adding and editing a SNMP Set Action

This action sends an SNMP Set to a device in order to change a specific SNMP action. You can configure SNMP Set actions to perform a number of tasks, including rebooting a device, changing the state of a network remotely, disabling or enabling a device feature, etc.

The SNMP Set action can use any SNMP credential defined in the WhatsUp Gold Credential Library and supports all types of writable objects (strings, integers, timeticks, etc.).

If the action operation fails, errors are reported to the Action log.

To add or edit a SNMP Set action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New**, then select **SNMP Set** from the list to create a new SNMP Set action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **IP address.** Type the IP address or hostname of the device to which the action to send the SNMP Set.
 - **SNMP Credential.** Select the SNMP credential that the action is to use. This list is populated with credentials currently configured in the Credentials Library.
 - **Object Identifier.** Type the object identifier (OID) that the action is to use.
 - **Instance.** Type the instance that coincides with the OID that the action is to use.



Tip: You can browse (...) to select both the OID and instance.

- **Value Type.** Select the type of written object the action is to use.
- **Value to set.** Type a value for the type you selected.



Note: The action only allows you to set one value at a time.

- 4 Click **Advanced** and change the default advanced settings (optional).
 - **SNMP Timeout.** Use the slider to select the amount of time (in seconds) that you want WhatsUp Gold to wait before it generates an error while attempting to perform the action.
 - **Number of Retries.** Use the slider to select the number of times you want WhatsUp Gold to attempt the action.
- 5 Click **OK** to save changes.

Adding and editing a Sound Action

The sound file can be assigned to an action by creating an Action policy, or by adding an action to a specific device. For more information.



Note: The Desktop Actions application must be running for the Sound and Text-to-Speech actions to work. For more information, see About the Task Tray and Desktop Actions applications.



Note: If you want to bring the text-to-speech action sound to a Windows 2003 or Windows 2008 server class remote desktop (RDP) system, you need to enable audio mapping for the remote system Terminal Services Configuration.

1. In Windows, click **Start > Run**, in the Run dialog type **TSCC.msc**, then click **OK**.
 2. In the Connections folder, double-click **RDP-tcp**. The RDP-TCP Properties dialog appears.
 3. Select the **Client Settings** tab, then click to clear the Audio Mapping check box.
- When enabled, the text-to-speech action sound only plays on the remote desktop system.

To add or edit a sound action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New**, then select **Sound Action** from the list to create a new Sound action. Click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Sound file name.** Type the full path to the sound file, or click the folder icon to select it from your computer. The sound file name is located on the server where WhatsUp is running.
 - **Continuous play.** Select this option to have the sound play continuously until the Cancel Sound button is clicked on the main WhatsUp Gold toolbar.



Tip: To check the status of an action, or to cancel an action, on the console go to **Tools > Running Actions**.

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

Adding and editing a Service Restart Action

After you configure this Action, you can start or stop a Windows service when another device or monitor experiences a state change. In order for the Service Restart Action to work:

- Both the WhatsUp Gold computer and the target device (where the Windows service is to restart) must have identical user accounts.
- The Ipswitch WhatsUp Engine service needs to log on as a user account that belongs to the administrators group and that exists on the target machine.

To set up the service restart action:

- 1 Click **Windows Control Panel > Administrative Tools > Services**. Right click **Ipswitch WhatsUp Engine**, then select **Properties**.
- 2 Click the **Log On** tab, select **Log on as: This account**, then type the user name and password.



Important: If the service that is to be stopped or started by the action is running on a Windows XP machine, then the machine requires the following settings.

- **Set Local Security settings.** Click **Local Security Settings > Local Policies > Security Options > Network Access: Sharing and security model for local accounts > Classic - local users authenticate as themselves**.
- 3 In the Action Library, in the Service Restart action properties, complete the appropriate information:
 - **Name.** Type a name of the action. This displays in the Action Library.
 - **Description.** Type a short description for the action. This displays in the Action Library along with the entry Name.
 - **Host.** Click the browse button to select the desired host from your Network Neighborhood.
 - **User name (domain\username).** Type a user login to use with this monitor. In order to monitor the service on another machine, the WinEvent monitor has to be configured with the correct user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, then the expected user name is domain\user. If the device is on a workgroup, there are two possible user names: workgroup name\user or machine name\user. No user name and password is needed for local services (services on the machine where WhatsUp Gold is running).
 - **Password.** Type the password for the login used above.

To monitor Windows services on a XP machine with an account that has empty password, the XP Local Security Settings might have to be modified:

From **Administrative tools > Local Security Settings**, select **Security Settings > Local Policies > Security Options**. Next, right click on **Account: Limit local account use of blank passwords to console logon only**, then click **Properties**, and select **Disable**.

- **Service.** Click the browse (...) button to select the desired service associated with your host.
- **Command.** Use the list box to select either Start or Stop, depending on whether you want the associated alert to Start or Stop the service you have selected.



Tip: To check the status of an action, or to cancel an action, on the console go to **Tools > Running Actions**.

Adding and Editing a Web Alarm Action

For more information on how Web Alarms work, see the Working with Web Alarms topic.

To add or edit a Web alarm action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New**, then select **Web Alarm** from the list to create a new Web alarm action. Click **OK**.
- or -
Select the Web Alarm you want to change from the list of current actions, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Message.** Type a short message to send to the visual cue part of the Web Alarm in the web interface. You can use percent variable codes to display specific information in the message body.
 - **Play Sound.** Select this option to play the sound file whenever a web alarm action fires. Clear this option to only have the visual cue appear in the Web Interface.
 - **Sound file name.** Select a sound file that is installed in your `\Program Files\Ipswitch\WhatsUp\HTML\Nm.Web.UI\WebSounds` directory. Custom sounds added to this directory appear in the drop-down list.
- 4 Click **OK** to save changes.



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

The Web Alarm popup window

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



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



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

To access more information on one of the devices listed in the popup window, double-click the device to bring up its Device Status Dashboard.



Note: In order for a WhatsUp Gold user to view the Web Alarm popup window and hear the alarm that sounds, a user account must have the Manage Devices user right enabled. For more information, see About user rights.

Enabling and disabling Web Alarms

While you can mute and dismiss Web Alarms from the Web Alarms popup window, you cannot disable, or turn them off, from there. Instead, you enable and disable Web Alarms on the web interface on the Preferences dialog (click your username in the upper right of the application and clear **Enable web alarms**). You can also adjust the Web Alarms check interval from the User Preferences dialog. The **Check every** box indicates the number of seconds WhatsUp Gold waits before checking for new Web Alarms.

By default, Web Alarms are enabled on the web interface and are checked every 120 seconds.

Accessing Web Alarms on the web interface

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

The Web Alarm window. Click **Devices > Web Alarms**. The Web Alarms dialog appears.

The Web Alarms dashboard report. This is an optional dashboard report you can add to a view on the Home Dashboard. This report displays recent Web Alarms.

You can also create a dynamic group to provide easy access to your current network Web Alarms. For more information on Dynamic Groups in WhatsUp Gold, please see *Configuring Dynamic Groups* (on page 80).

Adding and Editing a Windows Event Log Action

This action allows you to configure log messages to post to the Windows Event Viewer.

To add or edit a Windows Event log action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** to create a new Windows Event log action. Select **Windows Event Log** from the list, then click **OK**.
- or -
Select the action you want to change from the list of current actions, and then click **Edit**.

- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library. Specify the Source for the messages that are logged to the Windows Event Viewer. The default source is the Ipswitch WhatsUp Log Action.
 - **Source.** The origin of messages logged to the Windows Event Viewer. The default source is the Ipswitch WhatsUp Log Action.
 - **Event ID.** Type an event ID for the messages that are logged to the Windows Event Viewer. The default event ID is 1000, the WhatsUp engine event ID.
 - **Level.** Select a level for messages logged to the Windows Event Viewer. You can select Error, Warning, or Information. The default level is Error.
 - **Log Message.** Type a log message that displays in the Windows Event Viewer. This message supports percent variables. The default log message is:
%Device.ActiveMonitorDownNames is %Device.State on %Device.Type:
%Device.HostName (%Device.Address).

Details:

Monitors that are down include: %Device.ActiveMonitorDownNames

Monitors that are up include: %Device.ActiveMonitorUpNames

Notes on this device (from device property page):

%Device.Notes

This message was logged on %System.Date at %System.Time

Ipswitch WhatsUp Gold



Tip: Right-click in the Log Message field to select the percent variables you would like to use in the action.

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

Using the WinPopup Action

The WinPopup Action displays a user-specified message in a pop-up window on a Windows NT system.

To configure a WinPopup Action:

- 1 Click the **Admin** tab, then click **Action Library**. The Action Library dialog appears.
- 2 In the Action Library, do one of the following:
Click **New**, then select **WinPopup** Action from the list. Click **OK**.
- or -
Select an existing WinPopup Action, then click **Edit**. The Action Properties page appears.

- 3 Enter or select the appropriate information in the following fields.
 - **Name.** Enter an identifying name for this winpopup action.
 - **Description.** Enter a short description of the action. This is displayed in the Action Library along with the entry in **Name**.
 - **Destination.** Specify the Windows NT host or domain that you want to receive this notification.
 - **Message.** Enter a text message using *percent variables* (on page 293) if needed.
 - **Refresh.** Click this button to refresh the **Destination** list. This populates the list with all of the targets you can choose in which to send a winpopup action.
- 4 Click **OK** to save changes.

About Percent Variables

Percent variables allow you to customize the message notification sent from an action.

These variables can be used in all of the WhatsUp Gold actions, though we do not recommend that you use them in the Active Script Action, as they may cause the action's code to break.

Percent Variables

You can customize an action's message by adding any of the percent variables in the following table.



Note: We do not recommend that you use percent variables in script text (Active Script Action), because they may resolve to text containing special characters (' ' (quotes), " " (double-quotes), % (percent), new line characters, and the like) that may break your script.

| Active Monitor Variables | Description |
|---|--|
| <code>%ActiveMonitor.Argument</code> | SNMP instance number. This is only used when an action is associated directly with an active monitor, and not the device as a whole. |
| <code>%ActiveMonitor.Comment</code> | The human readable name that coincides with the network switch. This is only used when an action is associated directly with an active monitor, and not the device as a whole. |
| <code>%ActiveMonitor.Name</code> | The name of the active monitor that fired an action. This is only used when an action is associated directly with an active monitor, and not the device as a whole. |
| <code>%ActiveMonitor.NetworkInterfaceAddress</code> | IP address for the network interface. This is only used when an action is associated directly with an active monitor, and not the device as a whole. |

| Active Monitor Variables | Description |
|-------------------------------------|--|
| <code>%ActiveMonitor.Payload</code> | <p>The payload returned by a WMI, Exchange, SQL, SNMP or Active Script active monitor. This is only used when an action is associated directly with an active monitor and not the devices as a whole.</p> <p>For Active Script Active Monitors, the payload is the text that is passed to the <code>SetResult()</code> method in the script.</p> |
| <code>%ActiveMonitor.State</code> | <p>The Current status of the monitor, such as "Down at least 5 min." This is only used when an action is associated directly with an active monitor, and not the device as a whole.</p> |

| Device Variables | Description |
|---|--|
| <code>%Device.ActiveMonitorDownNames</code> | List of down services using the abbreviated name if available. |
| <code>%Device.ActiveMonitorUpNames</code> | Full service names of all UP monitored services on a device. |
| <code>%Device.Address</code> | IP address (from device properties). |
| <code>%Device.Attribute.[Attribute Name]</code> | <p>Returns an attribute from the SNMP information available for the device, such as the Contact name. To specify the attribute, append the category name (listed below) to the end of the variable. For example: <code>%Device.Attribute.Contact</code>, returns the contact name.</p> <p>Default categories:</p> <ul style="list-style-type: none"> · *. Returns all attributes · Info1. Upgrade path from v8 · Info2. Upgrade path from v8 · Contact. Contact information from SNMP · Location. Location information from SNMP · Description. Description information from SNMP · Custom. If you have created a custom attribute you can use the name of that custom attribute in the percent variable. <p>Example:</p> <p><code>%Device.Attribute.Phone</code> <code>%Device.Attribute.RackPosition</code></p> <p>To avoid an error, always place a space or line break after the attribute name.</p> |

| Device Variables | Description |
|-------------------------|---|
| %Device.DatabaseID | Returns the database ID of a device. |
| %Device.DisplayName | Display Name (from General of device properties) |
| %Device.HostName | Host Name (from General of device properties) |
| %Device.Notes | Notes. (Notes are from the device properties Notes) |
| %Device.SNMPoid | SNMP Object identifier. |
| %Device.State | The state's description (such as "Down at least 2 min" or "Up at least 5 min") |
| %Device.Status | This shows the name of the active monitor, preceded by the device state id : 10 DNS |
| %Device.Type | Device Type (from General of device properties) |

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

| System Variables | Description |
|----------------------------------|---|
| %System.Date | The current system date. Configure the date format in Regional Options (from Program Options) |
| %System.DisplayNamesDownDevices | Display names of devices with down monitors |
| %System.DisplayNamesDownMonitors | Shows the name of a device and each monitor that is down on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping |
| %System.DisplayNamesUpDevices | Display names of up devices |

| System Variables | Description |
|--------------------------------|--|
| %System.DisplayNamesUpMonitors | Shows the name of a device and each monitor that is up on that device. The format of the response is 'device name':'monitor 1','monitor 2','...' Example: ARNOR: FTP, HTTPS, Ping |
| %System.InstallDir | Displays the directory on which WhatsUp Gold is installed |
| %System.NumberofDownDevices | Number of down devices on your network |
| %System.NumberOfDownMonitors | Shows the number of down monitors on your network |
| %System.NumberofUpDevices | Number of up devices on your network |
| %System.NumberOfUpMonitors | Shows the number of up monitors on your network |
| %System.Time | The current system time. The format is hh:mm:ss |

Testing an action

After you create an action, you can test it to make sure it works properly. You must access WhatsUp Gold through the console to access the Test option.

To test an action:

- 1 From the WhatsUp Gold console, click **Configure**, then click **Action Library**. The Action Library appears.
- 2 In the Action Library, select the action you want to test.
- 3 Click **Test**.
- 4 Review the action in the Action Progress dialog. Click **Details** to view more information about the progress of the action.

Assigning an action

After you configure an action in the Action Library, you must add it to the individual devices and monitors for which you want to receive notifications or related tasks performed.

You can assign one or more individual actions to a device, or an instance of an active or passive monitor assigned to a single device.



Note: When you assign an action to a device or monitor, an instance of that action is added to the device or monitor. Changes that you make to the action's configuration via the Action Library affect all instances of that action. For example, if you assign an action to four separate devices and then make changes from the Action Library, all four instances of that action adopt the changes.

Assigning an action to a device

To assign an action to a device:

- 1 In the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Device Properties - Actions dialog appears; the **Apply individual actions** option is selected by default.
- 3 Click **Add**. The Action Builder appears; you can choose to add an action from the Action Library, or create a new action.
- 4 Follow the directions in the Action Builder wizard.
- 5 At the end of the wizard, click **Finish** to add the action to the monitor.
- 6 On the Device Properties dialog, click **OK** to save changes.

Assigning an action to an active monitor

As you configure active monitors for a device, you have the opportunity to assign actions; however, it is not required that you assign them at that time. If you decide to assign an action to the monitor at a later time, you can do so through the device Properties.

To assign an action to an active monitor:

- 1 In the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Select the monitor to which you would like to assign an action, then click **Edit**. The Set Polling Properties dialog appears.
- 4 Make any adjustments to polling selections, then click **Next**. The Setup Actions for Monitor State Change dialog appears. The **Apply individual actions** option is selected by default.
- 5 Click **Add**. The Action Builder appears; you can choose to add an action from the Action Library, or create a new action.
- 6 Follow the directions in the Action Builder wizard.
- 7 At the end of the wizard, click **Finish** to add the action to the monitor.
- 8 On the Device Properties dialog, click **OK** to save changes.

Assigning an action to a passive monitor

As you configure passive monitors for a device, you have the opportunity to assign actions; however, it is not required that you assign them at that time. If you decide to assign an action to the monitor at a later time, you can do so through the device Properties.

To assign an action to a passive monitor:

- 1 In the Details or Map View, right-click a device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Passive Monitors**. The Device Properties -Passive Monitors dialog appears.
- 3 Select the monitor to which you would like to assign an action, then click **Edit**. The monitor properties dialog appears.
- 4 Click **Add**. The Action Builder appears.

- 5 Select the action you would like to assign to the monitor.
- 6 Optionally, create a **Blackout Schedule**.
- 7 Click **OK** to add the action to the monitor.

Removing an action

Because actions are assigned to devices and monitors on an individual basis, actions can only be removed on the device- and monitor-level, and must be deleted from the Action Library. Additionally, if you have assigned action policies to your devices, you can remove the action from the policy itself.

When you remove an action from a device or monitor, the action still exists in the Active Monitor Library and is available for use with other devices and monitors. When you delete an action, you remove it from the database, and from all devices and monitors to which it is assigned; further, all log data related to the action is lost. Therefore, we recommend that you only delete an action when you are absolutely positive that you will not use it in the future, and feel that the related log data is not useful to your monitoring records.

Removing an action from a device

To remove an action from a device:

- 1 From Details or Map View, right-click the device from which you want to remove the active monitor, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Device Properties - Actions dialog appears.
- 3 Select the action you want to remove, then click **Remove**. A dialog appears and asks you if you are sure you want to remove the action.
- 4 Click **OK** to remove the action.

Removing an action from an active monitor

To remove an action from an active monitor:

- 1 From the Device or Map View, right-click the device from which you want to remove the action, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Select the monitor from which you want to remove the associated action, then click **Edit**. The Active Monitor Properties dialog appears.
- 4 Click **Next**. The Actions associated with the active monitor are listed.
- 5 Select the action you want to remove, then click **Remove**. A dialog appears and asks you if you are sure you want to remove the action.
- 6 Click **Yes** to remove the action, then click **Finish**.

Removing an action from a passive monitor

To remove an action from a passive monitor:

- 1 From the Details or Map View, right-click the device from which you want to remove the action, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Passive Monitors**. The Device Properties - Passive Monitors dialog appears.
- 3 Select the monitor from which you want to remove the associated action, then click **Edit**. The Passive Monitor Properties dialog appears.

- 4 Under **Actions for this passive monitor**, select the action that you would like to remove, then click **Remove**. A dialog appears and asks you if you are sure you want to remove the action.
- 5 Click **OK** to remove the action.

Creating a Blackout Period

You can create a Blackout Period to have WhatsUp Gold suspend specific actions during a scheduled period of time. Use this feature to keep from sending a notification to someone who is on vacation, or to keep from sounding a Web Alarm when there is no one near-by to hear the alert.



Note: Polling dependencies & blackouts only apply to the collection of device active monitors.

To create a Blackout period:

- 1 On the device from which you want to create a Blackout Period, right-click, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Device Properties - Actions dialog appears.
- 3 Select the action for which you want to create the Blackout Period, then click **Edit**. The monitor properties dialog appears.
- 4 Click **Edit**. The Action Builder appears.
- 5 Click **Blackout Period**. The Weekly Blackout Schedule dialog appears.
- 6 Set the times for which you want the blackout to occur.



Note: The schedule that you set is repeated weekly.

- 7 Click **OK**.

Action Policies

Action policies allow you to group or sequence multiple actions together for use on any device or monitor.

If you make changes to actions in a policy, the changes are applied to all of the devices and monitors that use that particular policy.

For more information, see:

- *Adding and editing Action Policies* (on page 300)
- *Configuring an implicit Action Policy* (on page 301)

Creating an action policy

To create an action policy:

- 1 Click the **Admin** tab, then click **Action Policy Library**. The Action Policies dialog appears.
- 2 Click **New**. The New Action Policy dialog appears.
- 3 Enter a name in **Policy name**. This name is used to identify the policy later, so you should make sure the name is something that helps you remember what is contained in this policy.
- 4 Click **Add**. The Action Builder wizard appears.
- 5 Follow the directions in the wizard.
- 6 Click **Finish** at the end of the wizard to add the action to the policy.
- 7 Add as many actions as you need to complete the policy. You can move actions up and down in the list by clicking **Up** and **Down** above the action list.

If you select **Only execute first action**, WhatsUp Gold executes the actions in the list for each state, starting at the top, and stops as soon as an action successfully fires.

- 8 After you have added all of the you would like for the policy, click **OK** to create the policy and add it to the active list.



Note: During Device Discovery, you can assign an existing action policy (if one has been created previously), create a simple action policy through a wizard, or access the Action Policy Editor to create an action policy yourself.

Assigning an Action Policy to a Device

To assign an action policy to a device:

- 1 In Device or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Actions**. The Actions dialog appears.
- 3 Select **Apply this Action Policy**.
- 4 Click the list and select the action policy to apply.



Note: If the list is empty, click browse (...) and create a new action policy. Click **Add** to access the Action Builder dialog.

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

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

Adding and Editing an Action Policy

To add or edit an action policy:

- 1 Click the **Admin** tab, then click **Action Policy Library**. The Action Policies dialog appears.
- 2 Click **New** to create a new action policy.
- or -
Select the policy you want to change from the list of current action policies, and then click **Edit**.
- 3 Complete the appropriate information for the following fields.
 - **Policy Name.** Type a name for the policy. The name should be something you can easily associate with the actions performed in the policy.
 - **Actions in the policy.** This list shows all of the actions configured for this policy. The list displays which state change triggers what action.
 - Click **Add** to configure an action to add to the policy.
 - Select an action on the list and click **Edit** to change how the action is configured.
 - Select an action on the list and click **Delete** to remove the action from the list.
 - Select **Only execute first action (for each state)** to keep from firing multiple actions assigned to the current policy.
 - Use the **Up** and **Down** arrows to change the order of the actions.
- 4 Click **OK** to save changes.

Configuring an implicit action policy

The Implicit Action policy automatically assigns actions to all devices in your database. You cannot opt out of the Implicit Action policy.



Note: The Implicit Action Policy only assigns actions to devices. You must create separate action policies for device monitors.

If at any time during the normal operation of WhatsUp Gold you notice that actions are firing and you cannot find the action associated to the down device or monitor, remember to check the Implicit Action Policy.



Note: In previous versions of WhatsUp Gold, the Web Alarm action was included in the Implicit Action Policy. This is no longer true in Ipswitch WhatsUp Gold. For more information on the Web Alarm action, see *About Web Alarms* (on page 117).

To configure the Implicit Action Policy

- 1 Click the **Admin** tab, then click **Action Policy Library**. The Action Policies dialog appears.
- 2 Select the Implicit Action Policy, then click **Edit**. The Edit Action Policy dialog appears.
 - To add an action to the policy, click **Add**.
 - To modify an action in the policy, select it, then click **Edit**.
 - To delete an action from the policy, select it, then click **Remove**.
 - To have WhatsUp Gold execute only the first action in the list for each state, and stop when that action fires successfully, select **Only execute first action**.



Tip: Use **Up** and **Down** to modify an action's placement in the list.

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

Example: getting an Email alert when the Web server fails

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

First, you need to set up the monitors for your web server. Then, create an Email Action and assign it to the monitors.

Setting up monitors for a Web server and creating an Email Action that is assigned to monitors:

- 1 In either Details or Map View, right-click on the web server device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.
- 4 Use the following dialogs to add the HTTP active monitor to your web server device; this monitor checks that HTTP (port 80) is active.
 - a) On the Select Active Monitor Type dialog, select **HTTP**, then click **Next**. The Set Polling Properties dialog appears.
 - b) Ensure that the default settings are selected (**Enable polling for this Active Monitor** and **Use default network interface**), then click **Next**. The Setup Actions for Monitor State Changes dialog appears.
 - c) Select **Apply individual actions**, then click **Add**. The Select or Create Action dialog appears.
 - d) Select **Create a new action**, then click **Next**. The Select Action Type dialog appears.
 - e) In the **Select the actions type to create** list, select **E-Mail Action**, then click **Next**. The Select State Change dialog appears.
 - f) Select **Down** from the **Execute the action on the following state change** list, then click **Finish**. The New Email Action dialog appears.

- g) Enter the information using your mail and SMTP server settings:

New Email Action

Name:
MailtoWebmaster

Description:
E-mail Action

Configuration

SMTP Server:
192.168.5.5

Port:
25

Timeout (sec):
5

Mail to:
webmaster@yourdomain.com

Mail from:
WhatsUpGold@YourDomain.com

☒ SMTP server requires authentication

Username:
EmailUserAccount

Password:

☐ Use an encrypted connection (SSL/TLS)

Configuration | Mail Content | Alert Center Settings

OK Cancel

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

The screenshot shows a "New Email Action" window. It has a blue title bar with a question mark icon. The main area contains several input fields: "Name:" with the value "MailtoWebmaster", "Description:" with the value "E-mail Action", and "Mail Content". The "Mail Content" section includes a "Subject:" field with the text "%Device.Type is %Device.State (%Device.HostName).", a "Message body:" field containing a template with variables like %Device.ActiveMonitorDownNames, %Device.State, %Device.Type, %Device.HostName, %Device.Address, %Device.ActiveMonitorUpNames, %Device.Notes, and %System.Date at %System.Time. Below the message body is a note about right-clicking for percent variable support and two buttons: "Device Status" and "Mobile Device Status". At the bottom are three tabs: "Configuration", "Mail Content" (which is selected), and "Alert Center Settings". The "OK" and "Cancel" buttons are at the very bottom right.

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

Setting up an HTTP Content active monitor with an email alert:

- 1 In either Details or Map View, right-click on the web server device, then select **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties - Active Monitors dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.
- 4 Use the same process to add the HTTP active monitor; this monitor checks that the Web server returns valid content in response to an HTTP request.
 - a) On the Select Active Monitor Type dialog, select **HTTP**, then click **Next**. The Set Polling Properties dialog appears.
 - b) Ensure that the default settings are selected (**Enable polling for this Active Monitor** and **Use default network interface**), then click **Next**. The Setup Actions for Monitor State Changes dialog appears.

- c) Select **Apply individual actions**, then click **Add**. The Select or Create Action dialog appears.
- d) Select **Select an action from the Action Library**, then click **Next**. The Select Action and State dialog appears.
- e) Under **Select an action from the Action Library**, select **MailtoWebmaster**. This is the action that you created in the previous steps.
- f) Under **Execute the actions on the following state change**, select **Down**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.
- g) On the Select Action and State dialog, select **MailtoWebmaster**, then click **Finish** to save the changes and return to the Setup Actions for Monitor State Changes dialog.
- h) Click **Finish**.

The two active monitors and resulting email actions are now enabled.

When the Web server is down, the HTTP Active Monitor fails and triggers the Email Action, which sends an email message similar to the following:

```
Web1 is down on server: web1.YourDomain.com (192.168.5.5)
```

```
Details:
```

```
Monitors that are down include:
```

```
Monitors that are up include:
```

```
HTTP Content
```

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

```
Lamar Bldg; 2nd floor
```

```
-----
```

```
This mail was sent on 11/28/2007 at 15:34:01
```

```
Ipswitch WhatsUp Gold
```

If the Web server cannot return web content, the Email Action report reads:

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

Any details or notes specified in the action are also reported.

Using Scripting Actions

Active Script Actions can be configured to trigger when an active monitor's state changes. They can be programmed to perform a variety of tasks, from running automated remediation scripts to posting data to external, third party services via API.



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

For more information, see *Extending WhatsUp Gold with scripting* (on page 909).

Adding and editing an Active Script Action

This action allows you to write either VBScript or JScript code to perform a customized action. If the script returns an error code, the action failed.

To add or edit an active script action:

- 1 Click the **Admin** tab, then click **Action Library**.
- 2 Click **New** to create a new active script action, and then select **Active Script Action** from the list. Click **OK**.
- or -
From the list of current actions, select the action you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the action. This name displays in the Action Library.
 - **Description.** Type a short description. This description displays next to the action in the Action Library.
 - **Timeout.** The amount of time (in seconds) WhatsUp Gold should wait for the action script to run.



Note: Though the maximum timeout is 60 seconds, you are highly discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

- **Script type.** Select the scripting language that you want to use to write this active script (either VBScript or JScript).
- **Script text.** Write or insert your action code here.



Note: It is not recommended that you use percent variables in script text, because they may resolve to text containing special characters (' ' (quotes), " " (double-quotes), % (percent), new line characters, and the like) that may break your script.

This script action has a context object you can use to get specific information about the context of the action.

We have provided several code samples for you to create useful script actions for your devices.

All script features in WhatsUp Gold utilize the SNMP API.



Tip: To check the status of an action, or to cancel an action, on the console go to **Tools > Running Actions**.

Select a Device

Use this dialog to select the device(s) for which to add.

Click **+** to expand the preferred device group. The device list displays.

Select a single device, multiple devices, or device group from the list, then click **OK**.

Dynamic Groups - Delete Devices

Use this dialog to confirm that you want to delete the selected device(s) from a WhatsUp Gold dynamic group.

The devices you select to delete are shown in the **Display Name** column, and the groups in which those devices exist are listed in the **Groups** column.

Select the devices you want to delete, then click **OK** to remove the device permanently from WhatsUp Gold.



Caution: Devices deleted from this dialog are removed completely from WhatsUp Gold and cannot be recovered. All configuration information and historical data about deleted devices is discarded.

Configure Data Collection Advanced Settings

Use the following data collection settings for WhatsUp Gold to use as it attempts to collect data on the current device.

- **Timeout.** Enter the time (in seconds) that you want WhatsUp Gold to wait before it throws an error while attempting to collect data on a device.
- **Retry.** Enter the number of times you want WhatsUp Gold to attempt collecting data, when the device does not respond.
- **Determine uniqueness by.** This option is relevant to the Disk, Memory, and Interface performance monitors. Select to determine uniqueness by:
- **Interface index.** Select to determine uniqueness by the interface index.

- **Interface description.** Select to determine uniqueness by the interface description. This prevents interruptions in data gathering if a re-index occurs. This option is not relevant for CPUs because most Windows machine CPUs are named "Intel."
- **Poll interface traffic counters.** This option allows you to select either the default 32-bit counters, or high capacity 64-bit counters. Most devices support 32-bit counters, but a device with SNMP v2 or v3 counters can use the high capacity counters.



Important: If you monitor high capacity counters for a device, make sure that the device has a v2 or v3 credential assigned to it.



Note: If you do not select the Interface Utilization Performance Monitor to be used during the discovery scan for the device, 64-bit high capacity counters will not be used to poll interface traffic counters. After the discovery scan has completed, you will have to manually change the device's polling properties in the device properties to use the high capacity counters.

Using Network Tools to view real-time data

WhatsUp Gold includes two network tools you can use to view real-time data on network devices, the Web Task Manager and Web Performance Manager. These network tools provide the capability to view real-time device data directly from the WhatsUp Gold web interface.

Network Interfaces

This dialog displays all network interfaces currently configured for the device. Ipswitch WhatsUp Gold monitors all interfaces listed here, displaying the worst state of the interfaces as the device status.

- Click **Add** to configure a new network interface.
- Select an interface from the list and click **Edit** to make changes to the settings for that interface.
- Select an interface and click **Remove** to delete it from the list.
- Select an interface and click **Set default** to make the current device the default interface.

Add/Edit Network Interface

- **Polling type.** Select the type of polling you want WhatsUp Gold to use for this device.
- ICMP (TCP/UDP)
- IPX
- NetBIOS



Note: If NetBIOS is selected, the Host Name box must contain a valid NetBIOS name.

If IPX is selected, the **Address** box must contain a valid IPX address.

If NetBIOS or IPX is selected, you cannot monitor TCP/IP services on this device.

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

Ping Advanced Settings

Use this dialog to set advanced ping data collection settings.

- **Timeout.** The amount of time (in seconds) you want the system to wait before failing the connection to the computer.
- **Iterations.** The number of times WhatsUp Gold will attempt to send the command before the device is considered down.

Passive Monitor: Select Event Type

From the list, select the Passive Monitor type that you want to configure for this device, then click **Next** to continue.

Monitor Properties - Select Monitor Type

From the type of monitor list, select the active monitor type that you want to configure for this device. Click the browse (...) button to access the Active Monitor library and configure new or existing types.

Click **Next** to continue.

Monitor Properties - Set Polling Interval and Dependencies

Set polling options for the monitor.

- **Enable polling for this Active Monitor.** Select this option to have WhatsUp Gold poll the Active Monitor. Clear the option to stop polling.
- **Network interface to use for poll.** Select the configured network interface for the current device.

Passive Monitor: Actions

Configured alerts appear in the list, displaying the action type that is to be fired. You may have multiple actions on a single monitor.

- Click **Add** to configure an action for the monitor.
- Click the hyperlinked **Action** column to edit the settings for that action.
- Select a configured action and click **Remove** to delete the action from the list.

Monitor Properties - Setup Actions for Device State Changes

On this dialog, you can select an Action Policy to use on this monitor, or configure alerts specifically for this monitor.

Configured alerts appear in the 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 monitor.

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

- Click **Add** to configure an action for the monitor.
- 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 monitor) from the Action Log.

Active Monitor Advanced Properties

- **Argument.** The text entered in this box is appended to the OID for the interface on the device. By default, it identifies the number used by the SNMP interface.
- **Comment.** User defined text that appears in the Active Monitor list.
- **Use independent poll frequency for this monitor.** Select this option to have the device polled based on the frequency entered in the Poll frequency box.
- **Poll frequency.** Enter the amount of time (in seconds) between polls for this device. This box is not available unless the Use independent poll frequency for this monitor option has been selected.



Note: Independent poll frequency for all monitors is ignored when a monitor is specified as critical.

APC UPS Performance Monitor

Use this dialog to configure a global APC UPS Performance Monitor. Global performance monitors are configured in the Performance Monitor Library and can be applied to a device via its *Properties dialog* (on page 121).

This monitor collects statistical output power usage information and graphs APC UPS power utilization over time.

This monitor detects when UPS devices are close to maximum performance level, and what time of day networking devices connected to UPS devices are using the most power--both indicating the need to equally distribute the load across several UPS devices.

Enter or select the appropriate information in the following fields.

- **Collection interval.** Use the slider to select the amount of time (in minutes) that WhatsUp Gold should wait between collection attempts.
- **SNMP Timeout.** Use the slider to select the amount of time (in seconds) that you want WhatsUp Gold to wait before it throws an error while attempting to collect data.
- **SNMP Retries.** Use the slider to select the number of times you want WhatsUp Gold to attempt collecting data.

Click **OK** to save changes.

Select Action and State

Select the action you want executed when the selected state change occurs. The **Action to execute** pull-down menu is populated by entries in the Actions Library. Click the ... button to access this library to create new actions, or to edit the actions listed there.

If the action selected is an Up action, then you must make a selection in the **Only if the following state was reached** box. If the device reaches this state at any time, then reaches the Up state, the Up action is fired. This means that the state can change again before it reaches Up and since it reached at least the selected state, it still fires on the Up state.

Select **Maintenance** state if you want to fire an action when a device state changes to Up after it is in Maintenance mode.

Click **Blackout period** to schedule a blackout time for the action.

Select Credentials

In the credentials list, select the credential to use

- or -

Click the browse (...) button to browse to the Credentials Library.

Device Dependencies

There are two ways to set dependencies in WhatsUp Gold:

- **Using Device Properties.** Double-click on a device in My Network view (**View > Device View**) to display Device Properties, and click the Polling Icon. Click either the **Up Dependencies...** or the **Down Dependencies...** button to bring up the Device Dependencies dialog and configure the up or down dependency.
- **Using the Map View.** In My Network view, go to **View > Map View**. Right-click on a selected device and select **Set Dependencies** and either **Set Up Dependency on** or **Set Down Dependency on**. The cursor changes to the Set Dependency arrow. Click on any device in the current group to set the dependency. Selected **Display > Polling Dependency Arrows** to view the dependency between the two devices.

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

Device Dependencies dialog

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

- Checking the first box on the dialog to either poll only if Any one or Every one of the active monitors selected below are up or down on device, depending on the type of dependency you are setting.
- To select a device for the dependency, click the browse (...) button.
- Choose either All active monitors or Specific active monitors and check the active monitors you want to associate with the dependency.

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

An example statement would read:

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

About Dynamic Group Properties

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



Note: Dynamic groups in the web interface: Dynamic groups do not follow group access rights. Anyone with the ability to view the device group that 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 create a new Dynamic Group using the Dynamic Group Builder:

- 1 Enter a name and description for the new dynamic group:
 - **Group Name.** Enter a name for the Dynamic Group as it will appear in the WhatsUp Gold Device List.
 - **Description** (Optional). Enter a short description for the new Dynamic Group. This description is visible to all users who can open the dynamic group.
- 2 In **Filter**, select which groups to search for devices that match the dynamic group criteria.
 - Select **All devices** to show all devices that match the criteria of the dynamic group.
 - Select **All devices in the parent group** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located.
 - Select **All devices in the parent group and its children groups** to show all devices that match the criteria of the dynamic group and are located in the group in which the dynamic group is located or any of that group's children groups.
- 3 Create and edit rules to form an SQL filter for the Dynamic Group.

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

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

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

Validating your filter code

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

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

Converting your filter code

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

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

- 1 Enter the appropriate information into the following fields:
 - **Group name.** Enter a name for the dynamic group. This name appears on the device list.
 - **Description.** (Optional) Enter a statement that describes the dynamic group.
 - **SQL Filter.** Enter the SQL query statement that retrieves the list you want from the database. For the dynamic group to appear in your device list, the first line must be `'SELECT DISTINCT nDeviceID'`.
- 2 Click **OK** to save and add the Dynamic Group to your Device List.

Validating your filter code

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

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

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

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



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

Using the Dynamic Group Rule Editor

This is the second dialog of the WhatsUp Gold Dynamic Group Builder. Use this dialog to create or edit rules for use in the SQL filter for the new group.

Select the desired rule components from the list and enter in a variable in the empty field.

This is a list of rule types available for use with the WhatsUp Gold Dynamic Group Builder.

String rules

- **Active monitor.** Checks the Active Monitors configured for a device found at **Device Properties > Active Monitors**.
- **Device attribute.** Checks for a device Attribute name that matches the criteria entered in Attribute value. Device attributes are configured on the **Device Properties > Attributes** dialog.
- **Display name.** Checks the Display name field found at Device Properties > General.
- **IP address.** Checks the IP address field found at Device Properties > General. Also checks any additional network interface in the Additional Network Interfaces dialog.
- **Host name.** Checks the Host name field found at Device Properties > General. Also checks any additional network interface in the Additional Network Interfaces dialog.
- **Device type.** Checks the Device type field found at Device Properties > General.
- **SNMP OID.** Checks the SNMP OID field found at Device Properties > Credentials.

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

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

- ends with

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

"Yes/No" rules

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

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

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

You do not have to enter a variable for Yes/No rules, because the variable exists in the rule type itself. For example, if you're searching for devices that do not have SNMP credentials, the variable is the SNMP credential.

The criteria is whether a device has an SNMP credential (No). An example yes/no rule could read, "Match the following rule where: Has a Windows credential, Yes," where "Has a Windows credential" is the variable and "Yes" is the search criteria. This rule would search for devices that have Windows credentials.

"IP address is within" rules

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

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

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

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

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

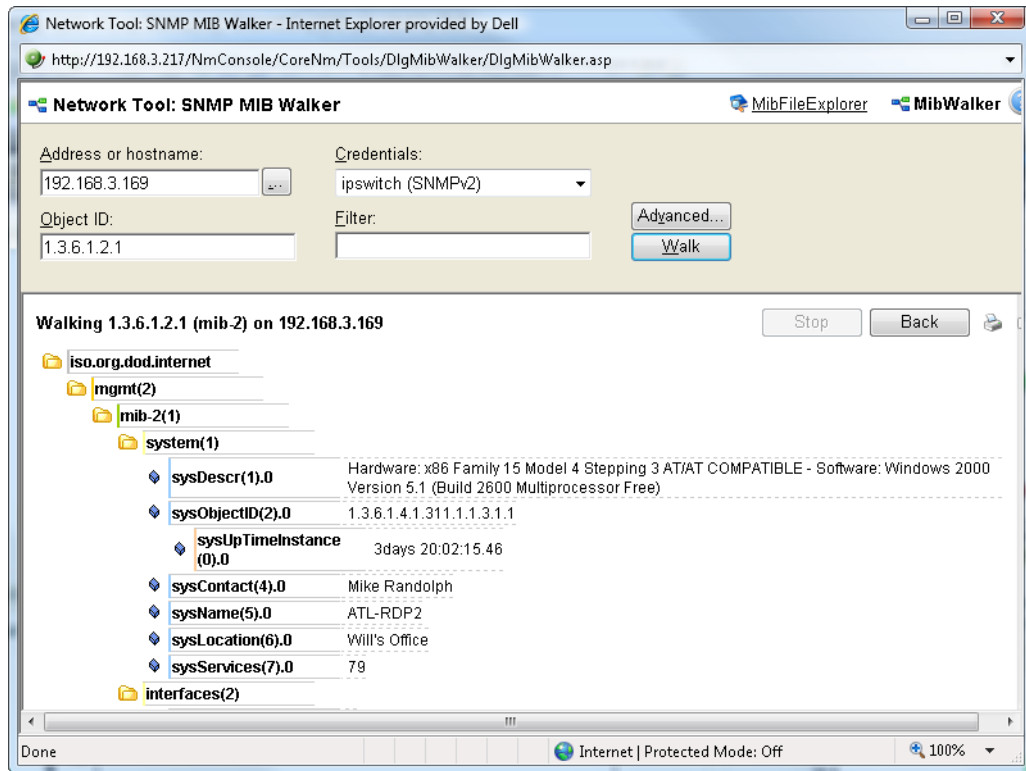
MIB Walker Advanced Parameters

Use this dialog to configure the advanced parameters for the SNMP MIB Walker network tool.

Enter the appropriate information in the following fields:

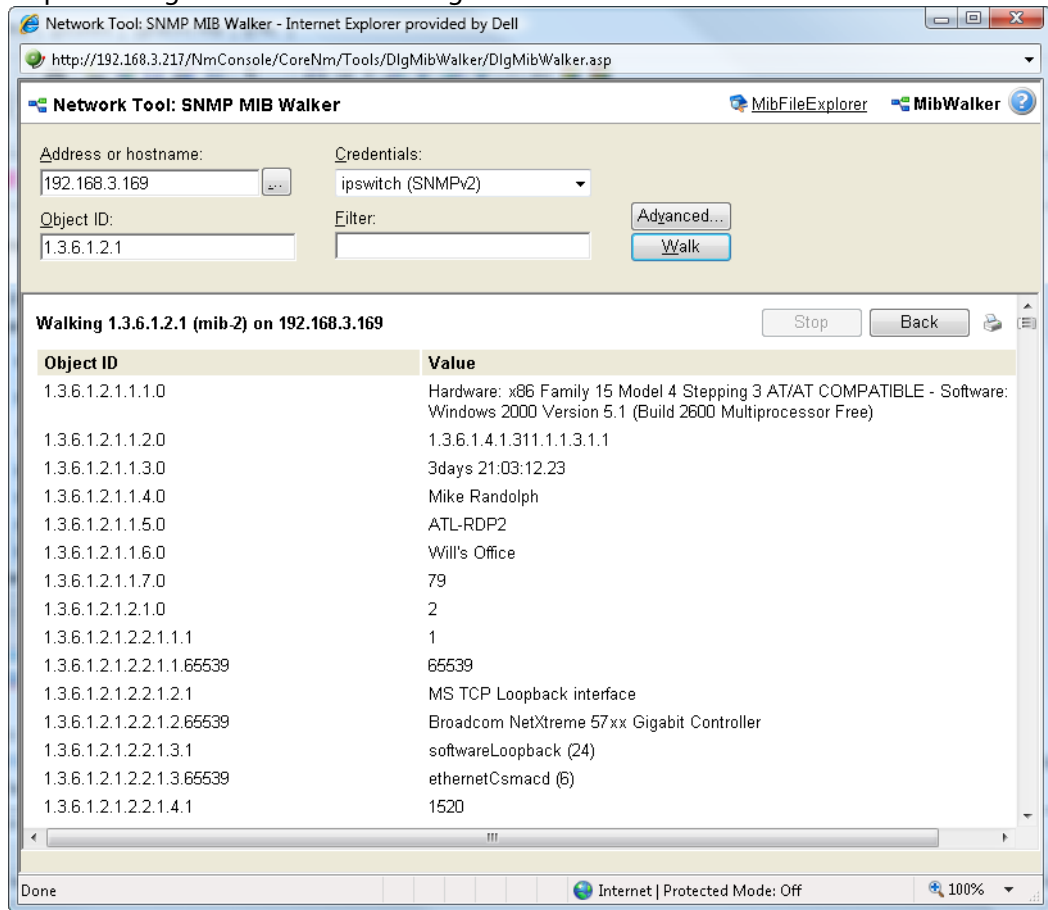
- **Timeout.** Enter a value for the timeout (in seconds).
- **Retries.** Enter a value for the number of retries on the search.
- **Output type.** Select the format for which you want the MIB object information displayed. There are three display formats:

- **Tree.** Lists the MIB object in a tree structure format. This format is most useful in showing the OID hierarchy.

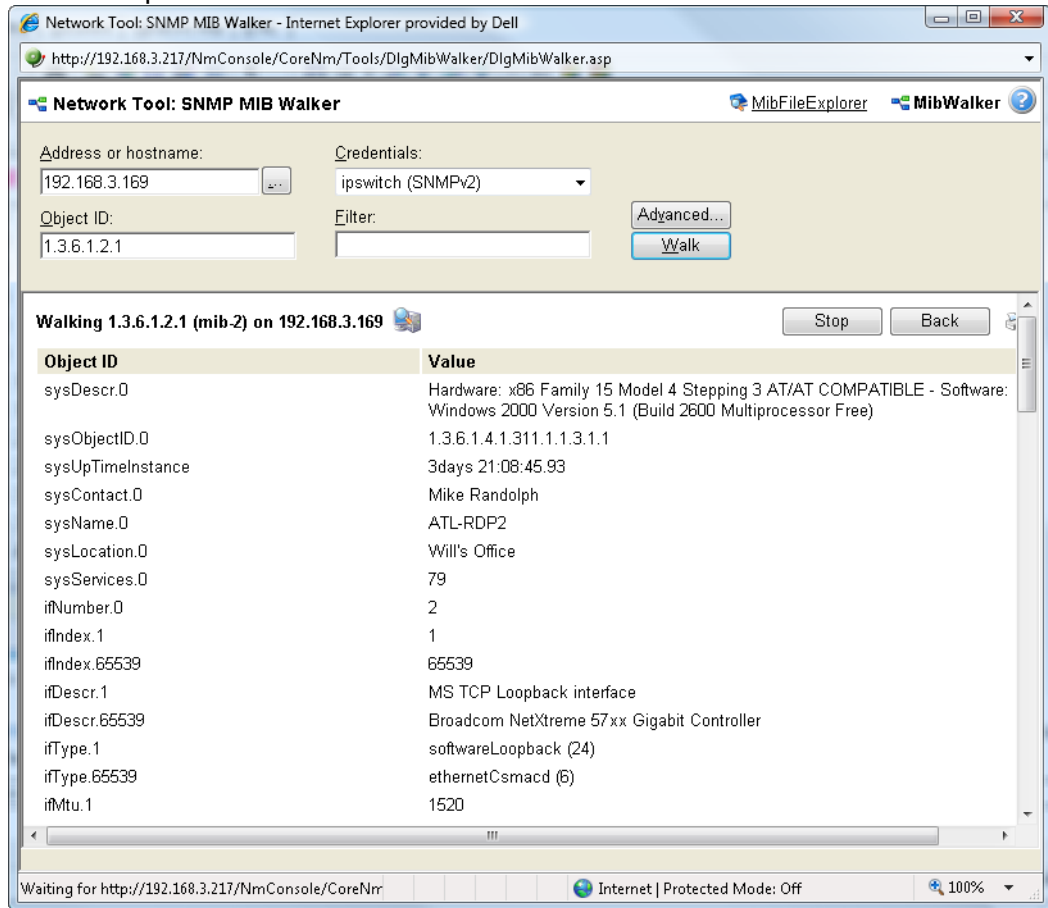


- **List - Numeric OIDs.** Lists the objects in a tabular format showing OIDs in a row numeric format. This format is especially helpful if you do not have the MIB file for the device objects. It provides the raw OID information that you can use in Custom Performance Monitors and Active Script Performance Monitors. Also, you can click the individual OID digits to display more or less MIB object information. For example, in the dialog below, if you click the left-most digit "1" in the OID 1.3.6.1.2.1.1.1.0, all of the available sub-nodes display. If you click the right-most digit "1", only the sub-nodes of this digit display. As you click OID digits, the digits further to the left expand the sub-node information of the respective digits.

As you click OID digits further to the right, the sub-node information expands for the respective digit and therefore more granular sub-node information.



- **List - Labels.** Lists the objects in a tabular format with user friendly labels. If the MIB for the object is not loaded, labels will default to numeric OIDs. Click an OID label name to expand the sub-nodes and view more information.



- **Maximum number of lines displayed.** Select the number of lines you want to view when the MIB file is searched/traversed. If you want to display all of the contents of the MIB file, select **Unlimited**.



Note: This value controls the number of lines the SNMP MIB Walker will render onscreen, not the number of lines in the MIB file it will process.

Click **OK** to save the advanced parameters.



Note: After you click **OK** to return to the SNMP MIB Walker main page, click **Walk** to see changes that you made in the Advanced dialog take affect.

Add/Edit WMI Performance Counter

Use this dialog to add a WMI performance counter to the WhatsUp Gold Web Performance Monitor. This counter will be displayed on the graph within the Web Performance Monitor.

To add a WMI performance counter to the Web Performance Monitor:

- 1 In the Add WMI Performance Counter dialog, enter the appropriate information into the following fields:
 - **Descriptive Name.** Enter a name for the performance counter. This name is displayed in the legend below the Web Performance Monitor's graph.



Tip: It is a good idea to leave the name field blank. Typically, when you select a counter (below) a default display name for the counter is supplied and will display itself in the name field.



Tip: If you are graphing items from more than one device, it is helpful to include the name of the device with the counter name, for example, "ServerXYZ: Processor Utilization."

- **Counter type/Instance.** Select a counter by clicking the browse (...) button. After you select a counter, the **Counter type** and **Instance** fields will populate with the type and instance of the counter you select.
- **Color.** Select a color for the counter by clicking the browse (...) button. This color is used in the Web Performance Monitor graph for this specific counter. If you are graphing multiple counters, this color differentiates it from the other counters.
- **Scale.** Use this to change the magnitude of the graphed values. For example, a value of 100 with a scale of 0.1 will display as 10. A value of 2912 on a scale of 0.01 will display as 29.12. The raw polled value is multiplied by the scale to determine the actual graphed value. The default scale is 1.0.



Tip: Scaling is useful when displaying multiple values on the same graph that have significantly different magnitudes.

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

Select WMI Performance Counter for WMI monitor

Through this dialog, select the WMI Performance Counter that you want to use in the WMI monitor you are creating/editing. As you navigate through the performance counters on the computer you are browsing, information about what that counter or group of counters consists of appears at the bottom of this dialog.

- **Select counters from computer.** This box shows the computer that you are currently browsing. If you want to view counters on another computer, click the browse button next to this box to access the Select Computer dialog.

- **Performance counter.** The counters available on the current system.
- **Performance instance.** The instance names for the counter selected in the Performance counter list.
- **Current value.** Select this option to display the current value of the counter selected in the Performance counter and Performance instance lists.

Selecting a Performance Counter

You can select the WMI Performance Counter you want to use in the WMI performance monitors you create or edit. As you navigate through the performance counters on the computer you are browsing, information about what that counter or group of counters consists of appears at the bottom of the dialog.

- **Computer name.** This box shows the computer that you are currently browsing. If you want to view counters on another computer, click the Browse (...) button next to this box to *select a computer* (on page 891).
- **Performance object.** Select a performance object from the box.
- **Performance counters.** The counters available on the current system. Select the counter and view information about that counter in the box below the list.
- **Performance instances.** The instance names for the counter selected in the Performance counter list.

Click **OK** to select the performance counter for use in the monitor.

Add/Edit SNMP Performance Counter

Use this dialog to add (or edit an existing counter) an SNMP performance counter to the WhatsUp Gold Web Performance Monitor. This counter will be displayed on the graph within the Web Performance Monitor.

To add a SNMP performance counter to the Web Performance Monitor:

- 1 In the Add SNMP Performance Counter dialog, enter the appropriate information into the following fields:
 - **Computer Name.** The name of the device connected to the Web Performance Monitor. This field is automatically populated for you.
 - **Descriptive Name.** Enter a name for the performance counter. This name is displayed in the legend below the Web Performance Monitor's graph.



Tip: It is a good idea to leave the name field blank. Typically, when you select a counter (below) a default display name for the counter is supplied and will display itself in the name field.



Tip: If you are graphing items from more than one device, it is helpful to include the name of the device with the counter name, for example, "ServerXYZ: Processor Utilization."

- **OID/Instance.** Select a SNMP counter by clicking the browse (...) button. After you select a counter, the **OID** and **Instance** fields will populate with the type and instance of the counter you select.
- **Color.** Select a color for the counter by clicking the browse (...) button. This color is used in the Web Performance Monitor graph for this specific counter. If you are graphing multiple counters, this color differentiates it from the other counters.
- **Scale.** Use this to change the magnitude of the graphed values. For example, a value of 100 with a scale of 0.1 will display as 10. A value of 2912 on a scale of 0.01 will display as 29.12. The raw polled value is multiplied by the scale to determine the actual graphed value. The default scale is 1.0.



Tip: Scaling is useful when displaying multiple values on the same graph that have significantly different magnitudes.

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

APC UPS Active Monitor

This monitor watches your American Power Conversion Uninterruptible Power Supply (APC UPS) device and alerts you when selected thresholds are met or exceeded, output states are reached, and/or abnormal conditions are met. For example, an alert can be sent when the UPS battery capacity is below 20%, when the battery temperature is high, when the battery is in bypass mode due to a battery overload state, and many other UPS alert conditions.

Enter or select the appropriate information in the following fields.

- **Name.** Enter a name for the active monitor. This name is displayed in the Active Monitor Library.
- **Description.** Enter a short description for the monitor. This name is displayed next to the monitor name in the Active Monitor Library.
- **Thresholds.** Select the threshold(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the thresholds. By default, all of the thresholds are selected for use in the monitor. By default, the following output states are selected for use in the monitor:
 - Battery Status
 - Battery Capacity
 - Battery Runtime
 - Output Load



Tip: Select a threshold, then click **Configure** to set its individual threshold settings.

- **Monitor the following output states.** Select the output state(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the output states. By default, the following output states are selected for use in the monitor:
 - Abnormal Condition Present
 - AVR Boost Active
 - AVR Trim Active
 - Bad Output Voltage
 - Batteries Discharged
 - Battery Charger Failure
 - Battery Communication Lost
 - Graceful Shutdown Initiated
 - Graceful Shutdown Issued by Downstream Device
 - Graceful Shutdown Issued by Upstream Device
 - High Battery Temperature
 - In Bypass due to Fan Failure
 - In Bypass due to Internal Fault
 - In Bypass due to Supply Failure
 - Low Battery
 - Low Battery/On Battery
 - Manual Bypass
 - No Batteries Attached
 - On
 - On Battery
 - On Line
 - Overload
 - Rebooting
 - Replace Battery
 - Runtime Calibration
 - Self Test In Progress
 - Serial Communication Established
 - Sleeping on a Timer
 - Sleeping until Utility Power Returns
 - Smart Boost or Smart Trim Fault

- Software Bypass
- Synchronized command is in progress



Tip: Use the list's vertical scroll bar to browse the output states.

- **Monitor the following abnormal conditions.** Select the abnormal condition(s) on which you want to be alerted. Refer to the APC UPS documentation for more information about the abnormal conditions. By default, all of the abnormal conditions are selected for use in the monitor.
 - Backfeed Protection Relay
 - Battery Failure
 - Battery Voltage High
 - Bypass Contactor Stuck in Bypass Condition
 - Bypass Contactor Stuck in On-Line Condition
 - Bypass not in Range, Either Frequency or Voltage
 - Extended Run Frame Fault
 - IIC Inter-Module Communication Failure
 - In Bypass due to an Internal Fault
 - In Bypass due to an Overload
 - In Maintenance Bypass
 - Input Circuit Breaker Tripped Open
 - Load (kVA) Alarm Threshold Violation
 - Main Intelligence Module Failure
 - No Batteries Installed
 - No Working Power Modules
 - Output Voltage out of Range
 - Power Module Failure
 - Redundancy Below Alarm Threshold
 - Redundancy Lost
 - Redundant Intelligence Module Failure
 - Redundant Intelligent Module in Control
 - Runtime Below Alarm Threshold
 - Site Wiring Fault
 - System Level Fan Failure
 - UPS Not Synchronized

- UPS Specific Fault Detected



Tip: Use the list's vertical scroll bar to browse the abnormal conditions.



Tip: Click **Advanced** to set the SNMP timeout and number of retries.

Click **OK** to save changes.

Diagnostic Tool

This tool diagnoses problems within your database by running a diagnostic scan.

To use the Diagnostic Tool:

- 1 To begin the scan, click the **Diagnostic** button.
- 2 After you have looked over and noted any problems, click **Close**.
 - To print the report, click the printer icon in the upper right corner of the window.

Re-enabling the Telnet protocol handler

The Telnet protocol handler is disabled by default in Microsoft Internet Explorer 7. In order to use the Telnet tool in WhatsUp Gold, you need to re-enable the Telnet protocol.

To re-enable the Telnet protocol:

- 1 Click **Start > Run**. The Run dialog box opens.
- 2 In the Open box, enter: `Regedit`, then click **OK**. The Registry Editor opens.
- 3 Go to the following key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl`
- 4 Under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl`, create a new key named `FEATURE_DISABLE_TELNET_PROTOCOL`.
- 5 Add a `DWORD` value named `ieexplore.exe` and set the value to 0 (decimal).
- 6 Close the Registry Editor and restart Microsoft Internet Explorer. The Telnet protocol is enabled.

Selecting a Performance Monitor Type

Use the picklist to select one of the following performance monitor types; after selecting the monitor type, click **OK**.

Active Script Performance Monitor (on page 250)

APC UPS Performance Monitor (on page 263)

SNMP Performance Monitor (on page 249)

SSH Performance Monitor (on page 250)

WMI Performance Monitor (on page 254)

Add Custom Link

Enter **Display Name** and **Hyperlink**, then click **OK** to create the custom link.

The following percent variables are valid in the **Hyperlink** field:

`%Device.Address`

`%Device.HostName`

`%Device.Attribute.X` (where X is the specific attribute name.)

For example, you could use `telnet://%Device.Address` or
`http://%Device.HostName/%Device.Attribute.Attribute1`

Add a Device Attribute

Enter **Attribute Name** and **Attribute Value**, then click **OK** to save the device attribute.

Bulk Field Change - Action Policy

How to get here

Select the **Apply this Action Policy** option to be able to select an action policy to use on the selected devices. The pull-down menu shows all action policies defined in the Action Policies dialog. Click the **Browse** button to access this dialog to create or edit an action policy.

Bulk Field Change - Active Monitor

How to get here

Use this dialog to add or remove an active monitor from multiple devices at once.

- **Operation.** Select Add or Remove. If you select Remove, only the selected devices with the active monitor you select below is modified.
- **Active monitor type.** Select an active monitor type to add to or remove from the selected devices. Use **Bulk Field Change > Active Monitor Properties** to make modifications to the active monitor settings on the devices, or modify each device manually after monitors are added.

Bulk Field Change - Active Monitor Properties

Use this dialog to make configuration changes to active monitors on multiple devices.



Important: If a selected device does not currently have the active monitor associated to it, no modifications will be made to that device. Only devices that have the active monitor will be changed.

- **Active monitors found in selected devices.** Select an active monitor from this pull-down menu. This list is populated with all active monitors found on the selected devices.
- **Enable polling.** Select **On**, **Off**, or **No Change**. On turns polling on for the selected active monitor, Off suspends polling on the monitor, and No Change makes no modification to the monitor.
- **Use independent poll frequency.** If you want to have WhatsUp Gold poll the active monitor at a non-default interval, select Yes from the list-box. Select No to return the interval to the application-wide default.
- **Set poll frequency to.** Select a time (in seconds) you want WhatsUp Gold to wait between polls on the selected active monitor.
- **Action policy.** Select an action policy to add to the selected active monitor for each selected device. The list is populated with all policies in the Action Library. Select None to remove existing action policies from the active monitor on the selected devices. Click the browse (...) button to access the library to view or modify the action policies.
- **Argument.** Enter an argument for the active monitor, or select None to remove arguments from the active monitor on the selected devices.
- **Operation.** Select an operation from the drop down menus.
- **Custom Value.** Enter a custom value for the active monitor.
- **Comment.** Enter a comment for the active monitor, or select None to remove comments from the active monitor on the selected devices.

Bulk Field Change - Attribute

How to get here

- Select a task from the **Operation** pull-down menu: **Add/Update** or **Remove**.
- In the **Attribute name** box, enter a name for the attribute you are adding to the selected devices.
- In the **Attribute value** box, enter the text for the attribute itself.

Bulk Field Change - Credentials

How to get here

Select the credentials you want to associate with the selected devices from the pull-down menus.

Credentials are configured in the Credentials Library. You can associate credentials manually on the Device Properties - Credentials dialog.

Bulk Field Change - Device Type

How to get here

Select a device type from the pull-down menu. The menu is populated by entries in the Device Types dialog. The Device Types dialog can be accessed directly by clicking the **Browse** button next to the **Device Type** box.

When you change your device type in this manner, only the display icon and custom menus are changed to the new type. Monitors and other settings are not affected by changing the device type.

Bulk Field Change - Down Dependency

How to get here

When this option is selected, WhatsUp Gold will only poll the selected devices if the active monitor(s) of the device selected from the pull-down list has failed. This is referred to as a *Down Dependency*.

Bulk Field Change - Maintenance Mode

How to get here

Select the **Force device(s) into maintenance mode now** option to place all selected devices in this mode. When in maintenance mode, the devices Active Monitors will not be polled, and actions will not be triggered. To resume polling and actions, take the device out of maintenance mode.

Bulk Field Change - Notes

Select an operation from the **Operation** pull-down menu (append, prepend, replace), then enter the text for that note that you want to add to the selected devices. Text is entered in the Notes dialog as a string. The append and prepend functions add new text to either the beginning or the end of the existing string of text.

- **Append.** Notes are added to the end of the line.
- **Prepend.** Notes are added to the front of the line.
- **Replace.** Replaces the current notes with the note entered on this dialog.



Note: The Bulk Field Change deliberately doesn't make any changes to the text you enter, but rather stores exactly what you specify. We have designed it this way so that you have the flexibility to make your own changes, such as including a line break.

Bulk Field Change - Passive Monitor

How to get here



Note: The Bulk Field Change for passive monitors is available from the WhatsUp Gold web interface only.



Use this dialog to add or remove passive monitors from multiple devices.

- **Operation.** Select **Add** or **Remove**. Selecting Remove only deletes the passive monitor you select below from selected devices originally configured with that specific passive monitor.
- **Passive monitor type.** Select a passive monitor type to add to, or remove from, the selected devices. Click the browse (...) button to bring up the Passive Monitor Library.
- **Passive monitor.** Select a passive monitor to add to, or remove from, the selected devices.

Use **Bulk Field Change > Passive Monitor Properties** to modify to devices' passive monitor properties.

Bulk Field Change - Passive Monitor Properties

Use this dialog to make configuration changes to passive monitors on multiple devices.



Note: If a selected device does not currently have the passive monitor associated to it, no modifications will be made to that device. Only devices that have the passive monitor will be changed.

- **Passive monitor types found in selected devices.** Select a passive monitor type from this pull-down menu. This list is populated with all passive monitor types found on the selected devices.
- **Passive monitor.** Select a passive monitor from this pull-down menu.
- **Operation.** Select Add action or Remove action. If you select Remove action, only the selected devices with the action you select below is modified.
- **Actions.** Select an action to add to or remove from the selected devices.

Bulk Field Change - Performance Monitor

How to get here

Select the performance monitor you want to configure for the selected devices, then select how often (in minutes) you want to collect data in the **Data collection interval (mins)** field.

Select **All** to have WhatsUp Gold collect data on all instances of that type on the selected devices, select **None** to stop collecting data for all instance of that type on the selected devices. For Interface, **Active** collects data from interfaces up at the exact time of the poll; **Custom Active** collects data from all custom active interfaces. **Default** for Ping polls the default interface you select in **Device Properties > General**.

- **CPU.** CPU Utilization data displayed in the CPU Utilization Report.
- **Disk.** Disk Utilization data displayed in the Disk Utilization Report.
- **Interface.** SNMP Interface data displayed in the Interface Report.
- **Memory.** Memory utilization data displayed in the Memory Utilization Report.
- **Ping.** Ping availability data displayed in the Group Ping Availability Report.

You can select individual data type instances for each device at **Device Properties > Device Properties - Performance Monitors**.

Bulk Field Change - Polling Interval

How to get here

The polling interval controls how often the selected devices are polled by WhatsUp Gold. Enter the number of seconds in the **Polling interval** box you want WhatsUp Gold to wait between polls.

Bulk Field Change - Up Dependency

How to get here

- **Poll only if [any one or every one] of the selected active monitors are 'Up' on device:** Select this option to have WhatsUp Gold only poll the selected device if the active monitor(s), for the selected device, are successful (in the up state). This is referred to as an *Up Dependency*.
- **Device box.** Enter the device name or IP address or click browse (...) to select from a list of devices to poll when active monitors are up for the selected device.
- **All active monitors.** Select this option to have all active monitors, associated with the selected device, polled for up dependency status.
- **Specific active monitors.** Select this option to have specific active monitors, associated with the selected device, polled for up dependency status. Select the active monitor types you want to poll in the **Monitor Name** list.

Hub Transport Server Role thresholds

The following table lists the threshold settings available for the Hub Transport Server category:

| Threshold | Description | Value |
|--------------------------------|--|------------------------|
| Aggregate Delivery Queue | The Aggregate Delivery Queue holds the aggregate value of all of the messages queued for delivery in all of the queues associated with the Hub Transport Server. | Default: 3000 messages |
| Active Remote Delivery Queue | The Active Remote Delivery queue holds messages that are being delivered to a remote server using SMTP. | Default: 250 messages |
| Active Mailbox Delivery Queue | The mailbox delivery queue holds messages that are being delivered to a mailbox server by using encrypted Exchange RPC. | Default: 250 messages |
| Submission Queue | A persistent queue that is used by the categorizer to gather all messages that have to be resolved, routed, and processed by Transport agents | Default: 100 |
| Active Non-SMTP Delivery Queue | The Active Non-SMTP Delivery queue holds messages that are being delivered to a remote server, using a protocol other than SMTP. | Default: 100 |
| Retry Mailbox Delivery Queue | The Retry Mailbox Delivery Queue holds messages with a status of | Default: 100 |

| Threshold | Description | Value |
|-------------------------------|--|--------------|
| | Retry that are being delivered using encrypted Exchange RPC. Messages are given a status of retry when the server cannot connect to the next hop. | |
| Retry Non-SMTP Delivery Queue | The Retry Mailbox Delivery Queue holds messages with a status of Retry that are being delivered using a protocol other than SMTP. | Default: 100 |
| Retry Remote Delivery Queue | The Retry Mailbox Delivery Queue holds messages with a status of Retry that are being delivered using SMTP. | Default: 100 |
| Unreachable Queue | The Unreachable queue is a persistent queue that contains messages that cannot be routed to their destinations. | Default: 100 |
| Largest Delivery Queue | The Largest Delivery queue identifies the largest of all of the delivery queues on the Exchange server. | Default: 200 |
| Poison Queue | The poison message queue is a special queue that is used to isolate messages that are detected to be potentially harmful to the Exchange 2007 system after a server failure. | Default: 0 |

Outlook Web Access Server Role thresholds

The following table describes the thresholds associated with the Outlook Web Access Server category:

| Threshold | Description | Value |
|-----------------------|---|---------------------------|
| Average Response Time | Sets the threshold for the average time in milliseconds that elapses between the beginning and end of an OEH or ASPX request. | Default: 100 milliseconds |
| Average Search Time | Sets the threshold for the average elapsed time waiting for a search to complete. | Default: 100 milliseconds |

Mailbox Server Role thresholds

The following table lists the threshold settings available for the Mailbox Server category:

| Threshold | Description | Value |
|---|---|--------------|
| RPC request currently executing within the information store process must be less than: | Sets the maximum threshold for the number of executing Remote Procedure Calls (RPC) in the Information Store process. | Default: 70 |
| RPC Averaged Latency must not exceed: | Sets the maximum threshold for average latency of the Remote Procedure Calls (RPC) in milliseconds | Default: 25 |
| RPC Number of Slow Packets must be less than: | Sets the maximum threshold for the Remote Procedure Call (RPC) packets within the past 1024 packets with latencies longer than 2 seconds. | Default: 3 |
| Messages Queued for Submission (Mailbox) must be less than: | Sets the maximum threshold for the number of submitted messages in the Mailbox that have not yet been processed by the transport layer. | Default: 50 |
| Messages Queued for Submission (Public) must be less than: | Sets the maximum threshold for the number of submitted messages by that have not yet been processed by the transport layer. | Default: 20 |
| Replication Receive Queue Size must be less than: | Sets the maximum threshold for the number of replication messages waiting to be processed. | Default: 100 |
| Slow Findrow Rate must not exceed: | Sets the maximum threshold for the rate at which the slower FindRow needs to be used in the mailbox store. A higher value indicates that applications are searching mailboxes, directly affecting server performance. | Default: 10 |
| Number of search tasks created per second must be less than: | Sets the maximum threshold for the number of search tasks created each second. | Default: 10 |
| Average Document Indexing Time must be less than: | Sets the maximum threshold in seconds for the length of time it takes to index documents. This value is reported in milliseconds and converted to seconds for this comparison. | Default: 30 |

Selecting or Creating an Action

Use this Wizard to setup an action to be executed when the specified state change occurs. New actions created through the wizard are added to the Action Library. After the action has been added to the library, it can be assigned to any device, active monitor, or action policy in your database.

Setting Advanced Properties for a HTTP Content Monitor

You can configure the user agent and custom headers for the HTTP Content Monitor.

Type or select the appropriate information in the following fields.

User agent

The user agent string identifies which web browser is making an HTTP request. You can use this to imitate your web site being visited by various browsers. Select a browser from the list. The user agent from the latest version of the browser is populated for the browser you select. You can use this agent string, or enter a different user agent string for the version of the browser that you want WhatsUp Gold to check.

Custom headers

Enter any specific headers for which you want the monitor to check. Enter a header as Field:Value. You can enter up to three custom headers.



Note: Errors can result when using invalid custom headers or when modifying headers that do not allow modification, such as the HTTP Host header. You can test custom headers by clicking Request URL contents on the New/Edit HTTP Content Monitor dialog. If there is a problem with the header, an error message displays the problem. For example,



"An error occurred with the requested website. Error: The 'Host' header cannot be modified directly. Parameter name: name."



In this example, a user entered `Host :myhost.com` as a custom header. However, the Host header cannot be modified and an error generated as a result.

Click **OK** to save changes.

Setting Advanced Properties for an Email Active Monitor

You can configure the advanced properties for the Email Monitor.

Type or select the appropriate information in the following fields.

SMTP Advanced Properties

- **SMTP server requires authentication.** Select this option if your SMTP server requires authentication.



Note: The Email Monitor supports CRAM-MD5, LOGIN and PLAIN authentication methods. The authentication method is not configurable. It is negotiated with the SMTP server automatically using the strongest mutually supported authentication method.

- **Username.** Type the username to be used with SMTP authentication.
- **Password.** Type the password of the username to be used with authentication.
- **Use an encrypted connection (SSL/TLS).** If your SMTP server supports encrypting data over a TLS connection (formerly known as SSL), select this option to encrypt SMTP traffic.



Note: For SMTP connections, WhatsUp Gold only supports explicit SSL sessions negotiated using the STARTTLS command.

- **Timeout.** Type the amount of time (in seconds) to wait for a response from the SMTP server for each command WhatsUp Gold issued. If this time limit is exceeded, the monitor fails.

Incoming server (IMAP or POP3) advanced properties



Note: WhatsUp Gold supports only clear text authentication method for retrieving mail. To protect your username and password while retrieving mail, you must use one of the SSL encryption methods.

- **Port.** Type the port on which your POP3 or IMAP server is running.
- **Use an encrypted connection.** Select this option to connect to a POP3 or IMAP server in an encrypted mode. Select one of the following encryption methods:
 - **Use implicit SSL.** Select this option to login to your POP3 or IMAP server in an encrypted mode.
 - **Use SSL with STLS.** Select this option to login to your POP3 or IMAP server in an unencrypted mode, and then switch to a TLS connection by sending STARTTLS or STLS command to the server.



Important: When connecting using STARTTLS, the connection is encrypted before any authentication information is sent or any mail is retrieved.

- **Timeout.** Type the amount of time (in seconds) to wait for a response from the IMAP/POP3 server for each command WhatsUp Gold issued. If this time limit is exceeded, the monitor fails.



Note: If your IMAP server is configured to move the test message sent by the monitor to a folder other than the Inbox, the monitor fails. WhatsUp Gold only detects messages in the Inbox folder on an IMAP server.

Click **OK** to save changes.

Configure CPU Threshold

Enter the percentage of CPU capacity that, when exceeded, causes the monitor to fail.

Home

In This Chapter

| | |
|--|-----|
| Understanding and using dashboards | 339 |
| Types of dashboards | 352 |
| Using Favorites | 358 |
| Dashboard reports | 362 |

Understanding and using dashboards

In This Chapter

| | |
|--|-----|
| Learning about dashboards | 339 |
| Overview of dashboard report categories | 340 |
| Adding dashboard reports to a dashboard view | 342 |
| Searching for dashboard reports..... | 345 |
| Working with dashboard views..... | 345 |
| Changing dashboard content..... | 348 |
| Using the dashboard report menu | 348 |
| Configuring a dashboard report | 349 |
| Moving dashboard reports within a dashboard view | 350 |
| Navigating dashboard views..... | 351 |

Learning about dashboards

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

Dashboards in WhatsUp Gold are user-specific, and are configurable to include *dashboard reports* (on page 342) specific to users' needs. Dashboards contain multiple *views*, displayed as tabs, that let you organize groupings of dashboard reports according to the type of information they display. You can click on different view tabs within a dashboard to display different views within the same dashboard.

When you begin customizing your dashboard views, consider the types of information you need to view most often, the devices to which you need to pay closest attention, and the level of detail you want to monitor through a particular dashboard view. You should also take into consideration the type of dashboard, and the types of dashboard reports you can add to a particular dashboard type.

Types of dashboards

The **Home** dashboard can display both Home- and Device-level dashboard reports. You can place any dashboard report on a Home dashboard. You can mix and match summary, group, and device-specific data in this type of dashboard.

Changes that you make to a dashboard view affect only your user account. If you decide to completely change all of the dashboard views under your account, your user account is the only account affected by these changes. For more information, see *Managing dashboard views* (on page 868).

Device Status dashboards display only Device-level dashboard reports. Only dashboard reports specific to a single device can be placed on a device dashboard. When you switch to a different device in context, the reports displayed show data for the newly selected device. For more information, see *Adding dashboard reports to a dashboard view* (on page 342).

The **Top 10** dashboard displays Top 10 reports for your network devices.

Overview of dashboard report categories

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

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

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

- **Memory Utilization.** These dashboard reports display information that pertains to device and network memory levels.
- **Performance (Historic and Last Poll).** These dashboard reports display information gathered from WMI and SNMP Performance Monitors regarding your network devices' CPU, disk, interface, and memory utilization; and ping latency and availability.
- **Ping Availability and Response Time.** These dashboard reports display information that pertains to device ping availability, response time, and packet loss.
- **Problem Areas.** These are trouble-shooting dashboard reports that allow you to investigate network issues.
- **Remote/Central** (included in the WhatsUp Gold Distributed, and MSP Editions). These include a variety of dashboard reports for the Remote Sites that you are monitoring with the WhatsUp Gold Central Site.
- **Split Second Graphs Split Second Graphs** (included in the WhatsUp Gold Premium, Distributed, and MSP Editions). These are real-time graphs that display information on SNMP and WMI performance counters. These reports allow you to include the real-time information available on the *Web Performance Monitor* (on page 141) network tool and the *Web Task Manager* (on page 143) network tool in any dashboard view.
- **Threshold.** These dashboard reports display information on your network CPU, disk, interface, and memory utilization, and ping function; at or above a specific threshold.
- **Top 10.** These dashboard reports display the top devices on your network according to their CPU, disk, interface, and memory utilization, and ping function.
- **Virtualization.** These dashboard reports display information about vCenter servers, virtual hosts and their associated virtual machines. You can see details about the virtual host or vCenter server, a list of the virtual machines, as well as CPU, disk, interface, and memory utilization for virtual machines.
- **Wireless** (included in the WhatsUp Gold Premium, Distributed, and MSP Editions). These dashboard reports display information about Wireless Access Point (WAP) devices and the devices connected to the WAPs, transmit and receive errors, and syslog messages.

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

Tail of State Change Log

| Start time | Device | Monitor | State |
|-------------------|--------------------------------|---------|----------------------|
| Tue 04/19 9:04 AM | VEGA | Ping | Up at least 5 min |
| Tue 04/19 9:01 AM | man623.ipswitch.mipswitch.com | Ping | Up at least 5 min |
| Tue 04/19 9:00 AM | VEGA | Ping | Up |
| Tue 04/19 8:59 AM | 192.168.8.213 | Ping | Down at least 5 min |
| Tue 04/19 8:59 AM | imq1115.ipswitch.mipswitch.com | Ping | Up at least 5 min |
| Tue 04/19 8:58 AM | VENUS2 | Ping | Up at least 5 min |
| Tue 04/19 8:58 AM | 192.168.8.213 | Ping | Down at least 2 min |
| Tue 04/19 8:56 AM | man623.ipswitch.mipswitch.com | Ping | Up |
| Tue 04/19 8:56 AM | testxp | Ping | Down at least 20 min |
| Tue 04/19 8:55 AM | 192.168.8.213 | Ping | Down |

Actions Fired in Last 4 Hours

| Date | Source | Action Name | Trigger |
|-----------------------------|--------|-------------|---------|
| No action activity records. | | | |

All Completely Down Devices

| Device | Status |
|--|---------------------------|
| 192.168.8.213 | Ping/Down at least 5 min |
| ATL-DSTANSEL4 | Ping/Down at least 20 min |
| ATL-JRosenberg2.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| ATL-JRosenberg2.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| at-bn101re.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| at-mmcamber.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| at-sayonrit.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| ATL-SOFTTEST | Ping/Down at least 20 min |
| at-usability2.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| bmj_wug_current.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| CHEETAH | Ping/Down at least 20 min |
| ip-soug-sporell.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| IPSTEST-WRHYNER | Ping/Down at least 20 min |
| PSWITCH-L408U | Ping/Down at least 20 min |
| q-chinese2003sp2.qa.local | Ping/Down at least 20 min |
| lme in 2008eq.ipswitch.mipswitch.com | Ping/Down at least 20 min |
| replication-2 | Ping/Down at least 20 min |
| replication-3 | Ping/Down at least 20 min |
| SP-HV-2003 | Ping/Down at least 20 min |
| tdcmk-2k80-64.ipswitch.mipswitch.com | Ping/Down at least 20 min |

Adding dashboard reports to a dashboard view

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

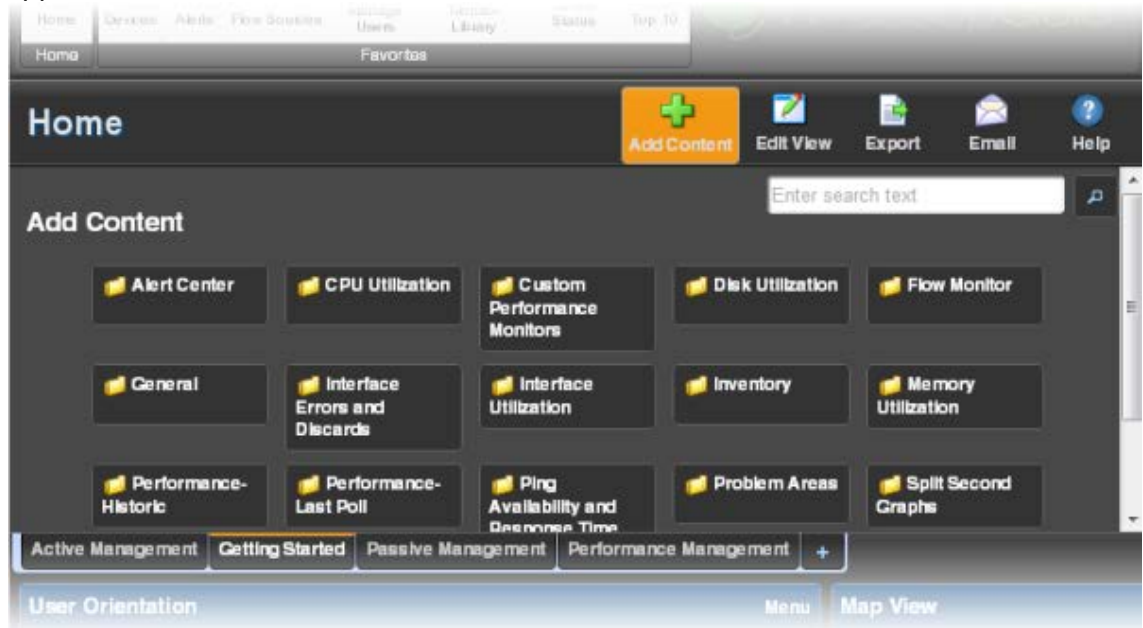


The reports available to add to the current dashboard vary, depending on the dashboard view type. Home dashboard views can include any available dashboard report, while you can only add reports which apply to a single device to a Device Status dashboard view. Reports are grouped into categories based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

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

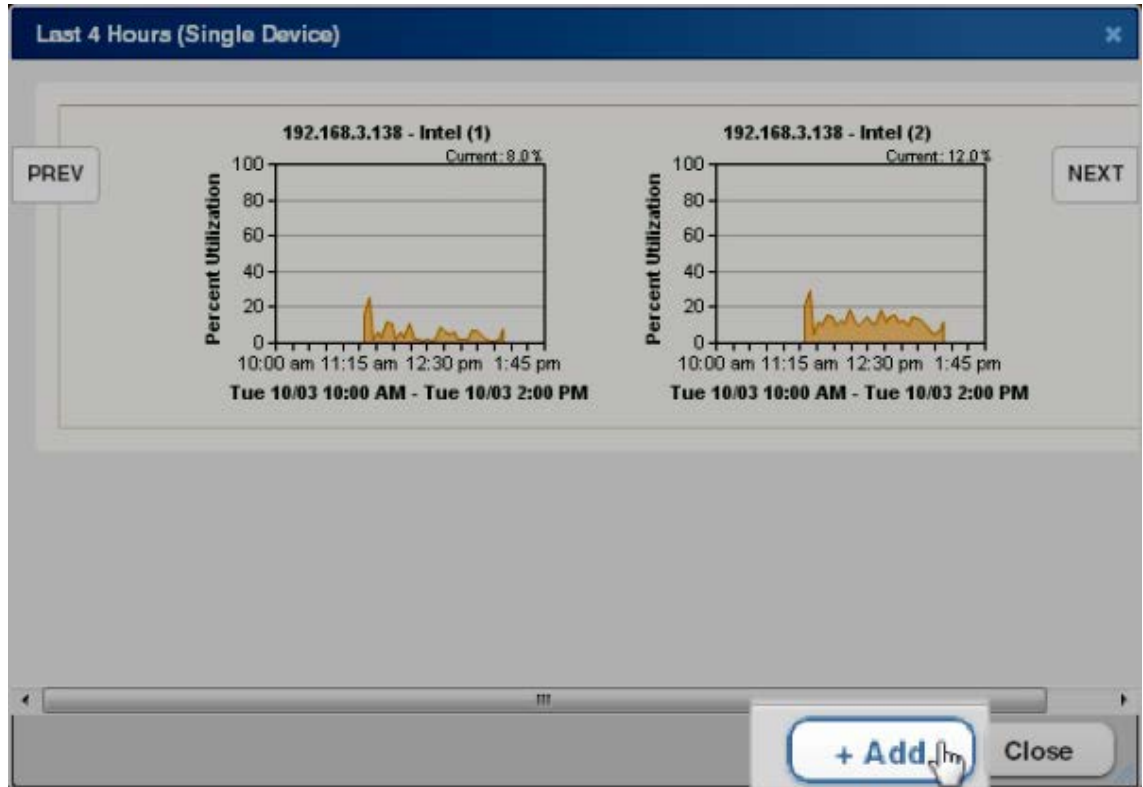
To add reports to a dashboard view:

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

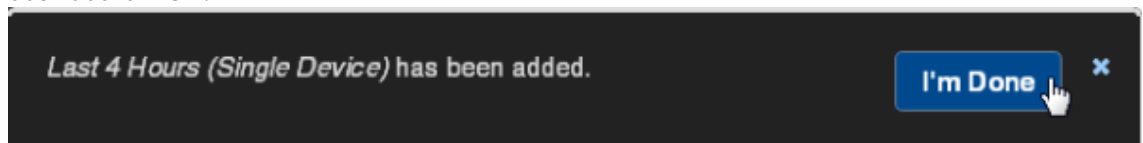


- 3 Select the category of report you want to add by clicking the related folder. The reports in that category display.
- 4 Click the report you want to add. A preview of the report displays.

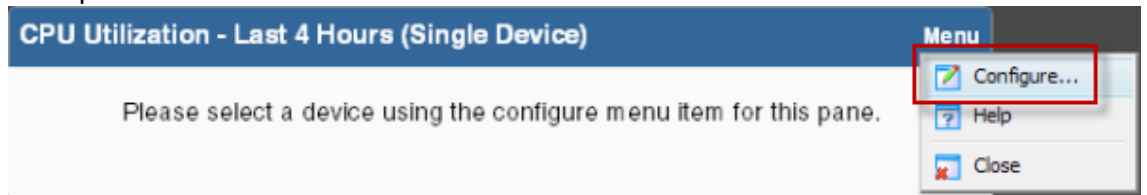
- 5 Click the **Next** and **Prev** buttons to cycle through the next and previous reports within the category.
- 6 Click **Add**.



- 7 Continue selecting and adding reports until you have added all of the reports. You can add up to 15 reports to a single view.
- 8 When you have finished adding reports, click **Close** to close the report dialog.
- 9 Click **I'm Done** to return to the dashboard view. The newly added reports appear in the dashboard view.



- To configure a report in your dashboard, click **Menu > Configure** in the title bar of the report.



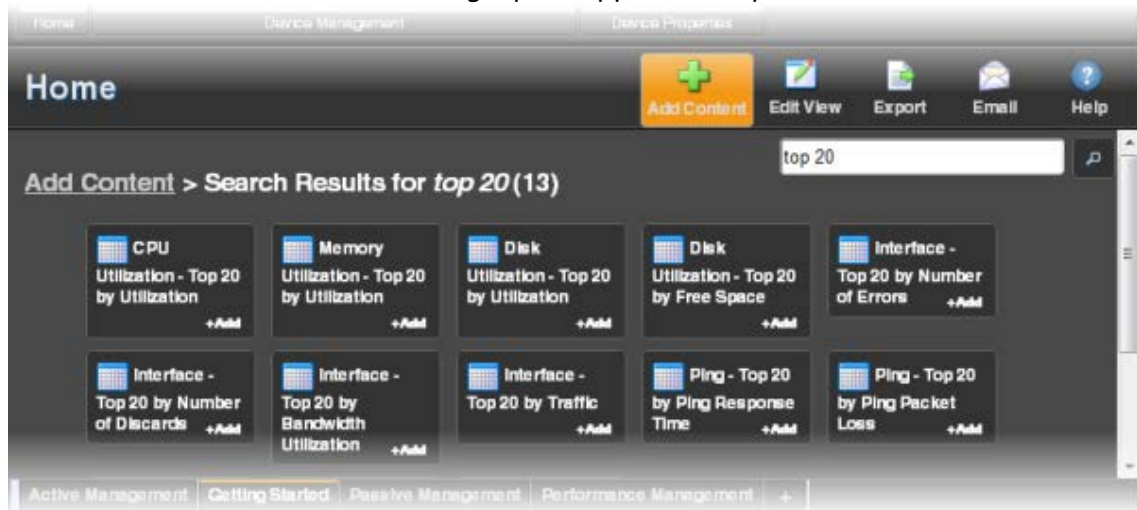
- To remove a report from a dashboard view, click **Menu > Close**.

Searching for dashboard reports

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

To search for reports:

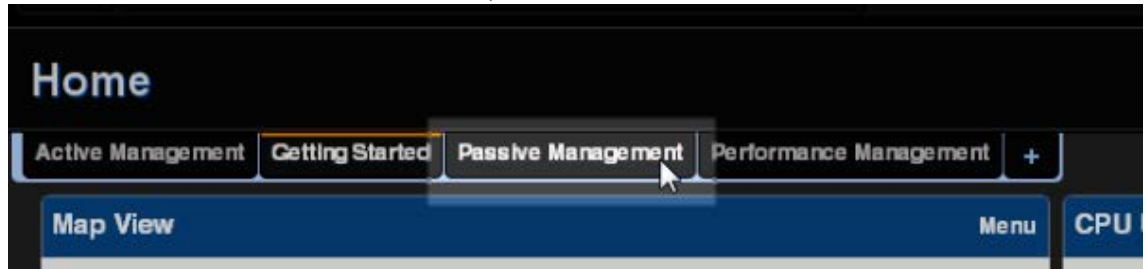
- 1 From the Home, Top 10, or Device Status dashboard, click **Add Content**. The Add Content pane appears.
- 2 Type all or part of the report name in the box at the top of the Add Content pane.
- 3 Click the **Search** button. The matching reports appear in the pane.



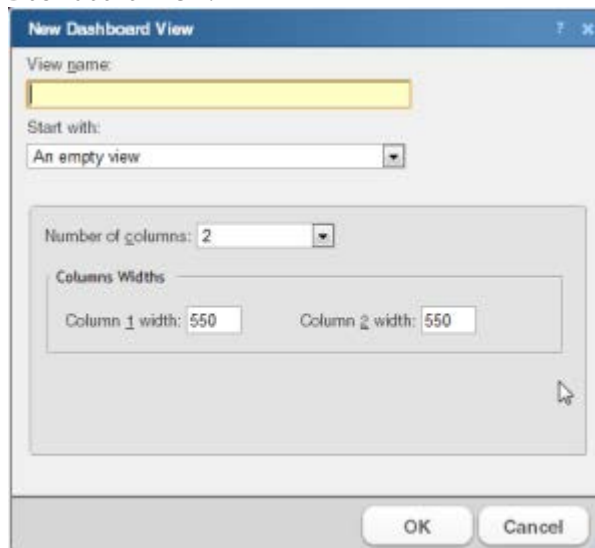
Working with dashboard views

WhatsUp Gold comes with a several pre-configured dashboard *views*. You can create your own dashboard views to use in addition to the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting.

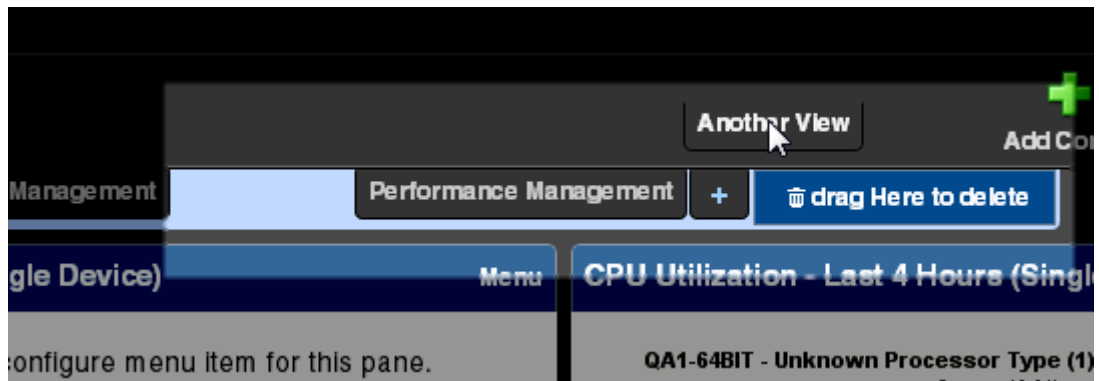
- To manage views for multiple users, see *Managing dashboard views* (on page 868).
- To switch to a different dashboard view, click another view tab in the dashboard.



- To add a new dashboard view, click the + in the row of tabs to open the New Dashboard View.



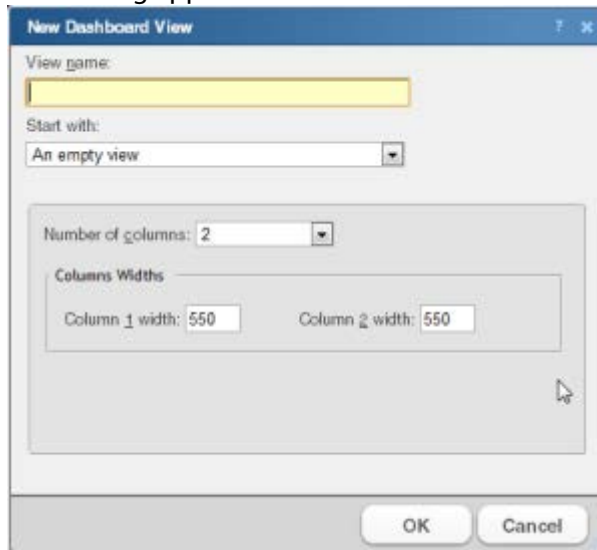
- To delete a view, click and drag the associated tab. The Delete tab appears to the right of the tab row. Drag the view tab you want to delete over the **Delete** tab. The view is removed.



- Click **Edit View** to edit the settings for the current dashboard view.
- Click **Add Content** to open the Add Content pane and select additional reports to add to the current view.
- To change the order of the dashboard view tabs, click and drag a tab to a new location.

To create a new dashboard view:

- 1 From the dashboard where you want to add the new view, click **+**. The New Dashboard View dialog appears.



- 2 Enter the appropriate information in the following fields:
 - **View name.** Type a relevant name for the new view. This name is used to identify a view in the dashboard, so select a name that is meaningful and helps you to distinguish it from other views.
 - **Start with.** Select the existing dashboard view type on which to base the new view, or select **An empty view** to create a new custom view.
 - **Number of columns.** Enter a value for the number of columns you wish to have in the new dashboard view (1 -4). Keep in mind, the more columns you include, the smaller the data displayed inside a dashboard.



Note: This option appears only when you start with an empty view.

- **Column widths.** Enter a width for each of the dashboard view columns. You are prompted for a value for each column you selected in the previous step.



Note: This option appears only when you start with an empty view.

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

To edit a dashboard view:

- 1 Click **Edit View** in the toolbar. The Edit Dashboard View dialog appears.
- 2 Enter the appropriate information in the following fields:
 - **View name.** The dashboard title as it appears on the dashboard view tab and in the Manage Dashboard Views dialog.
 - **Number of columns.** The number of columns in the dashboard.
 - **Column width.** The width of each column in the dashboard (in pixels).
- 3 Click **OK** to save changes.

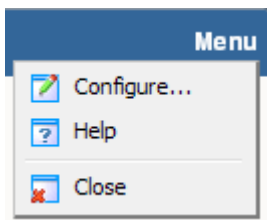
Changing dashboard content

Dashboard reports are smaller versions of the monitor reports listed on the Monitoring tab. The dashboard reports are displayed within WhatsUp Gold dashboard views. For more information, see *Understanding and using dashboards* (on page 339).

- To add a report, click **Add Content** on the WhatsUp Gold toolbar to bring up the Add Content pane. From this pane, you can select multiple dashboard reports from multiple categories. A preview for the dashboard report displays when you select it. For more information see, *Adding dashboard reports to a Device Status dashboard* (on page 354).
- To remove a report, click **Menu > Configure** for that dashboard report and then select **Close**. Keep in mind that when you remove a report, any customizations you have made to it are lost.
- To move a dashboard report, click the report title bar and drag it to a new space in the dashboard view.
- To change the settings for a dashboard report, click **Menu > Configure** in the title bar of that report.

Using the dashboard report menu

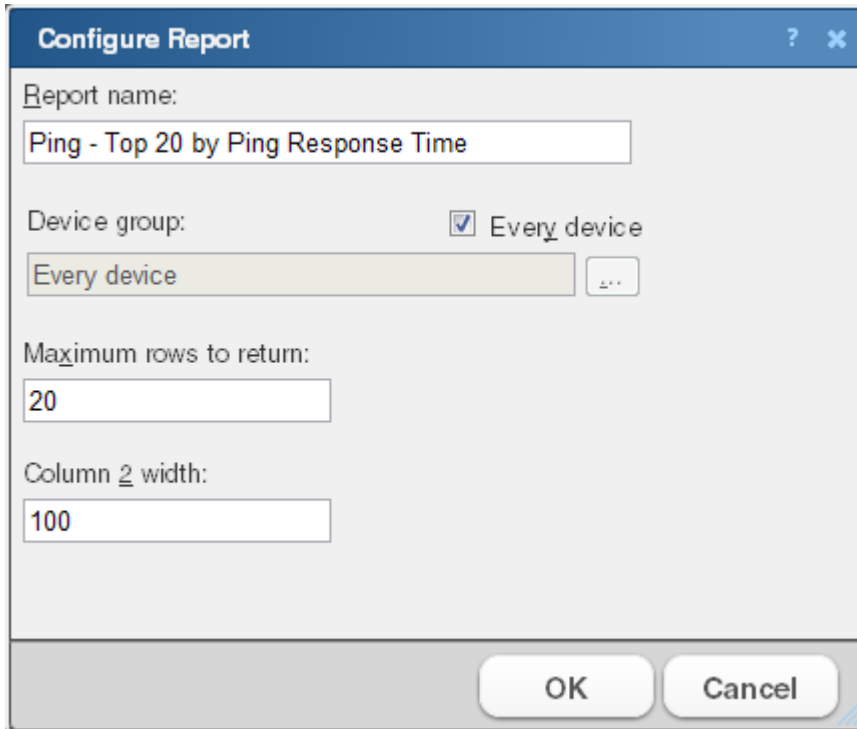
Each dashboard report has a menu on the right side of its title bar. From the Dashboard Report Menu, you can access help for a specific dashboard report, go to the configuration dialog for a report, or close the report. Closing a report removes it from the dashboard view. Keep in mind that after you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



Configuring a dashboard report

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

- Change the report title
- Select a device or device group for the report
- Set the height and width of the report
- Specify the width of certain report columns



The image shows a 'Configure Report' dialog box with a blue title bar containing a question mark and a close button. The dialog has a light gray background. It contains four input fields: 'Report name:' with the text 'Ping - Top 20 by Ping Response Time'; 'Device group:' with a checked checkbox and the text 'Every device', followed by a dropdown menu showing 'Every device' and a small square button; 'Maximum rows to return:' with the value '20'; and 'Column 2 width:' with the value '100'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Configure Report ? x

Report name:
Ping - Top 20 by Ping Response Time

Device group: ☒ Every device
Every device [button]

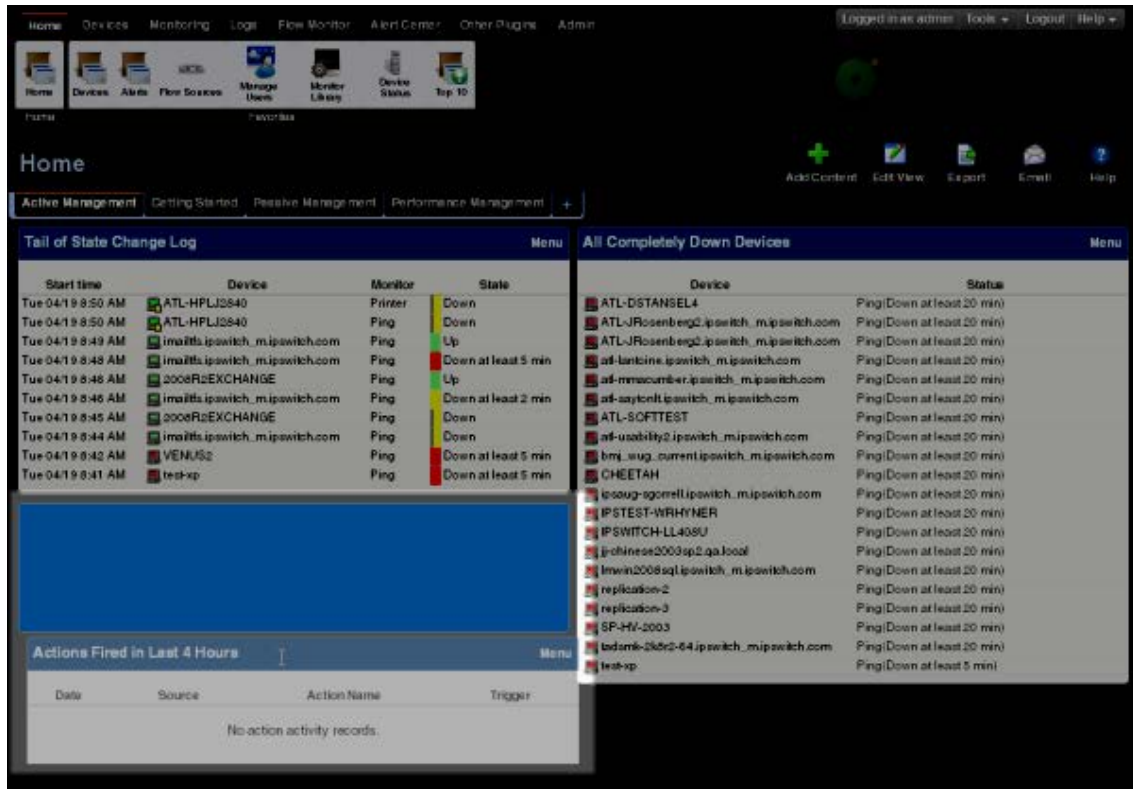
Maximum rows to return:
20

Column 2 width:
100

OK Cancel

Moving dashboard reports within a dashboard view

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

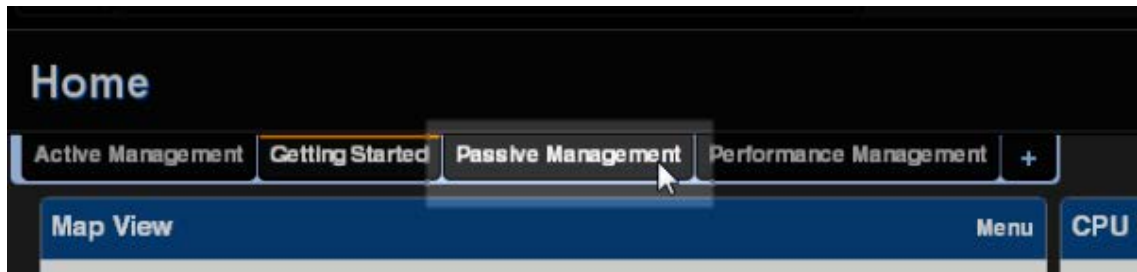


To move a dashboard report:

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

Navigating dashboard views

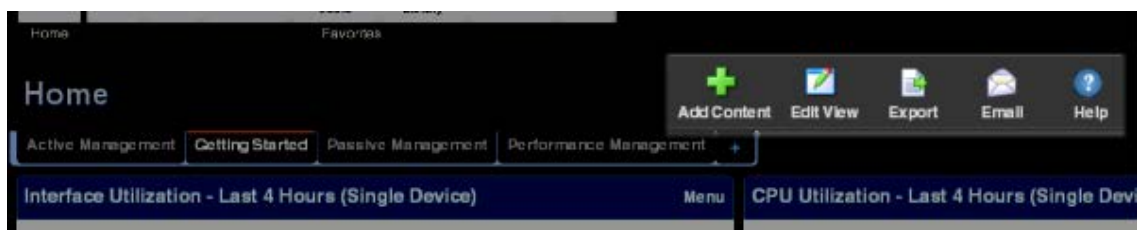
Navigate from one dashboard view to another by clicking the dashboard view tabs. You can also use the WhatsUp Gold toolbar to add content to a dashboard view, edit your dashboard and dashboard views, export and schedule report emails, and access the WhatsUp Gold help system.



The WhatsUp Gold Toolbar

Use the WhatsUp Gold toolbar to perform the following activities:

- **Add Content.** Open the Add Content pane and add reports to your dashboard view.
- **Edit View.** Edit your current dashboard view settings.
- **Export.** Export the currently displayed data to a file.
- **Email.** Email or schedule reports. For more information, see *Scheduling Reports* (on page 625).
- **Help.** View online help topics for the window you are currently viewing.



Types of dashboards

In This Chapter

| | |
|--------------------------------|-----|
| About types of dashboards..... | 352 |
| Home Dashboard | 353 |
| Device Status dashboard | 354 |
| Top 10 Dashboard..... | 356 |

About types of dashboards

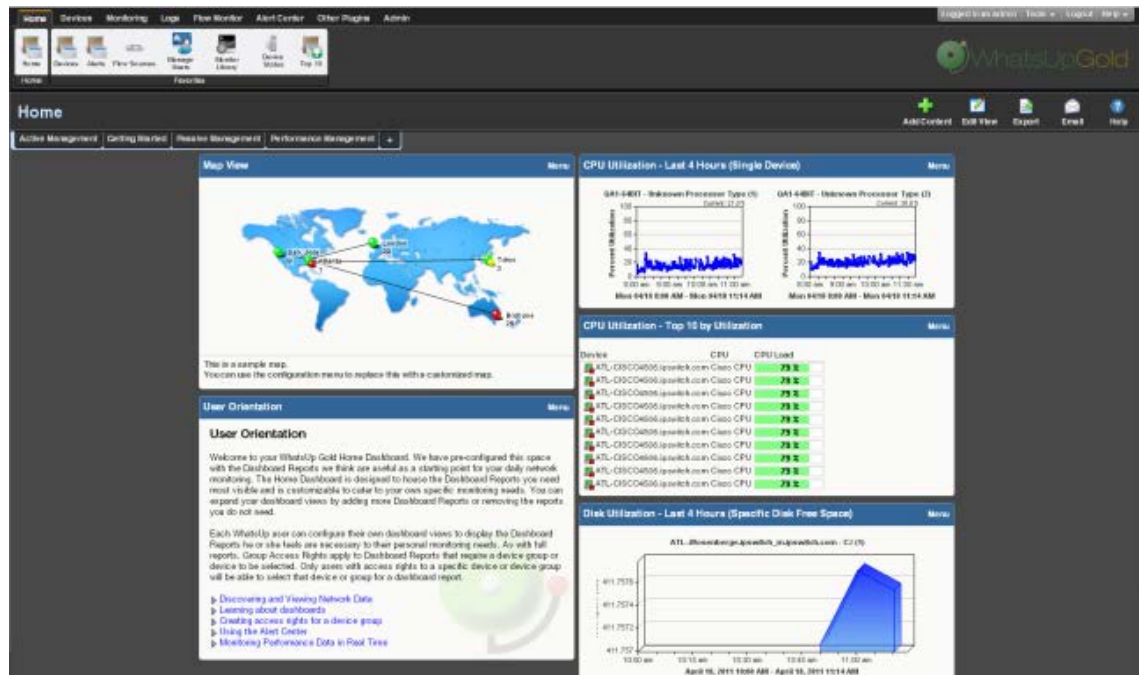
The WhatsUp Gold web interface includes three types of dashboards:

- *Home* (on page 353)
- *Device Status* (on page 354)
- *Top 10* (on page 356)

Each of the dashboard types supports multiple user-defined views. Up to 15 small reports known as *dashboard reports* can display within each view. These dashboard reports show content ranging from Current Interface and CPU Utilization to Syslog messages. As these reports are configurable on a per user basis, users can add content that is most relevant to their roles.

Home Dashboard

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



The Home Dashboard can display both Home- and Device-level dashboard reports. You can place any dashboard report on a Home dashboard; mixing and matching summary, group, and device-specific data.

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

The Home Dashboard includes these starter views:

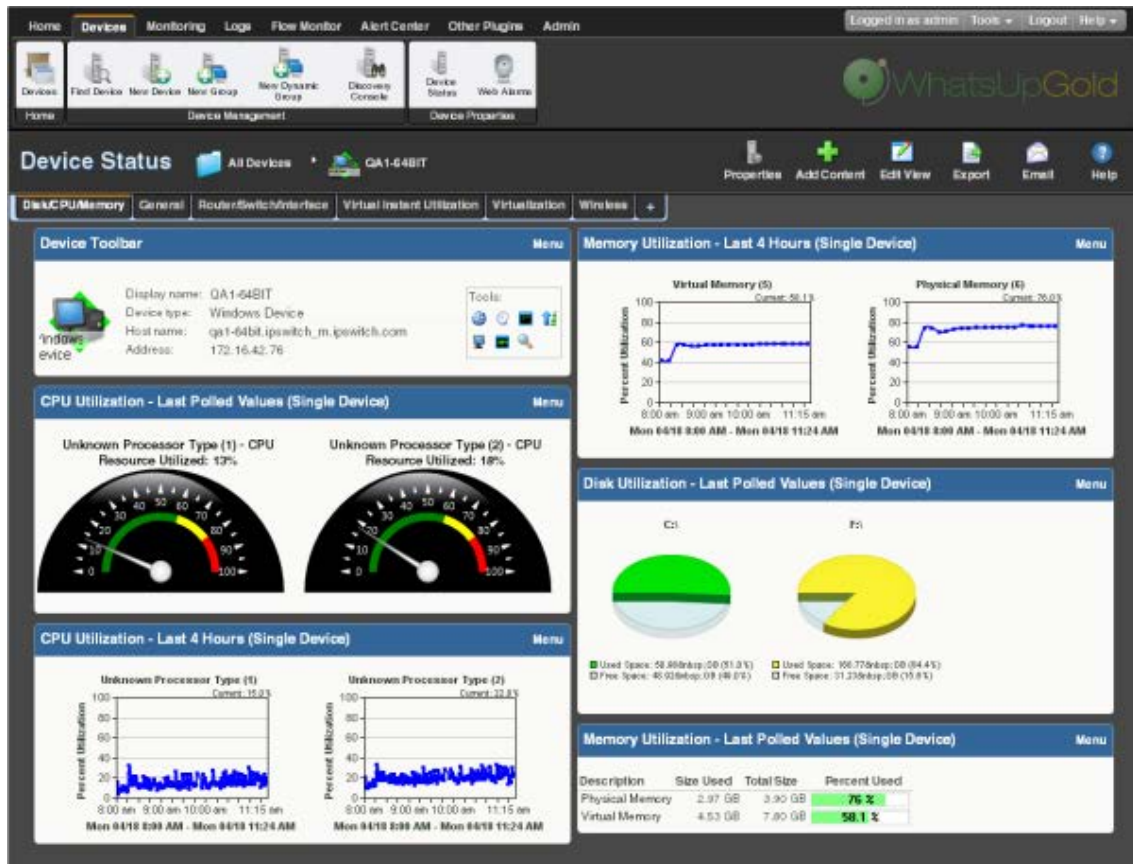
- Active Management
- Getting Started
- Passive Management
- Performance Management

Each dashboard view includes several default dashboard reports that you can decide to keep, alter, or remove. You can also add other dashboard reports to these views. For more information, see *Adding dashboard reports to a dashboard view* (on page 342).

You can create your own dashboard views for the Home dashboard through the *Manage Dashboard Views* (on page 868) dialog.

Device Status dashboard

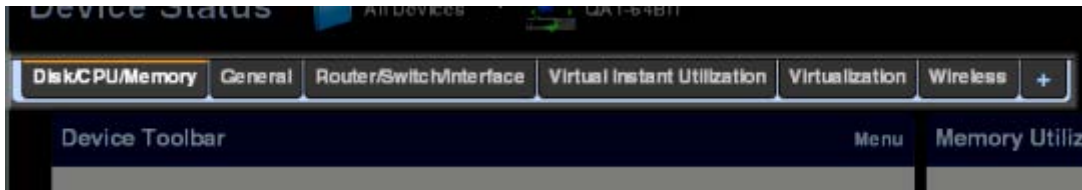
The Device Status dashboard is used to view information about a specific device. You can only add single device dashboard reports to the Device Status dashboard.



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

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

- Virtualization
- Wireless



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

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

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

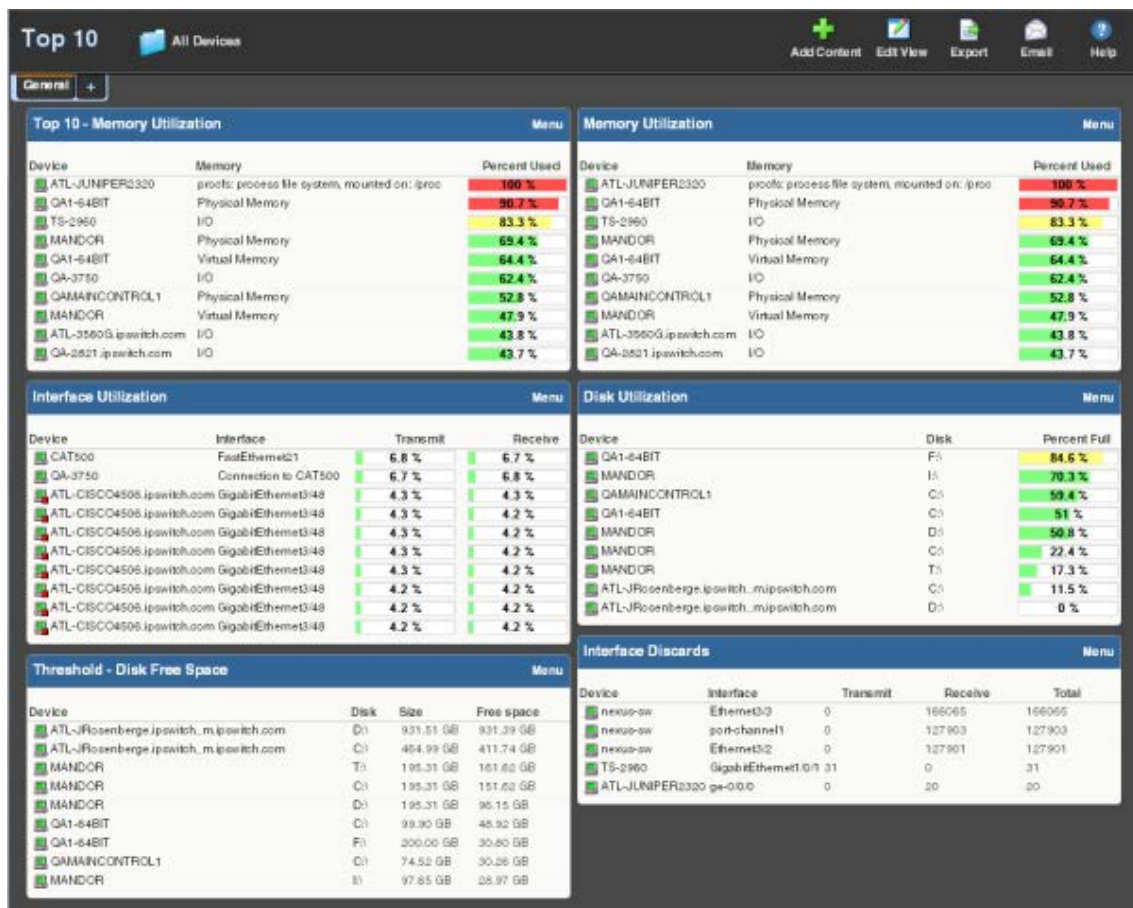


For more information, see *Adding dashboard reports to a dashboard* (on page 342).

Top 10 Dashboard

The WhatsUp Gold Top 10 dashboard displays Top 10 reports for your network devices. The Top 10 dashboard shows devices, at a glance, that may be potential problems and to provide information on the current health of your network devices. It is pre-configured to include reports that display data on the top network devices by:

- Interface Errors
- Interface Discards
- Interface Utilization
- Interface Traffic
- Ping Response Time
- Disk Utilization
- CPU Utilization
- Memory Utilization



You can add any of the *Top 10 reports* (on page 561) to the Top 10 dashboard.

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

- Add the reports you want to see here by clicking **Add Content**. For more information, see *Adding dashboard reports to a dashboard view* (on page 342).

- Change options for individual reports by clicking **Menu** > **Configure** for each report.
- Add additional views by clicking the +. Remove views by dragging them to the trash. For more information, see *Working with dashboard views* (on page 345).

The Top 10 dashboard also displays threshold reports. These reports let you set a threshold to filter out items that do not match a specified criteria. For example, the Interface Utilization Threshold report could have been used (in the example above) instead of the Interface Top 10 report, to filter out the interfaces that are not above 50% utilization. Using this approach, only interfaces with significant usage would be shown.

Thresholds

Report percentages are displayed in colors that represent the utilization thresholds:

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

Using Favorites

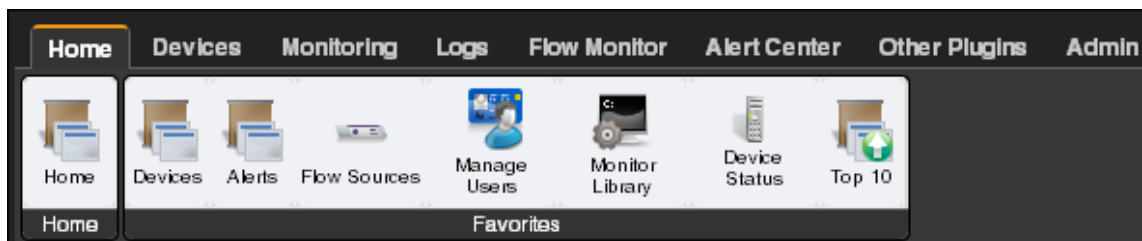
In This Chapter

| | |
|----------------------------------|-----|
| Using the Favorites toolbar..... | 612 |
| Adding Favorites..... | 612 |
| Editing Favorites | 614 |

Using the Favorites toolbar

WhatsUp Gold Favorites let you create your own customized toolbar by adding the WhatsUp Gold options you use most often to a single tab. You can edit and organize your favorites the way that best fits your needs. For more information, see *Adding Favorites* (on page 358).

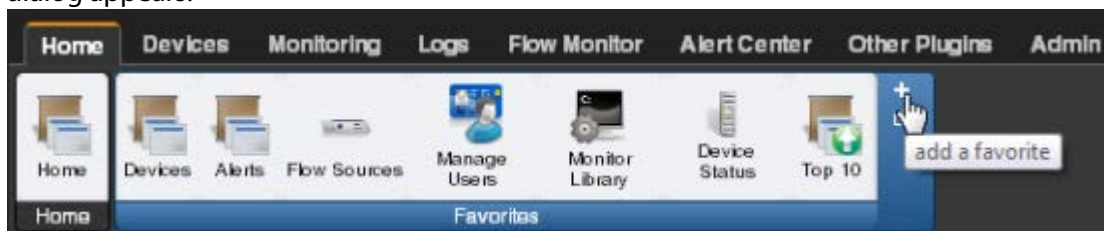
Access WhatsUp Gold Favorites by clicking the **Home** tab.



Adding Favorites

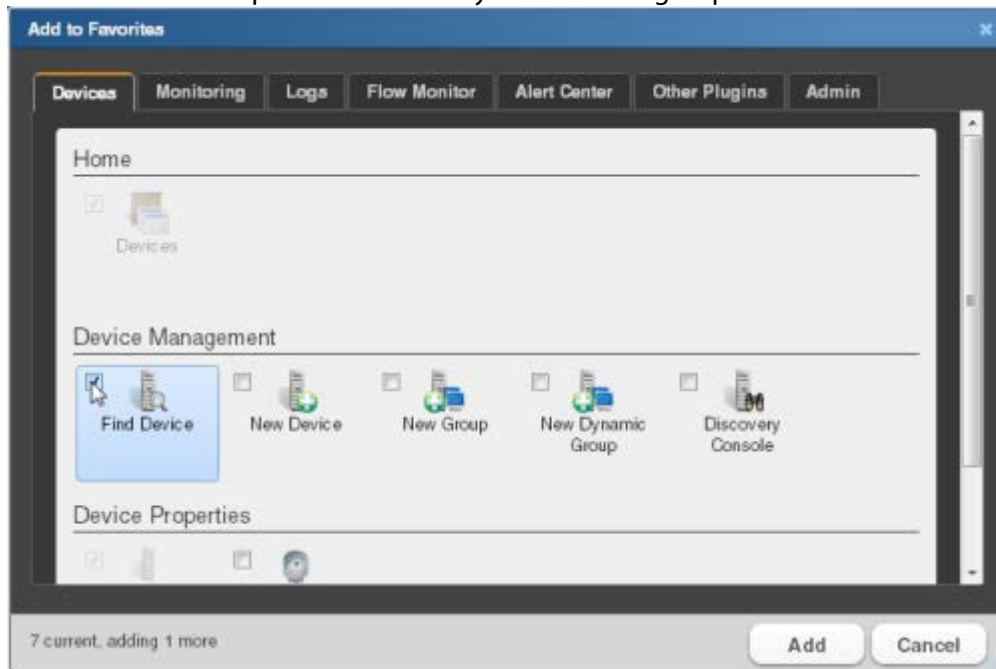
To add a favorite:

- 1 Click the **Home** tab.
- 2 Click the + (Add Favorites) to the right of the Favorites group. The Add to Favorites dialog appears.



- 3 From the dialog, select the tab containing the option you want to add. The buttons available on that tab appear in the pane.

- 4 Select the box to the left of each button you want to add to the Favorites group. A running total appears in the lower left of the pane as you select additional buttons to add. You can have up to 12 buttons in your Favorites group.



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

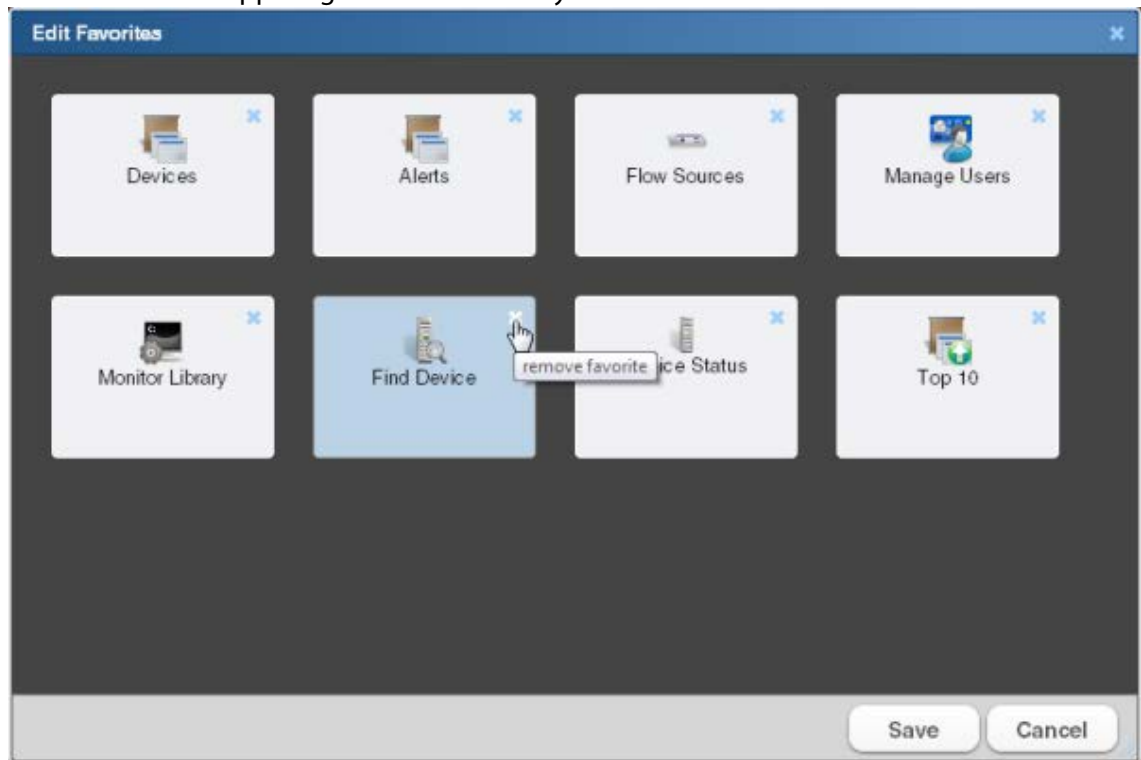
Editing Favorites

To remove buttons from your Favorites toolbar:

- 1 From the Home tab, click **Edit Favorites**. The Edit Favorites dialog appears.



- 2 Click the **X** at the upper right of each button you want to remove from the toolbar.



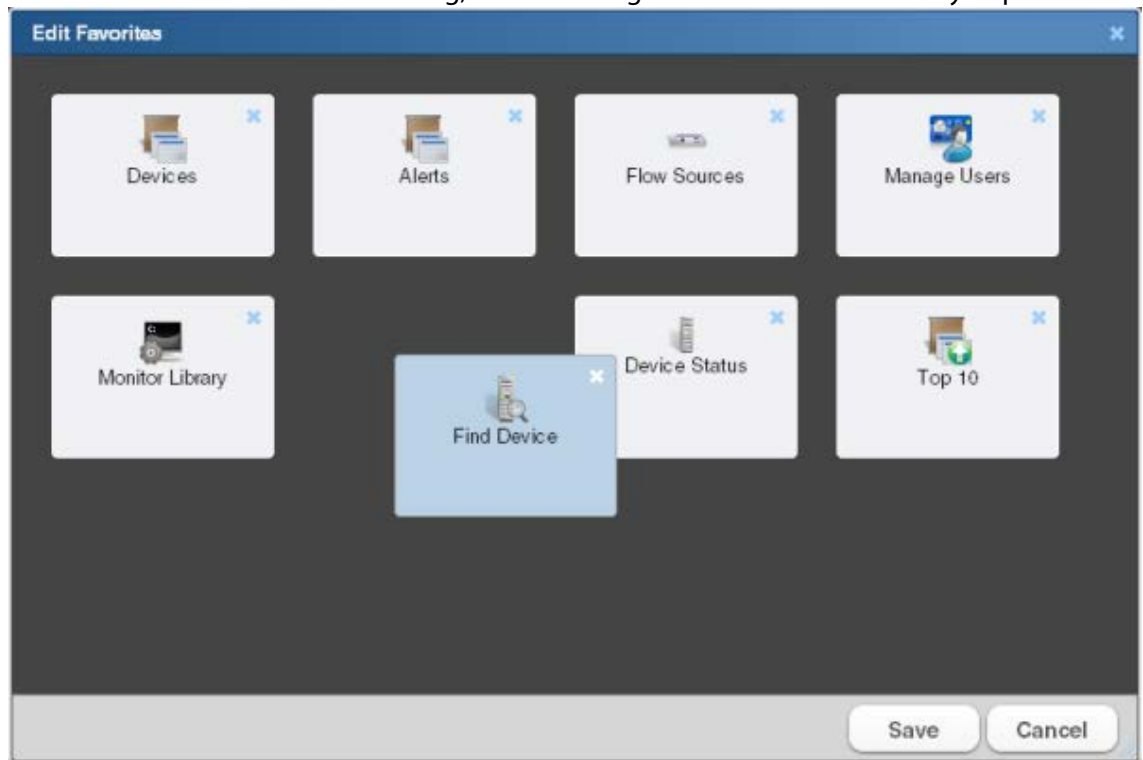
- 3 When you have deleted all of the buttons from the Favorites group that you want to remove, click **Save**. The buttons are removed from your Favorites toolbar.



Note: If you delete all of the buttons from the Favorites group, the WhatsUp Gold default Favorites appear in the group when you save.

To change the order of your Favorites:

- 1 From the Home tab, click **Edit Favorites**. The Edit Favorites dialog appears.
- 2 From within the Edit Favorites dialog, click and drag the buttons to the order you prefer.



- 3 When the buttons are in the preferred order, click **Save**. The dialog closes and the toolbar updates with the new button order.

Dashboard reports

In This Chapter

| | |
|---|-----|
| CPU Utilization reports | 363 |
| Custom Performance Monitor reports..... | 369 |
| Disk Utilization reports | 374 |
| Flow Monitor reports | 382 |
| General reports..... | 407 |
| Interface Errors and Discards reports | 423 |
| Interface Utilization reports | 431 |
| Inventory reports | 441 |
| Memory Utilization reports..... | 445 |
| Performance-Historic reports..... | 451 |
| Performance-Last Poll reports | 469 |
| Ping Availability and Response Time reports | 481 |
| Problem Areas reports | 489 |
| Problem Areas Specific Device | 501 |
| Remote/Central reports | 507 |
| Split Second Graph reports..... | 536 |
| Threshold reports | 552 |
| Top 10 reports..... | 561 |
| Virtualization reports..... | 570 |
| Wireless reports..... | 577 |
| ELM reports..... | 585 |
| Dashboard Report - Remote Site | 587 |
| Creating and modifying user accounts | 587 |
| Using the Remote/Central dashboard reports | 589 |

CPU Utilization reports

In This Chapter

| | |
|--|-----|
| CPU Utilization dashboard reports..... | 363 |
| CPU Utilization Last X hours/days (Single Device)..... | 364 |
| CPU Utilization Last X hours/days (Specific CPU)..... | 365 |
| Last Polled CPU Utilization (Specific CPU) | 365 |
| Last Polled CPU Utilization (Single Device) | 366 |
| Top 10: CPU Utilization | 367 |

CPU Utilization dashboard reports

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

| CPU Utilization dashboard reports | Type | Description |
|-----------------------------------|------|--|
| Last 30 days (specific CPU) | Home | Details CPU utilization percentages for a specific CPU for one device of the last 30 days. |

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

CPU Utilization Last X hours/days (Single Device)

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

CPU Utilization Last X hours/days (Specific CPU)

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

Last Polled CPU Utilization (Specific CPU)

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

There are five types of graphs to choose from:

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

Last Polled CPU Utilization (Single Device)

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

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

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the browse (...) button.
 - To view a graphical representation of the report data, select **Use a graph to display the values**.
 - If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types*. (on page 610)
- 3 Click **OK** to save changes.

Top 10: CPU Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Custom Performance Monitor reports

In This Chapter

| | |
|--|-----|
| Custom Performance Monitor dashboard reports | 369 |
| Custom Performance Monitor Values Last X hours/days (Single Device) | 370 |
| Custom Performance Monitor Values Last X hours/days (Specific Monitor) | 371 |
| Last Polled Custom Performance Monitor Values (Single Device) | 372 |
| Custom Performance Monitor Top 10 (Specific Monitor) | 372 |
| Threshold: Custom Performance Monitor | 373 |

Custom Performance Monitor dashboard reports

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

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

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

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

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

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

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

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

Last Polled Custom Performance Monitor Values (Single Device)

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

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

To configure this dashboard report in WhatsUp Gold:

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

Custom Performance Monitor Top 10 (Specific Monitor)

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

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

To configure this dashboard report in WhatsUp Gold:

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

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

Threshold: Custom Performance Monitor

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

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

Each entry in the report contains the following information:

Device. The monitored network device.

Value. The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

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

Disk Utilization reports

In This Chapter

| | |
|---|-----|
| Disk Utilization dashboard reports..... | 374 |
| Disk Utilization Last X hours/days (Single Device)..... | 375 |
| Disk Free Space Last X hours/days (Specific Disk) | 376 |
| Disk Utilization Last X hours/days (Specific Disk)..... | 376 |
| Disk Utilization Last Polled Value (Specific Disk)..... | 377 |
| Disk Utilization: Last Polled Values (Single Device)..... | 378 |
| Threshold: Disk Utilization | 379 |
| Threshold: Disk Free Space | 379 |
| Top 10: Disk Utilization | 380 |

Disk Utilization dashboard reports

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

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

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

Disk Utilization Last X hours/days (Single Device)

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

To configure this dashboard report:

- 1 On the dashboard report menu, click **Configure**.
- 2 Enter the appropriate information:
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the Browse (...) button.
 - **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - **Graph type.** Select the type of graph you would like the report to display.
 - **Trend type.** Select the type of trend you would like the report to use.
 - **Dimensions.** Select the dimension in which you would like the graph to display.
 - **Width.** Enter a width for the report (in pixels).
 - **Height.** Enter a height for the report (in pixels).

- **Vertical Axis Scaling.** Select either auto or fixed scale.
- **Min.** Enter a number for the lowest point on the Y-axis.
- **Max.** Enter a number for the highest point on the Y-axis.
- **Graph the maximum.** Select this option to graph the maximum.

3 Click **OK** to save changes.

Disk Free Space Last X hours/days (Specific Disk)

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

To configure this dashboard report in WhatsUp Gold:

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

Disk Utilization Last X hours/days (Specific Disk)

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

To configure this dashboard report in WhatsUp Gold:

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

Disk Utilization Last Polled Value (Specific Disk)

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

There are five types of graphs to choose from:

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

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

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

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Name**. Enter a title for the dashboard report.
 - **Device**. Choose a device by clicking on the Browse (...) button.
 - **Disk to graph**. Select a disk to graph for devices with more than one disk.
 - **Graph type**. Choose the type and size of the graph.
- 3 Click **OK** to save changes.

Disk Utilization: Last Polled Values (Single Device)

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

- If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- 3 Click **OK** to save changes.

Threshold: Disk Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Threshold: Disk Free Space

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

- **Red.** Above 90%

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Top 10: Disk Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

- 2 Enter or select appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Flow Monitor reports

In This Chapter

| | |
|---|-----|
| General Flow Monitor dashboard reports | 382 |
| Interface Troubleshooting dashboard reports | 385 |
| Interface Traffic dashboard reports | 393 |
| Interface Details dashboard reports | 395 |

General Flow Monitor dashboard reports

| General Flow Monitor dashboard reports | Type | Description |
|--|------|---|
| Source List | Home | Displays all enabled Flow Monitor sources. |
| Database Size | Home | Displays summary information about the Flow Monitor database. |
| Archive Database Size | Home | Displays summary information about the Flow Monitor archive database. |
| Source | Home | Displays detailed information for a selected Flow Monitor source. |
| Interface | Home | Displays detailed information for a selected Flow Monitor interface. |

Flow: Archive Database Size

This dashboard report displays summary information about the Flow Monitor archive database.

- **Database Edition.** The Flow Monitor database edition; can be Express, Standard, or Enterprise.
Express - SQL Server 2005 Express Edition
Standard - SQL Server 2005 Standard Edition
Enterprise - SQL Server 2005 Enterprise Edition
- **Current Size.** The amount of archive database space currently in use.
- **Max Size.** The maximum size of the archive database.
- **Unused Space.** The amount of archive database space currently not in use.



Note: Graphs will only show for Microsoft SQL Server Express Editions, as other editions of Microsoft SQL Server have no size limitations. When the full Microsoft SQL Server database is used, N/A appears in this column because the dbase size is not limited.

- **Percent Used.** The percentage of database space currently in use.



Note: Graphs will only show for Microsoft SQL Server Express Editions, as other editions of Microsoft SQL Server have no size limitations. When the full Microsoft SQL Server database is used, N/A appears in this column because the dbase size is not limited.

For more information

Configuring this dashboard report

Flow: Database Size

This dashboard report displays summary information about the Flow Monitor database.

- **Database Edition.** The Flow Monitor database edition; can be Express, Standard, or Enterprise.
Express - SQL Server 2005 Express Edition
Standard - SQL Server 2005 Standard Edition
Enterprise - SQL Server 2005 Enterprise Edition
- **Current Size.** The amount of database space currently in use.
- **Max Size.** The maximum size of the database.
- **Unused Space.** The amount of database space currently not in use.



Note: Graphs will only show for Microsoft SQL Server Express Editions, as other editions of Microsoft SQL Server have no size limitations. When the full Microsoft SQL Server database is used, N/A appears in this column because the database size is not limited.

- **Percent Used.** The percentage of database space currently in use.



Note: Graphs will only show for Microsoft SQL Server Express Editions, as other editions of Microsoft SQL Server have no size limitations. When the full Microsoft SQL Server database is used, N/A appears in this column because the database size is not limited.

For more information

Configuring this dashboard report

Flow: Flow Interface

This dashboard report displays detailed information for a selected Flow Monitor source. The data displayed in this dashboard report is current to the last half-hour.

The Interface Traffic report for the last half-hour is displayed at the top of the interface's details.

- **Last active.** The last time traffic transmitted over the interface.
- **Interface type.** The type of interface; for example, Ethernet CSMA/CD.
- **In speed.** The speed (in bytes) at which data is flowing to the interface.
- **Out speed.** The speed (in bytes) at which data is flowing from the interface.
- **Status.** The status of the interface; either Up, Down, or Unknown.

Click the **Interface** name at the top of the report to view its Flow Monitor Interface Details report.

For more information

Configuring this dashboard report

Flow: Flow Source

This dashboard report displays detailed information for a selected Flow Monitor source. The data displayed in this dashboard report is current to the last half-hour.

- **IP address.** The source router's IP address.
- **NetFlow version.** The version of NetFlow supported by the router.
- **Packets received.** The number of packets received by the router over the last half-hour.
- **Packets lost.** The number of packets lost by the router over the last half-hour.
- **Reliability.** The percentage of packets received by the router of the last half-hour.
- **Flow rate.** The number of flows per second (fps) occurring over the router for the last half-hour.
- **Last active.** The last time traffic transmitted over the router.
- **Flow traffic status.** Whether Flow Monitor is receiving traffic from the router; either receiving, or not receiving.

A list of the source interfaces are listed at the bottom of the dashboard report. Click an **Interface** name to view the Flow Monitor Interface Details report for that interface.

For more information

Configuring this dashboard report

Flow: Source List

This dashboard report lists all of the enabled Flow sources. Click an interface to drill down into reports specific to the interface.

- **Flow Sources.** Routers and interfaces enabled for Flow data collection are listed in this column. Routers are listed by IP address and display name; interfaces are listed below routers. The sources listed in this dashboard report are configured on the Flow Sources dialog.



Note: Interfaces can be hidden; if you don't see an interface listed on this dashboard report, check to see if it has been hidden via the Flow Interface dialog.

- **In Traffic.** Interface inbound traffic is reported as a percentage of usage according to the interface's speed, and as the number of inbound bytes per second.
- **Out Traffic.** Interface outbound traffic is reported as a percentage of usage according to the interface's speed, and as the number of outbound bytes per second.

The report displays the number of overall flows per minute for each router.



Note: The traffic data displayed in this dashboard report is for the last half-hour.

For more information

Configuring this dashboard report

Interface Troubleshooting dashboard reports

Interface Troubleshooting dashboard reports

| | Type | Description |
|---|------|---|
| Top Senders with Most Conversation Partners | Home | Displays the senders with the most conversation partners in the selected direction on the selected interface |
| Top Receivers with the most conversation partners | Home | Displays the devices receiving the most traffic from the highest number of other devices in the selected direction on the selected interface. |
| Top Senders with the Most Failed Connections | Home | Displays the devices that initiated the highest number of unsuccessful TCP connection attempts, or SYN packets, in the selected direction on the selected interface. |
| Top Receivers with the Most Failed Connections | Home | Displays the devices to which the greatest number of other devices have failed to connect. This dashboard report shows only connection attempts, or SYN packets, sent in the selected |

**Interface Troubleshooting
dashboard reports**

| | Type | Description |
|--------------------------|------|---|
| ICMP Types | Home | direction on the selected interface. Displays a summary graph of the top Internet Control Message Protocol (ICMP) errors occurring on the selected interface during the time period selected for the Interface Details report. |
| Packet Size Distribution | Home | Displays a bar chart where each bar represents the percentage of packets that fall within a given size range in bytes. |

Flow Monitor: Top Senders with Most Conversation Partners

This dashboard report displays the senders with the most conversation partners in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce) on the selected interface. A conversation is a connection between two devices that are transmitting information to one another over a single port. Conversation partner data is useful in determining the devices on and off the network that are sending the most information to other devices and/or Web sites. Also, a device with too many conversation partners could be using unauthorized peer-to-peer applications.

By default, devices are listed by hostname, however you can configure this report to list the devices by IP address by selecting **Display IP Address instead of Hostname** on the report configuration dialog.

- **Sender.** Displays the host name of the top sender with the most conversation partners.
- **Number of Partners.** Displays the number of conversation partners with which the sender has connected.
- **Percent of Top n.** Displays the percentage ranking of the item within the top n items of the category.



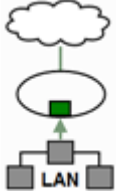
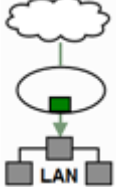
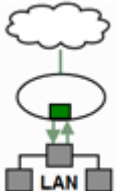
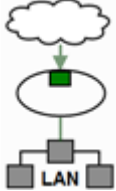
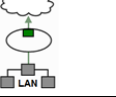
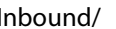
Tip: You can hover over a host name to display popup information about the host name's IP address. If you right-click on the host-name, a filter will be created that uses the host as the filter criteria and the Interface Details dashboard will reload with this filter applied.

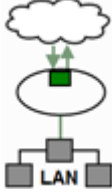
For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| Internal interface | Inbound  | The devices on the LAN segment connected to the selected internal interface sending information to the most conversation partners/outside devices. |
| | Outbound  | The outside devices sending information to the most conversation partners/devices on the LAN segment connected to the selected internal interface. |
| | Inbound/ Outbound  | The devices sending the most information across the selected internal interface. |
| External interface | Inbound  | The devices connected to the selected external interface sending information to the most conversation partners/ devices on an internal LAN segment. |
| | Outbound  | The devices on internal LAN segments sending information to the most conversation partners/devices connected to the selected external interface. |
| | Inbound/ Outbound  | The devices sending the most information across the selected |

| Interface | Traffic Direction | Report displays... |
|-----------|---|---------------------|
| | Outbound  | external interface. |

Linking to Flow Monitor reports from WhatsUp Gold

Configuring this dashboard report

Flow Monitor: Top Senders

This dashboard report shows the devices generating the most traffic traveling in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce) on the selected interface.

You can choose to display and sort sender traffic by bytes, packets, or flows using the **Display and sort by** option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.

By default, devices are listed by hostname, however you can configure this report to list the devices by IP address by selecting **Display IP Address instead of Hostname** on the report configuration dialog.

- **Sender.** Displays the hosts that are the top senders on the interface.
- You can select one of the following units to display and sort the specific items in the report using the **Display and sort by** option on the report configuration dialog. The selected option will appear as the first column header in the report and will be used to sort the top "n" items.
- **Bytes.** Displays the total number of bytes transmitted for the specific item in the report category for the selected date range.
- **Packets.** Displays the total number of packets for the specific item in the report category for the selected date range.
- **Flows.** Displays the total number of flows for the specific item in the report category for the selected date range.
- **Rate.** Displays the average bit rate, packet rate or flow rate, in multiples of the selected unit (e.g. Kbps, Mbps, or Gbps) for the specific item in the report category for the selected date range.
- **Utilization.** Displays the percentage of the total available bandwidth used by the specific item in the report category for the selected date range.



Note: Utilization is displayed as N/A if a speed is not specified for the interface, or if you have selected to display packets or flows in the report. If you are displaying bytes, you can set the interface speed on the Flow Interface dialog. To navigate to the Flow Interface dialog, right-click on the interface and then click **Configure > Source > Edit**.

- **Percentage.** Displays the percentage of the total traffic for the specific item in the report category for the selected date range.
- **Others (row title).** The optional **Others** row title displays a summation of all of the unspecified items of the report category. The unspecified items are those items not specifically displayed in the top "n" items. The **Others** row provides a comparison between the specified items, or top "n" items selected for display, and the rest of the traffic on the interface. When displayed, the Others row will provide perspective as to the relative size of the specified items in comparison to the total traffic on the interface.
- **Totals (row title).** Displays the total of all of the items in the report category, specified and unspecified (**Others**). This row shows the interface totals for each column in the report.



Tip: You can hover over a host name to display popup information about the host name's IP address. If you right-click on the host-name, a filter will be created that uses the host as the filter criteria and the Interface Details dashboard will reload with this filter applied.



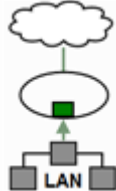
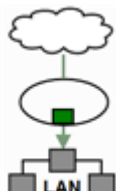
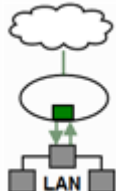
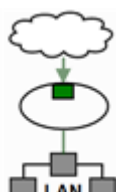

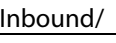
Tip: You can hover over information in the **Bytes** column to display popup information with average data speed as a percentage of the total interface capacity.

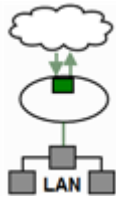
For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|--|
| Internal interface | Inbound  | The top senders among devices on the LAN segment connected to the selected internal interface that are communicating with outside devices. |
| | Outbound  | The top senders among outside devices that are communicating with devices on the LAN segment connected to the selected internal interface. |
| | Inbound/ Outbound  | The top senders among all devices that are transmitting traffic across the selected internal interface. |
| External interface | Inbound  | The top senders among devices connected to the selected external interface that are communicating with devices on an internal LAN segment. |
| | Outbound  | The top senders among devices on internal LAN segments that are communicating with devices connected to the selected external interface. |
| | Inbound/ Outbound  | The top senders among all devices that are transmitting traffic |

| Interface | Traffic Direction | Report displays... |
|-----------|---|---|
| | Outbound  | across the selected external interface. |

Flow Monitor: Top Senders with Most Failed Connections

This dashboard report displays the devices that initiated the highest number of unsuccessful TCP connection attempts, or SYN packets, in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce) on the selected interface.

Essentially, the listed host has tried to establish a TCP connection to another device but has not succeeded. Devices listed in this report may be conducting port scanning--a practice used by hackers to find potential intrusion points on a network.

By default, devices are listed by hostname, however you can configure this report to list the devices by IP address by selecting **Display IP Address instead of Hostname** on the report configuration dialog.

- **Sender.** Displays the host name of the top sender with the most failed connections.
- **Connection Attempts.** Displays the number of failed connection attempts.
- **Percent of Top n.** Displays the percentage ranking of the item with the top n items of the category.



Tip: You can hover over a hostname to display popup information about the host name's IP address. If you right-click the hostname, a filter is created that uses the host as the filter criteria and the Interface Details dashboard reloads with this filter applied.



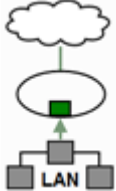
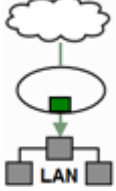
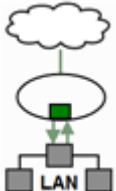
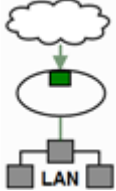
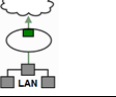

Note: WhatsUp Gold Flow Monitor can only find failed connections on sources that are not sending sampled data.


For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| Internal interface | Inbound  | The devices on the LAN segment connected to the selected internal interface the most failed attempts to send information to outside devices. |
| | Outbound  | The outside devices with the most failed attempts to send information to devices on the LAN segment connected to the selected internal interface. |
| | Inbound/ Outbound  | The devices with the most failed communication attempts across the selected internal interface. |
| External interface | Inbound  | The devices connected to the selected external interface with the most failed attempts to send information to devices on an internal LAN segment. |
| | Outbound  | The devices on internal LAN segments with the most failed attempts to send information to devices connected to the selected external interface. |
| | Inbound/  | The devices with the most failed communication attempts |

| Interface | Traffic Direction | Report displays... |
|-----------|---|---|
| | Outbound  | across the selected external interface. |

Interface Traffic dashboard reports

Interface Traffic dashboard reports

| | Type | Description |
|--------------------------------|------|--|
| Interface Traffic | Home | Displays the incoming and outgoing traffic transmitted over the selected interface for the chosen time period. |
| Incoming Interface Traffic | Home | Displays the percentage of the total inbound traffic on an interface that is leaving through each of the output interfaces. |
| Outgoing Interface Traffic | Home | Displays the percentage of the total outbound traffic through an interface, that entered through each of the input interfaces. |
| Incoming Interface Utilization | Home | Displays a graph of the selected interface's incoming traffic as a percentage of available bandwidth for the chosen time period. |
| Outgoing Interface Utilization | Home | Displays a graph of the outgoing utilization on selected interface for the chosen time period. |

Flow: Incoming Interface Traffic

The Incoming Interface Traffic dashboard report displays the percentage of the total inbound traffic on an interface that is leaving through each of the output interfaces.

Occasionally a misconfiguration can cause a device to send traffic back through the interface where it was received. In Flow Monitor, this is called Bounce traffic. Flow Monitor alerts you to this abnormal traffic pattern by displaying a flag next to the interface(s) where the error is occurring.

Below the chart, a table is provided that includes the number of bytes, packets and flows for each output interface, as well as the percentage of the total inbound traffic leaving through that interface.

Flow: Incoming Interface Utilization

This dashboard report displays a graph of the selected interface's incoming traffic as a percentage of available bandwidth for the chosen time period.



Tip: If you experience an unusually low interface utilization, this could be because you have Flow Monitor collecting on a router which is not the network bottleneck. Changing the interface speed on the Flow Sources dialog will give a more accurate reading of its utilization.

Flow: Interface Traffic

This dashboard report shows the incoming and outgoing traffic transmitted over the selected interface for the chosen time period.

Interface traffic is graphed in bytes over time. The 95th percentile for both inbound and outbound interface traffic is graphed for the chosen time period.

You can easily lower the time graph scale on the configuration dialog to see the lower level traffic that is more difficult to see at the default scale setting.

You can choose to display and sort sender traffic by bytes, packets, or flows using the Display and sort by option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.



Tip: You can hover over information in the **Bytes** column to display popup information with average data speed as a percentage of the total interface capacity.

Click the interface name at the top of this dashboard report to view the Flow Monitor Interface Overview report for the selected interface.

Flow: Outgoing Interface Traffic

The Outgoing Interface Traffic dashboard report displays the percentage of the total outbound traffic through an interface, that entered through each of the input interfaces.

Occasionally a misconfiguration can cause a device to receive traffic it has just sent. Flow Monitor alerts you to this abnormal traffic pattern by displaying a flag next to the interface(s) where the error is occurring.

Below the chart, a table is provided that includes the number of bytes, packets and flows for each input interface, as well as the percentage of the total outbound traffic that is coming into that interface.

Flow: Outgoing Interface Utilization

This Flow Monitor dashboard report displays a graph of the outgoing utilization on selected interface for the chosen time period.

Outbound interface utilization is graphed by percentage over time.



Tip: If you experience an unusually low interface utilization, this could be because you have Flow Monitor collecting on a router which is not the network bottleneck. Changing the interface speed on the Flow Sources dialog will give a more accurate reading of its utilization.

Interface Details dashboard reports

Interface Details dashboard reports

| | Type | Description |
|--------------------------------------|------|---|
| Top Protocols | Home | Displays the transport layer protocols (TCP, UDP, ICMP, etc.) used the most, traveling in the selected direction on the selected interface. |
| Top Applications | Home | Displays the applications used by devices generating the most traffic traveling in the selected direction on the selected interface. |
| Top Senders | Home | Displays the devices generating the most traffic traveling in the selected direction on the selected interface. |
| Top Receivers | Home | Displays the devices receiving the most traffic traveling in the selected direction on the selected interface. |
| Top Sender/Receiver Domains | Home | Displays the top domains whose devices are generating traffic/to which traffic is routed over the selected interface in the selected direction. |
| Top Sender/Receiver Countries | Home | Displays the geographic locations of the devices sending/receiving the most traffic traveling in the selected direction on the selected interface. |
| Top Sender/Receiver Groups | Home | Displays the sender/receiver groups generating the most traffic traveling in the selected direction on the selected interface. |
| Top Sender/Receiver TLD | Home | Displays the top level domains (the last portion of an Internet domain name, such as .com, .edu, or .us) whose devices are generating traffic/to which traffic is routed over the selected interface in the selected direction. |
| Top Types of Service | Home | Displays the top Quality of Service (QoS) types that are generating the most traffic traveling in the selected direction on the selected interface. |
| Top Conversations | Home | Displays the conversations between devices generating the most traffic traveling in the selected direction on the selected interface. |
| Top NBAR Applications - Flow Details | Home | Displays the top applications as identified using Cisco's NBAR classification engine. |
| Top Ports | Home | Displays the top ports to which traffic is routed on the selected interface in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce). |

Flow Monitor: Top Sender Domains

This dashboard report displays the top domains whose devices are generating traffic that is routed over the selected interface in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce). The traffic displayed for each domain is the sum of the traffic generated by each device on that domain.



Note: The domains listed in this dashboard report are obtained from the last two parts of a host name.

Domain data is useful in determining where the persons on a network are spending the most time. If you see a domain that isn't network-friendly, you can drill down by adding a filter for the domain and detect the device or devices visiting the suspect Web location.

You can choose to display and sort sender traffic by bytes, packets, or flows using the **Display and sort by** option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.

- **Receiver.** Displays the hosts that are the top receivers on the interface.
- **Sender Domain.** Displays the top sender domain.
- You can select one of the following units to display and sort the specific items in the report using the **Display and sort by** option on the report configuration dialog. The selected option will appear as the first column header in the report and will be used to sort the top "n" items.
- **Bytes.** Displays the total number of bytes transmitted for the specific item in the report category for the selected date range.
- **Packets.** Displays the total number of packets for the specific item in the report category for the selected date range.
- **Flows.** Displays the total number of flows for the specific item in the report category for the selected date range.
- **Rate.** Displays the average bit rate, packet rate or flow rate, in multiples of the selected unit (e.g. Kbps, Mbps, or Gbps) for the specific item in the report category for the selected date range.
- **Utilization.** Displays the percentage of the total available bandwidth used by the specific item in the report category for the selected date range.



Note: Utilization is displayed as N/A if a speed is not specified for the interface, or if you have selected to display packets or flows in the report. If you are displaying bytes, you can set the interface speed on the Flow Interface dialog. To navigate to the Flow Interface dialog, right-click on the interface and then click **Configure > Source > Edit**.

- **Percentage.** Displays the percentage of the total traffic for the specific item in the report category for the selected date range.
- **Others (row title).** The optional **Others** row title displays a summation of all of the unspecified items of the report category. The unspecified items are those items not specifically displayed in the top "n" items. The **Others** row provides a comparison between the specified items, or top "n" items selected for display, and the rest of the traffic on the interface. When displayed, the Others row will provide perspective as to the relative size of the specified items in comparison to the total traffic on the interface.
- **Totals (row title).** Displays the total of all of the items in the report category, specified and unspecified (**Others**). This row shows the interface totals for each column in the report.



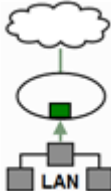
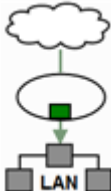
Tip: You can hover over information in the **Bytes** column to display popup information with average data speed as a percentage of the total interface capacity.

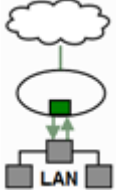
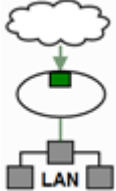
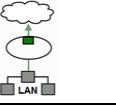
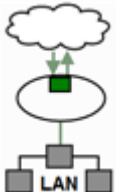
For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| Internal interface | Inbound  | The top domains used by devices on the LAN segment connected to the selected internal interface to send information to outside devices. |
| | Outbound  | The top domains used by outside devices to send information to the devices on the LAN segment connected to the selected internal interface. |
| | Inbound/ Outbound | The top domains used by all devices transferring information across the selected internal interface. |

| Interface | Traffic Direction | Report displays... |
|--------------------|--|---|
| |  | |
| External interface | Inbound  | The top domains used by devices connected to the selected external interface to send information to devices on an internal LAN segment. |
| | Outbound  | The top domains used by devices on internal LAN segments to send information to devices connected to the selected external interface. |
| | Inbound/ Outbound  | The top domains used by all devices sending information across the selected external interface. |

Linking to Flow Monitor reports from WhatsUp Gold

Configuring this dashboard report

Flow Monitor: Top Sender Groups

This dashboard report shows the sender groups generating the most traffic traveling in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce) on the selected interface. Sending Group data is useful in determining which groups on the network are using the most bandwidth by sending the most information.

Groups are user defined sets of hosts that allow customized reporting and are configured via the Flow Groups dialog. (**Configure > Flow Groups**).

You can choose to display and sort sender traffic by bytes, packets, or flows using the **Display and sort by** option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.

- **Sender Group.** The group name, used to represent a user defined set of hosts.
- You can select one of the following units to display and sort the specific items in the report using the **Display and sort by** option on the report configuration dialog. The selected option will appear as the first column header in the report and will be used to sort the top "n" items.
- **Bytes.** Displays the total number of bytes transmitted for the specific item in the report category for the selected date range.
- **Packets.** Displays the total number of packets for the specific item in the report category for the selected date range.
- **Flows.** Displays the total number of flows for the specific item in the report category for the selected date range.
- **Rate.** Displays the average bit rate, packet rate or flow rate, in multiples of the selected unit (e.g. Kbps, Mbps, or Gbps) for the specific item in the report category for the selected date range.
- **Utilization.** Displays the percentage of the total available bandwidth used by the specific item in the report category for the selected date range.



Note: Utilization is displayed as N/A if a speed is not specified for the interface, or if you have selected to display packets or flows in the report. If you are displaying bytes, you can set the interface speed on the Flow Interface dialog. To navigate to the Flow Interface dialog, right-click on the interface and then click **Configure > Source > Edit**.

- **Percentage.** Displays the percentage of the total traffic for the specific item in the report category for the selected date range.
- **Others (row title).** The optional **Others** row title displays a summation of all of the unspecified items of the report category. The unspecified items are those items not specifically displayed in the top "n" items. The **Others** row provides a comparison between the specified items, or top "n" items selected for display, and the rest of the traffic on the interface. When displayed, the Others row will provide perspective as to the relative size of the specified items in comparison to the total traffic on the interface.
- **Totals (row title).** Displays the total of all of the items in the report category, specified and unspecified (**Others**). This row shows the interface totals for each column in the report.



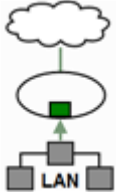
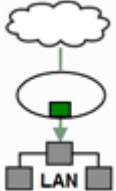
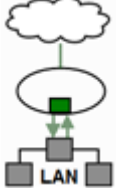
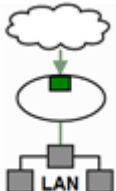
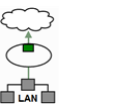
Tip: You can hover over information in the **Bytes** column to display popup information with average data speed as a percentage of the total interface capacity.

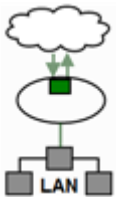
For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| Internal interface | Inbound  | The top groups used by devices on the LAN segment connected to the selected internal interface to communicate with outside devices. |
| | Outbound  | The top groups used by outside devices to communicate with devices on the LAN segment connected to the selected internal interface. |
| | Inbound/ Outbound  | The top groups used by all devices transmitting traffic across the selected internal interface. |
| External interface | Inbound  | The top groups used by devices connected to the selected external interface to communicate with devices on an internal LAN segment. |
| | Outbound  | The top groups used by devices on internal LAN segments to communicate with devices connected to the selected external interface. |
| | Inbound/ Outbound | The top groups used by all devices transmitting traffic across the selected external interface. |

| Interface | Traffic Direction | Report displays... |
|-----------|---|--------------------|
| |  | |

Flow Monitor: Top Sender TLD

This dashboard report displays the top level domains (the last portion of an Internet domain name, such as .com, .edu, or .us) whose devices are generating traffic that is routed over the selected interface in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce). The traffic displayed for each TLD is the sum of the traffic generated by each device on that TLD.

In most cases, the TLD for a device is the same as the country that is listed in the Top Sender and Receiver Countries dashboard reports. However, in the case of the TLD, the country is where the domain name was obtained, and not necessarily where the host is located.

Sender TLD traffic is reported by type in bytes and as a percentage of the top x results from the current interface for the selected time period.



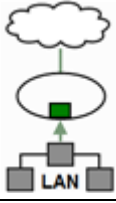
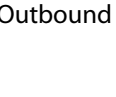
Tip: You can hover over information in the **Bytes** column to display popup information with average data speed as a percentage of the total interface capacity.

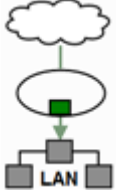
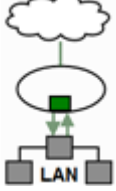
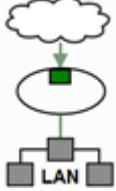
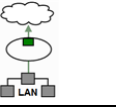
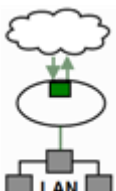
For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| Internal interface | Inbound  | The top domain types used by devices on the LAN segment connected to the selected internal interface that are receiving traffic from outside devices. |
| | Outbound  | The top domain types used by outside devices that are receiving traffic from devices on the LAN segment connected to the selected internal interface. |

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| |  | |
| | Inbound/ Outbound  | The top domain types used by all devices transferring traffic across the selected internal interface. |
| External interface | Inbound  | The top domain types used by devices connected to the selected external interface that are receiving traffic from devices on an internal LAN segment. |
| | Outbound  | The top domain types used by devices on internal LAN segments that are receiving traffic from devices connected to the selected external interface. |
| | Inbound/ Outbound  | The top domain types used by all devices transmitting traffic across the selected external interface. |

Flow: Top Types of Service

This dashboard report displays the top Type of Services (ToS) based on traffic traveling in the selected direction (Inbound, Outbound, Inbound and Outbound, or Bounce) on the selected interface. ToS are used by routers to prioritize the traffic that is transmitted over a router. For instance, VoIP data may be given a higher ToS than general network use to ensure that the quality of the VoIP audio is not degraded by high network utilization.

You can choose to display and sort sender traffic by bytes, packets, or flows using the **Display and sort by** option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.

- **Type of Service.** Displays the ToS differentiated services code point (DSCP).
- You can select one of the following units to display and sort the specific items in the report using the **Display and sort by** option on the report configuration dialog. The selected option will appear as the first column header in the report and will be used to sort the top "n" items.
- **Bytes.** Displays the total number of bytes transmitted for the specific item in the report category for the selected date range.
- **Packets.** Displays the total number of packets for the specific item in the report category for the selected date range.
- **Flows.** Displays the total number of flows for the specific item in the report category for the selected date range.
- **Rate.** Displays the average bit rate, packet rate or flow rate, in multiples of the selected unit (e.g. Kbps, Mbps, or Gbps) for the specific item in the report category for the selected date range.
- **Utilization.** Displays the percentage of the total available bandwidth used by the specific item in the report category for the selected date range.



Note: Utilization is displayed as N/A if a speed is not specified for the interface, or if you have selected to display packets or flows in the report. If you are displaying bytes, you can set the interface speed on the Flow Interface dialog. To navigate to the Flow Interface dialog, right-click on the interface and then click **Configure > Source > Edit**.

- **Percentage.** Displays the percentage of the total traffic for the specific item in the report category for the selected date range.
- **Others (row title).** The optional **Others** row title displays a summation of all of the unspecified items of the report category. The unspecified items are those items not specifically displayed in the top "n" items. The **Others** row provides a comparison between the specified items, or top "n" items selected for display, and the rest of the traffic on the interface. When displayed, the Others row will provide perspective as to the relative size of the specified items in comparison to the total traffic on the interface.
- **Totals (row title).** Displays the total of all of the items in the report category, specified and unspecified (**Others**). This row shows the interface totals for each column in the report.



Note: For the purposes of this report, Flow Monitor defines ToS as the first 6 bits of a Type of Service (ToS) byte, or the Differentiated Services Code Point (DSCP).



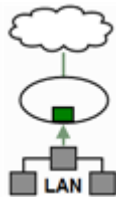
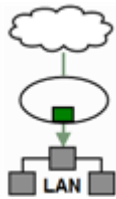
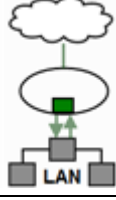
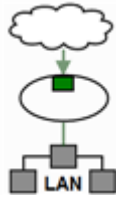
Tip: You can hover over information in the **Bytes** column to display popup information with average data speed as a percentage of the total interface capacity.



For more information

About interface traffic directions



Note: For illustration purposes, the descriptions and diagrams in the table below assume that traffic is passing from an internal interface to an external interface or vice versa. In reality, traffic may pass from an internal interface to another internal interface, an external interface to another external interface, or traffic may be routed out the same interface it enters.

| Interface | Traffic Direction | Report displays... |
|--------------------|---|---|
| Internal interface | Inbound  | The top types of service used by devices on the LAN segment connected to the selected internal interface to communicate with outside devices. |
| | Outbound  | The top types of service used by outside devices to communicate with devices on the LAN segment connected to the selected internal interface. |
| | Inbound/ Outbound  | The top types of service used by all devices transmitting traffic across the selected internal interface. |
| External interface | Inbound  | The top types of service used by devices connected to the selected external interface to communicate with devices on an internal LAN segment. |

| Interface | Traffic Direction | Report displays... |
|-----------|---|---|
| | Outbound  | The top types of service used by devices on internal LAN segments to communicate with devices connected to the selected external interface. |
| | Inbound/ Outbound  | The top types of service by all devices transmitting traffic across the selected external interface. |

General reports

In This Chapter

| | |
|---|-----|
| General dashboard reports | 407 |
| General: Custom Links | 408 |
| General: Database Size | 409 |
| General: Database Table Usage | 410 |
| General: Device Active Monitor States | 411 |
| General: Device Attributes | 411 |
| General: Device Custom Links | 412 |
| General: Device Dependencies | 412 |
| General: Device Notes | 412 |
| General: Device Performance Monitor Summary | 413 |
| General: SNMP Details | 413 |
| General: Device Status | 414 |
| General: Device Toolbar | 415 |
| General: Free Form Text/HTML | 415 |
| General: Group Status | 416 |
| General: Interface Details | 417 |
| General: Map View | 418 |
| General: Monitors Applied | 419 |
| General: Search Knowledge Base | 419 |
| General: Summary Counts | 420 |
| General: Web User Activity Log | 420 |

General dashboard reports

| General dashboard reports | Type | Description |
|---------------------------|--------|---|
| Device Notes | Device | Displays device notes configured in Device Properties > Notes . |
| Device Attributes | Device | Displays device attributes configured in Device Properties > Attributes . |
| Device SNMP Details | Device | Displays device SNMP details. |
| Device Status | Device | Displays device details, active monitors, attributes, and the device |

| General dashboard reports | Type | Description |
|--|--------|---|
| | | groups to which a device belongs. |
| Device Toolbar | Device | Displays device details configured in Device Properties > General . |
| Device Custom Links | Device | Displays any custom links assigned to a device in Device Properties > Custom Links . |
| Device Dependencies | Device | Shows the state of a device and any devices that are up or down dependent on that device. |
| Monitors Applied | Home | Displays a list of any Active, Passive, or Performance monitors assigned to the selected device. |
| Device Active Monitor States | Device | Lists all of a device's Active Monitors and their current state. |
| Device Performance Monitor Summary | Device | Displays a polling summary for the device currently in context. |
| Map View | Home | Displays a smaller version of a network map. |
| Group Status | Home | Displays a summary for the selected device group. |
| Database Size | Home | Displays a graphical representation of the WhatsUp Gold database at the time of the last poll. |
| Database Table Usage | Home | Displays a graphical representation of the WhatsUp Gold top five database tables. If Flow Monitor is installed, Flow Monitor or Flow Monitor Archive database views can be configured to display in the dashboard report. |
| Custom Links | Home | Displays any custom links that you add to the dashboard report. |
| Free Form Text/HTML | Home | Displays any free form text or HTML code that you add to the dashboard report. |
| Web User Activity Log | Home | Displays a log of when a user logs on or off the web interface, and the actions taken while logged on. |
| Interface Details (specific interface) | Home | Displays SNMP information reported by a specific network interface. |
| User Orientation | Home | Displays information regarding the new the new web interface, dashboard, and dashboard reports. |
| Search Knowledge Base | Home | Allows you to search the WhatsUp Gold Knowledge Base. |

General: Custom Links

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

To configure this dashboard report in WhatsUp Gold:

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

General: Database Size

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

The graph uses color to show the current status:

Red. Above 75%

Yellow. Between 50% and 75%

Green. 50% or less

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



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

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Graph type.** Select the type of graph you would like the report to display.
 - **Pie.** A 3-D pie graph that displays available database space in green, and used space in red.
 - **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the database percentage used.
 - **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the database percentage used.
 - **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the database percentage used.
 - **Text.** A numerical representation of the database percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).
- 3 Click **OK** to save changes.

General: Database Table Usage

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



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



Tip: You can use the Alert Center to set database threshold alerts for WhatsUp Gold and Flow Monitor. For more information, see *Configuring a WhatsUp Health threshold* (on page 795).

To configure this dashboard report in WhatsUp Gold:

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

General: Device Active Monitor States

This device-level dashboard report lists all of a device's Active Monitors and their current state. Adding this report to a Device Status dashboard will update you on the health of a crucial device's Active Monitors, as well as list what Active Monitors are currently configured for the device. If you only want to see down Active Monitors, see Problem Areas: Down Active Monitors *Problem Areas Specific Device: Down Active Monitors* (on page 501).

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

To configure this dashboard report in WhatsUp Gold:

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

General: Device Attributes

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



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

To configure this dashboard report in WhatsUp Gold:

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

General: Device Custom Links

This dashboard report displays a customizable list of web links in a dashboard view.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter a title for the dashboard report in the **Report name** field.
- 3 Make any changes to the report:
 - Click **Add** to add a new URL to the list.
 - Click **Edit** to change the settings for a URL.
 - Click **Remove** to delete a URL from the list.
- 4 Click **OK** to save changes.

General: Device Dependencies

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

This dashboard report contains the following fields:

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

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

To configure this dashboard report in WhatsUp Gold:

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

General: Device Notes

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



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

To configure this dashboard report in WhatsUp Gold:

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

General: Device Performance Monitor Summary

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

The dashboard report includes the following fields:

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

To configure this dashboard report in WhatsUp Gold:

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

General: SNMP Details

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

General: Device Status

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

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

Device type. The type of device.

Host name. The host name for the device.

Address. The address of the device.

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

Attributes. Any additional information about the device.

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

To configure this dashboard report in WhatsUp Gold:

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

General: Device Toolbar

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



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

To configure this dashboard report in WhatsUp Gold:

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

General: Free Form Text/HTML

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

This free-form dashboard report supports:

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

To configure this dashboard report in WhatsUp Gold:

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

- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Type a title for the report.
 - **Free form text/HTML.** Type your HTML code or text in this box.
- 3 Click **OK** to save changes.

General: Group Status

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

- Monitored devices
- Up devices



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

- Down devices



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

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



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



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

To configure this dashboard report in WhatsUp Gold:

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

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

General: Interface Details

This General Dashboard report displays SNMP information reported by a specific interface. To gather this data, you must have the *SNMP Credentials* (on page 75) configured for the device in its Device Properties.

Device Information

The top section of the Dashboard report shows the current state of the device, as well as the display name and device type. Click the device name to go to that device's *Device Status* (on page 354) report.

Interface Information

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

- **Interface name.** The name and IP address of the interface. Click the interface name to access the *Interface Utilization* (on page 641) report for this interface.
- **Type.** The type code of the interface as defined in the MIB file for the interface.
- **Index.** The SNMP index of the interface.
- **Description.** Usually the interface or port name on the device.

Polling Information

- **Status.** The current status of the device as reported through SNMP. Click the status code to access the Router/Switch/Interface view of the Device Status report.
 - 1 - up
 - 2 - down
 - 3 - testing
 - 4 - unknown
 - 5 - dormant
 - 6 - notPresent
 - 7 - lowerLayerDown
- **Last poll time.** The date and time of the last successful poll.
- **Last poll time interval.** The time (in seconds) between the last two successful polls.

Received octets

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

Transmitted octets

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

Configuration

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

General: Map View

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

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

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the browse (...) button.
 - **Width.** Enter a width for the map boundary box in pixels.
 - **Height.** Enter a height for the map boundary box in pixels.

You can select these optional items:

- **Draw device type icons.** This includes device type icons in the map. Devices are represented by dots when this option is not selected.
- **Show unconnected links.** This displays links unconnected links in the map.
- **Show dependency arrows.** This displays arrows that indicating up and down dependencies on group devices in the map.
- **Clip device labels.** This removes device labels from the map.
- **Wrap device labels.** This wraps device labels in the map.

3 Click **OK** to save changes.

General: Monitors Applied

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

The report body displays:

- A listing of monitors by type and name.



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

To configure this dashboard report in WhatsUp Gold:

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

General: Search Knowledge Base

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

To perform a Knowledge Base search from this dashboard report:

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

To configure this dashboard report in WhatsUp Gold:

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

General: Summary Counts

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

- Monitored devices
- Up devices
- Down devices
- Devices with down Active Monitors
- Devices in Maintenance
- Active Monitors
- Down Active Monitors
- Up interfaces
- Down interfaces
- Actions fired in the last 4 hours

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

General: Web User Activity Log

This home-level dashboard report displays a log of when a user logs on or off the web interface, and the actions taken while logged on. All messages found in this Log are also written to the Windows Event log.

- **Web user.** The specific WhatsUp Web user to which the message pertains.
- **Date.** The date of the message.
- **Category.** The type of message. Possible categories and example details:
- **Devices.** Indicates a change to a device or device group, for example, "Created device '%1'"
- **Action.** Indicates changes made to action types, for example, "Modified action type '%1'"
- **Device Properties.** Indicates changes made to device properties, for example, "Removed passive monitor type '%1' from '%2'"
- **Active Monitor.** Indicates changes made to active monitor types, for example, "Modified active monitor type '%1'"
- **Action.** Indicates changes made to action types, for example, "Deleted action type '%1'"
- **Action Policy.** Indicates changes made to action policies, for example, "Created action policy type '%1'"
- **System.** Indicates changes to the overall system, for example, "Modified 'ip security settings'"
- **Bulk Field Change operations.** Indicates that a bulk field change successfully executed, for example, "'Maintenance bulk field changes' for %1"
- **Login.** A record of user logins and logouts, for example, "Logged in"
- **User.** Indicates changes made to user accounts, for example, "Deleted user '%1'"
- **Credentials.** Indicates changes made to credentials, for example, "Changed credentials '%1'"
- **Passive Monitor.** Indicates changes made to passive monitors, for example, "Modified passive monitor type '%1'"
- **Performance Monitor.** Indicates changes made to performance monitors, for example, "Modified performance monitor type '%1'"
- **Dashboards.** Indicates changes made to dashboards, for example, "Modified dashboard 'General'"
- **Flow.** (available with Flow Monitor only) Indicates changes made to Flow Interface Details, for example, "Modified Flow dashboard report: 'General'"
- **Details.** The details of the activity.

To configure this dashboard report in WhatsUp Gold:

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

Interface Errors and Discards reports

In This Chapter

| | |
|--|-----|
| Interface Errors and Discards dashboard reports | 423 |
| Interface Discards Last X hours/days (Single Device) | 425 |
| Interface Discards Last X hours/days (Specific Interface) | 425 |
| Interface Errors Last X hours/days (Single Device) | 427 |
| Interface Errors Last X hours/days (Specific Interface) | 427 |
| Interface Errors and Discards - Last Polled Values (Single Device) . | 429 |
| Interface Errors and Discards: Top X by Number of Discards | 429 |
| Interface Errors and Discards:Top X by Number of Errors..... | 430 |

Interface Errors and Discards dashboard reports

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


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

Interface Discards Last X hours/days (Single Device)

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

To display a single interface, use the *Performance: Interface Discards Last X hours/days - Specific Interface* (on page 425) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface discards, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface discard values that are of real concern.
- **Min.** Enter a number for the lowest point on the Y-axis.
 - **Max.** Enter a number for the highest point on the Y-axis.
 - **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
 - **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
 - 3 Click **OK** to save changes.

Interface Discards Last X hours/days (Specific Interface)

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

To display more than one interface, use the *Interface Discards (last X hours/days - Single Device* (on page 425) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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



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

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

Interface Errors Last X hours/days (Single Device)

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

To display a single interface, use the *Performance: Interface Errors (Last X hours/days - Specific Interface)* (on page 427) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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



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

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

Interface Errors Last X hours/days (Specific Interface)

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

To display more than one interface, use the *Interface Errors (last X hours/days - Single Device)* (on page 427) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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



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

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

Interface Errors and Discards - Last Polled Values (Single Device)

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Interface Errors and Discards: Top X by Number of Discards

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

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

To configure this dashboard report in WhatsUp Gold:

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

Interface Errors and Discards:Top X by Number of Errors

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

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

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization reports

In This Chapter

| | |
|--|-----|
| Interface Utilization dashboard reports | 431 |
| Interface Utilization: Interface Traffic Last X hours/days (Single Device) | 432 |
| Interface Utilization (Specific Interface Traffic) | 433 |
| Interface Utilization Last X hours/days (Single Device) | 434 |
| Interface Utilization Last X hours/days (Specific Interface Utilization) | 435 |
| Last Polled Interface Utilization Value (Specific Interface) | 436 |
| Last Polled Interface Utilization Values (Single Device) | 437 |
| Threshold: Interface Utilization | 437 |
| Top 10 by Interface Utilization | 438 |
| Top 10 by Interface Traffic | 439 |
| Threshold: Interface Traffic | 439 |

Interface Utilization dashboard reports

| Interface Utilization dashboard reports | Type | Description |
|--|--------|--|
| Last Polled Interface (single device) | Device | Shows the interface utilization for all network interfaces at the time of the last poll. |
| Last Polled Interface (specific interface) | Home | Shows the interface utilization for a specific network interface at the time of the last poll. |
| All Interfaces over 80% Bandwidth Utilization* | Home | Lists all network interfaces with a utilization greater than 80%. |
| All Interfaces over 90% Bandwidth Utilization | Home | Lists all network interfaces with a utilization greater than 90%. |
| Top 10 with Traffic Threshold* | Home | Lists the top 10 devices based on their current interface traffic. |
| Top 10 by Bandwidth Utilization* | Home | Lists the top 10 devices based on their current interface utilization. |
| Top 20 by Bandwidth Utilization | Home | Lists the top 20 devices based on their current interface utilization. |
| Top 10 by Traffic* | Home | Lists the top 10 devices based on their current interface traffic. |
| Top 20 by Traffic | Home | Lists the top 20 devices based on their current interface traffic. |
| Last 4 hours (single device) | Device | Details all interface utilization percentages for one device over the last 4 hours. |

| Interface Utilization dashboard reports | Type | Description |
|--|-------------|---|
| Last 8 hours (single device) | Device | Details all interface utilization percentages for one device over the last 8 hours. |
| Last 7 days (single device) | Device | Details all interface utilization percentages for one device over the last 7 days. |
| Last 30 days (single device) | Device | Details all interface utilization percentages for one device over the last 30 days. |
| Last 4 hours (specific interface utilization) | Home | Details utilization for a specific interface for one device over the last 4 hours. |
| Last 8 hours (specific interface utilization) | Home | Details utilization for a specific interface for one device over the last 8 hours. |
| Last 7 days (specific interface utilization) | Home | Details utilization for a specific interface for one device over the last 7 days. |
| Last 30 days (specific interface utilization) | Home | Details utilization for a specific interface for one device over the last 30 days. |
| Last 4 hours (specific traffic interface) | Home | Details traffic for a specific interface for one device over the last 4 hours. |
| Last 8 hours (specific traffic interface) | Home | Details traffic for a specific interface for one device over the last 8 hours. |
| Last 7 days (specific traffic interface) | Home | Details traffic for specific interface for one device over the last 7 days. |
| Last 30 days (specific traffic interface) | Home | Details traffic for a specific interface for one device over the last 30 days. |
| Interface Traffic - Last 4 Hours (single device) | Device | Details traffic for all interfaces for one device over the last four hours. |
| Interface Traffic - Last 8 hours (single device) | Device | Details traffic for all interfaces for one device over the last eight hours. |
| Interface Traffic - Last 7 days (single device) | Device | Details traffic for all interfaces for one device over the last seven days. |
| Interface Traffic - Last 30 days (single device) | Device | Details traffic for all interfaces for one device over the last 30 days. |

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

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

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

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



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

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization (Specific Interface Traffic)

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

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization Last X hours/days (Single Device)

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

To display a single interface, use the *Interface Utilization (Last 4 Hours - Specific Interface)* (on page 435) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization Last X hours/days (Specific Interface Utilization)

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

To display more than one interface, use the *Interface Utilization (All Interfaces)* (on page 434) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

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

3 Click **OK** to save changes.

Last Polled Interface Utilization Value (Specific Interface)

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

There are five types of graphs to choose from:

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

Last Polled Interface Utilization Values (Single Device)

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Threshold: Interface Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Top 10 by Interface Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report:

- 1 Select **Configure** from the dashboard report menu.
- 2 Enter the appropriate information.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Top 10 by Interface Traffic

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

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

To configure this dashboard report in WhatsUp Gold:

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

Threshold: Interface Traffic

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

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

To configure this dashboard report in WhatsUp Gold:

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

Inventory reports

In This Chapter

| | |
|---|-----|
| Inventory dashboard reports | 441 |
| Inventory: Total Actions Applied by Type | 441 |
| Inventory: Active Monitors Applied by Type | 442 |
| Inventory: Total Devices by Type..... | 442 |
| Inventory: Devices with Specific Attribute | 443 |
| Inventory: Total Passive Monitors by Type..... | 443 |
| Inventory: Total Performance Monitors by Type | 444 |

Inventory dashboard reports

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

Inventory: Total Actions Applied by Type

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

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

To configure this dashboard report in WhatsUp Gold:

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

Inventory: Active Monitors Applied by Type

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

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

To configure this dashboard report in WhatsUp Gold:

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

Inventory: Total Devices by Type

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

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

To configure this dashboard report in WhatsUp Gold:

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

Inventory: Devices with Specific Attribute

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

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

To configure this dashboard report in WhatsUp Gold:

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

Inventory: Total Passive Monitors by Type

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

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

To configure this dashboard report in WhatsUp Gold:

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

Inventory: Total Performance Monitors by Type

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

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

To configure this dashboard report in WhatsUp Gold:

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

Memory Utilization reports

In This Chapter

| | |
|--|-----|
| Memory Utilization dashboard reports | 445 |
| Memory Utilization Last X hours/days (Single Device) | 446 |
| Memory Utilization Last X hours/days (Specific Aspect) | 446 |
| Last Polled Memory Utilization (Specific Aspect) | 447 |
| Last Polled Memory Utilization (Single Device)..... | 448 |
| Threshold: Memory Utilization | 449 |
| Top 10: Memory Utilization..... | 450 |

Memory Utilization dashboard reports

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

| Memory Utilization dashboard reports | Type | Description |
|--------------------------------------|------|---|
| Last 7 days (specific aspect) | Home | Details utilization of a specific memory type for one device over the last 7 days. |
| Last 30 days (specific aspect) | Home | Details utilization of a specific memory type for one device over the last 30 days. |

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

Memory Utilization Last X hours/days (Single Device)

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

To configure this dashboard report in WhatsUp Gold:

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

Memory Utilization Last X hours/days (Specific Aspect)

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

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

To configure this dashboard report in WhatsUp Gold:

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

Last Polled Memory Utilization (Specific Aspect)

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

There are five types of graphs to choose from:

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

Last Polled Memory Utilization (Single Device)

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the browse (...) button.
 - To view a graphical representation of the report data, select **Use a graph to display the values**.
 - If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- 3 Click **OK** to save changes.

Threshold: Memory Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

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

Top 10: Memory Utilization

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report:

- 1 Select **Configure** from the dashboard report menu.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 (in pixels).
- 2 Click **OK** to save changes.

Performance-Historic reports

In This Chapter

| | |
|--|-----|
| Performance-Historic dashboard reports..... | 451 |
| CPU Utilization Last X hours/days (Single Device)..... | 453 |
| CPU Utilization Last X hours/days (Specific CPU)..... | 454 |
| Custom Performance Monitor Values Last X hours/days (Single Device) | 455 |
| Custom Performance Monitor Values Last X hours/days (Specific Monitor) | 455 |
| Disk Free Space Last X hours/days (Specific Disk) | 456 |
| Disk Utilization Last X hours/days (Single Device)..... | 457 |
| Disk Utilization Last X hours/days (Specific Disk)..... | 458 |
| Interface Discards Last X hours/days (Single Device) | 458 |
| Interface Discards Last X hours/days (Specific Interface)..... | 460 |
| Interface Errors Last X hours/days (Single Device) | 460 |
| Interface Errors Last X hours/days (Specific Interface) | 462 |
| Interface Utilization: Interface Traffic Last X hours/days (Single Device) | 463 |
| Interface Utilization (Specific Interface Traffic) | 464 |
| Interface Utilization Last X hours/days (Single Device) | 464 |
| Interface Utilization Last X hours/days (Specific Interface Utilization) | 465 |
| Memory Utilization Last X hours/days (Single Device) | 466 |
| Memory Utilization Last X hours/days (Specific Aspect) | 467 |
| Ping Availability Last X hours/days (Single Device) | 467 |
| Ping Response Time Last X hours/days (Single Device) | 468 |

Performance-Historic dashboard reports

| Performance - Historic dashboard reports | Type | Description |
|--|--------|---|
| Custom Performance Monitor Values (last 4 hours - single device) | Device | Details custom Performance Monitor values for one device over the last 4 hours. |
| Interface Utilization (last 4 hours - single device) | Device | Details all interface utilization percentages for one device over the last 4 hours. |

| Performance - Historic dashboard reports | Type | Description |
|--|-------------|---|
| CPU Utilization (last 4 hours - single device) | Device | Details all CPU utilization percentages for one device over the last 4 hours. |
| Memory Utilization (last 4 hours - single device) | Device | Details all memory utilization percentages for one device over the last 4 hours. |
| Disk Utilization (last 4 hours - single device) | Device | Details all disk utilization percentages for one device over the last 4 hours. |
| Ping Response Time (last 4 hours - single device) | Device | Details all ping response times for device interfaces over the last 4 hours. |
| Ping Availability (last 4 hours - single device) | Device | Details all ping availability for a device interfaces over the last 4 hours. |
| Interface Traffic (last 4 hours - specific interface) | Home | Details interface traffic for a specific device interface over the last 4 hours. |
| Custom Performance Monitor Values (last 4 hours - specific monitor) | Home | Details a device's specific custom Performance Monitor values over the last 4 hours. |
| Interface Utilization (last 4 hours - specific interface) | Home | Details utilization percentages for a specific interface for one device over the last 4 hours. |
| CPU Utilization (last 4 hours - specific CPU) | Home | Details utilization percentages for a specific CPU for one device over the last 4 hours. |
| Disk Utilization (last 4 hours - specific disk) | Home | Details utilization percentages for a specific disk for one device over the last 4 hours. |
| Disk Free Space - Last 4 Hours (specific disk) | Home | Details the percentage of available disk space over the last four hours for one disk on one device. |
| Memory Utilization - Last 4 Hours (specific aspect) | Device | Details utilization percentages for a specific memory type for one device over the last 4 hours. |
| Interface Traffic - Last 4 Hours (single device) | Device | Details traffic for all interfaces for one device over the last four hours. |
| Interface Errors - Last 4 Hours (single device) | Device | Details the percentage of interface errors for outbound and inbound traffic on one device over the last four hours. |

| Performance - Historic dashboard reports | Type | Description |
|--|--------|--|
| Interface Discards - Last 4 hours (single device) | Device | Details the percentage of interface discards for inbound and outbound traffic for all interfaces on a specific device. over the last four hours. |
| Interface Errors - last 4 hours (specific interface) | Device | Details the percentage of interface errors for outbound and inbound traffic on one device interface over the last four hours. |
| Interface Discards - Last 4 hours (specific interface) | Device | Details the percentage of interface discards for inbound and outbound traffic for one interface on a specific device over the last four hours. |

CPU Utilization Last X hours/days (Single Device)

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

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

CPU Utilization Last X hours/days (Specific CPU)

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

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

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

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

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

To configure this dashboard report in WhatsUp Gold:

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



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

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

Disk Free Space Last X hours/days (Specific Disk)

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

To configure this dashboard report in WhatsUp Gold:

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

Disk Utilization Last X hours/days (Single Device)

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

To configure this dashboard report:

- 1 On the dashboard report menu, click **Configure**.
- 2 Enter the appropriate information:
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the Browse (...) button.
 - **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - **Graph type.** Select the type of graph you would like the report to display.
 - **Trend type.** Select the type of trend you would like the report to use.

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

Disk Utilization Last X hours/days (Specific Disk)

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

To configure this dashboard report in WhatsUp Gold:


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

Interface Discards Last X hours/days (Single Device)

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

To display a single interface, use the *Performance: Interface Discards Last X hours/days - Specific Interface* (on page 425) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface discards, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface discard values that are of real concern.
- **Min.** Enter a number for the lowest point on the Y-axis.
 - **Max.** Enter a number for the highest point on the Y-axis.
 - **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
 - **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

Interface Discards Last X hours/days (Specific Interface)

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

To display more than one interface, use the *Interface Discards (last X hours/days - Single Device)* (on page 425) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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



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


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

Interface Errors Last X hours/days (Single Device)

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

To display a single interface, use the *Performance: Interface Errors (Last X hours/days - Specific Interface)* (on page 427) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

Tip: WhatsUp Gold ships with Auto Scale selected for the Vertical Axis Scaling. Depending on your network characteristics, Auto Scale may cause graphs to have extreme peaks on the graph. After you configure a graph, you may want to watch your network performance for a period of time to determine the typical number of interface errors, then set the Vertical Axis Scaling to a fixed scale with a min and max scale that is tuned for your network. This will help you better identify the interface error values that are of real concern.
- **Min.** Enter a number for the lowest point on the Y-axis.
 - **Max.** Enter a number for the highest point on the Y-axis.
 - **Maximum number of graphs to draw.** Enter the maximum number of interface utilization graphs you want to display.
 - **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.
- 3 Click **OK** to save changes.

Interface Errors Last X hours/days (Specific Interface)

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

To display more than one interface, use the *Interface Errors (last X hours/days - Single Device)* (on page 427) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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



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

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

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

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

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



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

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization (Specific Interface Traffic)

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

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization Last X hours/days (Single Device)

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

To display a single interface, use the *Interface Utilization (Last 4 Hours - Specific Interface)* (on page 435) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

Interface Utilization Last X hours/days (Specific Interface Utilization)

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

To display more than one interface, use the *Interface Utilization (All Interfaces)* (on page 434) dashboard report.

To configure this dashboard report in WhatsUp Gold:

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

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

Memory Utilization Last X hours/days (Single Device)

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

To configure this dashboard report in WhatsUp Gold:

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

Memory Utilization Last X hours/days (Specific Aspect)

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

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

To configure this dashboard report in WhatsUp Gold:

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

Ping Availability Last X hours/days (Single Device)

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

To configure this dashboard report in WhatsUp Gold:

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

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

Performance-Last Poll reports

In This Chapter

| | |
|--|-----|
| Performance-Last Poll dashboard reports..... | 469 |
| Last Polled CPU Utilization (Single Device) | 470 |
| Last Polled CPU Utilization (Specific CPU) | 471 |
| Last Polled Custom Performance Monitor Values (Single Device) . | 471 |
| Last Polled Custom Performance Monitor Values (Specific Monitor) | 472 |
| Disk Utilization: Last Polled Values (Single Device)..... | 473 |
| Disk Utilization Last Polled Value (Specific Disk)..... | 474 |
| Interface Errors and Discards - Last Polled Values (Single Device) . | 475 |
| Last Polled Interface Utilization Values (Single Device)..... | 475 |
| Last Polled Interface Utilization Value (Specific Interface) | 476 |
| Last Polled Memory Utilization (Single Device)..... | 477 |
| Last Polled Memory Utilization (Specific Aspect) | 478 |
| Performance: Last Polled Ping Response Time (Specific Interface) | 479 |

Performance-Last Poll dashboard reports

| Performance - Last Poll dashboard reports | Type | Description |
|--|-------------|---|
| Custom Performance Monitor Values (single device) | Device | Shows the values for all custom Performance Monitors for a single device at the time of the last poll. |
| Interface Utilization (single device) | Device | Shows the interface utilization for all device interfaces for a single device at the time of the last poll. |
| CPU Utilization (single device) | Device | Shows the CPU utilization for all CPUs for a single device at the time of the last poll. |
| Memory Utilization (single device) | Device | Shows the memory utilization for all memory types for a single device at the time of the last poll. |
| Disk Utilization (single device) | Device | Shows the disk utilization for all of disks for a single device at the time of the last poll. |
| Custom Performance Monitor Values (specific monitor) | Home | Shows the values for a specific device custom Performance Monitor. |
| Interface Utilization (specific interface) | Home | Shows the utilization of a specific device interface at the time of the last poll. |

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

Last Polled CPU Utilization (Single Device)

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

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

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the browse (...) button.
 - To view a graphical representation of the report data, select **Use a graph to display the values**.
 - If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types*. (on page 610)
- 3 Click **OK** to save changes.

Last Polled CPU Utilization (Specific CPU)

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

There are five types of graphs to choose from:

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

Last Polled Custom Performance Monitor Values (Single Device)

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

- **Name.** The name of the performance monitor as listed in the Performance Monitor Library.

- **Poll Time.** The time the last poll took place.
- **Time Delta.** The time between the last two polls.
- **Value.** The value of the last poll.

To configure this dashboard report in WhatsUp Gold:

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

Last Polled Custom Performance Monitor Values (Specific Monitor)

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

There are five types of graphs to choose from:

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



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

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

To configure this dashboard report in WhatsUp Gold:

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

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



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

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

Disk Utilization: Last Polled Values (Single Device)

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

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

Each entry in the report contains the following information:

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

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the browse (...) button.
 - To view a graphical representation of the report data, select **Use a graph to display the values**.
 - If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- 3** Click **OK** to save changes.

Disk Utilization Last Polled Value (Specific Disk)

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

There are five types of graphs to choose from:

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

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

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

To configure this dashboard report in WhatsUp Gold:

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

- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Choose a device by clicking on the Browse (...) button.
 - **Disk to graph.** Select a disk to graph for devices with more than one disk.
 - **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

Interface Errors and Discards - Last Polled Values (Single Device)

This device-level dashboard report provides details for the number of interface transmit (outbound) and receive (inbound) errors, and transmit and receive discards for the specified device. Adding this dashboard report to a dashboard allows you to monitor and troubleshoot devices that are experiencing interface errors and discard problems.

Each entry in the report contains the following information:

- **Description.** The selected device interface.
- **Transmit Errors.** The number of packets transmitted through the device interface with errors.
- **Receive Errors.** The number of packets received through the device interface with errors.
- **Transmit Discards.** The number of packets transmitted through the device interface that were discarded.
- **Receive Discards.** The number of packets received through the device interface that were discarded.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the Browse (...) button.
 - **Column 1 width.** The width of the column in the dashboard in pixels.
- 3 Click **OK** to save changes.

Last Polled Interface Utilization Values (Single Device)

This device-level dashboard report displays current interface utilization percentages for all interfaces on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's interface(s) to keep up with the number of packets they are currently transmitting and receiving. The colors in the second Transmit and Received columns coincide with the WhatsUp Threshold colors:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Description.** The particular interface.
- **Speed.** The interface speed.
- **Transmit (kbps).** The number of packets transmitted in kbps.
- **Receive (kbps).** The number of packets received in kbps.
- **Transmit.** The percentage of packets transmitted.
- **Receive.** The percentage of packets received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the **Browse (...)** button.
- 3 Click **OK** to save changes.

Last Polled Interface Utilization Value (Specific Interface)

This home-level dashboard report provides graphical illustration of an interface utilization at the time of the last poll. Placing this dashboard report in a dashboard will allow you to view an interface status quickly, even from across the room.

There are five types of graphs to choose from:

- **Pie.** A 3-D pie graph that displays available interface space in green, and used space in red.
- **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the interface percentage used.
- **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the interface percentage used.
- **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the interface percentage used.

- **Text.** A numerical representation of the interface percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the interface size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device for the report by clicking on the **Browse (...)** button.
 - **Interface to graph** (available in some dialogs). For devices that have more than one interface, select an interface to graph.
 - **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

Last Polled Memory Utilization (Single Device)

This device-level dashboard report displays current memory utilization percentages for all memories on a selected device. Displaying this dashboard report in a device dashboard allows you to monitor an important device's memory(s) to watch for spikes in memory utilization. The colors displayed in the Percent Used column coincide with the WhatsUp threshold colors:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Description.** The particular memory.
- **Size Used.** The size of memory in use at the time of the last poll.
- **Total Size.** The total size of the memory.
- **Percentage Used.** The percentage of the total size of the memory in use at the time of the last poll.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the browse (...) button.
 - To view a graphical representation of the report data, select **Use a graph to display the values**.
 - If you select the above option, select the **Graph type** with which report data will be displayed. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- 3** Click **OK** to save changes.

Last Polled Memory Utilization (Specific Aspect)

This home-level dashboard report provides graphical illustration of device memory utilization at the time of the last poll. Placing this dashboard report in a dashboard allows you to view device memory status quickly.

There are five types of graphs to choose from:

- **Pie.** A 3-D pie graph that displays available memory space in green, and used space in red.
- **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the memory percentage used.
- **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the memory percentage used.
- **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the memory percentage used.
- **Text.** A numerical representation of the memory percentage used. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

Under each type of graph, the memory size is listed in MBs, along with the percentages for used and free space.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device for the report by clicking the Browse (...) button.
 - **Memory aspect to graph.** For devices with more than one memory aspect, select a memory aspect to graph.
 - **Graph type.** Choose the type and size of the graph.
- 3 Click **OK** to save changes.

Performance: Last Polled Ping Response Time (Specific Interface)

This home-level dashboard report provides graphical illustration of a device's ping response time. Placing this dashboard report in a dashboard will allow you to view device ping response time status quickly.

There are five types of graphs to choose from:

- **Pie.** A 3-D pie graph that displays available ping response time in green.
- **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the the ping response time.
- **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the ping response time.
- **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the ping response time.
- **Text.** A numerical representation of the ping response time. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - Red. Above 90%
 - Yellow. Between 80% and 90%
 - Green. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

To configure this dashboard report:

- 1 On the dashboard report menu, click **Configure**.
- 2 Enter or select the appropriate information for the following fields:
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the **Browse** (...) button.
 - **Interface.** Select the interface that you want to monitor.
 - **Graph type.** Select the type of graph you would like the report to display.

- **Maximum ping response time.** Enter a value (in milliseconds) for the maximum ping response time.
- 3 Click **OK** to save changes.

Ping Availability and Response Time reports

In This Chapter

| | |
|--|-----|
| Ping Availability and Response Time dashboard reports | 481 |
| Threshold: Ping Availability | 482 |
| Threshold: Ping Packet Loss | 483 |
| Threshold: Ping Response Time | 484 |
| Ping Availability Last X hours/days (Single Device) | 484 |
| Ping Response Time Last X hours/days (Single Device) | 485 |
| Performance: Last Polled Ping Response Time (Specific Interface) | 486 |
| Top 10: Ping Availability..... | 486 |
| Top 10: Ping Packet Loss..... | 487 |
| Top 10: Ping Response Time..... | 488 |

Ping Availability and Response Time dashboard reports

| Ping Availability and Response Time dashboard reports | Type | Description |
|---|--------|--|
| Last 4 hours (single device response time) | Device | Shows the ping response time for all interfaces for a specific device over the last 4 hours. |
| Last 8 hours (single device response time) | Device | Shows the ping response time for all interfaces for a specific device over the last 8 hours. |
| Last 7 days (single device response time) | Device | Shows the ping response time for all interfaces for a specific device over the last 7 days. |
| Last 30 days (single device response time) | Device | Shows the ping response time for all interfaces for a specific device over the last 30 days. |
| Last 4 hours (single device availability) | Device | Shows the ping availability for all interfaces for a specific device over the last 4 hours. |
| Last 8 hours (single device availability) | Device | Shows the ping availability for all interfaces for a specific device over the last 8 hours. |
| Last 7 days (single device availability) | Device | Shows the ping availability for interfaces for a specific device over the last 7 days. |
| Last 30 days (single device availability) | Device | Shows the ping availability for all interfaces for a specific device over the last 30 days. |
| Last Polled Response Time (specific interface) | Home | Shows the last ping response time of a specific device interface at the time of the last poll. |

| Ping Availability and Response Time dashboard reports | Type | Description |
|--|-------------|--|
| Top 10 by Ping Response Time* | Home | Lists the top 10 devices based on current ping response time. |
| Top 20 by Ping Response Time | Home | Lists the top 20 devices based on current ping response time. |
| Top 10 by Ping Packet Loss* | Home | Lists the top 10 devices based on current ping packet loss. |
| Top 20 by Ping Packet Loss | Home | Lists the top 20 devices based on current ping packet loss. |
| Top 10 by Ping Availability* | Home | Lists the top 10 devices based on their current ping availability. |
| Top 20 by Ping Availability | Home | Lists the top 20 devices based on their current ping availability. |
| Devices with Ping Response Time over 100 msec | Home | Lists all devices with a ping response time greater than 100 msec. |
| Devices with Ping Response Time over 500 msec | Home | Lists all devices with a ping response time greater than 500 msec. |
| Devices with Ping Packet Loss over 50% | Home | Lists all devices with a ping packet loss greater than 50%. |
| Devices with Ping Packet Loss over 75% | Home | Lists all devices with a ping packet loss greater than 75%. |
| Devices with Ping Availability over 50%* | Home | Lists all devices with a ping availability greater than 50%. |
| Devices with Ping Availability over 75% | Device | Lists all devices with a ping availability greater than 75%. |

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

Threshold: Ping Availability

This home-level dashboard report displays ping availability information for a specific device. A graph displays in the dashboard, charting the device response time to pings (in msec) over the amount of time defined by the specific report type.

- **Device.** The network device.
- **Interface.** The network interface.
- **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Ping Packet Loss

This home-level dashboard report displays packet loss information and percentages for devices in a specific group, based on the latest poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their ping packet loss by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Interface.** The network interface.
- **Sent.** The number of packets sent from the device.
- **Lost.** The total number of packets lost from the device
- **% Lost.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.

- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.
- **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- **Column 2 width.** Enter a width for the Description column (in pixels).

3 Click **OK** to save changes.

Threshold: Ping Response Time

This home-level dashboard report displays ping response times for devices in a specific device group. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at the Max and Avg columns for each device.

- **Device.** The network device.
- **Interface.** The network interface.
- **Max (ms).** The maximum response time in milliseconds.
- **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Ping Availability Last X hours/days (Single Device)

This device-level dashboard report displays an area graph that details the ping availability percentages for a device during a selected time period. Displaying this dashboard report in a dashboard can help you keep an eye on important or problem devices that have been experiencing ping problems.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the **Browse (...)** button.
 - **Date range.** Select a date range from the drop-down menu. The default is 4 hours.
 - **Graph type.** Select the type of graph you would like the report to display.
 - **Trend type.** Select the type of trend you would like the report to use.
 - **Dimensions.** Select the dimension in which you would like the graph to display.
 - **Width.** Enter a width for the report (in pixels).
 - **Height.** Enter a height for the report (in pixels).
 - **Vertical Axis Scaling.** Select either auto or fixed scale.
 - **Min.** Enter a number for the lowest point on the Y-axis.
 - **Max.** Enter a number for the highest point on the Y-axis.
- 3 Click **OK** to save changes.

Ping Response Time Last X hours/days (Single Device)

This home-level dashboard report displays ping availability information for devices in a specific group. This dashboard report charts device response time to pings (in msec) over the length of time defined by the specific report.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the **Browse (...)** button.
 - **Date range.** Select a date range from the drop-down menu.
 - **Graph type.** Select the type of graph you would like the report to display.
 - **Trend type.** Select the type of trend you would like the report to use.
 - **Dimensions.** Select the dimension in which you would like the graph to display.
 - **Width.** Enter a width for the report (in pixels).
 - **Height.** Enter a height for the report (in pixels).
 - **Vertical Axis Scaling.** Select either auto or fixed scale.
 - **Min.** Enter a number for the lowest point on the Y-axis.
 - **Max.** Enter a number for the highest point on the Y-axis.
 - **Graph the maximum.** Select this option to display a graph of the maximum value over the selected time period.

- 3 Click **OK** to save changes.

Performance: Last Polled Ping Response Time (Specific Interface)

This home-level dashboard report provides graphical illustration of a device's ping response time. Placing this dashboard report in a dashboard will allow you to view device ping response time status quickly.

There are five types of graphs to choose from:

- **Pie.** A 3-D pie graph that displays available ping response time in green.
- **Gauge.** A semi-circle graph (much like a car speedometer) with a pointer that indicates the the ping response time.
- **Horizontal bar.** A horizontal bar graph (much like a ruler) with a pointer that indicates the ping response time.
- **Vertical bar.** A vertical bar graph (much like a thermometer) with a pointer that indicates the ping response time.
- **Text.** A numerical representation of the ping response time. The percentage is displayed in colors that coincide with the WhatsUp threshold colors:
 - Red. Above 90%
 - Yellow. Between 80% and 90%
 - Green. 80% or less

Along with the various types of graphs to choose from, you can also pick the display size of the graph (small, medium, or large).

To configure this dashboard report:

- 1 On the dashboard report menu, click **Configure**.
- 2 Enter or select the appropriate information for the following fields:
 - **Name.** Enter a title for the dashboard report.
 - **Device.** Select a device by clicking the **Browse (...)** button.
 - **Interface.** Select the interface that you want to monitor.
 - **Graph type.** Select the type of graph you would like the report to display.
 - **Maximum ping response time.** Enter a value (in milliseconds) for the maximum ping response time.
- 3 Click **OK** to save changes.

Top 10: Ping Availability

This home-level dashboard report displays the top devices in a group based on their ping availability percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level.

- **Device.** The network device.
- **Interface.** The network interface.
- **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the *Ping Availability* (on page 650) report.
- **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Top 10: Ping Packet Loss

This home-level dashboard report displays the top devices in a group based on their ping packet loss percentages at the time of the last poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at the colors associated with each packet loss percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Interface.** The network interface.
- **Sent.** The number of packets sent.
- **Lost.** The number of packets lost.
- **% Loss.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
 - **Top count.** Enter the number of records to display in the dashboard report.
- 3 Click **OK** to save changes.

Top 10: Ping Response Time

This home-level dashboard report displays the top devices in a group based on their ping response times. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at each device's Max and Avg columns.

- **Device.** The network device.
- **Interface.** The network interface.
- **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas reports

In This Chapter

| | |
|---|-----|
| Problem Areas dashboard reports | 489 |
| Problem Areas: Actions Fired in the Last X Hours..... | 490 |
| Problem Areas: All Completely Down Devices | 491 |
| Problem Areas: All Down Interfaces | 491 |
| Problem Areas: Device Group Mini Status..... | 492 |
| Problem Areas: Devices with Down Active Monitors | 493 |
| Problem Areas: Devices with Down Critical Monitors..... | 494 |
| Problem Areas: General Error Log | 494 |
| General: Summary Counts..... | 495 |
| Problem Areas: Tail of Action Activity Log | 495 |
| Problem Areas: Tail of Passive Monitor Error Log | 496 |
| Problem Areas: Tail of SNMP Trap Log..... | 496 |
| Problem Areas: Tail of State Change Log..... | 497 |
| Problem Areas: Tail of Syslog | 498 |
| Problem Areas: Tail of Windows Event Log..... | 499 |
| Problem Areas: Unacknowledged Devices | 499 |
| Problem Areas: Web Alarms | 500 |

Problem Areas dashboard reports

| Problem Areas dashboard reports | Type | Description |
|-----------------------------------|--------|--|
| Devices with Down Active Monitors | Device | Displays down Active Monitors for a device. |
| All Down Interfaces | Device | Displays down interfaces for a device. |
| Tail of State Change Log | Device | Displays the tail of the State Change Log for a specified device. |
| Tail of Syslog | Device | Displays the tail of the Syslog full report for a specified device. |
| Tail of Windows Event Log | Device | Displays the tail of the Windows Event Log for a specified device. |
| Tail of SNMP Trap Log | Device | Displays the tail of the SNMP Trap Log for a specified device. |
| Tail of Action Activity Log* | Device | Displays the tail of the Action Activity Log for a specified device. |
| Tail of Passive Monitor Error Log | Device | Displays the tail of the Passive Monitor Error Log for a specified device. |

| Problem Areas dashboard reports | Type | Description |
|-----------------------------------|--------|---|
| Web Alarms | Device | Displays any web alarms fired for a specified device. |
| All Completely Down Devices | Home | Displays down devices for a specified device group. |
| All Down Interfaces | Home | Displays down interfaces for a specified device group. |
| Devices with Down Active Monitors | Home | Displays devices with down Active Monitors within a specified device group. |
| Unacknowledged Devices | Home | Displays unacknowledged devices within a specified device group. |
| Tail of State Change Log | Home | Displays a tail of the State Change Log for your network. |
| Summary Counts* | Home | Displays a summary of a specified device group. |
| Tail of Syslog | Home | Displays the tail of the Syslog full report for your network. |
| Tail of Windows Event Log | Home | Displays the tail of the Windows Event Log for your network. |
| Tail of SNMP Trap Log | Home | Displays the tail of the SNMP Trap Log for your network. |
| Tail of Action Activity Log* | Home | Displays the tail of the Action Activity Log for your network. |
| Tail of Passive Monitor Error Log | Home | Displays the tail of the Passive Monitor Error Log for your network. |
| Device Group Mini Status | Home | Lists all devices in a device group and displays their status by color. |
| Web Alarms | Home | Shows a snap shot of the most recent web alarms fired on your network. |
| General Error Log | Home | Displays the tail of the General Error Log for your network. |
| Actions Fired in the Last 4 Hours | Home | Displays all devices that have fired an action in the last four hours. |

*Available as Remote Dashboard Reports in WhatsUp Gold Remote and Central Site Editions.

Problem Areas: Actions Fired in the Last X Hours

This dashboard report displays devices that have fired an action over a selected period of time. Placing this dashboard report in a dashboard can give you a snapshot of the health and success of actions on your network.

- **Date.** The date the action was fired. Click a date to bring up the Action Log.
- **Source.** The device from which the action was fired. Click a device to bring up the Device Status Report.
- **Action Name.** The name of the action as listed in the Active Monitor Library.
- **Trigger.** The trigger for the action, either Up or Down. Click a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices.
 - **Last hours.** Enter the number of hours from which you would like information displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column in pixels.
 - **Maximum rows to return.** Enter a value for the number of rows of data displayed within the report.
- 3 Click **OK** to save changes.

Problem Areas: All Completely Down Devices

This dashboard report displays down devices for a specified group. Adding this dashboard report to a dashboard helps you monitor your network status by displaying which devices are down.

- **Device.** The network device.
- **Status.** The status of the device after the last poll.

You can maximize your available monitor space by limiting the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the Browse (...) button. Select **Every device** to select all devices.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 in pixels.
- 3 Click **OK** to save changes.

Problem Areas: All Down Interfaces

This dashboard report displays down interfaces for a specified group. Adding this dashboard report to a dashboard allows you to monitor network status by displaying all interfaces that are down.

- **Device.** The network device.
- **Status.** The status of the interface after the last poll.

You can maximize your available monitor space by limiting the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the Browse (...) button. Select Every device to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Device Group Mini Status

This dashboard report lists all devices in a group and displays their status by color, allowing you to quickly scan and observe the statuses of devices in a group. Displaying multiple mini status reports within a dashboard view allows you to watch more than one group on your network at once, and can help you monitor important or problem areas more efficiently. You can also optionally display active monitors associated with the devices in a selected group, which is helpful in identifying which services on your network are down.

To help maximize the available viewing area on your monitor, you can change the size of each mini status report. Even if the font size is too small to read at first glance, you can use the mouse over text to find out the identity of a device. The static rows of the mini status also aid in device recognition, as devices always stay in the same row regardless of their current state.

Status icon colors are the same as the WhatsUp Gold state colors:

- **Green** is Up
- **Red** is Down
- **Gray** is Unknown

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the browse (...) button. To select every device on the network, select Every device.
 - **Every device.** Select this option to display every device in the system. However, only devices that you have permissions to view display.
 - **Style.** Select the style and size in which you would like the mini status displayed.
 - **Normal.** Displays device and active monitor status with icons.
 - **High Contrast.** Displays device and active monitor status with bright colors.
 - **Show Active Monitors.** Select this option to display the active monitors associated with the group devices.
 - **Active Monitors per Row.** Select the number of active monitors displayed per row.
 - **Active Monitors Cell Width.** Enter a cell width in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Devices with Down Active Monitors

This dashboard report displays devices with down active monitors for a select group. Adding this dashboard report to a dashboard view helps you watch your network status by showing you which devices are down, and the status of active monitors.

- **Device.** The network device.
- **Status.** The status of the device active monitor after the last poll.

To help maximize the available viewing area on your monitor, you can limit the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the Browse (...) button. Select Every device to select all devices.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Devices with Down Critical Monitors

This home-level dashboard report displays devices with down critical monitors for a specified device group. Adding this dashboard report to a dashboard allows you to easily keep-up with your network's status by showing you which devices are down, and the status of critical monitors.

- **Device.** The network device.
- **Status.** The status of device's critical monitor after the last poll.

You can maximize your screen real-estate by limiting the number of rows displayed in the report or shortening the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the Browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

Problem Areas: General Error Log

This dashboard report displays any error received by WhatsUp Gold. Displaying this dashboard report within a dashboard view helps you keep tabs on all of your network errors.

This dashboard report includes the following fields:

- **Date.** The date the error took place.
- **Category.** The type of error.
- **Source.** Where the error originated.
- **Details.** The details of the error.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 4 width.** Enter a width for column 4 (in pixels).

- 3 Click **OK** to save changes.

General: Summary Counts

This general dashboard report gives a summary of a group by the total number of:

- Monitored devices
- Up devices
- Down devices
- Devices with down Active Monitors
- Devices in Maintenance
- Active Monitors
- Down Active Monitors
- Up interfaces
- Down interfaces
- Actions fired in the last 4 hours

Each entry in the report contains the following information:

- **Count.** The total number of that specific type of passive monitor on the network.
- **Total number of.** The device status types.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- 3 Click **OK** to save changes.

Problem Areas: Tail of Action Activity Log

This dashboard report shows the tail (last 10 records) of the Action Log. Placing this dashboard report in a dashboard lets you see the success rate of actions fired. This enables you to monitor important devices easily and to quickly address any issues. The dashboard report is linked to the full Action Log, which shows all of the actions that WhatsUp Gold has attempted to fire based on the configuration of the action.

- **Date.** The date the action was fired. Click a date to bring up the Action Log.
- **Source.** The source of the action. Click a source to bring up the Device Status report.
- **Action Name.** The name of the Action.
- **Trigger.** The trigger for the action (either Up or Down). Click a trigger to open the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
 - **Column 3 width.** Enter a width for the column (in pixels).
- 3** Click **OK** to save changes.

Problem Areas: Tail of Passive Monitor Error Log

This universal problem areas dashboard report shows any passive monitor errors that have occurred for the specified devices.

- **Date.** The date the error occurred.
- **Device.** The network device.
- **Category.** The category code of the error. Possible values include Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error).
- **Details.** Text that describes the error that was received.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. To select every device on the network, select **Every device**.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 4 width.** Enter a width for the Details column (in pixels).
- 3** Click **OK** to save changes.

Problem Areas: Tail of SNMP Trap Log

This dashboard report displays the tail (last 10 records) of the SNMP Trap Log. Placing this dashboard report in a dashboard displays system-wide SNMP traps. For more information, the dashboard report is linked to the full SNMP Trap Log, which provides a history of SNMP traps that have occurred during the time period displayed at the bottom of the report.

- **Date.** The date and time the trap occurred.
- **Device.** The device from which the trap was sent.
- **SNMP Trap Type.** The type of trap.
- **Payload.** The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed within a packet or other transmission unit.



Note: In order for entries to be added to this report, the SNMP Trap listener must be enabled, and either a SNMP trap passive monitor must be added to a device or unsolicited SNMP traps must be accepted. For more information, see *Enabling the SNMP Trap Listener* (on page 873).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Source column in pixels.
 - **Column 4 width.** Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Tail of State Change Log

This dashboard report shows the tail (last 10 records) of the State Change Timeline. Placing this dashboard report in a dashboard can help you visualize the monitor health for a device and also decrease the monitoring of crucial devices. For more information, see the full State Change Timeline, which is linked to this dashboard report. The State Change Log shows a time line of when each monitor changed from one state to another during the displayed time period.

- **Start time.** The date and time of the state change. Click a time to bring up the State Change Timeline for a single device.
- **Device.** The device on which the action is configured. Click a device to bring up the Device Status report.
- **Monitor.** The active monitor by type. Click an active monitor to bring up the Active Monitor Availability report for that monitor.

- **State.** The state of the condition at the time of the poll. Click a state to bring up the State Change Timeline for that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 3 width.** Enter a width for the Monitor column (column 3) in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Tail of Syslog

This dashboard report displays the tail (last 10 records) of the Syslog Entries Report. Placing this dashboard report in a dashboard grants visual access to Syslog log entries for the system. For more information, this dashboard report is linked to the Syslog Entries report, which shows Syslog events logged for the system during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Syslog listener must be enabled, and either a Syslog passive monitor must be added to a device or unsolicited messages must be accepted. For more information, see *Enabling the Syslog listener* (on page 875).

- **Date.** The date and time the Syslog entry was received by WhatsUp Gold.
- **Device.** The device for which the message was configured.
- **Syslog Type.** The type of message.
- **Payload.** The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed within a packet or other transmission unit.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Device column in pixels.
 - **Column 4 width.** Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Tail of Windows Event Log

This dashboard report displays the tail (last 10 records) of the Windows Event Log. Placing this dashboard report in a dashboard displays system-wide Windows events. For more information, this dashboard report is linked to the Windows Event Log, which shows Windows events logged during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Windows Event Log listener must be enabled. For more information on the Windows Event Log listener, see *Enabling the Windows Event Log Listener* (on page 874).

- **Date.** The date and time the event was received by WhatsUp Gold.
- **Device.** The device or program that originated the entry.
- **WinEvent Type.** The type of Windows Event.
- **Payload.** The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed with the event message.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Device column in pixels.
 - **Column 4 width.** Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

Problem Areas: Unacknowledged Devices

This home-level dashboard report displays unacknowledged devices in a specific group. Adding this dashboard report to a dashboard alerts you of unacknowledged devices in a group at a glance, allowing you to quickly resolve issues.

- **Device.** The network device.
- **Device Type.** The type of device.
- **Unacknowledged For.** The amount of time the device has gone unacknowledged.
- **In Maintenance.** Either Yes or No.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 3 width.** Enter a width for column 3 (in pixels).
- 3 Click **OK** to save changes.

Problem Areas: Web Alarms

This dashboard report shows a snapshot of the most recent web alarms fired on your network. Add this dashboard report to a highly visible dashboard so that recent issues can be noted and addressed if needed.

- **Date.** The date the alarm was fired. Click on a date to bring up the Web Alarms Report.
- **Source.** The source of the alarm, such as a device or active monitor. Click on a source to bring up the Device Status report. The icon next to the display name of the item shows the current state of that item.
- **Message.** The message produced by the web alarm.
- **Trigger.** This is the state that caused the web alarm to trigger. Click on a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Source column in pixels.
 - **Column 3 width.** Enter a width for the Message column in pixels.
- 3 Click **OK** to save changes.

Problem Areas Specific Device

In This Chapter

| | |
|---|-----|
| Problem Areas Specific Device: Down Active Monitors | 501 |
| Problem Areas Specific Device: Device Down Interfaces..... | 501 |
| Problem Areas Specific Device: Tail of Action Activity Log | 502 |
| Problem Areas Specific Device: Tail of Passive Monitor Error Log .. | 503 |
| Problem Areas Specific Device: Tail of SNMP Trap Log | 503 |
| Problem Areas Specific Device: Tail of State Change Log..... | 504 |
| Problem Areas Specific Device: Tail of Syslog | 505 |
| Problem Areas Specific Device: Tail of Windows Event Log | 505 |
| Problem Areas Specific Device: Web Alarms | 506 |

Problem Areas Specific Device: Down Active Monitors

This device-level dashboard report displays the down active monitors for a device and their current state. The Down Active Monitors dashboard report displays the following information for a device:

- **Monitor.** The type of Active Monitor.
- **State.** The state of the Monitor after the last poll.

Adding this report to a Device Status dashboard keeps you updated on the health of the active monitors for an important device. If no active monitors appear in the report, none are currently down.

To see all Active Monitors on a device regardless of down state, see *General: Device Active Monitors* (on page 411).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click Browse (...) to select a device.
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Device Down Interfaces

This dashboard report displays down interfaces for a specific device.

- **Interface.** The network interface.
- **Status.** The status of the interface after the last poll.

Adding this dashboard report to a dashboard lets you quickly view the status of a particular device by showing you what interfaces are down on a device.

To help maximize the available viewing area on your monitor, limit the number of rows displayed in the report or decrease the width of the Status column.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Status column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Tail of Action Activity Log

This device-level dashboard report shows the tail (last 10 records) from the Action Log for a specified device. Placing this dashboard report in a device dashboard grants visual access to the success rate of actions fired for a particular device. Crucial devices can be monitored easily, and problems can be dealt with swiftly. For more information, the dashboard report is linked to the full Action Log, which shows all of the actions that WhatsUp Gold has attempted to fire on the device, based on the configuration of the action.

- **Date.** The date the action was fired. Click on a date to bring up the Action Log.
- **Source.** The source of the action. Click on a source to bring up the Device Status report.
- **Trigger.** The action's trigger. Either Up or Down. Click on a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Top count.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Tail of Passive Monitor Error Log

This dashboard report shows any performance monitor error logs that have occurred for a specified device.

- **Date.** The date the error occurred.
- **Category.** The category code of the error. Either Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error.)
- **Details.** Text that describes the error that was received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click Browse (...) to select a device.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 3 width.** Enter a width for the Details column.
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Tail of SNMP Trap Log

This device-level dashboard report displays the tail (last 10 records) of the SNMP Trap Log for a specified device. Placing this report in a device report grants visual access to SNMP traps for a particular device. For more information, the report is linked to the full SNMP Trap Log, which provides a history of SNMP traps that have occurred for a device during the time period displayed at the bottom of the report.

- **Date.** The date and time the trap occurred.
- **Device.** The device where the trap originated.
- **SNMP Trap Type.** The type of trap.
- **Payload.** the vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed within a packet or other transmission unit.



Note: In order for entries to be added to this report, the SNMP Trap listener must be enabled and an SNMP Trap passive monitor must be added to the device. For more information, see *Enabling the SNMP Trap Listener* (on page 873).

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of rows you would like displayed in the report.
 - **Column 2 width.** Enter a width for the Device column (in pixels).
 - **Column 4 width.** Enter a width for the Payload column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Tail of State Change Log

This device-level dashboard report shows the tail (last 10 records) from the State Change Timeline for a specified device. Placing this dashboard report in a device dashboard can visualize a device's monitor health and help ease the task monitoring crucial devices. For more information, the dashboard report is linked to the full State Change Log, which shows a time line of when each monitor on a device changed from one state to another during the displayed time period.

- **Start time.** The date and time of the state change. Click on a time to bring up the Device List.
- **Device.** The device the action is configured on. Click on a device to bring up the Device Status dashboard.
- **Monitor.** The active monitor by type.
- **State.** The state of the condition at the time of the poll. Click on a state to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Name.** Enter a title for the dashboard report.
 - **Top count.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Device column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Tail of Syslog

This device-level dashboard report displays the tail (last 10 records) from the Syslog Entries Report for a specified device. Placing this dashboard report in a device dashboard grants visual access to Syslog log entries for a particular device. For more information, this dashboard report has been linked to the Syslog Entries report, which shows Syslog events logged for the selected device during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Syslog listener must be enabled, and a Syslog passive monitor must be added to a device. For more information, see *Enabling the Syslog Listener* (on page 875).

- **Date.** The date and time the Syslog entry was received by WhatsUp Gold.
- **Syslog Type.** The type of message.
- **Payload.** The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed within a packet or other transmission unit.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Click browse (...) to select a device.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 3 width.** Enter a width for the Payload column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Tail of Windows Event Log

This dashboard report displays the tail (last 10 records) of the Windows Event Log for a specific device. Placing this dashboard report in a dashboard displays system-wide Windows events. For more information, this dashboard report is linked to the Windows Event Log, which shows Windows events logged during the time period displayed at the bottom of the report.



Note: In order for entries to be added to this report, the Windows Event Log listener must be enabled. For more information on the Windows Event Log listener, see *Enabling the Windows Event Log Listener* (on page 874).

- **Date.** The date and time the event was received by WhatsUp Gold.
- **WinEvent Type.** The type of Windows Event.

- **Payload.** The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed with the event message.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click browse (...) to select a device.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 3 width.** Enter a width for the Payload column (in pixels).
- 3 Click **OK** to save changes.

Problem Areas Specific Device: Web Alarms

This dashboard report shows a snapshot of the most recent web alarms fired on a particular device.

The following fields appear in this dashboard report:

- **Date.** The date the alarm was fired. Click a date to bring up the Web Alarms Report.
- **Message.** The message produced by the web alarm.
- **Trigger.** This is the state that caused the web alarm to trigger. Click a trigger to bring up the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the report.
 - **Device.** Browse for the device to display web alarms for.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column in pixels.
 - **Column 3 width.** Enter a width for the Payload column in pixels.
- 3 Click **OK** to save changes.

Remote/Central reports

In This Chapter

| | |
|---|-----|
| Remote/Central dashboard reports..... | 508 |
| Remote Reports: Remote Group List | 508 |
| Remote Reports: Remote Sites | 509 |
| Remote Reports: Remote Sites Overview | 510 |
| Remote Reports: Tail of Remote Site Log dashboard report | 511 |
| Remote Reports: Active Monitor States..... | 512 |
| Remote Reports: Device Status | 512 |
| Remote Reports: Monitor Status | 513 |
| Remote Reports: Summary Counts | 513 |
| Remote Reports: Tail of Action Activity Log dashboard report | 514 |
| Remote Reports: Top 10 Ping Response Time | 515 |
| Remote Report: Top 10 Ping Response Time over 1ms..... | 516 |
| Remote Reports: Top 10 Ping Packet Loss..... | 517 |
| Remote Reports: Top 10 Ping by Packet Loss over 50%..... | 518 |
| Remote Reports: Top 10 CPU by Utilization..... | 519 |
| Remote Reports: Top 10 CPU by Utilization over 80% dashboard report | 520 |
| Remote Reports: Top 10 Memory by Utilization dashboard report | 521 |
| Remote Reports: Top 10 Memory by Utilization over 80% dashboard report | 522 |
| Remote Reports: Top 10 Disk Utilization dashboard report | 523 |
| Remote Reports: Top 10 Disk Utilization over 80% dashboard report | 524 |
| Remote Reports: Top 10 Disk Free Space dashboard report | 525 |
| Remote Reports: Top 10 Disk Free Space Over 1024 MB dashboard report | 526 |
| Remote Reports: Top 10 Interface Utilization dashboard report | 527 |
| Remote Reports: Top 10 Interface Utilization Over 80% dashboard report | 528 |
| Remote Reports: Top 10 Interface Traffic Utilization Over 80% dashboard report | 529 |
| Remote Reports: Top 10 Interface with Traffic Over 50 Kbps dashboard report | 530 |
| Remote Reports: Top 10 Custom Performance Monitor dashboard report | 531 |
| Remote Reports: Top 10 Custom Performance Monitor with Threshold dashboard report | |

| | |
|---|-----|
| | 532 |
| Remote Reports: Top 10 Ping Availability dashboard report | 533 |
| Remote Reports: Top 10 Ping Availability Over 50%..... | 534 |

Remote/Central dashboard reports

| Remote/Central dashboard reports | Type | Description |
|--|------|--|
| (Only available in distributed editions) | | |
| Summary Counts (Remote) | Home | Provides a summary for a remote site by the total number of its monitored devices, up devices, down devices, devices with down active monitors, devices in maintenance, active monitors, down active monitors, up interfaces, down interfaces, actions fired in the last four hours. |
| Active Monitor States (Remote) | Home | Displays Active Monitor states for a remote site at the time of the last refresh. |
| Tail of Action Activity Log (Remote) | Home | Provides the tail (last 10 records) of the Action Log for a device group on a remote site. |
| Device Status (Remote) | Home | Displays a status summary for devices on a remote site at the time of the last refresh. |
| Monitor Status (Remote) | Home | Displays a status summary for monitors on a remote site at the time of the last refresh. |
| Remote Site List | Home | Lists all sites configured for use in WhatsUp Gold Remote and Central Site Editions. |
| Tail of Remote Site Log | Home | Provides the tail (last 10 records) of the Remote Site Log. |
| Remote Site Overview | Home | Displays an overview of information on a remote site configured for use in your WhatsUp Gold Distribute Solution. |
| Group List (Remote) | Home | Lists all subgroups in a remote site's My Network Group and their status at the time of the last refresh. |

Remote Reports: Remote Group List

This remote reports dashboard report lists all groups configured in a remote server's WhatsUp Gold My Network group and their status at the last refresh time. For more information, see Using the Remote/Central dashboard reports.

The report displays the following information:

- **Remote server.** The remote server selected for the report.
- Last run.
- **Group name.** The name of the remote server's My Network group.
- **Display name.** The names of all subgroups configured on the selected remote server.
- **Status.** The status of the groups at the time of the last run.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- 3 Click **OK** to save changes.

Remote Reports: Remote Sites

This Remote Report dashboard report lists all sites configured for use with WhatsUp Gold Remote and Central Site Editions. For more information, see *Using the Remote/Central dashboard reports* (on page 589).

This report displays the following information:

- **Display Name.** The Remote Site's display name.
- **Local device.** The device associated with the Remote Site. This device is often the computer that is running the WhatsUp software to monitor a Remote Site.
- **Last connect time.** The last time WhatsUp Gold connected to the Remote Site.
- **Last refresh time.** The last time data gathered from the Remote Site was refreshed.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Column 3 width.** Enter a width (in pixels) for the Last connect time column.
 - **Column 4 width.** Enter a width (in pixels) for the Last refresh time column.
- 3 Click **OK** to save changes.

Remote Reports: Remote Sites Overview

This remote reports dashboard report displays an overview of information on a Remote Site configured for use in your WhatsUp Gold Distributed Solution. For more information, see *Using the Remote/Central dashboard reports* (on page 589).

The name of the Remote Site is displayed in the upper-left side of the report. The **Last snapshot** is the time information gathered from the Remote Site was refreshed to display in this dashboard report.

The dashboard report displays the following information about the Remote Site:

- **Http address.** The Http address specified for the site at **Configure > Program Options > Central Site Configuration**.
- **Last connect time.** The last time WhatsUp Gold connected to the Remote Site.
- **Last refresh time.** The last time data gathered from the Remote Site was refreshed to display updated data.
- **# of devices.** The number of devices on the Remote Site.
- **# of monitors.** The number of monitors configured for the devices on the Remote Site.
- **# of queries.** The number of queries running on the Remote Site.
- **Display name.** The Remote Site device's display name.
- **Device type.** The Remote Site device's type.
- **Host name.** The Remote Site device's host name.
- **Address.** The Remote Site device's address.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.

- **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Local device.** Allows users, with rights, the ability to select a local device to associate the Remote Site with. Click the browse (...) button to select a device. This device is often the computer that is running the WhatsUp software on a Remote Site. Associating a local device allows you to view the device status from the Remote Site, keeping you informed about the connection status with the Remote Site. It also provides easy access to the Network Tools for the local device you selected.

Click **OK** to save changes.

Remote Reports: Tail of Remote Site Log dashboard report

This home-level Remote Reports dashboard report displays the tail (last 10 records) of the Remote Site Log. The report displays information for both a WhatsUp Gold Client and a Server, depending on which version of WhatsUp Gold you are running. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Date.** The date the error took place.
- **Type.** The type of the error message received.
- **Message.** The error message received.
- **Remote Site.** The Remote Site on which the failed connection took place.



Note: The Remote site column is only displayed when you are running the Server Distributed version of WhatsUp Gold.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.

- **Column 1 width.** Enter a width for the column in pixels.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Active Monitor States

This remote report dashboard report lists all Active Monitors assigned to devices on the selected Remote Site. For more information, see Using the Remote/Central dashboard reports.

The table included in the dashboard report lists each device by display name, and the state of all Active Monitors assigned to each device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Remote active monitor type.** Select a remote active monitor type for the report. The default is All active monitor types.
 - **Internal monitor state.** Select an internal monitor state (All states, Up, Maintenance, Down, Unknown) for the report.
- 3 Click **OK** to save changes.

Remote Reports: Device Status

This remote dashboard report provides a status summary of all monitored devices on a Remote Site according to the last refresh time. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Display name.** The display name for the monitored device.
- **Devices up.** The number of monitored devices on the Remote Site in the Up state at the last connect time.
- **Devices down.** The number of monitored devices on the Remote Site in the Down state at the last connect time.

- **In maintenance.** The number of monitored devices on the Remote Site in the maintenance at the last connect time.
- **Last refresh time.** The last time data gathered from the Remote Site was refreshed to display updated data.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- 3 Click **OK** to save changes.

Remote Reports: Monitor Status

This remote dashboard report provides a status summary of all monitors configured for the monitored devices on a Remote Site according to the last refresh time. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Display name.** The monitored device's display name.
- **Monitors up.** The total number of monitors on the Remote Site in the Up state at the last connect time.
- **Monitors down.** The total number of monitors on the Remote Site in the Down state at the last connect time.
- **Last refresh time.** The last time data gathered from the Remote Site was refreshed to display updated data.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- 3 Click **OK** to save changes.

Remote Reports: Summary Counts

This remote reports dashboard report provides a summary for a Remote Site by the total number of:

- Monitored devices
- Up devices
- Down devices
- Devices with down Active Monitors

- Devices in Maintenance
- Active Monitors
- Down Active Monitors
- Up interfaces
- Down interfaces
- Actions fired in the last 4 hours

For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains these pieces of information:

- **Count.** The total number of that specific type of passive monitor on the network.
- **Total number of.** The device status types.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- 3 Click **OK** to save changes.

Remote Reports: Tail of Action Activity Log dashboard report

This remote reports dashboard report shows the tail (last 10 records) of the Action Log for a device group on a Remote Site. Placing this dashboard report in a dashboard grants visual access to the success rate of actions fired for a particular device group on a Remote Site. Crucial devices can be monitored easily, and problems can be dealt with swiftly. For more information, the dashboard report is linked to the full Action Log, which shows all of the actions that WhatsUp Gold has attempted to fire on the group, based on the configuration of the action. For more information, see Using the Remote/Central dashboard reports.

The dashboard report displays the following information about the Remote Site:

- **Date.** The date the action was fired. Click on a date to bring up the Action Log.
- **Source.** The source of the action. Click on a source to bring up the Device Status report.
- **Action Name.** The name of the Action.
- **Trigger.** The trigger for the action. Either Up or Down. Click on a trigger to open the State Change Timeline.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.
 - **Note:** The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.
 - **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the hostname report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
 - **Column 3 width.** Enter a width for the Payload column in pixels.
- 3** Click **OK** to save changes.

Remote Reports: Top 10 Ping Response Time

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their ping response times. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at each device's Max and Avg columns. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The network interface.
- **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Remote Report: Top 10 Ping Response Time over 1ms

This home-level dashboard report displays ping response times by threshold for devices in a specific device group on a Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at devices with ping response times over 1ms. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The network interface.
- **Max (ms).** The maximum response time in milliseconds.
- **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the drop down menu.



Note: Though the default threshold is 1ms, you can change this threshold. If you do so, you should change the report title accordingly.

- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Column 2 width.** Enter a width for the column (in pixels).

3 Click **OK** to save changes.

Remote Reports: Top 10 Ping Packet Loss

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their ping packet loss percentages at the last poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at the colors associated with each packet loss percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The network interface.
- **Sent.** The number of packets sent.
- **Lost.** The number of packets lost.
- **% Loss.** The percentage of sent packets that have been lost.



Note: All of the data displayed in this dashboard report is based on the latest poll.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Ping by Packet Loss over 50%

This home-level dashboard report displays packet loss information and percentages for devices in a specific group from a Remote Site based on the latest poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their ping packet loss by glancing at each device's ping packet loss over 50%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The network interface.
- **Sent.** The number of packets sent from the device.
- **Lost.** The total number of packets lost from the device
- **% Lost.** The percentage of sent packets that have been lost.



Note: All of the data displayed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 50%, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Remote Reports: Top 10 CPU by Utilization

This home-level dashboard report displays the top devices in a group from a Remote Site based on their current CPU utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains these pieces of information.

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.

- **CPU.** The device's CPU description.
- **CPU Load.** The percentage of CPU currently in use.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 CPU by Utilization over 80% dashboard report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their current CPU utilization percentage thresholds. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load by glancing at each device's current CPU utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Description.** The device description.
- **CPU Load.** The percentage of the CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the drop down menu.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Memory by Utilization dashboard report

This home-level dashboard report displays the top devices in group on a Remote Site, based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory load by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.

- **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- **Percent Used.** The percentage of utilized memory.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Memory by Utilization over 80% dashboard report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory capacity by glancing at each device's current memory utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- **Percent Used.** The percentage of utilized memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Disk Utilization dashboard report

This home-level dashboard report displays the top devices based on their percentage of utilized disk space on a Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk load by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.

- **Disk.** The device's drive description.
- **Percent Full.** The percentage of the disk currently utilized.

For more information, see Using the Remote/Central dashboard reports.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Disk Utilization over 80% dashboard report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their percentage of disk utilization. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their disk utilization by glancing at each device's current disk utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Disk.** The device's drive description.
- **Percent Full.** The amount of utilized disk space on that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the drop down menu.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Disk Free Space dashboard report

This home-level dashboard report displays the top devices in a group on a Remote Site, based on their percentage of available free space on the Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current level of disk free space by glancing at the current disk percentage level for each device. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Disk.** The device's drive description.

- **Size.** The size of the disk in GB.
- **Free space.** The amount of free space on the disk in GB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.
 - **Note:** The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.
 - **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Disk Free Space Over 1024 MB dashboard report

This home-level dashboard report displays the top devices based on their available free space over 1024 MB on a Remote Site. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current level of disk free space by glancing at each device's current disk space level over 1024 MB.

For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Disk.** The device drive description.
- **Size.** The size of the disk in GB.
- **Free space.** The amount of free space on the disk in GB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 1024MB, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Interface Utilization dashboard report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface utilization percentages. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The device's interface description.
- **Transmit.** The number of packets transmitted from each interface.
- **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Interface Utilization Over 80% dashboard report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface utilization over 80%. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The device's interface description.
- **Transmit.** The number of packets transmitted from each interface.
- **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following fields.

- **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 80%, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column in pixels.

3 Click **OK** to save changes.

Remote Reports: Top 10 Interface Traffic Utilization Over 80% dashboard report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface utilization percentages. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The device interface description.
- **Transmit.** The number of packets transmitted from each interface.
- **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Interface with Traffic Over 50 Kbps dashboard report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their current interface with traffic over 50 Kbps. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The device's interface description.
- **Transmit.** The number of packets transmitted from each interface.
- **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

2 Enter or select the appropriate information for the following fields.

- **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
- **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the drop down menu.



Note: Though the default threshold is 50Kbps, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column in pixels.

3 Click **OK** to save changes.

Remote Reports: Top 10 Custom Performance Monitor dashboard report

This home-level dashboard report displays top devices in a remote group based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.
- **For group.** The group you selected to display in the report.
- **Device.** The device associated with the custom performance monitor. Clicking on the device will bring up its Device Status dashboard.
- **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list will be empty.
 - **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Custom Performance Monitor with Threshold dashboard report

This home-level dashboard report displays top devices in a group from a Remote Site, based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.
- **For group.** The group you selected to display in the report.

- **Device.** The device associated with the custom performance monitor. Clicking on the device will bring up its Device Status dashboard.
- **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list will be empty.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the drop down menu.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Ping Availability dashboard report

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their ping availability percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.

- **Device.** The network device.
- **Interface.** The network interface.
- **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the Ping Availability report.
- **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select Menu > Configure. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3 Click **OK** to save changes.

Remote Reports: Top 10 Ping Availability Over 50%

This home-level dashboard report displays the top devices in a group from a Remote Site, based on their ping availability percentage over 50%. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level. For more information, see Using the Remote/Central dashboard reports.

Each entry in the report contains the following information:

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.
- **Device.** The network device.
- **Interface.** The network interface.

- **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the Ping Availability report.
- **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select Menu > Configure. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Remote site.** Select a Remote Site for the report from the list.



Note: The Remote Sites in this list are populated on the WhatsUp Gold console at **Configure > Program Options > Central Site Configuration**.

- **Device Group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report displays the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and display when **Include 'Others'** is selected.
- **Threshold.** Enter a number for the threshold and select a threshold criteria symbol (under, equals, over) from the list.



Note: Though the default threshold is 50%, you can change this threshold. If you do so, you should change the report title accordingly.

- **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Split Second Graph reports

In This Chapter

| | |
|---|-----|
| Split Second Graph dashboard reports | 536 |
| Using Split Second Graph dashboard reports..... | 537 |
| Split Second Graph: CPU dashboard report..... | 537 |
| Split Second Graph: CPU Gauge dashboard report | 539 |
| Split Second Graph: Disk dashboard report | 540 |
| Split Second Graph: Interface dashboard report | 541 |
| Split Second Graph: Memory dashboard report | 542 |
| Split Second Graph: Performance Monitor dashboard report | 544 |
| Split Second Graph: Ping dashboard report..... | 545 |
| Split Second Graph: Ping Gauge dashboard report..... | 546 |
| Split Second Graph: Task Manager CPU dashboard report..... | 547 |
| Split Second Graph: Task Manager CPU Bar dashboard report | 548 |
| Split Second Graph: Task Manager Memory dashboard report | 549 |
| Split Second Graph: Task Manager Memory Bar dashboard report | 550 |

Split Second Graph dashboard reports

| Split Second Graph dashboard reports (not available in Standard Edition) | Type | Description |
|--|----------------|--|
| Performance Monitor | Home | Displays custom real-time graphs for an SNMP or WMI enabled device. |
| Interface | Home | Displays real-time interface utilization for an SNMP-enabled device. |
| CPU | Home Or Device | Displays real-time cpu utilization for all CPUs on an SNMP-enabled device. |
| CPU gauge | Home or device | Displays real-time cpu utilization for all CPUs on an SNMP-enabled device. |

| Split Second Graph dashboard reports | Type | Description |
|--------------------------------------|----------------|--|
| Ping | Home Or Device | Displays real-time ping response time for all network interfaces on a device. |
| Ping gauge | Home or device | Displays real-time ping response time for all network interfaces on a device. |
| Disk | Home or device | Displays real-time disk utilization for all disks on an SNMP-enabled device. |
| Memory | Home or Device | Displays real-time memory utilization for an SNMP enabled-device. |
| Task Manager CPU Line Graph | Home or Device | Displays the CPU usage of a WMI-enabled device as a line graph. |
| Task Manager Memory Usage Line Graph | Home or Device | Displays the memory usage of a WMI-enabled device as a line graph. |
| Task Manager CPU Bar Graph | Home or Device | Displays a bar graph of the CPU usage of a WMI-enabled device in real time. |
| Task Manager Memory Bar Graph | Home or Device | Displays a bar graph of the memory usage of a WMI-enabled device in real time. |

Using Split Second Graph dashboard reports

Split Second Graph dashboard reports allow you to embed real-time data available from InstantInfo popups, the Web Task Manager, and the Web Performance Monitor into any dashboard view.

For information on how to add a dashboard report to a dashboard view, see *Adding dashboard reports to a dashboard view* (on page 342).

Split Second Graph: CPU dashboard report

This dashboard report displays real-time CPU utilization for all CPUs on an SNMP-enabled device. The device must have SNMP credentials specified in **Device Properties** > **Credentials**. This report queries the specified device for a list of all CPUs and then polls and graphs each of them for the duration that the report is loaded in the web browser.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

Split Second Graph: CPU Gauge dashboard report

This dashboard report displays real-time CPU utilization for all CPUs on an SNMP-enabled device. The device must have SNMP credentials specified in Device **Properties > Credentials**. This report queries the specified device for a list of all CPUs and then polls and graphs each of them for the duration that the report is loaded in the web browser.



Note: The transparent dial indicates the CPU minimum or maximum utilization percentage and the solid dial indicates the current CPU utilization percentage. If there are two CPUs on a device, only data for one CPU displays on the gauge at a time. Click a CPU in the legend (Intel 1 or Intel 2) to place focus on a particular CPU gauge.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the dashboard report title bar, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Graph type.** Select a graph size for the gauge, either Small, Medium, or Large.
 - **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** This value determines the amount of time that WhatsUp Gold uses to determine the gauge's average value. For example, if the gauge's data interval is set to 60 seconds, the value reported on the gauge is calculated by averaging the minimum value and the maximum value reported over that 60 second timeframe.
- 3 Click **OK** to save changes.

Split Second Graph: Disk dashboard report

This dashboard report displays real-time disk utilization for all disks on a SNMP enabled device. The device must have SNMP credentials specified in **Device Properties > Credentials**. This report queries the specified device for a list of all disks and then polls and graphs each of them for the duration that the report is loaded in the Web browser.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.

- **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

Split Second Graph: Interface dashboard report

This dashboard report displays real-time interface utilization for an SNMP enabled device. The device must have SNMP credentials specified in **Device Properties > Credentials**.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.



Note: This dashboard report is only available on Home dashboard views.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Interface name.** For devices with more than one interface, select a device by click the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.

- **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
- **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

3 Click **OK** to save changes.

Split Second Graph: Memory dashboard report

This dashboard report displays real-time memory utilization for a SNMP enabled device. The device must have SNMP credentials specified in Device Properties > Credentials. This report queries the specified device to determine if it can report memory utilization and then polls and graphs it for the duration that the report is loaded in the Web browser.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 2 Click **OK** to save changes.

Split Second Graph: Performance Monitor dashboard report

For more information on building custom graphs, please see the Web Performance Monitor help.



Note: This dashboard report is only available on Home dashboard views.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Click browse (...) and select the device you want to monitor.
 - **Interface to graph.** Select the device interface to graph from the list.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - **Auto Scale** adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - **Fixed Scale** shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see *Graph Types* (on page 610).
- **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.
- **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

Split Second Graph: Ping dashboard report

This dashboard report displays real-time PING response time for all network interfaces on a device. This report queries the database for a list of all configured network interfaces and then polls and graphs each of them for the duration that the report is loaded in the web browser.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Interface to graph.** Select which interface to ping.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Vertical Axis Scale.** Select how you want the vertical axis, or Y axis, of this graph to display.
 - Auto Scale adjusts the axis value based on the minimum and maximum values of the data being displayed.
 - Fixed Scale shows the data on the scale you enter in the Min and Max boxes.



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

- **Graph Type.** Select the type of graph you would like to display. To learn about the various types of graphs available, please see Graph Types.
- **Trend Type.** Select the type of trend line you want to see on the report. This line shows the average value of data for the duration the graph is displayed in the Web browser. Choose None, Line, or Curve.
- **Dimensions.** Select the dimension in which you would like the graph to display. Select 3D or 2D to change the dimensions of the lines/bars in your charts.

- **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.

Split Second Graph: Ping Gauge dashboard report

This dashboard report displays real-time PING response time for all network interfaces on a device. This report queries the database for a list of all configured network interfaces and then polls and graphs each of them for the duration that the report is loaded in the Web browser.

- 1 To configure this dashboard report in WhatsUp Gold:
- 2 In the title bar of the dashboard report pane, select Menu > Configure. The Configure Report dialog appears.
- 3 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Interface to graph.** For devices with more than one interface, select an interface to graph by clicking the Browse (...) button.
 - **Graph type.** Select a graph size for the gauge, either Small, Medium, or Large.
 - **Maximum ping response time (ms).** The maximum number displayed on the gauge. Enter a number (in ms) for this maximum time.
 - **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** This value determines the amount of time that WhatsUp Gold uses to determine the gauge's average value. For example, if the gauge's data interval is set to 60 seconds, the value reported on the gauge is calculated by averaging the minimum value and the maximum value reported over that 60 second timeframe.
- 4 Click **OK** to save changes.

Split Second Graph: Task Manager CPU dashboard report



This dashboard report displays the CPU usage of specific device as a line graph. The device must have Windows credentials specified in **Device Properties > Credentials**. This dashboard report shows current real-time data as well as historical data plotted on the line graph. The graph shows up to x seconds of historical data.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

Split Second Graph: Task Manager CPU Bar dashboard report

This dashboard report displays a bar graph of the CPU usage of a specific device in real time. The device must have Windows credentials specified in **Device Properties > Credentials**. You must configure this dashboard report and select a device before any data is reported.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

Split Second Graph: Task Manager Memory dashboard report

This dashboard report displays the memory usage of specific device as a line graph. The device must have Windows credentials specified in **Device Properties > Credentials**. This dashboard report shows current real-time data as well as historical data plotted on the line graph. The graph shows up to x seconds of historical data.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

- 3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

Split Second Graph: Task Manager Memory Bar dashboard report

This dashboard report displays a bar graph of the memory usage of a specific device in real time. The device must have Windows credentials specified in **Device Properties > Credentials**. You must configure this dashboard report and select a device before any data is reported.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Refresh interval (seconds).** Enter an amount of time (in seconds) for how often you would like the graph to refresh. Essentially, when the graph refreshes, it is polling for more data and then displaying that new data.



Note: The faster the refresh interval, the more granular the chart data will be. Slower poll intervals will result in data that is more normalized and will have less detail.

- **Data interval (seconds).** Enter an amount of time (in seconds) for how long you would like the data in the graph to be displayed. Think of this as the X axis for the graph.



Note: Specifying larger values for this setting is allowed, but may adversely affect the refresh interval for a graph. The optimum value is determined by the memory and speed of your Web server.

3 Click **OK** to save changes.



Note: This dashboard report can only be used with devices that are WMI-enabled.

Threshold reports

In This Chapter

| | |
|---|-----|
| Threshold dashboard reports | 552 |
| Threshold: CPU Utilization..... | 553 |
| Threshold: Custom Performance Monitor | 553 |
| Threshold: Disk Free Space | 554 |
| Threshold: Disk Utilization | 555 |
| Threshold: Interface Traffic | 556 |
| Threshold: Interface Utilization | 557 |
| Threshold: Memory Utilization | 557 |
| Threshold: Ping Availability | 558 |
| Threshold: Ping Packet Loss | 559 |
| Threshold: Ping Response Time | 559 |

Threshold dashboard reports

| Threshold dashboard reports | Type | Description |
|-----------------------------|------|--|
| Ping Response Time* | Home | Displays the top devices based on their current ping response time thresholds. |
| Ping Packet Loss | Home | Displays the top devices based on their current ping packet loss thresholds. |
| CPU Utilization | Home | Displays the top devices based on their current CPU utilization percentage thresholds. |
| Memory Utilization | Home | Displays the top devices based on their current memory utilization percentage thresholds. |
| Disk Utilization | Home | Displays the top devices based on their current disk utilization percentage thresholds. |
| Disk Free Space* | Home | Displays the top devices based on their current disk free space thresholds. |
| Interface Utilization | Home | Displays the top devices based on their current interface utilization percentage thresholds. |
| Interface Traffic* | Home | Displays the top devices based on their current interface traffic thresholds. |
| Ping Availability | Home | Displays the top devices based on their current ping availability thresholds. |

| Threshold dashboard reports | Type | Description |
|-----------------------------|------|--|
| Custom Performance Monitor | Home | Displays the value for performance monitors on devices over, under or equal to a configured threshold value. |

Threshold: CPU Utilization

This home-level dashboard report displays the top devices based on their current CPU utilization percentage thresholds. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Description.** The description of the device.
- **CPU Load.** The percentage of the CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Custom Performance Monitor

This home-level dashboard report displays the top devices based on a selected custom WMI or SNMP performance monitor.

The top of the report displays the name of the selected custom performance monitor and to which device group the report applies.

Each entry in the report contains the following information:

Device. The monitored network device.

Value. The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
2. Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Performance monitor.** Choose a performance monitor from the drop-down menu. If there are no performance monitors listed in the drop-down menu, you must first configure a custom WMI or SNMP performance monitor from the Performance Monitor Library.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria from the separate list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
3. Click **OK** to save the changes.

Threshold: Disk Free Space

This home-level dashboard report displays the top devices based on their percentage of available free disk space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk capacity by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Disk.** The device's drive description.
- **Size.** The size of the disk in MB.
- **Free space.** The amount of free space on the disk in MB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column in pixels.
- 3 Click **OK** to save changes.

Threshold: Disk Utilization

This home-level dashboard report displays the top devices based on their percentage of disk utilization. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their disk utilization by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Disk.** The description of the drive.
- **Percent Full.** The amount of utilized disk space on that device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter the or select appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Interface Traffic

This home-level dashboard report displays interface traffic information for a specified device group based on the number of packets both sent and received. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current interface traffic rates by glancing at the numbers in the transmit and receive columns for each device.

- **Device.** The network device.
- **Interface.** The interface description.
- **Transmit.** The number of packets sent.
- **Receive.** The number of packets received.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Interface Utilization

This home-level dashboard report displays the top devices based on their percentage of transmitted and received packets. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their interface utilization by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Interface.** The network interface.
- **Transmit.** The percentage of packets transmitted by a device.
- **Receive.** The percentage of packets received by a device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Memory Utilization

This home-level dashboard report displays the top devices based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory capacity by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- **Percent Used.** The percentage of utilized memory.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Ping Availability

This home-level dashboard report displays ping availability information for a specific device. A graph displays in the dashboard, charting the device response time to pings (in msec) over the amount of time defined by the specific report type.

- **Device.** The network device.
- **Interface.** The network interface.
- **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Ping Packet Loss

This home-level dashboard report displays packet loss information and percentages for devices in a specific group, based on the latest poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their ping packet loss by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Interface.** The network interface.
- **Sent.** The number of packets sent from the device.
- **Lost.** The total number of packets lost from the device
- **% Lost.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the drop down menu.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3 Click **OK** to save changes.

Threshold: Ping Response Time

This home-level dashboard report displays ping response times for devices in a specific device group. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at the Max and Avg columns for each device.

- **Device.** The network device.
- **Interface.** The network interface.

- **Max (ms).** The maximum response time in milliseconds.
- **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices regardless of their subgroups.
 - **Threshold.** Enter a number for the threshold and select a threshold criteria symbol from the list.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the Description column (in pixels).
- 3** Click **OK** to save changes.

Top 10 reports

In This Chapter

| | |
|--|-----|
| Top 10 dashboard reports..... | 561 |
| Top 10: CPU Utilization | 562 |
| Custom Performance Monitor Top 10 (Specific Monitor) | 562 |
| Top 10: Disk Free Space..... | 563 |
| Top 10: Disk Utilization | 563 |
| Interface Errors and Discards: Top X by Number of Discards | 564 |
| Interface Errors and Discards:Top X by Number of Errors..... | 565 |
| Top 10 by Interface Traffic..... | 565 |
| Top 10 by Interface Utilization..... | 566 |
| Top 10: Memory Utilization..... | 566 |
| Top 10: Ping Availability..... | 567 |
| Top 10: Ping Packet Loss..... | 568 |
| Top 10: Ping Response Time..... | 569 |

Top 10 dashboard reports

| Top 10 dashboard reports | Type | Description |
|----------------------------|------|--|
| Ping Response Time | Home | Displays the top devices based on their current ping response time. |
| Ping Packet Loss | Home | Displays the top devices based on their current ping packet loss. |
| CPU Utilization | Home | Displays the top devices based on their current CPU utilization. |
| Memory Utilization | Home | Displays the top devices based on their current memory utilization. |
| Disk Utilization | Home | Displays the top devices based on their current disk utilization. |
| Disk Free Space | Home | Displays the top devices based on their current disk free space. |
| Interface Utilization | Home | Displays the top devices based on their current interface utilization. |
| Interface Traffic | Home | Displays the top devices based on their current interface traffic. |
| Custom Performance Monitor | Home | Displays the value for performance monitors on devices over, under or equal to a configured threshold value. |
| Ping Availability | Home | Displays the top devices based on their current ping availability. |

| Top 10 dashboard reports | Type | Description |
|--------------------------|------|---|
| Interface Errors | Home | Displays the top devices based on total interface errors. |
| Interface Discards | Home | Displays the top devices based on total interface discards. |

Top 10: CPU Utilization

This home-level dashboard report displays the top devices based on their current CPU utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current CPU load. Report percentages are displayed in colors that represent the CPU utilization thresholds:

- Red. Above 90%
- Yellow. Above 80%
- Green. 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **CPU.** The device CPU description.
- **CPU Load.** The percentage of CPU currently in use.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 (in pixels).
- 3 Click **OK** to save changes.

Custom Performance Monitor Top 10 (Specific Monitor)

This home-level dashboard report displays top devices in a group based on their association with a custom WMI or SNMP performance monitor. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their custom performance monitor values.

- **Custom performance monitor.** The custom performance monitor you chose to watch in this dashboard report.
- **For group.** The group you selected to display in the report.
- **Device.** The device associated with the custom performance monitor. Clicking on the device opens its Device Status dashboard.
- **Value.** The value returned from the custom performance monitor.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the browse (...) button. Select **Every device** to select all devices regardless of their subgroups.
 - **Performance monitor.** The custom performance monitor you want to monitor in this report. This list is populated with any custom performance monitors you have configured in the Performance Monitor Library. If you have not configured any custom performance monitors, the list is empty.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
- 3 Click **OK** to save changes.

Top 10: Disk Free Space

This home-level dashboard report displays the top devices based on their percentage of available free space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current level of disk free space by glancing at the current disk percentage level for each device.

- **Device.** The network device.
- **Disk.** The drive description.
- **Size.** The size of the disk in GB.
- **Free space.** The amount of free space on the disk in GB.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Choose a device group for monitoring. Select **Every device** to select all devices.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Top 10: Disk Utilization

This home-level dashboard report displays the top devices based on their percentage of utilized disk space. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current disk load by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Disk.** The drive description.
- **Percent Full.** The percentage of the disk currently utilized.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Interface Errors and Discards: Top X by Number of Discards

This home-level dashboard report displays the top device interfaces with packet discards for inbound and outbound data during a selected time period.

- **Device.** The network device name.
- **Interface.** The interface description.
- **Transmit.** The number of discarded packets transmitted from each interface.
- **Receive.** The number of discarded packets received from each interface.
- **Total.** Provides the number of packets discarded for each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.

- **Device group.** Select all devices or a specific device group for the dashboard report. Select **Every device** or clear **Every device** if you want to select a specific device group, then click the browse (...) button to select the device group you want to include in this dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Interface Errors and Discards:Top X by Number of Errors

This home-level dashboard report displays the top device interfaces with packet errors for inbound and outbound data during a selected time period.

- **Device.** The network device name.
- **Interface.** The interface description.
- **Transmit.** The number of packets transmitted from each interface.
- **Receive.** The number of packets received from each interface.
- **Total.** Provides the number of packet errors for each interface.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select all devices or a specific device group for the dashboard report. Select **Every device** or clear **Every device** if you want to select a specific device group, then click the browse (...) button to select the device group you want to include in this dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Top 10 by Interface Traffic

This home-level dashboard report displays the top devices in a group based on their current interface traffic as a total of packets transmitted and received.

- **Device.** The network device.
- **Interface.** The device's interface description.
- **Transmit.** The number of packets transmitted from each interface.
- **Receive.** The number of packets received from each interface.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column in pixels.
- 3** Click **OK** to save changes.

Top 10 by Interface Utilization

This home-level dashboard report displays the top devices in a group based on their interface utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial interfaces and their current utilization by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Interface.** The interface description.
- **Transmit.** The percentage of packets transmitted from each interface.
- **Receive.** The percentage of packets received from each interface.

To configure this dashboard report:

- 1** Select **Configure** from the dashboard report menu.
- 2** Enter the appropriate information.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3** Click **OK** to save changes.

Top 10: Memory Utilization

This home-level dashboard report displays the top devices based on their memory utilization percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current memory load by glancing at the colors associated with each percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Memory.** The memory type. For example, Physical Memory or Virtual Memory.
- **Percent Used.** The percentage of utilized memory.

To configure this dashboard report:

- 1 Select **Configure** from the dashboard report menu.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for column 2 (in pixels).
- 2 Click **OK** to save changes.

Top 10: Ping Availability

This home-level dashboard report displays the top devices in a group based on their ping availability percentages. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at each device's current ping availability percentage level.

- **Device.** The network device.
- **Interface.** The network interface.
- **Polled Min.** Amount of total time (in minutes) that passed during the time period selected in the *Ping Availability* (on page 650) report.
- **Unavailable.** Amount of total time (in minutes) that the device was unavailable in the group.
- **Percent Available.** The total availability percentage for the device.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records you would like displayed in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Top 10: Ping Packet Loss

This home-level dashboard report displays the top devices in a group based on their ping packet loss percentages at the time of the last poll. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices by glancing at the colors associated with each packet loss percentage level:

- **Red.** Above 90%
- **Yellow.** Between 80% and 90%
- **Green.** 80% or less

Each entry in the report contains the following information:

- **Device.** The network device.
- **Interface.** The network interface.
- **Sent.** The number of packets sent.
- **Lost.** The number of packets lost.
- **% Loss.** The percentage of sent packets that have been lost.



Note: All of the data listed in this dashboard report is based on the latest poll.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device group.** Select a device group by clicking the **Browse (...)** button. Select **Every device** to select all devices regardless of their subgroups.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
 - **Top count.** Enter the number of records to display in the dashboard report.
- 3 Click **OK** to save changes.

Top 10: Ping Response Time

This home-level dashboard report displays the top devices in a group based on their ping response times. Placing this dashboard report in a dashboard allows you to keep tabs on crucial devices and their current ping response times by glancing at each device's Max and Avg columns.

- **Device.** The network device.
- **Interface.** The network interface.
- **Avg (ms).** The average response time in milliseconds.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Maximum rows to return.** Enter the number of records to display in the dashboard report.
 - **Column 2 width.** Enter a width for the column (in pixels).
- 3 Click **OK** to save changes.

Virtualization reports

In This Chapter

| | |
|---|-----|
| Virtualization: Virtual Host..... | 570 |
| Virtualization: Virtual Machine Current Instant CPU Utilization | 571 |
| Virtualization: Virtual Machine Current Disk Utilization | 572 |
| Virtualization: Virtual Machine Current Interface Utilization | 572 |
| Virtualization: Virtual Machine Current Memory Utilization | 573 |
| Virtualization: Virtual Server | 574 |
| Virtualization: Virtual Server Attributes | 575 |
| Virtualization: WhatsVirtual Events | 576 |

Virtualization: Virtual Host

This home-level dashboard report displays details about a virtual host. Placing this dashboard report in a dashboard allows you to track details about the virtual host, as well as the number and power states of virtual machines associated with the virtual host.

- **VM Host details for.** Displays the name, host name and IP address of the VM host.
- **Virtual Devices.** Lists the virtual devices associated with the VM host.
- **Host Attributes.** List the attributes of the VMware server software running on the VMware host.
- **Name.** The name of the VMware server software running on the VMware host.
- **VIM Version.** The version of the VMware server software running on the VMware host.
- **API Version.** The version of the VMware Application Programming Interface (API) used to gather information and issue commands to the virtual machines hosted by the VMware host.
- **Build.** The build number of the VMware server software running on the VMware host.
- **Boot Time.** The time and date of the latest boot of the VMware host server.
- **Hardware Information.** Information about the hardware of the VMware host server.
- **Vendor.** The name of the vendor who manufactured the CPUs used by the VMware host server.
- **Model.** The model number of the CPUs available to the VMware host server.
- **CPU Cores.** The number of CPU cores available to the VMware host server.
- **CPU Packages.** The number of CPU packages available to the VMware host server.
- **CPU Threads.** The total number of CPU threads available to the VMware host server.

- **CPU Frequency.** The CPU frequency of the CPU cores available to the VMware host server.
- **CPU Model.** The CPU model of the CPUs available to the VMware host server.
- **VM Information.** Information about the virtual machines associated with the VMware host server.
- **Total VM's.** The total number of virtual machines associated with the VMware host server.
- **Powered On.** The number of virtual machines in the Powered On state.
- **Powered Off.** The number of virtual machines in the Powered Off state.
- **Suspended.** The number of virtual machines in the Suspended state.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Select Devices or Groups.** Click to select the virtual hosts, or groups containing virtual hosts, to display in the report.
- 3 Click **OK** to save the changes.

Virtualization: Virtual Machine Current Instant CPU Utilization

The Virtual Machines Current CPU Utilization dashboard report provides a list of the virtual machines associated with a virtual host or vCenter server, and CPU utilization values for each virtual machine.

- **Virtual Machine.** Displays the name of the virtual machine as reported by the virtual host.
- **1 hour Avg.** Displays the average CPU utilization for the past hour.
- **1 hour Max.** Displays the maximum CPU utilization in the past hour.
- **Current.** Displays the current CPU utilization.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click the browse (...) button. The Select a Device dialog appears.
- 3 Select the server you want to view in the report.
- 4 Click **OK**. The Select a Device dialog closes and the Configure Graph menu appears.
- 5 Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Virtualization: Virtual Machine Current Disk Utilization

The Virtual Machines Current Disk Utilization home dashboard report provides a list of the virtual machines associated with a virtual host or vCenter server, and disk utilization values for each virtual machine.

- **Virtual Machine.** Displays the name of the virtual machine as reported by the virtual host.
- **1 hour Avg.** Displays the average bit rate for Read and Write disk operations for the past hour.
- **1 hour Max.** Displays the maximum bit rate for Read and Write disk operations in the past hour.
- **Current.** Displays the current bit rate for Read and Write disk operations.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click the browse (...) button. The Select a Device dialog appears.
- 3 Select the server you want to view in the report.
- 4 Click **OK**. The Select a Device dialog closes and the Configure Graph menu appears.
- 5 Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Virtualization: Virtual Machine Current Interface Utilization

The Virtual Machines Current Memory Utilization report provides a list of the virtual machines associated with a virtual host or vCenter server, and interface utilization values for each virtual machine.

- **Virtual Machine.** Displays the name of the virtual machine as reported by the virtual host or vCenter server.
- **1 hour Avg.** Displays the interface average transmit (Tx) and receive (Rx) rates in bits per second for the past hour.
- **1 hour Max.** Displays the interface maximum transmit (Tx) and receive (Rx) rates in bits per second in the past hour.
- **Current.** Displays the interface current transmit (Tx) and receive (Rx) rates in bits per second.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.

- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click the browse (...) button. The Select a Device dialog appears.
- 3 Select the server you want to view in the report.
- 4 Click **OK**. The Select a Device dialog closes and the Configure Graph menu appears.
- 5 Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Virtualization: Virtual Machine Current Memory Utilization

The Virtual Machines Current Memory Utilization dashboard report provides a list of the virtual machines associated with a virtual host or vCenter server, and memory utilization values for each virtual machine.

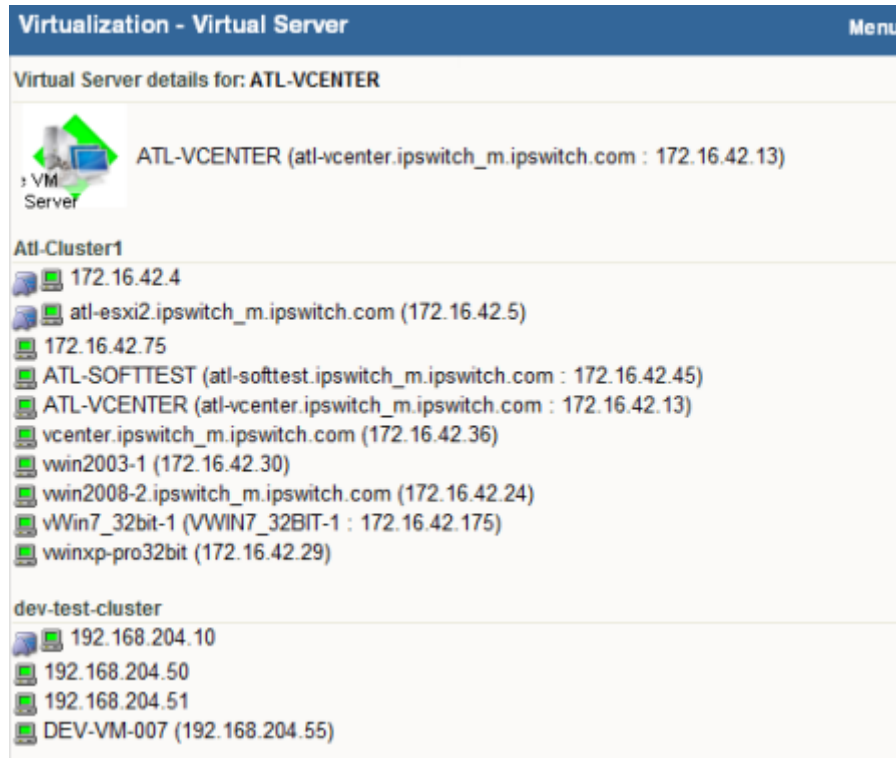
- **Virtual Machine.** Displays the name of the virtual machine as reported by the virtual host or vCenter server.
- **1 hour Avg.** Displays the average Active, Granted and Consumed memory allocations in bytes for the past hour.
- **1 hour Max.** Displays the maximum Active, Granted and Consumed memory allocations in bytes in the past hour.
- **Current.** Displays the current Active, Granted and Consumed memory allocations in bytes.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click the browse (...) button. The Select a Device dialog appears.
- 3 Select the server you want to view in the report.
- 4 Click **OK**. The Select a Device dialog closes and the Configure Graph menu appears.
- 5 Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Virtualization: Virtual Server

The Virtual Server dashboard report displays details about your virtual environment. When you select a managing server, like a vCenter server or virtual host, this report returns a list containing all of the virtual machines managed by the virtual server. The list identifies each device by hostname and IP address. If you have selected a vCenter server, and there are clusters in the virtual environment, the report returns a list of devices managed by the vCenter server grouped by cluster. This report can be used in both Home and Device dashboards, however you must select a vCenter server or virtual host for the report to return data.



To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click the browse (...) button. The Select a Device dialog appears.
- 3 Select the server you want to view in the report.
- 4 Click **OK**. The Select a Device dialog closes and the Configure Graph menu appears.
- 5 Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Virtualization: Virtual Server Attributes

This dashboard report displays details about a virtual host or vCenter server. Placing this dashboard report in a dashboard allows you to track details about a virtual host or vCenter server, as well as the number and power states of virtual machines associated with the virtual host or vCenter server.

- **VM Server details for.** Lists the virtual server IP address or host name.



Tip: Click on the IP address or host name to see the Device Status report.

- **Server Attributes.** List the attributes of the VMware server software running on the VMware host or vCenter server.
- **Name.** Displays the name of the VMware server software running on the VMware host or vCenter server.
- **VIM Version.** Displays the version of the VMware server software running on the VMware host or vCenter server.
- **API Version.** Displays the version of the VMware Application Programming Interface (API) used to gather information and issue commands to the virtual machines hosted by the VMware host or vCenter server.
- **Build.** Displays the build number of the VMware server software running on the VMware host or vCenter server.
- **Hardware Information.** Displays information about the hardware of the VMware host, only the Vendor will be available for a vCenter server.
- **Vendor.** Displays the name of the vendor who manufactured the CPUs used by the VMware host or vCenter server.
- **Model.** Displays the model number of the CPUs available to the VMware host.
- **CPU Cores.** The number of CPU cores available to the VMware host.
- **CPU Packages.** The number of CPU packages available to the VMware host.
- **CPU Threads.** The total number of CPU threads available to the VMware host.
- **CPU Frequency.** The CPU frequency of the CPU cores available to the VMware host.
- **CPU Model.** The CPU model of the CPUs available to the VMware host.



Note: Hardware information will be displayed only if the selected device is a VMware host for which credentials were supplied and selected during a VMware scan.

- **VM Information.** Information about the virtual machines associated with the VMware host or vCenter server.
- **Total VMs.** The total number of virtual machines associated with the VMware host or vCenter server.
- **Powered On.** The number of virtual machines in the *Powered On* state.

- **Powered Off.** The number of virtual machines in the *Powered Off* state.
- **Suspended.** The number of virtual machines in the *Suspended* state.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report.
 - **Device.** Click the browse (...) button. The Select a Device dialog appears.
- 3 Select the server you want to view in the report.
- 4 Click **OK**. The Select a Device dialog closes and the Configure Graph menu appears.
- 5 Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Virtualization: WhatsVirtual Events

The WhatsVirtual Events dashboard report displays events that WhatsVirtual is configured to collect from the vCenter server. The events appear in reverse chronological order, so that the last event received appears at the top of the list.

- **Date.** Displays the date and time that the event was received by the vCenter server.
- **Target.** Displays the virtual server, host or virtual device that was the target of the event. The display format is either *<Datacenter - VMware Host name - virtual machine name>*, or *<vCenter server name>*.
- **User.** Displays the user that initiated the event.
- **Message.** Displays the message received from the vCenter server that describes the event.

Configure Graph

You can configure the WhatsVirtual dashboard report from the Configure Graph dialog.

To access the Configure Graph dialog:

Click **Menu > Configure**. The Configure Graph dialog appears.

Use this dialog to configure the maximum number of rows to return in the WhatsVirtual Events dashboard report.

To set the maximum number of rows to return:

On the Configure Report menu, type the maximum number of rows you want the report to display in the **Maximum rows to return** box.

To save your changes:

Click **OK** when you have completed your configuration. Click **Cancel** to cancel the configuration without making changes.

Wireless reports

In This Chapter


| | |
|---|-----|
| Wireless dashboard reports | 577 |
| Wireless: Wireless Active Clients | 577 |
| Wireless: Wireless Details..... | 579 |
| Wireless: Wireless Errors | 581 |
| Wireless: Last 10 Syslog Messages..... | 582 |

Wireless dashboard reports

| Wireless dashboard reports | Type | Description |
|----------------------------|------|--|
| Wireless Active Clients | Home | Displays connection information about the wireless devices connected to the selected wireless access point (WAP). |
| Wireless Client Stats | Home | Displays statistical information about the wireless devices connected to the selected wireless access point (WAP). |
| Last 10 Syslog Messages | Home | Displays log information about events and activities that occur on the selected wireless access point (WAP). |
| Wireless Details | Home | Displays in-depth information about the selected wireless access point (WAP). |

Wireless: Wireless Active Clients

This home-level dashboard report lists the clients currently connected to the wireless access point (WAP) and displays important statistical information for each wireless device connected to the WAP. You can also click the (WAP) device name link, at the top of the report, to access the device status report. For more information, see *Understanding the Device Status dashboard* (on page 354).

If you use the WhatsUp Flow Monitor plug-in with WhatsUp Gold, you can click the  icon to drill down into the Flow Monitor reports for specific source and destination information about the wireless device and its conversation partners.

The first two columns are fixed attributes (Name and IP Address) and the remaining columns are user configurable. You can configure the dashboard report to display the following parameters in addition to the default attributes: MAC Address, Signal Strength, Data Rate, Connected Since, SSID, Bytes Sent, Bytes Received, Duplicate Packets, MSDU Retries, MSDU Fails, WEP Errors for each wireless device, MIC Errors, and MIC Missing Frames.

The following wireless client information is available in this report by default:

- **Name.** Lists the wireless device name. This is the Cisco IOS device hostname if the other end of the association is a bridge, access point, or repeater. If it is a wireless client, this is the configured client name. If this value is not available, then a lookup of the client's manufacturer is done based on client's MAC address. The associated OID is 1.3.6.1.4.1.9.9.273.1.2.1.1.13.
- **IP Address.** Lists the wireless device IP address. The associated OID is 1.3.6.1.4.1.9.9.273.1.2.1.1.16.
- **SSID.** Lists the Service Set Identifier (SSID), or assigned device name, associated with the radio interface to broadcast its identity. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.6.1.2.



Note: There can be multiple SSIDs for each radio.

- **MAC Address.** Lists the wireless device Media Access Control (MAC) address (physical address).
- **Signal Strength.** Indicates the connection strength of the wireless device to the WAP. Each bar indicates 20% signal strength. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.3.

| Signal bar | Signal Strength |
|------------|-----------------|
| | None |
| | Poor |
| | Fair |
| | Good |
| | Very Good |
| | Excellent |

- **Data Rate.** Indicates the current data transmit rate for this client. Rate value is within the range from 2 to 127, corresponding to data rates in increments of 500 kb/s from 1 Mb/s to 63.5 Mb/s. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.1.
- **Connected Since.** Lists the time that the wireless device connected to the WAP. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.2.

The following wireless client information is available as options for this report:

- **Bytes Sent.** Lists the number of bytes sent by the wireless device to the wireless access point (WAP). The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.9.
- **Bytes Received.** Lists the number of bytes received by the wireless device from the wireless access point (WAP). The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.7.
- **Duplicate Packets.** Lists the number of packets sent by the client (received by the WAP) for which the Sequence Control field in the packet header indicates that the packet is a duplicate. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.10.
- **MSDU Retries.** Lists the number of times a MAC Service Data Unit (MSDU) is successfully transmitted after one or more retransmissions for this client. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.11.


- **MSDU Fails.** Lists the number times a MAC Service Data Unit (MSDU) is not transmitted successfully for this client due to the number of transmit attempts exceeding retry limit. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.12.
- **WEP Errors.** Lists the number of Wired Equivalent Privacy (security algorithm) errors that occurred during the data transmission between the wireless device and the (WAP). The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.13.
- **MIC Errors.** Lists the number of message integrity code (MIC) errors occurred for this client. MIC is an algorithm used to gauge the integrity of a message. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.14.
- **MIC Missing Frames.** Lists the number of missing message integrity code (MIC) packets for this client. MIC is an algorithm used to gauge the integrity of a message. The associated OID is 1.3.6.1.4.1.9.9.273.1.3.1.1.15.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information for the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Select Devices or Groups.** Click to select a device or group of devices to add to the report.
 - **Column 3 - 6.** Select the wireless client information you want to display in each column of this dashboard report.
- 3 Click **OK** to save changes.

Wireless: Wireless Details

This home-level Wireless Details dashboard report displays a variety of hardware and data details about the selected wireless access point (WAP). If the WAP includes support for multiple radios, for example, 802.11g and 802.11n devices, the values for each radio are provided in a separate column (maximum of three radio columns). You can also click the (WAP) device name link, at the top of the report, to access the device status report. For more information, see *Understanding the Device Status dashboard* (on page 354).

If you use the WhatsUp Flow Monitor plug-in with WhatsUp Gold, you can click the  icon to drill down into the Flow Monitor reports for specific source and destination information about the wireless device and its conversation partners.

The following wireless client information is available in this report by default:

- **Station ID.** The default value is the station's assigned, unique MAC address. The associated OID is 1.2.840.10036.1.1.1.1.
- **Connection Count.** Lists the active devices associated with the WAP on each of the IEEE 802.11 interfaces. Possible active devices include wireless clients, repeaters, and bridges. The associated OID is 1.3.6.1.4.1.9.9.273.1.1.2.

- **Max Client Stations.** Indicates the maximum number of WAP stations (IEEE 802.11) that may associate with this radio interface. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.1.7.
- **Role.** Indicates the role of this station. For example, *Root access point*. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.1.1.
- **Manufacturer.** Lists the name of the WAP manufacturer. If the manufacturer name is not available, a lookup using the manufacturer OUI obtained using the associated OID (1.2.840.10036.3.1.2.1.1) is attempted.
- **Product ID.** Lists the product identifier that is unique to the manufacturer. The associated OID is 1.2.840.10036.2.1.1.9.
- **Product Version.** Lists the manufacturer's product version. The associated OID is 1.2.840.10036.3.1.2.1.4.
- **Radio Standard.** Specifies which IEEE 802.11 Standard applies to this radio. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.2.1.1.6.
- **SSIDs.** Lists the Service Set Identifier (SSID), or assigned device name, associated with the radio interface to broadcast its identity. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.6.1.2.



Note: There can be multiple SSIDs for each radio.

- **Data Rates.** Lists the set of data rates at which the station may transmit data. Each octet contains a value representing a rate. Each rate is within the range from 2 to 127, corresponding to data rates in increments of 500 kbit/s from 1 Mbit/s to 63.5 Mbit/s, and is for receiving data. This value is reported in transmitted Beacon, Probe Request, Probe Response, Association Request, Association Response, Reassociation Request, and Reassociation Response frames. The associated OID is 1.2.840.10036.1.1.1.11.
- **Regulatory Domain.** Lists the current regulatory domain. The associated OID is 1.2.840.10036.4.1.1.2.
- **Carrier Set.** Lists the WAP radio frequencies that are in operation. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.2.1.1.1.
- **Current Channel.** Lists the number of the current operating frequency channel. The associated OID is 1.2.840.10036.4.1.1.1.
- **Beacon Period.** Lists the number of time units (TUs) that a station uses for scheduling Beacon transmissions. This value is transmitted in Beacon and Probe Response frames. The associated OID is 1.2.840.10036.1.1.1.12.
- **Antenna Diversity.** Indicates the type(s) of wireless antennas used in the WAP. Support for diversity, encoded as: X'01'-diversity is available and is performed over the fixed list of antennas defined in dot11DiversitySelectionRx. X'02'-diversity is not supported. X'03'-diversity is supported, and control of diversity is also available. The associated OID is 1.2.840.10036.4.2.1.2.
- **WEP Enabled.** When listed as *true*, indicates that the IEEE 802.11 Wired Equivalent Privacy (WEP) option is implemented. The associated OID is 1.2.840.10036.1.1.1.7.
- **Max WEP Data Rate.** Lists the maximum transmit bit rate supported by the radio when using WEP encryption. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.1.4.

- **Cisco Ext Enabled.** When listed as *true*, indicates that the Cisco Aironet extensions to the basic IEEE 802.11 protocols are enabled. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.1.2.
- **VoIP Ext Enabled.** When listed as *true*, indicates that support for Voice-over-IP (VoIP) phones is enabled. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.1.1.9.


To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
- 3 Click **OK** to save changes.

Wireless: Wireless Errors

This home-level Wireless Errors dashboard report displays information about all wireless access point (WAP) transmit and receive errors. If the WAP includes support for multiple radios, for example, 802.11g and 802.11n devices, the error values for each radio are provided in a separate column.

You can also click the (WAP) device name link, at the top of the report, to access the Device Status Dashboard. For more information, see *Understanding the Device Status dashboard* (on page 354).

If you use the WhatsUp Flow Monitor plug-in with WhatsUp Gold, you can click the  icon to drill down into the Flow Monitor reports for specific source and destination information about the wireless device and its conversation partners.

The following wireless client information is available in this report by default:

- **Station ID.** The default value is the station's assigned, unique MAC address. The associated OID is 1.2.840.10036.1.1.1.1.
- **Carrier Set.** Lists the WAP radio frequencies that are in operation. The associated OID is 1.3.6.1.4.1.9.9.272.1.1.2.1.1.1.

Receive Errors

- **ACK Failures.** Lists the number of times the Transmission Control Protocol acknowledgement (ACK) is not received when expected. The associated OID is 1.2.840.10036.2.2.1.9.
- **FCS Errors.** Lists the number of times a Frame Check Sequence (FCS) error is detected in a received MAC Protocol data unit (MPDU). The associated OID is 1.2.840.10036.2.2.1.12.

- **WEP Undecryptable.** Lists the number of times a frame is received with the Wired Equivalent Privacy (WEP) subfield of the Frame Control field set to one and with the WEPOn value for the key mapped to the Transmitter's (TA's) MAC address. This indicates that the frame should not have been encrypted or that frame is discarded due to the receiving station (STA) not implementing the privacy option. The associated OID is 1.2.840.10036.2.2.1.14.
- **Frame MAC CRC Errors.** Lists the number of times a frame received has any Message Authentication Code cyclic redundancy check (MAC CRC) errors. The associated OID is 1.3.6.1.4.1.9.9.272.1.2.1.1.1.2.
- **SSID Mismatches.** Lists the number of times a beacon or probe response frame is received for which the Service Set Identifier (SSIDs) in the frame do not match any of the supported SSIDs. The associated OID is 1.3.6.1.4.1.9.9.272.1.2.1.1.1.3.

Transmit Errors

- **Transmit Failed.** Lists the number of times a MAC Service Data Unit (MSDU) is not transmitted successfully due to the number of transmit attempts exceeding either the dot11ShortRetryLimit or dot11LongRetryLimit. The associated OID is 1.2.840.10036.2.2.1.3.
- **Single Retries.** Lists the number of times a MAC Service Data Unit (MSDU) is successfully transmitted after one retransmission. The associated OID is 1.2.840.10036.2.2.1.4.
- **Multiple Retries.** Lists the number of times a MAC Service Data Unit (MSDU) is successfully transmitted after one or more retransmissions. The associated OID is 1.2.840.10036.2.2.1.5.
- **Deferred Energy Detect Errors.** Lists the number of times a frame transmission is deferred due to energy detection errors. The associated OID is 1.3.6.1.4.1.9.9.272.1.2.1.1.1.1.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
- 3 Click **OK** to save changes.


Wireless: Last 10 Syslog Messages

This home-level Wireless Log Messages dashboard report displays a history of syslog messages generated by the selected wireless access point (WAP).








Tip: By default, this dashboard report displays the last ten log messages only. You can click **Menu > Configure** to change the number of default log messages to display in the dashboard report.

You can also click the (WAP) device name link, at the top of the report, to access the device status report. For more information, see *Understanding the Device Status dashboard* (on page 354).

If you use the WhatsUp Flow Monitor plug-in with WhatsUp Gold, you can click the  icon to drill down into the Flow Monitor reports for specific source and destination information about the wireless device and its conversation partners.

The following wireless client information is available in this report:

- **Severity.** Lists the severity of the wireless device error. The associated OID is 1.3.6.1.4.1.9.9.41.1.2.3.1.3.

| Severity icon | Severity Description |
|---|-------------------------------|
|  | Emergency, alert, or critical |
|  | Error |
|  | Warning |
|  | Notice or info |
|  | Debug |

- **Facility.** Name of the facility that generated the message. For example: 'SYS'. The associated OID is 1.3.6.1.4.1.9.9.41.1.2.3.1.2.
- **Message.** Lists the wireless device log error to help identify the issue. The associated OID is 1.3.6.1.4.1.9.9.41.1.2.3.1.5.



Note: If the text of the message exceeds 255 bytes, the message will be truncated to 254 bytes and a '*' character will be appended, indicating that the message has been truncated.

- **Time Logged.** Lists the date and time that the error message occurred. The associated OID is 1.3.6.1.4.1.9.9.41.1.2.3.1.6.

To configure this dashboard report in WhatsUp Gold:

- 1** In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2** Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - **Device.** Select a device for the report by clicking the browse (...) button.
 - **Maximum rows to return.** Enter the number of default log messages to display in the dashboard report.
- 3** Click **OK** to save changes.

ELM reports

In This Chapter

Event Log Management (ELM) Reports in WhatsUp Gold Overview 585

Event Log Management (ELM): Summary Reports.....585

Event Log Management (ELM): Alarm Reports.....586

Event Log Management (ELM) Reports in WhatsUp Gold Overview

WhatsUp Gold version 15.0 provides integration with the Event Log Management central database. For access to ELM reports and data, you must also have ELM products, specifically WhatsUp Event Archiver and / or WhatsUp Event Alarm, configured to send collected log data to a MS SQL Server. WhatsUp Gold accesses report data through stored procedures in the ELM database.

ELM report integration supports the following six core log types:

- Application
- Directory service
- DNS server
- File replication service
- Security
- System

To view ELM data in WhatsUp Gold, you must first use the *ELM Configuration Integration tool* (on page 1166) to add, select, or delete ELM database instances that WhatsUp Gold can access. If needed, you can use the configurator tool to work with multiple ELM database instances.

ELM data integration with WhatsUp Gold allows you to create the following types of reports:

- *ELM Summary Dashboard Reports* (on page 585)
- *ELM Alarm Dashboard Reports* (on page 586)
- *ELM Plugin Full Reports* (on page 1171)

Event Log Management (ELM): Summary Reports

ELM summary *dashboard reports* (on page 348) display ELM Event Archiver-specific database table information. There are three different ELM summary reports:

- Summary Counts
- Failure Audits By Computer
- Failure Audits By User

The Summary Counts report displays the number of events associated with monitored computer and users accounts over a user-defined time frame, including critical events, warning events, and informational events.

- Click the **Monitored Computers** link to display the ELM Events by Computer report, which lists all computers in the ELM database tables and their associated number of events.
- Click the **User Accounts** link to display the number of Success Audits and Failure Audits associated with each username in the ELM database tables.

The Failure Audits By Computer report displays a list of failure audits over a user-defined time frame, associated with each computer being monitored by ELM. Click a computer name to see report details.

The Failure Audits By User reports displays a list of failure audits associated with each user being monitored by ELM, over a user-defined time frame. Click a username to see report details.

For information about configuring ELM summary reports, see *Configuring ELM Summary Reports* (on page 1170).

For more information about dashboard reports, see the *Adding dashboard reports to a dashboard view* (on page 342) help topic.

Event Log Management (ELM): Alarm Reports

ELM Alarm *dashboard reports* (on page 348) display ELM Event Alarm-specific database table information. There are three different ELM alarm reports:

- Critical Event Alarms
- Warning Event Alarms
- Informational Event Alarms

The Critical Event Alarms report displays a list of critical events along with event details present in the Event Alarm tables from a given SQL Server ELM database instance. Critical events include error and failure audit event types. To view the details associated with a critical event, click the **Event Information** link. The Event Alarm Description dialog opens, displaying a description of the critical event alarm.

The Warning Event Alarms report displays a list of warning events along with event details present in the Event Alarm tables from a given SQL Server ELM database instance. Warning events only include warning event types. To view the details associated with a warning event, click the **Event information** link. The Event Alarm Description dialog opens, displaying a description of the warning event alarm.

The Informational Event Alarms report displays a list of informational events along with event details present in the Event Alarm tables from a given SQL Server ELM database instance. Informational events include information and success audit event types. To view the details associated with an informational event, click the **Event Information** link. The Event Alarm Description dialog opens, displaying a description of the informational event alarm.

For information on configuring ELM Alarm reports, see *Configuring ELM Alarm Reports* (on page 1171).

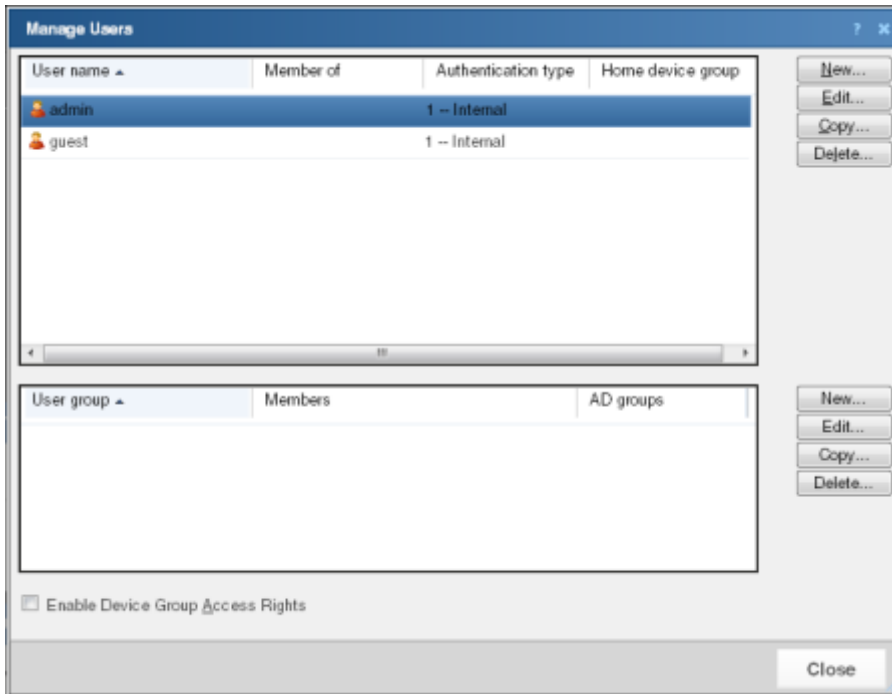
For more information about dashboard reports, see the *Adding dashboard reports to a dashboard view* (on page 342) help topic.

Dashboard Report - Remote Site

- **Remote Site.** The remote server for which the report is configured.
- **Last snapshot.** The time the "snapshot" displayed in this report was taken from the Remote Site.

Creating and modifying user accounts

User accounts that are granted the **Manage User** right can create and edit user accounts.



To create a new or edit a WhatsUp Gold user account:

- 1 Click the **Admin** tab, then click **Manage Users**. The Manage Users dialog appears.
- 2 Click **New**. The Add User dialog appears.

- or -

Select a user account and then click **Edit**. The Edit User dialog appears.

- 3 Enter the appropriate information.
 - **User name.** Enter the name of the user.
 - **Authentication type.** Select the method of authenticating the user.
 - **Internal.** Use the internal user database built in to WhatsUp Gold.
 - **LDAP.** Use an external LDAP database.
 - **Language.** Select the language to display for the user.
 - **Internal password.** Enter a password for the user. This option is disabled if **Authentication Type** is set to LDAP.
 - **Confirm password.** Confirm the user's password. This option is disabled if **Authentication Type** is set to LDAP.
 - **Home device group.** Select the device group that the user will see when they log into the WhatsUp Gold web interface. If they have the correct group access rights, they will be able to navigate out of this group.
 - **User rights.** Select the rights that correspond to the actions you want to allow the user to complete.
 - **Check all rights.** Select this option grant the user rights to perform all of the actions listed.
 - **Member of.** Add the groups the user is a member of in this box.

- **Show rights inherited from group membership + user rights.** Select this option to display the rights the user inherits from group membership.
 - **Check all.** Selects all available user rights.
 - **Clear all.** Clears all user rights selections.
- 4 Click **OK** to save changes.
 - 5 If you have enabled Group Access Rights, you will be prompted if you would like to specify Group Access Rights for the new user account.



Select **Yes** to open the Device Group Properties dialog for the user's home group.



- or -

Select **No** to close the dialog and return to the Manage Users dialog.

For more information, see About User Rights.

Using the Remote/Central dashboard reports

While the Remote Site dashboard reports work very much like dashboard reports in WhatsUp Gold Standard and Premium Editions, there are a few items to note about the reports that help you identify them as Remote/Central dashboard reports rather than local network dashboard reports.

- The Remote Site dashboard report header includes a network icon next to the Remote Site name to differentiate the Remote Sites from the local network devices (see 1).
- When you mouse-over a Remote Site name, address, group name, status, etc., a shortcut icon  displays to indicate that you can click to drill-down through information on the Remote Site (see 2). When you click the shortcut icon , a new web browser window opens for the selected Remote Site.



Important: Make sure that you select the option **Access Remote Reports** for each user that you want to provide access to the Remote Site reports. Also, make sure that you select the option **Configure Remote Sites** if you want a user to be able to access and change options in the Configure Remote Sites dialog (from the WhatsUp Gold console, click **Configure > Program Options > Remote Site Configuration**). For more information, see Configuring user accounts.



The Last snapshot information indicates the last date and time the Remote Site data was sent to the Central Site (see 3).

- The date and time information turns blue if it has been longer than 5 minutes since the remote site last updated.
- The date and time information turns red if it has been longer than 10 minutes since the remote site last updated.

The screenshot displays the 'Home' dashboard of the Ipswitch WhatsUp Gold interface. The top navigation bar includes tabs for 'Default', 'Remote Site View', 'Getting Started', 'Alerts and Actions', 'Default Distributed Overview', and 'J2's Central/Remote'. The main content area is divided into several sections:

- Remote Site Overview (1):** Displays information for 'RemoteSite 1'. It includes fields for 'Http address', 'Last connect time', and 'Last Snapshot'. The 'Last Snapshot' field is circled with a red '2'. Below this, it states 'A local device is not associated with the remote site'.
- Summary Counts (Remote):** A table showing various counts for 'RemoteSite 1'. The 'Last snapshot' is 'Mon 05:09 9:05 AM'.
- Active Monitor States (Remote) (3):** Displays 'RemoteSite 1' with a 'Last snapshot' of 'Mon 05:09 9:05 AM'. It shows 'Monitor type: All active monitor types' and 'Monitor state: Down'. Below this, it states 'No records were found'.
- Tail of Action Activity Log (Remote):** Displays 'RemoteSite 1' with a 'Last snapshot' of 'Mon 05:09 9:05 AM'. It shows a table with columns 'Date', 'Source', 'Action Name', and 'Trigger'. Below this, it states 'No action activity records'.
- Threshold - Ping by Response Time Over 1 ms (Remote):** Displays 'RemoteSite 1' with a 'Last snapshot' of 'Mon 05:09 9:05 AM'. It shows a table with columns 'Device', 'Interface', 'Max (ms)', and 'Avg (ms)'. Below this, it states 'No ping performance monitor records'.

Monitoring

In This Chapter

| | |
|--|-----|
| Working with monitor reports..... | 592 |
| Using Favorites..... | 612 |
| Using WhatsUp Gold monitor reports | 616 |
| Performance monitor reports | 630 |
| Network monitor reports..... | 641 |
| Using Device monitor reports..... | 659 |

Working with monitor reports

In This Chapter

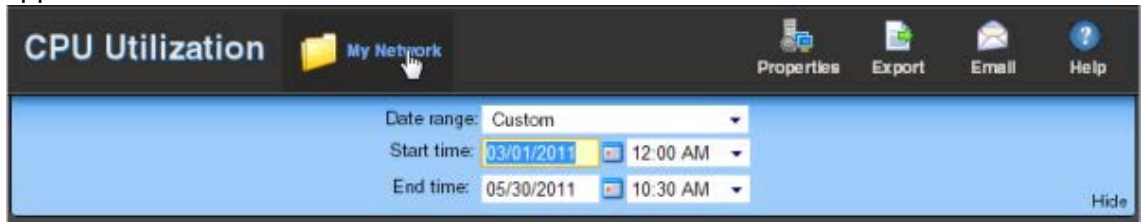
| | |
|--|-----|
| Viewing device reports..... | 592 |
| Viewing group reports..... | 594 |
| Changing the report date range | 596 |
| Using Business Hours settings in monitor reports | 598 |
| Viewing real-time data in monitor reports..... | 600 |
| About report refresh intervals | 601 |
| Changing the date range..... | 602 |
| Using the Zoom tool | 603 |
| Using paging options..... | 603 |
| Changing preferences | 604 |
| Using the WhatsUp Gold toolbar buttons..... | 606 |
| Configuring monitor report charts | 606 |
| Resizing and sorting report columns | 607 |
| Disabling Instant Info popups | 608 |
| Understanding the Graph Types..... | 610 |

Viewing device reports

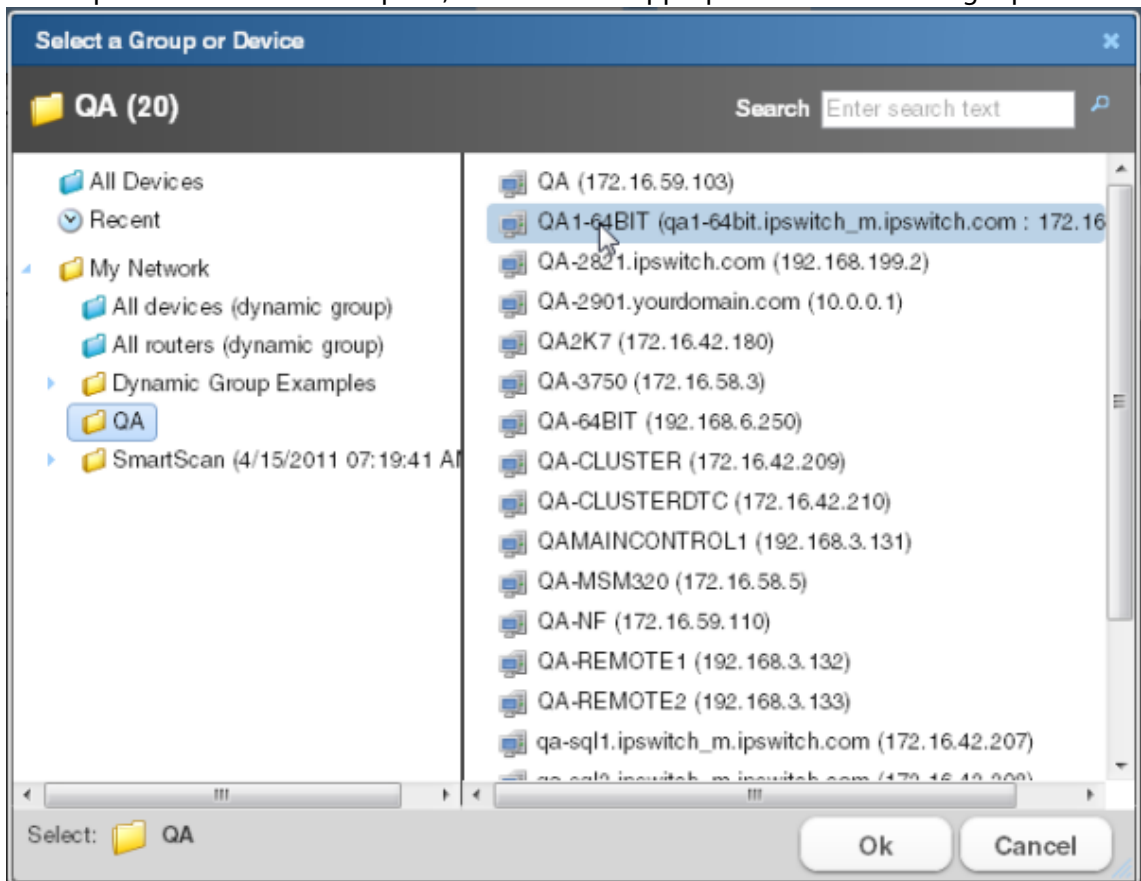
Device reports display information related to specific devices. For example, you can view reports for a specific Cisco router with Interface Utilization performance monitors.

To view a report for a specific device:

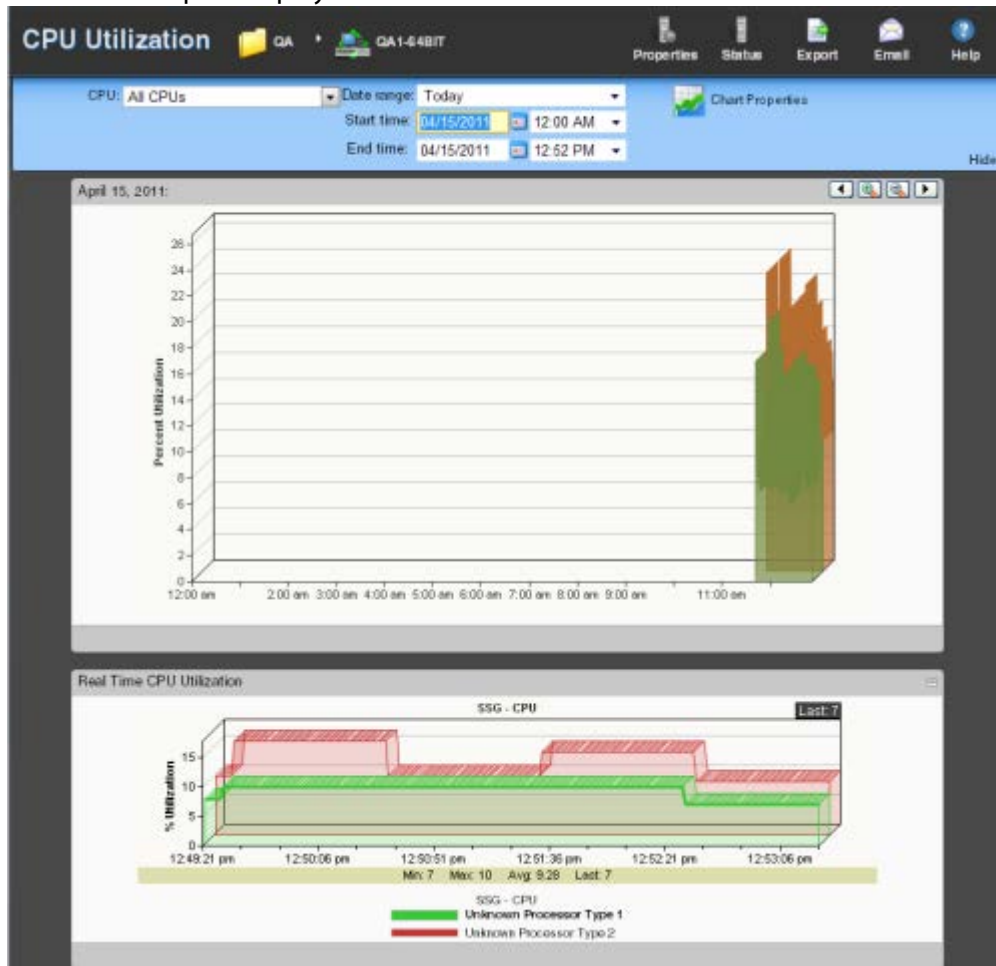
- 1 Click the **Monitoring** tab, then select the report you want to view.
- 2 In the page title bar, click the device context. The Select a Group or Device dialog appears.



- 3 Click a parent folder in the left pane, and select the appropriate device in the right pane.



- 4 Click **OK** to make your selection. The selected device displays as the new context and the monitor report displays information for the selected device.



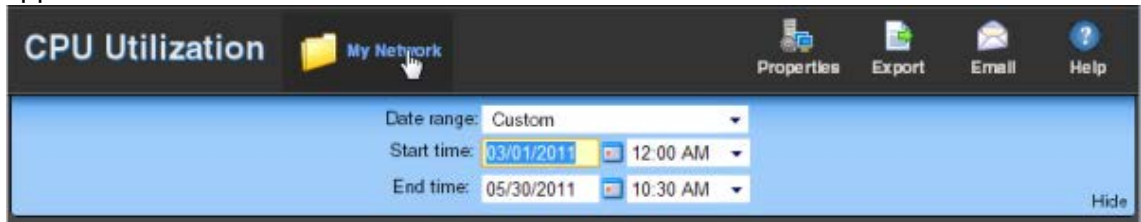
- Clicking the current device context opens the device picker and lets you select a device or group from a list of devices and groups on your network.
- Clicking other monitor report buttons on the navigation bar lets you view other reports for the same device.
- The report **Date/Time Picker**, located in the middle of the page, allows you to easily change the time period for the report you are viewing.
- Selecting **Export** allows you to export your data using the following options: Export to Text, Export to Excel, or Export to PDF.
- Selecting **Email** lets you email and schedule reports. For more information, see *Scheduling reports* (on page 625).

Viewing group reports

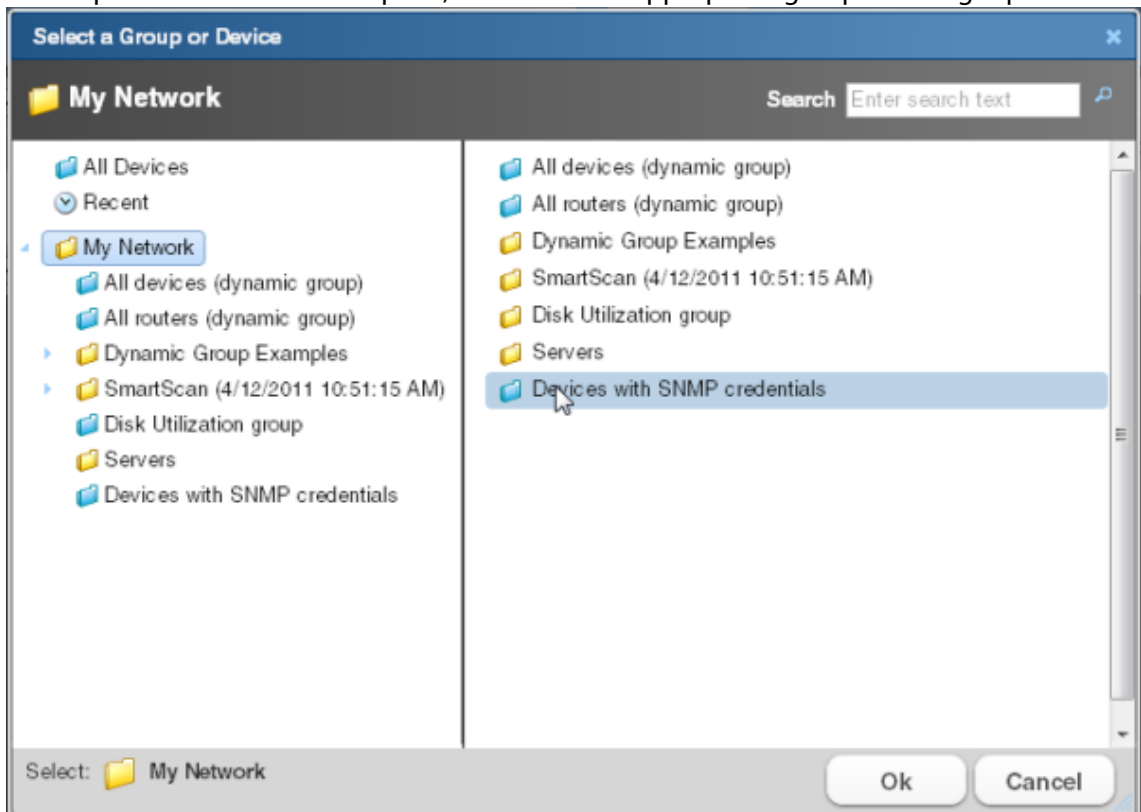
Group reports display information related to specific groups. For example, you can view reports for Cisco devices with Interface Utilization performance monitors.

To view a report for a specific device group:

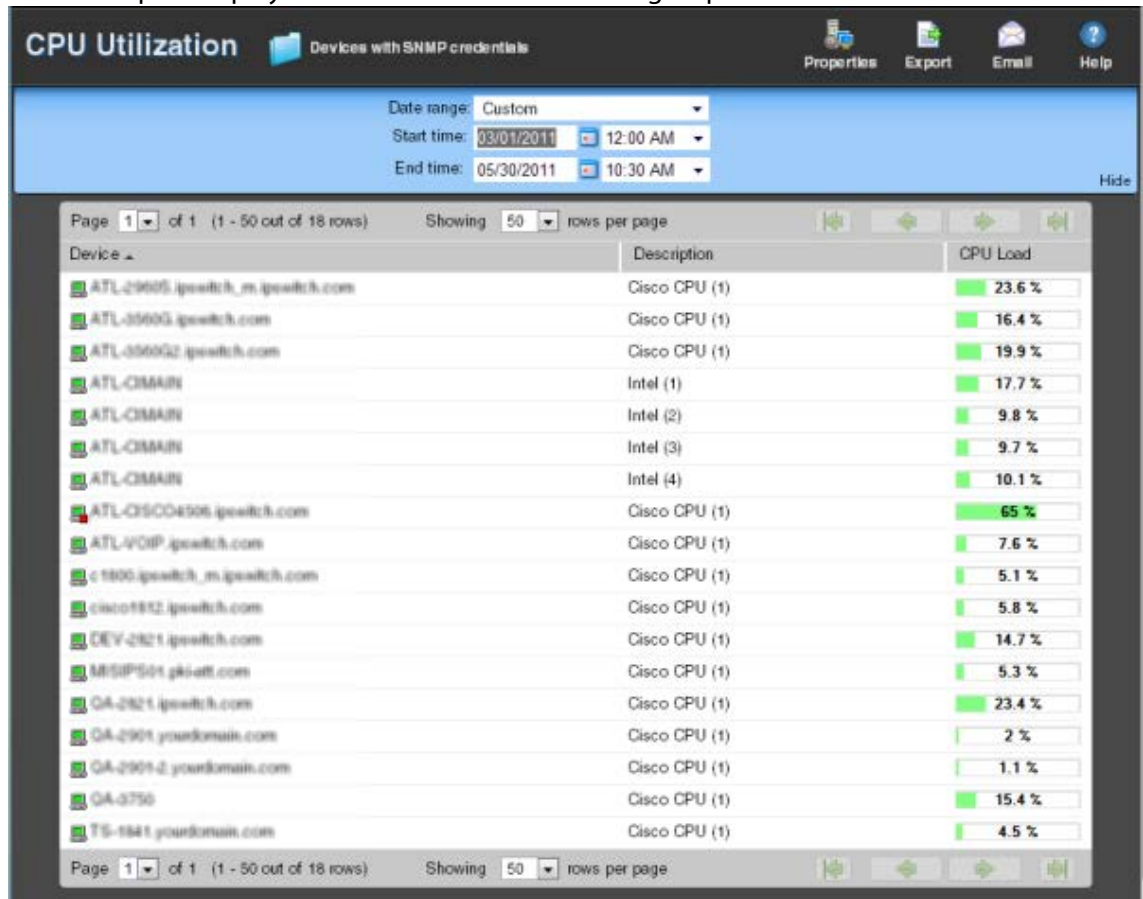
- 1 Click the **Monitoring** tab, then select the report you want to view.
- 2 In the page title bar, click the device context. The Select a Group or Device dialog appears.



- 3 Click a parent folder in the left pane, and select the appropriate group in the right pane.



- 4 Click **OK** to make your selection. The selected group displays as the new context and the monitor report displays information for the selected group.



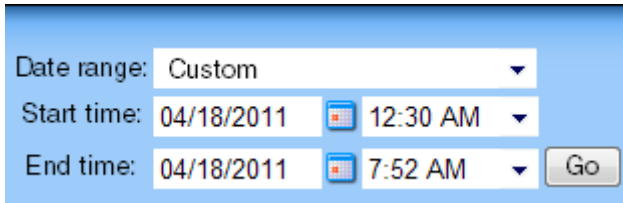
- Clicking the current device context opens the device picker and lets you select a device or group from a list of devices and groups on your network.
- Clicking other monitor report buttons on the navigation bar lets you view other reports for the same group.
- The report **Date/Time Picker**, located in the middle of the page, allows you to easily change the time period for the report you are viewing. In the **Date range** list, you can specify business hours. This allows you to view the network activity only for the hours you specify.
- Selecting **Export** allows you to export your data using the following options: Export to Text, Export to Excel, or Export to PDF.
- Selecting **Email** lets you email and schedule reports. For more information, see *Scheduling reports* (on page 625).

Changing the report date range

Date/Time picker

Most monitor reports have a date range selection tool (date/time picker) that you can use to change the range of data you are viewing in the report. This tool controls the quantity of information displayed for a report.

You can select both start and end times for the report.



You can select from the following date ranges:

- Today
- Yesterday
- Last Week
- Previous Month
- Week To Date
- Month To Date
- Last 2 Hours
- Last 4 Hours
- Last 8 Hours
- Last 3 Days
- Last 7 Days
- Last 30 Days
- Custom

Additionally, some monitor reports also include these options:

- All Hours
- Standard Business Hours
- Edit Business Hours



Note: For more information on editing business hours, see *Using Business Hours settings in monitor reports* (on page 598).



Note: The date and time format for monitor reports matches the format specified in the WhatsUp Gold console (**Configure > Program Options > Regional**).

Zoom tool

The Zoom toolbar zooms the current date range in or out using the zoom in or zoom out icons. The arrows on the toolbar control moving the selected date range forward and backward.



Clicking outside the chart

Another way to move the report date backward and forward is to click in the space between the chart and the chart border. Clicking the space to the right of the chart moves the selected date forward, while clicking to the left moves the selected date backward.

Using Business Hours settings in monitor reports

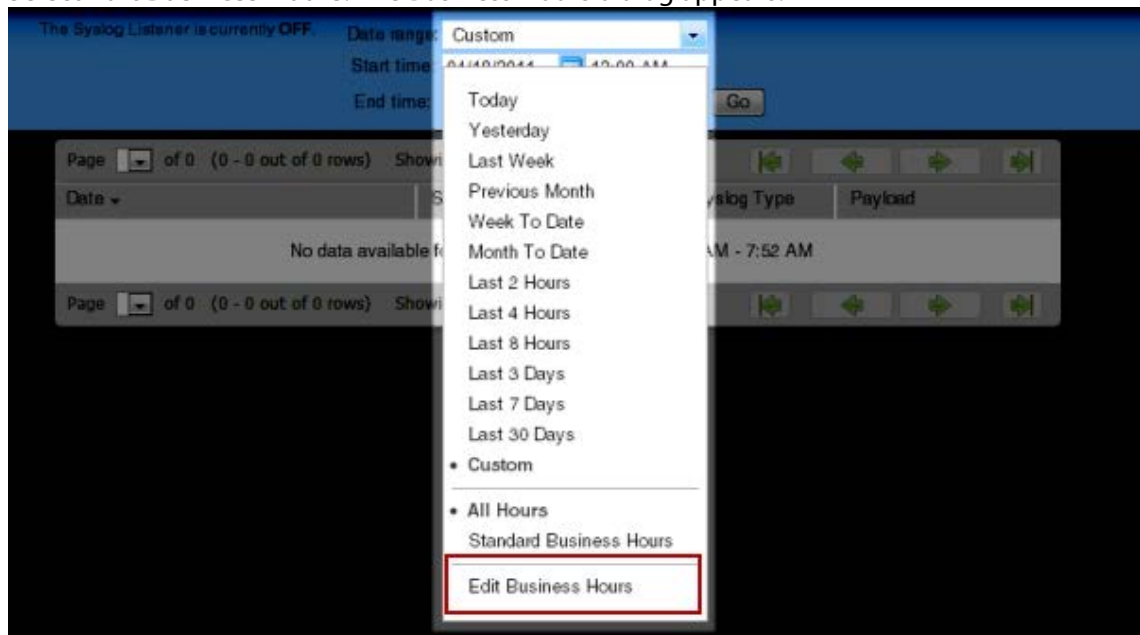
You can select **Standard Business Hours** for many WhatsUp Gold and Flow Monitor reports using the **Date range** list. Selecting this option limits report views to standard business operation hours, which default to Monday - Friday from 9:00 am - 5:00 pm. You can add, edit, and delete business hour report times in the Business Hours dialog.



Note: The Business Hours setting is available for group reports only.

To change/edit Standard Business Hours:

- 1 In any report, click the **Date Range** list.
Select **Edit Business Hours**. The Business Hours dialog appears.



- 2 Click **Add Hours** to add a new set of business hours for report time ranges. Type a name for the new business hours setting, and then click **OK**.

- or -

Select a name in the list to edit an existing business hours setting, and then click **OK**.

- 3 Select the **Link days** option if you want to use the same start and end time for each scheduled day.
- 4 Select the days you want to include in the business hours setting, then use the slider bar to adjust the start and end times for the report.
- 5 Click **OK** to save your changes.



Note: You must have the appropriate account rights to view and make changes to business hours.

Viewing real-time data in monitor reports

For all monitor reports where real-time data is available, a second graph is available below the historical data graph. This second graph displays poll data for the report in real-time, updating every second.



About report refresh intervals

Reports are refreshed at an interval specified in the User Preferences dialog called the report refresh interval. The default report refresh interval is 120 seconds.

The screenshot shows the 'Preferences for admin' dialog box with the following sections:

- General**: Language is set to 'English'. There is a 'Change your password...' button and a checked checkbox for 'Show Getting Started Pane'.
- Refresh intervals**: A sub-header reads 'All intervals shown in Seconds'. It contains four input fields: 'Dashboard report:' (120), 'Full report:' (120, highlighted with a red box), 'Devices list:' (120), and 'Check every: (seconds):' (120).
- Reports**: A dropdown menu is set to '50' with the text 'records per page for long reports by default'. There is an unchecked checkbox for 'Collapse legends on split second graph dashboard reports'.
- Web Alarms**: A checked checkbox for 'Enable web alarms'.
- Instant Info**: A section titled 'Show popups on...' with three checked checkboxes: 'Dashboard reports', 'Device list', and 'Full reports'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.



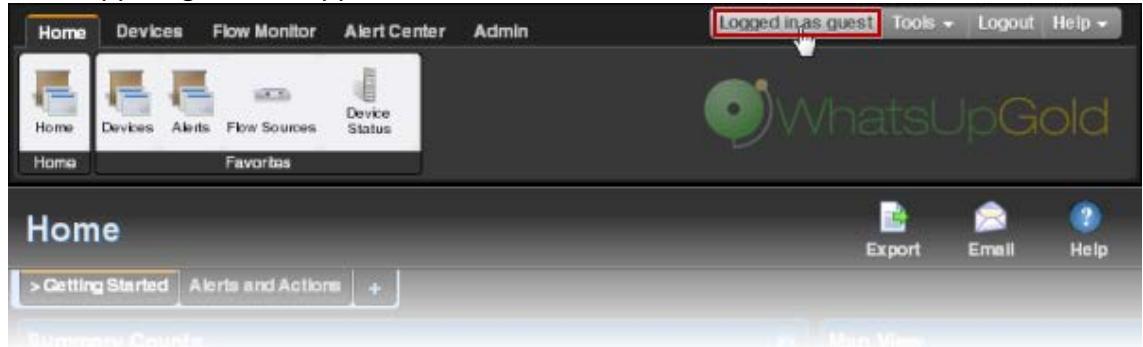
Note: The report refresh interval is user specific and is only applied to the user account logged in when the change is made.

To change the report refresh interval:

- 1 Click the **Admin** tab, then click **Preferences**.

- or -

Click the **Logged in as [username]** link, where [username] is your account log in name, in the upper right of the application.



- 2 Enter a new time (in seconds) for the report refresh interval in the **Full report** field. This setting controls how frequently the monitor reports update.
- 3 Click **OK** to save changes.

Changing the date range

Use the time and date menus in the control bar to select the time period you want to view the data for. You can select a pre-configured time period from the **Date Range** list, or select **Custom** and enter the start and end time manually. If no data exists for that time period, the following message displays: **No data available for the selected date range**.

To change the date range for a report or log:

- Click the calendar icon next to the date field to select the specific date from the calendar.
- Click the left and right arrows on the calendar to browse through the months.
- In the Date range list, click **Today** to navigate back to the current date. When you click a date, the calendar closes and the field is populated with the selected date.



Note: The date and time format on this report or log matches the format specified in the WhatsUp Gold console (**Configure > Program Options > Regional**).







You can also use the report *zoom tool* (on page 603) to select a date and time for monitor reports.

To control the date/time picker display:

- Hide the control bar by clicking the **Hide** link in the control bar. The selected date/time range displays instead and allows more rows of the report or log to display.
- To redisplay the date/time picker, click anywhere in the control bar summary.

Using the Zoom tool

Use the zoom tool to navigate through a monitor report. The zoom tool is associated with charts and changes the displayed date and time interval of a report as you page right and left, or zoom in and out.





| Click: | To: |
|---|--|
|  Page right | Move the report date forward. For example, clicking the Page right button changes the date from today to tomorrow. The page right button appears in monitor reports. |
|  Zoom in | Decrease the amount of time displayed in the report. For example, click the Zoom in button decreases the display time from 24 hours to 12 hours. |
|  Zoom out | Increase the amount of time displayed in the report. For example, clicking the Zoom out button increases the display time from 12 hours to 24 hours. |
|  Page left | Move the report date backward. For example, clicking the Page left button changes the date from today to yesterday. The page left button appears in monitor reports. |
|  Page up | Go back one page of data. The page up button appears in logs. |
|  Page down | Go forward one page of data. The page down button appears in logs. |

Using paging options

At both the bottom and the top of the monitor report or log table are paging controls that allow you to move through large amounts of data.

Use the **Page** list to select the specific page to view. Next, use the **Showing ___ rows per page** list to specify the number of rows to display in the report. You can choose to display 25, 50, 100, 250, or 500 rows. The default maximum is 50 rows.

The paging buttons allow you to move from page to page, or go to the first or last page:

| Click: | To view: |
|--|---|
|  | <ul style="list-style-type: none"> The first page of values |
|  | <ul style="list-style-type: none"> The previous page of values |
|  | <ul style="list-style-type: none"> The next page of values |
|  | <ul style="list-style-type: none"> The last page of values |

Changing preferences

Access the Preferences dialog by clicking **Admin > Preferences**, or through your user account link in the upper right corner of any page. Use this dialog to change various Web user options. Changes made in this dialog only change settings for the current user Web account.

General

- **Language.** Select a language for the application.
- **Change your password.** Click this option to change your account password.
- **Show Getting Started Pane.** Select this option to display the Getting Started pane. The Getting Started pane includes links to resources to help you resolve issues and learn more about WhatsUp Gold.



Note: If you have an evaluator license, this field displays as **Show Evaluator Pane**. This option is not selectable with an evaluator license.

Refresh intervals

- **Dashboard report.** Enter a time (in seconds) for how often *dashboard reports* (on page 340) should refresh.
- **Full report.** Enter a time (in seconds) for how often *monitor reports* (on page 619) should refresh.
- **Devices list.** Enter a time (in seconds) for how often the content Devices tab should refresh.

Reports

- **Default records per page for long reports.** Enter a number to control the maximum number of rows reports and logs display. If a report contains a number of rows greater than the maximum number specified, you can use either the page controls to view the data. The default max records setting is 50.
- **Collapse legends on split second graph dashboard reports.** Select this option to hide the legends on split second graph dashboard reports until the mouse pointer moves over a graph. When multiple split second graph dashboard reports display in a dashboard view, selecting this option can help reduce the percentage of the screen area used by reports. This option affects split second graph dashboard reports only; legends are always displayed in popups.

Web Alarms

- **Enable web alarms.** Select this option to enable *Web alarms* (on page 117).



Note: Web alarms are enabled by default.

- **Check every.** If you enable Web alarms, enter a time (in seconds) for how often WhatsUp Gold should check for Web alarms.

Instant Info (popups)

- **Show popups on device list.** Select this option to enable popups on the device list. If this option is cleared, popups are not displayed when you hover device or group names in the device list.
- **Show popups on dashboard reports.** Select this option to enable popups on dashboard reports. If this option is cleared, popups are not displayed on dashboard reports.
- **Show popups on full reports.** Select this option to enable popups on monitor reports. If this option is cleared, popups are not displayed on monitor reports.










Note: By default, popups are enabled on both dashboard and reports.



Note: Popups are not available in WhatsUp Gold Standard Edition.

Using the WhatsUp Gold toolbar buttons

| Click: | To: |
|--|--|
|  Email | <ul style="list-style-type: none"> Email a report or log as a PDF attachment. Schedule the report or log to be emailed at regular intervals. |
|  Add Content | <ul style="list-style-type: none"> Add additional dashboard reports to the current dashboard view using the Add Content panel. |
|  Edit View | <ul style="list-style-type: none"> Edit settings for the currently displayed dashboard view. |
|  Properties | <ul style="list-style-type: none"> View group or device properties. |
|  Status | <ul style="list-style-type: none"> Display the Device Status of the device currently in context. This icon does not appear when a group is in the current context. |
|  Export | <ul style="list-style-type: none"> Export a report or log: <ul style="list-style-type: none"> To a text file To an Excel file To a PDF file |
|  Help | <ul style="list-style-type: none"> View help for the current page. |



Note: Different sets of icons appear on different types of pages.

Configuring monitor report charts

To configure a chart in a monitor report:

- 1 Click **Chart Properties** in the control bar. The Chart Properties dialog appears.
- 2 Make any changes to the following settings:
 - **Width.** Enter the chart width (in pixels).
 - **Height.** Enter the chart height (in pixels).
 - **Graph Type.** Select the type of chart to display:
 - Bar

- Line
- Area
- Spline
- Stepline

For more information on graph types, see *Understanding the Graph Types* (on page 610).



Tip: Auto scale is the best option when the minimum and maximum chart values are unknown.

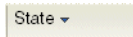
- **Trend Type.** Select the type of trend to display. This line shows the average value of data for the duration of the graph.
Options include:
 - None
 - Line
 - Curve
 - **Dimensions.** Select whether to display the chart as a 2D or 3D graph.
 - **Vertical Axis Scale.** Select how you want the vertical axis (the Y axis) for the graph to display:
 - **Auto Scale.** Select to adjust the axis based on the minimum and maximum values displayed. When Auto Scale is selected, small changes in the data may appear as a large data spike. Use Auto Scale to make changes in graph data more visible for graphs that are typically flat and do not have a lot of data variation.
 - **Fixed Scale.** Select to show the data on the scale you enter in the **Min** and **Max** boxes.
 - **Min.** Enter the minimum value to display in the graph. By default, this is zero, but for certain data sets a different minimum value may be more relevant.
 - **Max.** Enter the maximum value to display in the graph. By default, this is 100, but for certain data sets a different maximum value may be more relevant.
- 3 Click **OK** to accept the changes and close the dialog.

Resizing and sorting report columns

All monitor report columns can be resized. You can resize a report column by clicking on the edge of the report title box and moving it either left or right.

When a report column is resized, the new size is saved and used again each time the report is viewed.

Most monitor report columns can be sorted. You can sort by left-clicking a column heading. The report column then automatically sorts itself either ascending or descending. The sort direction is indicated with an upward, or downward pointing arrow.



As in column sizing, column sorting settings are saved and are used again each time the report is viewed.

Both column sizing and sorting are maintained on a per user basis, and only for the report where the column changes are made.

Disabling Instant Info popups

By default, Instant Info popups are available in both dashboard and full reports, but you can disable them if you prefer.

To disable Instant Info popups:

- 1 Click the **Logged in as [username]** link in the upper right corner of the page.
- or -
Click the **Admin** tab, then click **Preferences**. The Preferences dialog appears.



- 2 In the **Instant Info** section, clear the options for the areas where you do not want popups to appear.

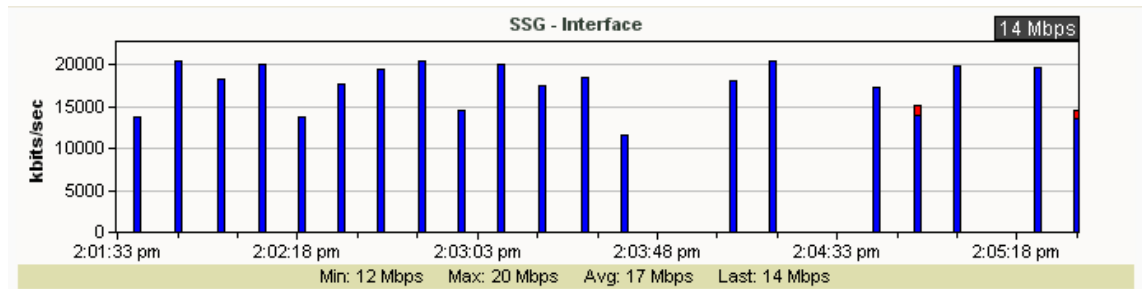


- 3 Click **OK** to save changes.

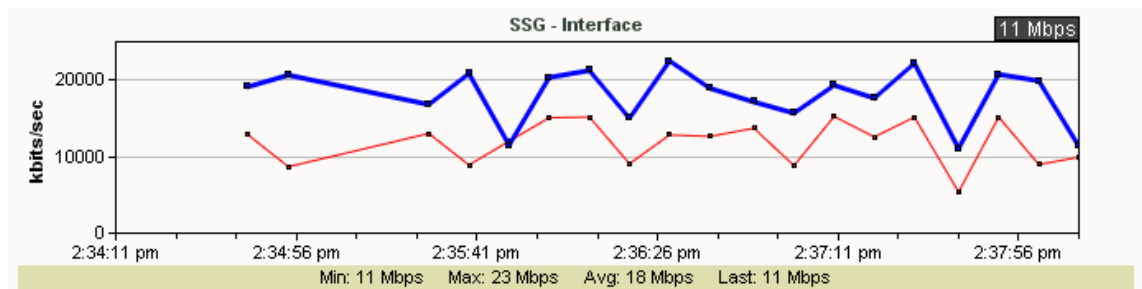
Understanding the Graph Types

The following graph types are available for use with WhatsUp Gold dashboard reports, including the Split Second Graph dashboard reports. All graphs have 2D and 3D options.

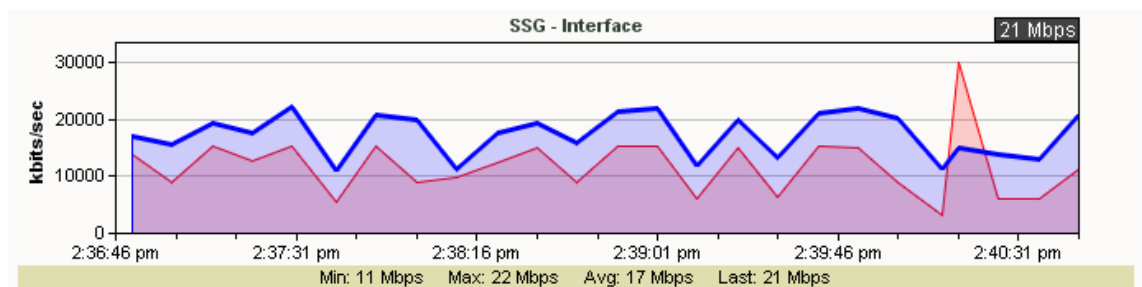
- **Bar.** A vertical bar is displayed for each data point.



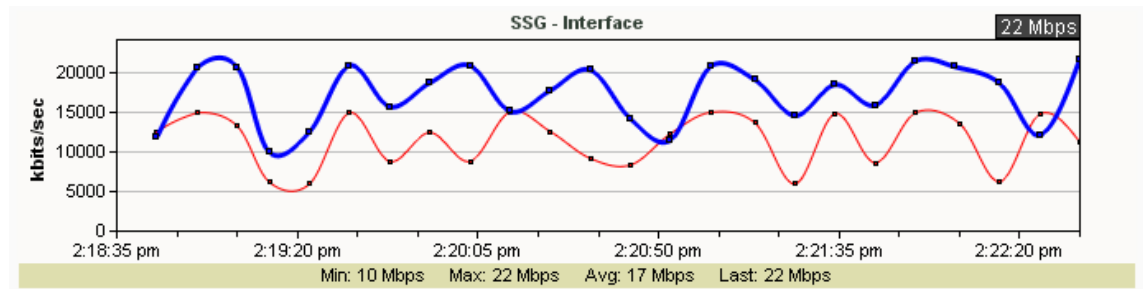
- **Line.** A segmented line connects each of the data points. These data points are represented as small squares. Line graphs are useful for viewing each individual data point or for viewing several counters on the same graph (when used with Split Second Graphs).



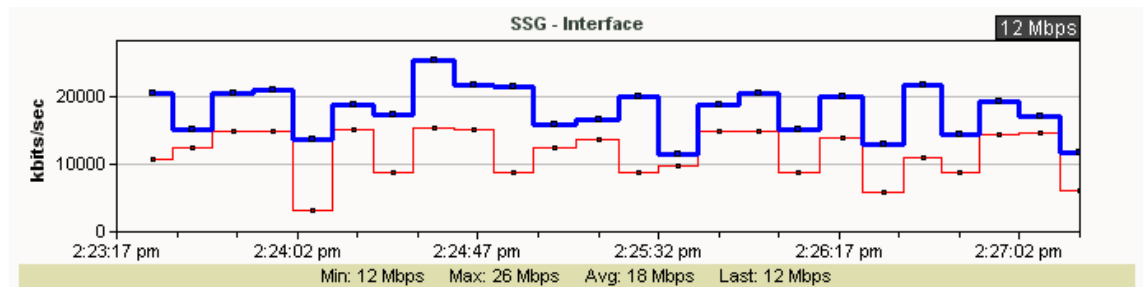
- **Area.** A solid line connects each data point. The area between the data point and the X-axis is filled with a semi-transparent background color. This graph type has the greatest visibility at a glance, but when used with Split Second Graphs, is only useful for viewing one to two performance counters at the most.



- **Spline.** This graph type is similar to the line graph type, but the line through the data points is drawn using a best-fit algorithm that interprets the area between data points.



- **Stepline.** This graph type uses horizontal and vertical lines to connect data points.



Using Favorites

Using the Favorites toolbar

WhatsUp Gold Favorites let you create your own customized toolbar by adding the WhatsUp Gold options you use most often to a single tab. You can edit and organize your favorites the way that best fits your needs. For more information, see *Adding Favorites* (on page 358).

Access WhatsUp Gold Favorites by clicking the **Home** tab.



Adding Favorites

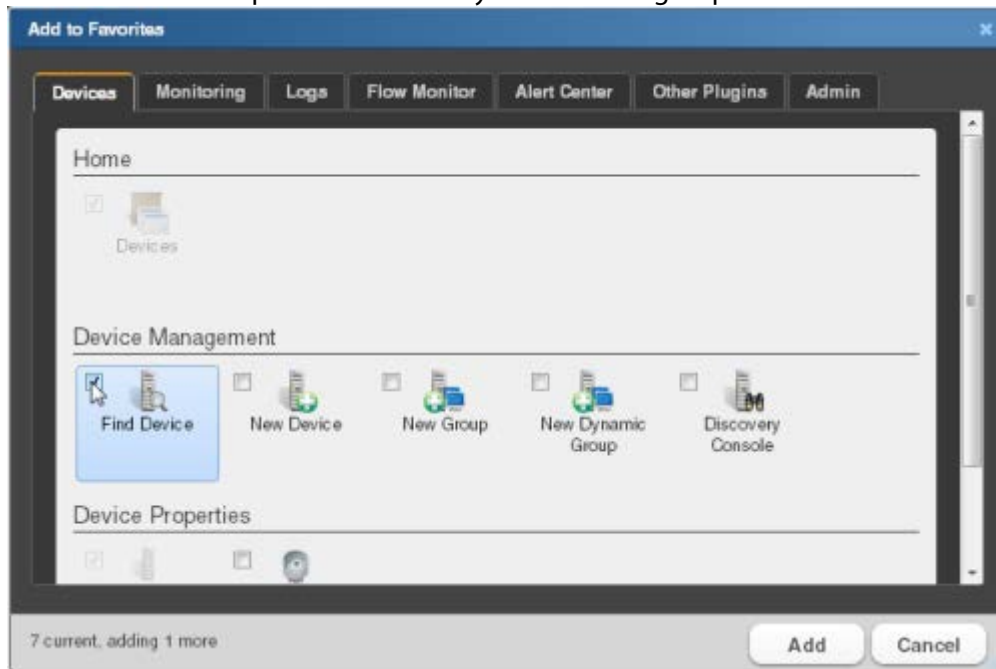
To add a favorite:

- 1 Click the **Home** tab.
- 2 Click the + (Add Favorites) to the right of the Favorites group. The Add to Favorites dialog appears.



- 3 From the dialog, select the tab containing the option you want to add. The buttons available on that tab appear in the pane.

- 4 Select the box to the left of each button you want to add to the Favorites group. A running total appears in the lower left of the pane as you select additional buttons to add. You can have up to 12 buttons in your Favorites group.



- 5 Continue clicking tabs and selecting buttons until you have added as many as you want to add.
- 6 Click **Add** to save your changes and add the selected buttons to your Favorites. The selected buttons appear in your Favorites toolbar.

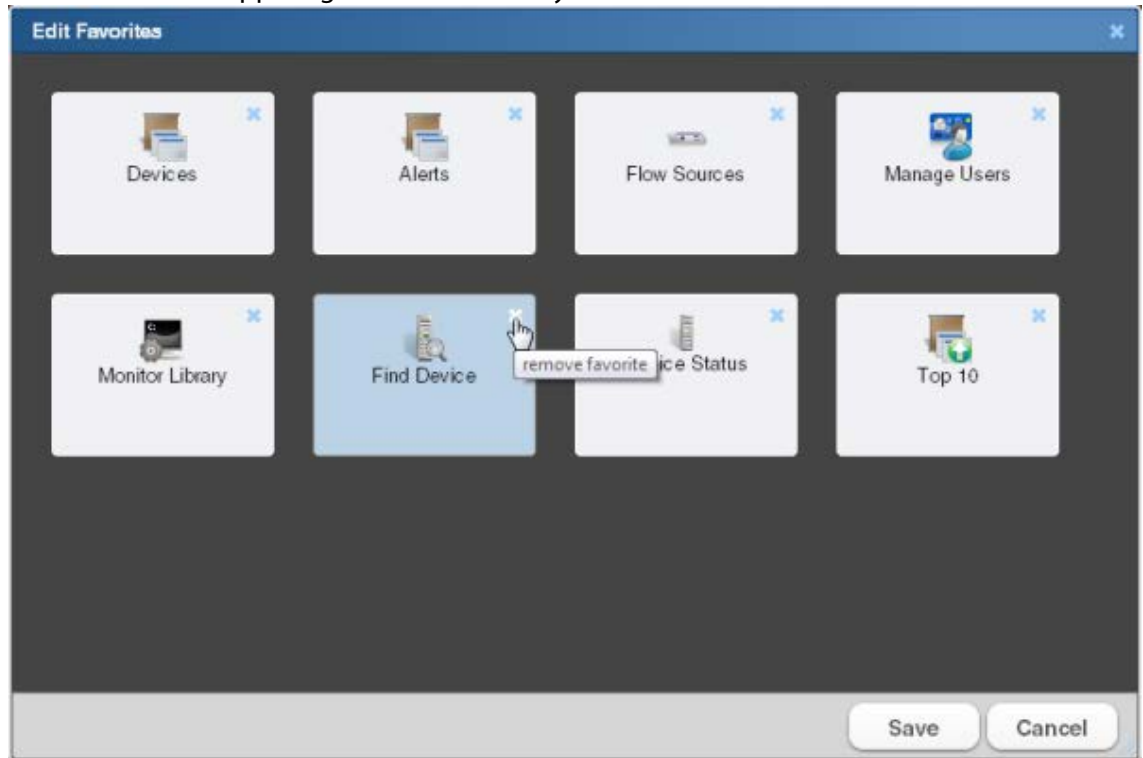
Editing Favorites

To remove buttons from your Favorites toolbar:

- 1 From the Home tab, click **Edit Favorites**. The Edit Favorites dialog appears.



- 2 Click the **X** at the upper right of each button you want to remove from the toolbar.



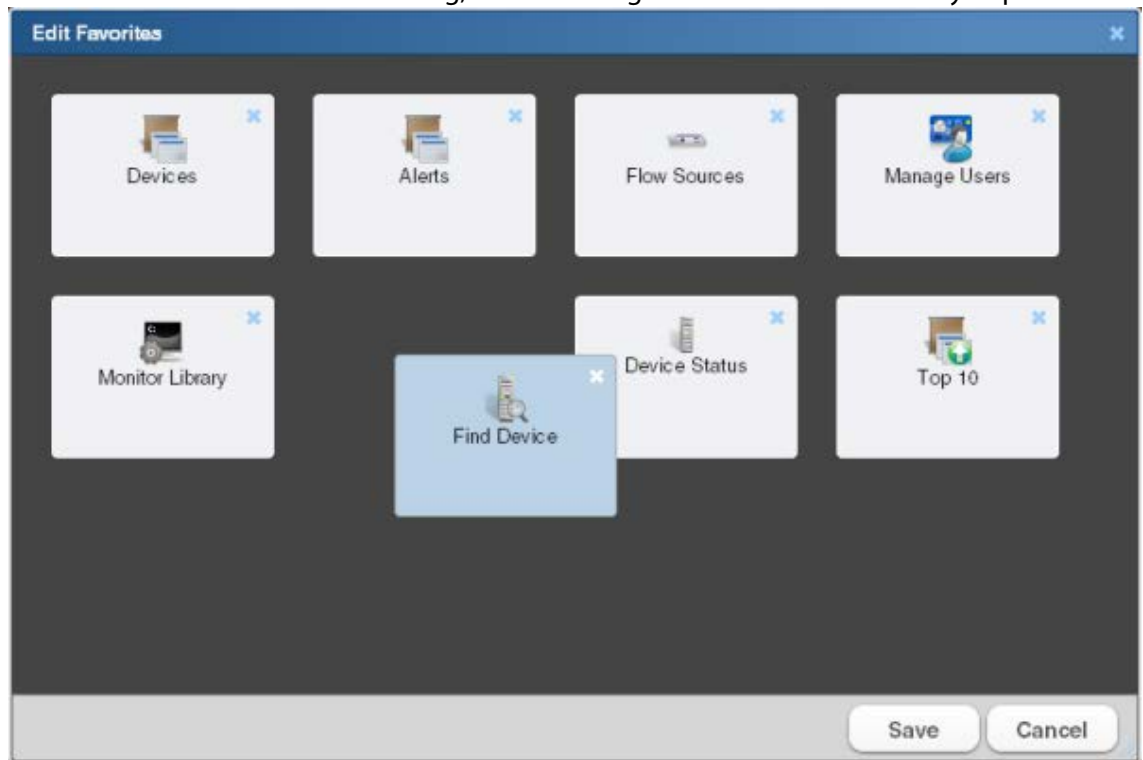
- 3 When you have deleted all of the buttons from the Favorites group that you want to remove, click **Save**. The buttons are removed from your Favorites toolbar.



Note: If you delete all of the buttons from the Favorites group, the WhatsUp Gold default Favorites appear in the group when you save.

To change the order of your Favorites:

- 1 From the Home tab, click **Edit Favorites**. The Edit Favorites dialog appears.
- 2 From within the Edit Favorites dialog, click and drag the buttons to the order you prefer.



- 3 When the buttons are in the preferred order, click **Save**. The dialog closes and the toolbar updates with the new button order.

Using WhatsUp Gold monitor reports

In This Chapter

| | |
|--|-----|
| List of reports and logs | 616 |
| Learning about monitor reports | 619 |
| Device Properties - Performance Monitors | 622 |
| Using the Performance Monitor Library..... | 624 |
| Scheduling reports..... | 625 |
| Exporting reports and logs | 626 |
| Emailing reports and logs..... | 627 |
| Printing reports and logs | 628 |
| Viewing scheduled reports | 628 |

List of reports and logs

The following is a list of all reports that are available in Ipswitch WhatsUp Gold.

| Name of report | What information it conveys |
|--|--|
| <i>Action Log</i> (on page 687) | A record of all Actions that WhatsUp Gold attempts to fire. |
| <i>Activity Log</i> (on page 698) | A history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the selected time period. |
| <i>General Error Log</i> (on page 688) | A record of error messages generated by WhatsUp Gold. |
| <i>Home Dashboard</i> (on page 353) | Your Home Dashboard for WhatsUp Gold. This dashboard contains four default views: Active Management, Getting Started, Passive Management, and Performance Management |
| <i>Passive Monitor Error Log</i> (on page 690) | A record of Passive Monitor errors reported by WhatsUp Gold. |
| <i>Performance Monitor Error Log</i> (on page 691) | A record of Performance Monitor errors reported by WhatsUp Gold for all devices or for a selected device. |
| <i>Recurring Action Log</i> (on page 700) | Results of Recurring Action executions. |

| Name of report | What information it conveys |
|---|--|
| <i>Recurring / Scheduled Report Log</i> (on page 699) | Results of Recurring and Scheduled Report executions. |
| <i>Remote Site Log</i> (on page 670) | A record of messages generated by Remote Server connection attempts. Available in WhatsUp Gold MSP and WhatsUp Gold Distributed editions. |
| <i>Remote Site Status</i> (on page 670) | View the Remote Location State of devices and Active Monitors. Available only in the central installation of WhatsUp Gold MSP and WhatsUp Gold Distributed editions. |
| <i>SNMP Trap Log</i> (on page 692) | A history of SNMP traps occurring during the selected time period for all devices or for a selected device. If the SNMP Trap Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log. |
| <i>Syslog</i> (on page 693) | Syslog events logged during the selected time period. If the Syslog Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Syslog Entries log. |
| <i>Web User Activity Log</i> (on page 701) | Shows the history of user activity on the system. |
| <i>Windows Event Log</i> (on page 696) | Shows Windows events logged for all devices or for a selected device during the selected time period. If the Windows Event Passive Monitor Listener is configured to listen for messages, any messages received are recorded in the Windows Event Log. |
| <i>WhatsVirtual Event Log</i> (on page 702) | Provides a record of events generated from virtual devices. |
| <i>Actions Applied</i> (on page 704) | 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. |
| <i>Active Monitor Availability</i> | Compare the amount of time the active monitors on your devices have been available. |
| <i>Active Monitor Outages</i> (on page 661) | Compare the amount of time the active monitors on your devices have been down. |
| <i>Blackout Summary Log</i> (on page 705) | A detailed view of actions that were not fired during a blackout period. |

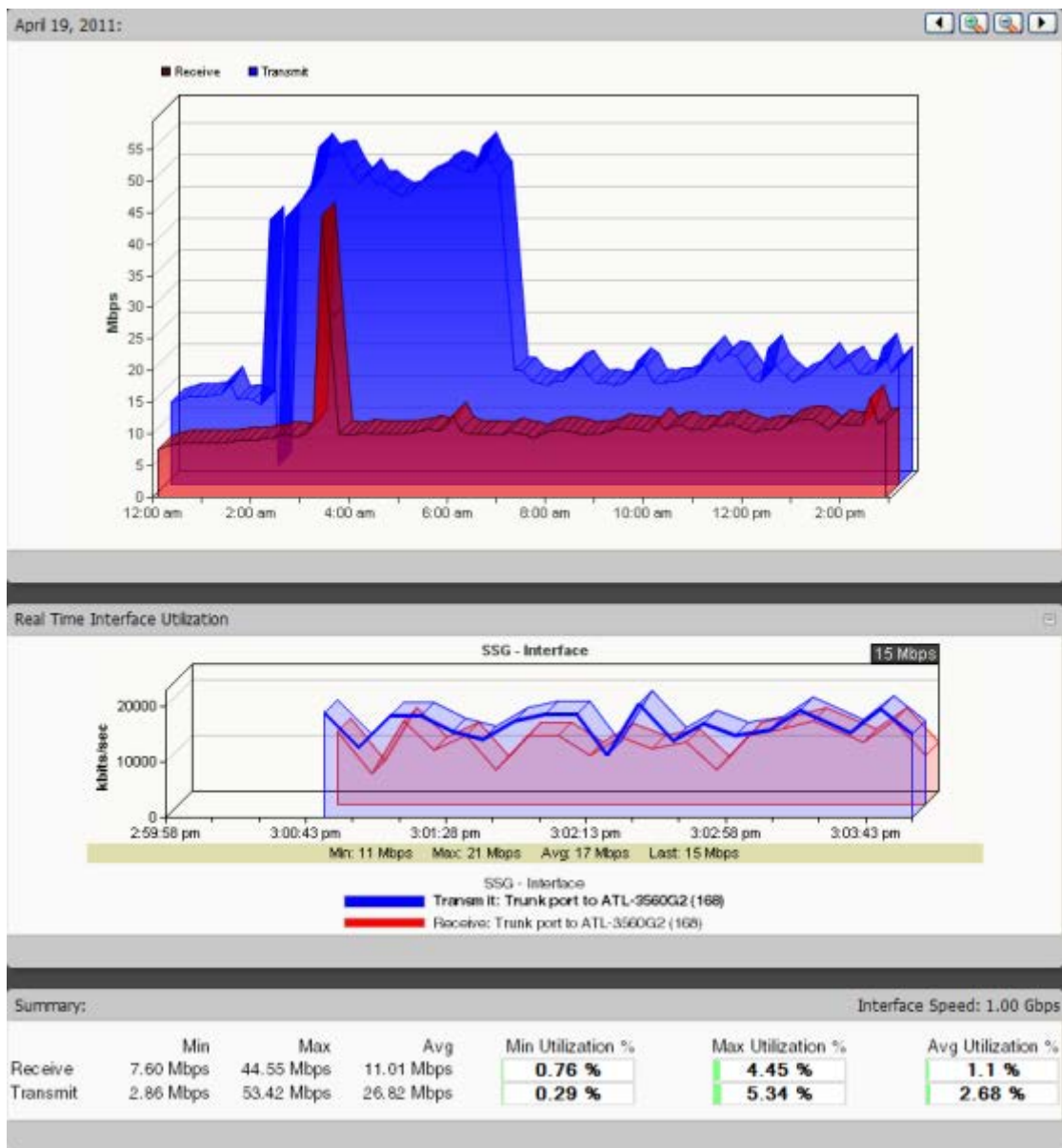
| Name of report | What information it conveys |
|---|---|
| <i>CPU Utilization</i> (on page 631) | CPU utilization statistics for devices by group or device. |
| <i>Device Uptime</i> (on page 662) | Shows the percentage of uptime, maintenance, unknown, down, and availability for devices by group. |
| <i>Disk Utilization</i> (on page 633) | Disk space utilization statistics for devices and by group. |
| <i>Device Health</i> (on page 664) | The current status of monitored devices in a group, or for a selected device, along with each monitor configured on each device. If a device is selected, the current status of the selected device and all monitors applied display. Each monitor shows its own device state, the current status of each item, how long the device has been in that status, and the time that status was first reported. |
| <i>Interface Utilization</i> (on page 641) | Interface utilization for devices by group or for a selected device (by percentage). |
| <i>Interface Traffic</i> (on page 644) | Interface traffic for devices by group or for a selected device (in bps). |
| <i>Memory Utilization</i> (on page 636) | Memory utilization statistics for devices by group or for a selected device. |
| <i>Monitors Applied</i> (on page 707) | A list of monitors applied to devices in the group currently in context. |
| <i>Ping Availability</i> (on page 650) | Ping availability statistics for devices by group or device. |
| <i>Ping Response Time</i> (on page 647) | Ping response times for devices by group or for an individual device. |
| <i>Quarterly Availability Summary</i> (on page 708) | Shows the availability summary for a group. |
| <i>State Change Acknowledgement</i> (on page 666) | When a device state changes, regardless of any action that has been placed on the device, WhatsUp Gold uses the Acknowledgement feature to make you aware that the state change occurred. This report can be used to view the devices in a group that require acknowledgement. |
| <i>State Change Timeline</i> (on page 667) | A timeline displaying when each monitor changed from one state to another during the selected time period. Information is displayed for selected devices and for groups. |
| <i>State Summary</i> (on page 710) | A summary of device states organized by device group. |

| Name of report | What information it conveys |
|--|--|
| <i>Top 10</i> (on page 356) | A collection of Top 10 dashboard reports. |
| WhatsConfigured Task Log | A record of all log messages generated by WhatsConfigured. This report is filterable by device and task. |
| <i>Custom Performance Monitors</i> (on page 639) | View information on groups and devices collected by custom monitors. |
| <i>Device Status</i> (on page 354) | A detailed look at a specific device. |
| <i>WhatsConnected Device Info</i> (on page 672) | A detailed view of network information gathered by WhatsConnected. |

Learning about monitor reports

Monitor reports display performance and historical data collected during the operation of the application. You can use these reports to troubleshoot and monitor your network and devices.

You can view monitor information for a device:



You can view monitor information for a group:

| Page 1 of 2 (1 - 36 out of 36 rows) | | Showing 25 rows per page | | | | | |
|-------------------------------------|-------------------------------------|--------------------------|-----------|--------------|-------------|-----------------|----------------|
| Device | Description | Transmit % | Receive % | Avg Transmit | Avg Receive | Bytes Transm... | Bytes Received |
| QA-2821.ipswit... | 199.x Network (1) | 0.79 % | 0.09 % | 7.94 Mbps | 828.41 Kbps | 77.20 GB | 9.00 GB |
| QA-3750 | Connection to CAT500 (10101) | 7.18 % | 7.33 % | 7.18 Mbps | 7.33 Mbps | 69.84 GB | 71.30 GB |
| QA-2821.ipswit... | 58.x Network (2) | 0.08 % | 0.78 % | 791.58 Kbps | 7.79 Mbps | 7.70 GB | 75.78 GB |
| QA-2821.ipswit... | GigabitEthernet0/1.1 (6) | 0.08 % | 0.78 % | 791.34 Kbps | 7.79 Mbps | 7.69 GB | 75.78 GB |
| QA1-64BIT | Local Area Connection (13) | 0.06 % | 0.57 % | 617.77 Kbps | 5.65 Mbps | 6.01 GB | 54.96 GB |
| QA-3750 | GigabitEthernet1/0/2 (10102) | 0.03 % | 0.01 % | 274.40 Kbps | 121.18 Kbps | 2.67 GB | 1.18 GB |
| QA1-64BIT | Local Area Connection 3-WFP Ligh... | 0 % | 0.06 % | 265.89 Kbps | 2.69 Mbps | 2.58 GB | 26.12 GB |
| QA1-64BIT | Local Area Connection 3-QoS Pack... | 0 % | 0.06 % | 265.89 Kbps | 2.69 Mbps | 2.58 GB | 26.12 GB |
| QA1-64BIT | Local Area Connection 3 (14) | 0 % | 0.06 % | 265.89 Kbps | 2.69 Mbps | 2.58 GB | 26.12 GB |
| QA-3750 | GigabitEthernet1/0/20 (10120) | 0.05 % | 0.05 % | 52.61 Kbps | 49.91 Kbps | 523.70 MB | 496.86 MB |
| QA-2901.yourd... | Connection to QA-3750 (1) | 0.05 % | 0.05 % | 48.49 Kbps | 49.13 Kbps | 482.66 MB | 489.12 MB |
| QA-2901.yourd... | Connection to QA-2901-2 (2) | 0 % | 0 % | 31.04 Kbps | 31.44 Kbps | 308.96 MB | 312.95 MB |
| QA-3750 | Vlan1 (1) | 0 % | 0 % | 6.87 Kbps | 8.70 Kbps | 68.36 MB | 86.64 MB |
| QA-3750 | GigabitEthernet1/0/3 (10103) | 0 % | 0 % | 5.05 Kbps | 264.85 bps | 50.29 MB | 2.64 MB |
| QAMAINCONT... | Broadcom NetXtreme Gigabit Ether... | 0 % | 0 % | 2.48 Kbps | 22.51 Kbps | 24.67 MB | 224.13 MB |
| QA-MSM320 | Wireless port 1 (7) | 0 % | 0 % | 1.62 Kbps | 0 bps | 16.08 MB | 0 Bytes |
| QA-MSM320 | Port 1 (5) | 0 % | 0 % | 944.25 bps | 4.75 Kbps | 9.40 MB | 47.31 MB |
| QA-MSM320 | Bridge (12) | 0 % | 0 % | 630.15 bps | 3.91 Kbps | 6.27 MB | 38.96 MB |
| QA1-64BIT | Local Area Connection* 5 (6) | 0 % | 0 % | 0 bps | 0 bps | 0 Bytes | 0 Bytes |
| QA-2901.yourd... | GigabitEthernet0/3 (3) | 0 % | 0 % | 0 bps | 0 bps | 0 Bytes | 0 Bytes |
| QA1-64BIT | Local Area Connection* (2) | 0 % | 0 % | 0 bps | 0 bps | 0 Bytes | 0 Bytes |
| QA-2821.ipswit... | GigabitEthernet0/1.2 (7) | 0 % | 0 % | 0 bps | 0 bps | 0 Bytes | 0 Bytes |
| QA1-64BIT | Local Area Connection* 10 (10) | 0 % | 0 % | 0 bps | 0 bps | 0 Bytes | 0 Bytes |
| QA-3750 | Null0 (14501) | 0 % | 0 % | 0 bps | 0 bps | 0 Bytes | 0 Bytes |

Access monitor reports by clicking the **Monitoring** tab and then selecting the appropriate button for the type of report you want to view.

Monitor report categories

Monitor reports in WhatsUp Gold are grouped according to the type of information displayed within each report.

There are three categories of monitor reports:

- **Performance.** Reports which display information about thresholds. Determine which resources on your network are under- or over-utilized using Performance monitor reports.
- **Network.** Reports which display reports related to network statistics about traffic through your network. Network reports include such parameters as speed, response times, and success or failure in contacting devices.
- **Device.** These reports display information about specific devices that you select to monitor for parameters such as outages and uptime percentages.

Advantages of monitor reports

- Larger than dashboard reports, monitor reports give you a broader data view, which is useful in pinpointing the time an event occurred or when viewing multiple graphed items. Many dashboard reports link to monitor reports, so that you can access this larger data view to troubleshoot.

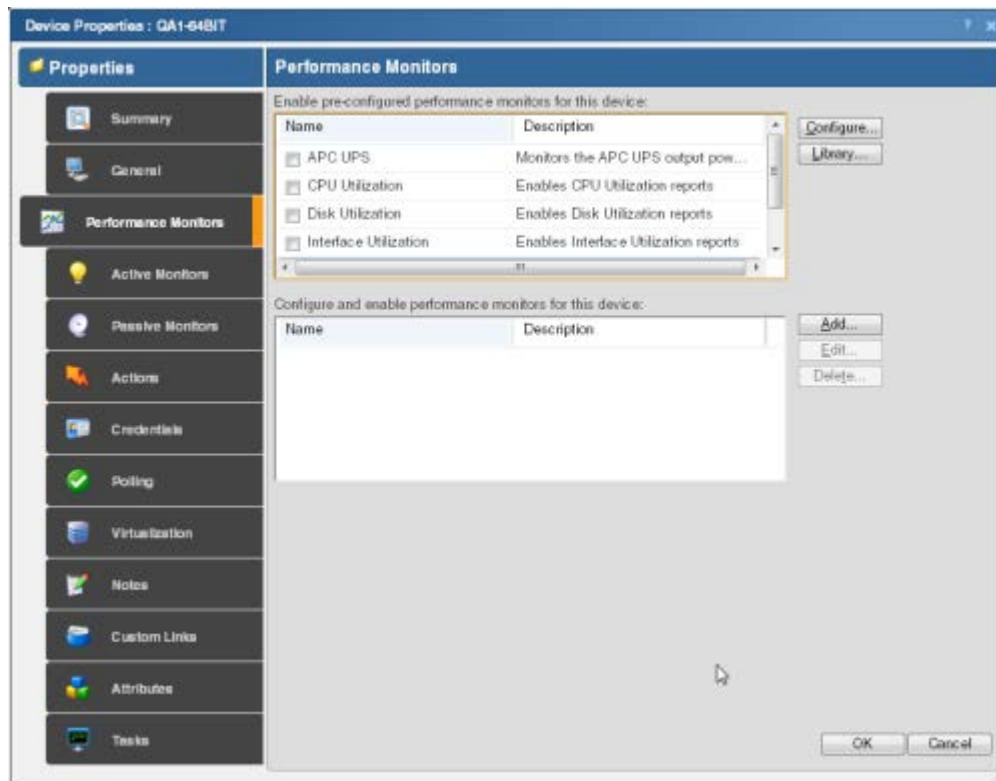
- The date range on full reports can be zoomed in or out so that you can get a smaller or larger picture of what's going on with an aspect of the network.
- Click the options within the same tab in the navigation bar to quickly access other monitor reports. The currently selected group or device and date range is applied to the next monitor report you access.
- The data in monitor reports can be exported to a formatted text file, Microsoft Excel, or a PDF. You can also email reports as a PDF, or send on scheduled intervals.

Device Properties - Performance Monitors

Use Performance Monitors dialog to configure and manage performance monitors for the selected device. For more information, see *Using Performance Monitors* (on page 121).



Note: For some performance monitors, the SNMP credential on the device must be configured. For WMI performance monitors, the Windows credential is required.



- **Enable pre-configured performance monitors for this device.** Select options in this list to enable monitors. The following monitors are populated by entries in the *Performance Monitor Library* (on page 247), but cannot be edited or changed from their default settings. These monitors are ready to be added to devices.
- **CPU Utilization.** Monitors the CPU utilization on the selected device.
- **Disk Utilization.** Monitors the available disk space for the selected device.
- **Interface Utilization.** Monitors all interfaces on the selected device.

- **Memory Utilization.** Monitors memory utilization on the selected device.
- **Ping Latency and Availability.** Monitors how often and quickly the device responds to a ping check.

If you select a specific performance monitor without configuring the monitor manually, the default collection type is automatically selected. The collection type refers to the item on the current device that is being monitored (This does not pertain to the custom WMI and SNMP monitors that may appear):

- CPU - All
- Disk - All
- Interface - All, Default, or Specific
- Memory - All
- Ping - All

For example, if you have multiple CPUs running on the device, WhatsUp Gold gathers statistics on all of them by default.

- **Configure.** Click to configure additional data stream options for the global performance monitor.



Note: If an error occurs, a warning message appears directing you to the problem. If it is a timeout error, you are prompted to open the Advanced dialog to change the **Timeout** value. For any other error, you are returned to this dialog.

- **Library.** Click for options to create (**New**), **Edit**, **Copy**, or **Delete** performance monitor library items to use on all devices.
- **Configure and enable performance monitors for this device.** Use this section of the dialog to add customized APC UPS, Printer, Active Script, SNMP, or WMI performance monitors to only be used on this device. The monitors added here do not appear in the Performance Monitor Library, and cannot be used on other devices unless it is manually created for that device.
- Click **New** to configure a new monitor.
- Select an existing monitor, then click **Edit** to change the current monitor configuration or double-click an existing monitor to change the configuration.
- Select a performance monitor type, then click **Delete** to remove it from the list.

For information on the Active Script Performance Monitor, see *Adding and Editing an Active Script Performance Monitor* (on page 250).



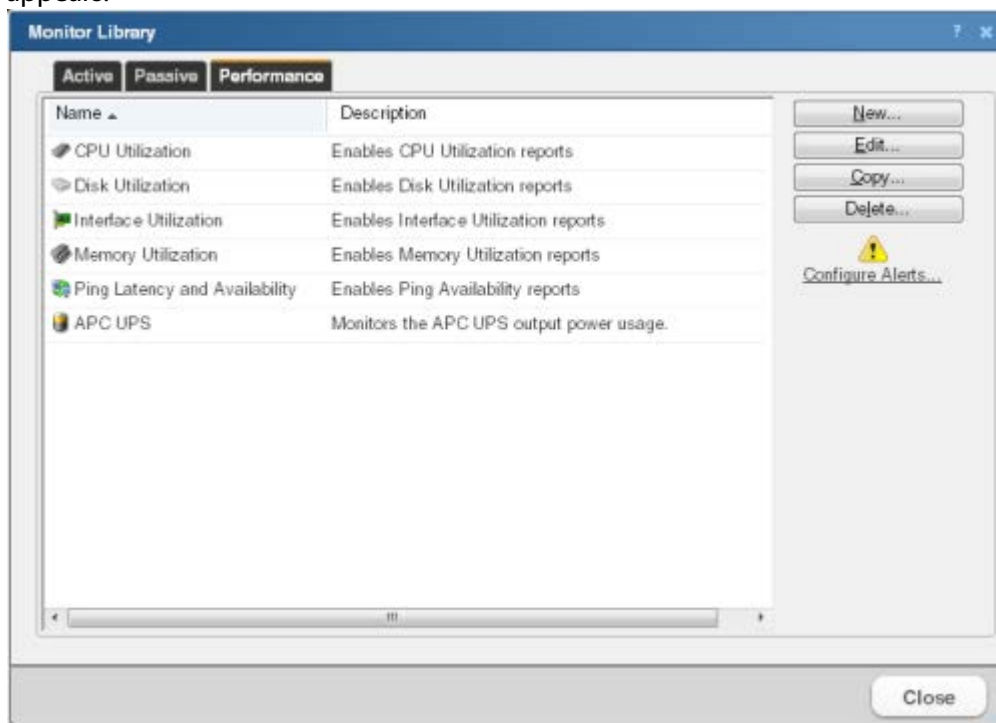
Note: If you are attempting to monitor a Cisco device with either the CPU or Memory Performance Monitors, the Cisco device must support Cisco IOS 12.2(3.5) or later.

Using the Performance Monitor Library

The Performance Monitor Library stores and displays the Performance Monitors that have been created for WhatsUp Gold. Performance monitors gather information about specific WMI and SNMP values from network devices. There are several default performance monitors, such as CPU and Disk Utilization, available in the library and you can add new monitors to the library. Performance monitors can be applied to devices from the Device Properties dialog for that device.

To access the Performance Monitor Library:

- 1 Click the **Admin** tab, and then click **Monitor Library**. The Monitor Library dialog appears.



- 2 If it is not already selected, click the **Performance** tab.
- 3 Use the Performance Monitor Library dialog to configure new or existing performance monitor types:
 - Click **New** to configure a custom performance monitor.
 - Select an existing performance monitor, then click **Edit** to modify its configuration.
 - Click **Copy** to create a duplicate of a monitor. You can use the Copy option to create new monitors based on existing monitors.



Note: The five default global monitors cannot be edited, copied or deleted: CPU Utilization, Disk Utilization, Interface Utilization, and Ping Latency and Availability.

- Select an existing performance monitor, then click **Delete** to remove it from the list.



Caution: When you delete a performance monitor from the Performance Monitor Library, any instance of that monitor is also deleted, and all related report data is also lost.

- Click **Configure Alerts** to view the Alert Center Threshold Library.

For more information on Performance Monitors, see *Enabling performance monitors* (on page 622).

Scheduling reports



Tip: In some cases, exported reports show more detailed data than that of the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To send a log or monitor report as a scheduled report:

- 1 Open the monitor report you want to email.
- 2 Click **Email** in the WhatsUp Gold toolbar.
- 3 Select **Email / Schedule Report**. The **Email Report** dialog appears.
- 4 Enter the following information for the **Email Options** tab:
 - **To.** The email address of the account which is to receive the report
 - **From.** The address you want to appear as the sender of the report.
 - **Subject.** The subject line you want to appear in the report email.
 - **Include url in email.** Select to also include the report as a web link.
 - **Alternate host.** When **Include url in email** is selected, you can choose to alter the way the URL appears to the end user. This is a useful option if users outside of your network need to access the server using a different name or address than the default address of the WhatsUp Gold server.
- 5 Select **PDF Options**, if appropriate. See *Exporting reports and logs* (on page 626) more information.
- 6 Click the **Email Server** tab.
- 7 Enter the following information for the email server:
 - **SMTP Server.** The name of the mail server.
 - **SMTP Port number.** If necessary, change the SMTP port number. The default value is 25.
 - **Timeout.** The amount of time to retry connecting to the SMTP server before giving up.
 - **Use SMTP authentication.** Select this option if the SMTP server requires authentication.

- **Username.** The username WhatsUp Gold should use to authenticate.
 - **Password.** The password WhatsUp Gold should use to authenticate.
 - **Use an encrypted connection.** Select this option if the SMTP server requires an encrypted connection.
- 8 Click **Schedule**.
 - 9 Enter a name for the report.
 - 10 Select **Disable this schedule** if you want to prevent WhatsUp Gold from running and sending scheduled reports.
 - 11 In the **Send email** section, make the following selections:
 - **Interval**
 - **Start Time**
 - 12 Complete the settings in the box that display after you make your interval selection. These options change according to the Interval selection.
 - 13 Click **OK** to save your scheduled report.

Exporting reports and logs



Tip: In some cases, exported reports show more detailed data than that of the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To export to text format:

- 1 Open the report you want to export.
- 2 Click **Export**.
- 3 Select **Export to Text**.
- 4 Clear or select the following options:
 - **Include report title**
 - **Include column names**
- 5 Select an option from the **Column delimiter** menu.
- 6 Select an option from the **Text qualifier** menu.
- 7 Click **OK** to export the report to a text file.

To export to Microsoft Excel format:

- 1 Open the report you want to export.
- 2 Click **Export**.
- 3 Select **Export to Excel**.
- 4 Clear or select the following options:
 - **Include report title**
 - **Include column names**
- 5 Click **OK** to export the report in Excel format.

To export to PDF format:

- 1 Open the report you want to export.
- 2 Click **Export**.
- 3 Select **Export to PDF**. The Export to PDF dialog appears.
- 4 Select the following options:
 - **Page size**. Select a page size from the menu.
- or -
 - **Auto size**. Select this option to automatically adjust the page size to fit all content on the PDF.
 - **Page orientation**. When a page size is selected, select **Portrait** or **Landscape** PDF.
 - Select the **Live links** option if you want to include clickable URL links in the PDF report.
 - Select **Current page** to export the currently viewed page, or select **All pages** to export all pages in the report.
- 5 Click **Export** to export the report to a PDF.

Emailing reports and logs



Tip: In some cases, exported reports show more detailed data than that of the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To email a report as a PDF:

- 1 Open the report you want to email.
- 2 Click **Email**.
- 3 Click **Email / Schedule Report**. The **Email Report** dialog appears.
- 4 Click **Email Options**. Complete the following information:
 - **To**. The email address of the account receiving the report
 - **From**. The address that appears as the sender of the report
 - **Subject**. The subject line appearing in the report email
 - **Include url in email**. Select to also include the report as a web link
 - **Alternate host**. When **Include url in email** is selected, you can choose to alter the way the URL appears to the end user. This is a useful option if users outside of your network need to access the server using a different name or address than the default address of the WhatsUp Gold server.
- 5 Select the appropriate **PDF Options**. See *Exporting reports and logs* (on page 626) for more information.
- 6 Click **Email Server**.

- 7 Enter the following information for the email server:
 - **SMTP Server.** The name of the mail server
 - **SMTP Port number.** If necessary, change the SMTP port number. The default value is 25.
 - **Timeout.** The length of time to retry connecting to the SMTP server before abandoning the attempt
 - **Use SMTP authentication.** Select this option if the SMTP server requires authentication.
 - **Username.** The username WhatsUp Gold uses to authenticate to the mail server
 - **Password.** The password WhatsUp Gold uses to authenticate to the mail server
 - **Use an encrypted connection.** Select this option if the SMTP server requires an encrypted connection.
- 8 Click **Send Email** to send a PDF email immediately, or click **Schedule** to complete the scheduled email settings. See *Scheduling reports* (on page 625) for more information.

Printing reports and logs

- 1 Open the report you want to export.
- 2 Right-click anywhere inside the report window, then select **Print**.
 - or -
 - Click **File** > **Print** from the browser menu options.

Viewing scheduled reports

The Scheduled Reports option lets you view, edit, disable, delete, and send scheduled reports configured using the WhatsUp Gold web interface **Email** > **Email / Schedule Report**.

To view scheduled reports:

- 1 Click **Email**.
- 2 Click **Scheduled Reports**. The currently scheduled reports display in the Scheduled Reports dialog.

The Scheduled Reports dialog provides the following information about each report:

- **Name.** Lists the name of the scheduled report.
- **User.** Lists the user that set up the scheduled report.
- **Schedule.** Lists the intervals that the report is scheduled to be emailed.
- **Show scheduled reports from all users** (optional). When selected, you can view reports that other users have scheduled. This option is available to users with user rights for **Manage Scheduled Report** enabled. For more information, see About user rights.

Click one of the following options to manage scheduled reports:

- **Edit.** Select a report you want to modify, then click **Edit**. The scheduled report opens in the Scheduled Report dialog where you can change the report settings.
- **Disable.** Select a report you want to stop sending at scheduled intervals, then click **Disable**. To return a report to a scheduled interval, select the report, then click **Enable**.
- **Delete.** Select a report you want to remove, then click **Delete**.
- **Send Email.** Select a report, then click **Send Email**. The scheduled email report is sent to the intended recipients immediately.

Performance monitor reports

In This Chapter

| | |
|--|-----|
| Learning about performance monitors..... | 630 |
| CPU Utilization..... | 631 |
| Disk Utilization..... | 633 |
| Memory Utilization | 636 |
| Custom | 639 |

Learning about performance monitors

The performance monitor reports deliver information about system thresholds for resources in your network.

Use performance monitor reports to view performance data (CPU, disk, interface, and memory utilization) for devices. These reports track utilization and availability information for these device components. Performance monitors gather performance counter data from network devices that have SNMP or WMI enabled. For more information, see *Creating custom performance monitors* (on page 260).

In addition to the default performance monitor reports, you can create custom monitors which let you view specific performance information for APC UPS, Printer, Active Script, SNMP, SSH, and WMI performance counters.

Add and edit the following performance monitors through the Performance Monitor Library.

Apply performance monitors to individual devices through the Device Properties dialog. From the Device Properties Performance Monitor dialog, you can enable:

- **Pre-configured performance monitors.** These are the default monitors that are stored in the Monitor Library.
- **Individual (device-specific) performance monitors.** These are custom monitors that require configuration for specific devices.



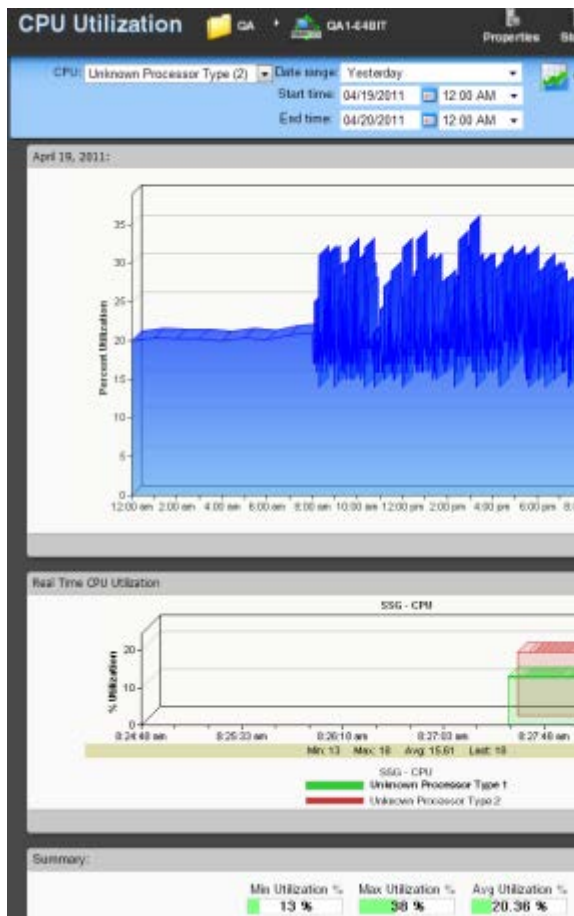
Note: Unlike the other performance monitors, because a printer monitor is specific to an individual printer device, you can only add the Printer Performance Monitor as an individual performance monitor in the Device Properties Performance Monitor dialog.

CPU Utilization

This performance monitor report displays CPU utilization percentages collected during the selected time period from the device displayed at the top of the report.

- Configure the data collection for a device by selecting a device from the Device list and selecting **Properties > Performance Monitors > CPU Utilization**.
- Configure the data collection for a group by selecting a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the CPU menu.

Device Report:



Group Report:

| Device | Description |
|------------------------|------------------------|
| GA1-64BIT | Unknown Processor Type |
| GA1-64BIT | Unknown Processor Type |
| GA-2821.ipswitch.com | Cisco CPU (1) |
| GA-2901.yourdomain.com | Cisco CPU (1) |
| GA-3750 | Cisco CPU (1) |
| GAMAINCONTROL1 | Intel (1) |
| GAMAINCONTROL1 | Intel (2) |

Monitor report body for group reports

The group report displays a list of all devices in the group and the current CPU load for each CPU in each monitored device for that group. To view the CPU Utilization report for a specific device, click the CPU displayed in the Description column. WhatsUp Gold opens the CPU Utilization device report for that device.

Monitor report body for device reports

Below the control bar is a graph showing the CPU utilization for the selected time period for the device displayed in the title bar. Each point on the graph corresponds with an entry in the graph data table below.

If the currently viewed device contains multiple CPUs, you can select which CPU information to view by making a selection from the CPU menu in the control bar.

When multiple CPUs are present, the following selections are also available:

- The CPU menu lists all available CPUs in the device. You can select any CPU and view utilization information for that CPU.
- **All CPUs (average).** The average utilization across all CPUs in the device.
- **All CPUs.** A combined graph displaying utilization for all CPUs.

Split Second Graph - Real-Time CPU Utilization for devices

When you view a device, a Split Second Graph displays under the real-time utilization data for CPUs. When you view a group, hover over the CPU description in the Description column to view the Split Second Graph for that device.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the average CPU utilization percentages collected during the time period:

- **Min Utilization %.** The minimum CPU utilization percentage experienced.
- **Max Utilization %.** The maximum CPU utilization percentage experienced.
- **Avg Utilization %.** The average CPU utilization percentage across all sample data for this time period.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).



Note: If you are viewing data for all CPUs on a device the summary section displays the lowest of the minimum CPU utilization percentages experienced across all CPUs, and the highest of the maximum CPU utilization percentages experienced across all CPUs. The average CPU utilization percentage is calculated across all sample data for all CPUs

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Disk Utilization

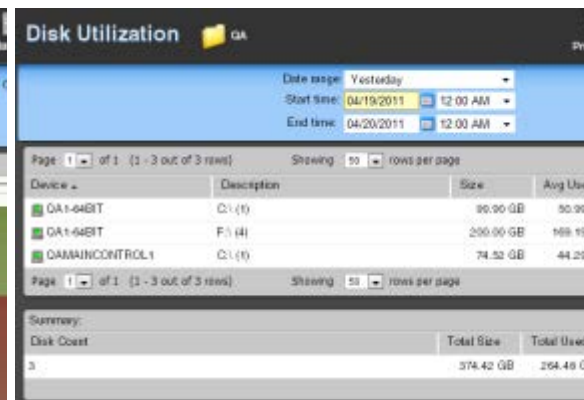
This performance monitor report displays disk utilization percentages collected during the selected time period for the group or device displayed at the top of the report.

- Configure the data collection for a device by selecting a device from the Device list and selecting **Properties > Performance Monitors > Disk Utilization**.
- Configure the data collection for a group by selecting a group from the Device picker, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Disk** menu.

Device Report:



Group Report:



Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, be sure to change the **Determine uniqueness by option** in the Advanced Data Collection settings for this performance monitor to description. For more information on advanced data collection settings, see Configuring Data Collection Advanced Settings.

Monitor report body for group reports

The group report displays a list of all devices in the group and the current disk utilization for each disk in each monitored device. To view the Disk Utilization monitor report for a specific device, click the disk displayed in the Description column. WhatsUp Gold opens the Disk Utilization device report for that device.

Monitor report body for device reports

Below the control bar is a graph showing the disk utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

The group report displays a list of all devices in the group and the current disk utilization for the primary disk (if multiple disks are present in the device). To view the Disk Utilization monitor report for a specific device, click displayed in the Description column. WhatsUp Gold redirects you to the CPU Utilization device report for that device.

Below the date/time picker is a graph showing the disk utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

When multiple disks are present in the selected device, the following selections are also available from the **Disk** menu:

- The Disks menu lists all available disks in the device. You can select any disk and view utilization information for that disk.
- **All Disks.** A combined graph displaying utilization for all disks.

Split Second Graph - Real-Time Disk Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time disk utilization.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the average disk utilization percentages collected during the time period:

- **Total Size.** The size of the disk being monitored.
- **Min Used.** The minimum amount of disk space used.
- **Max Used.** The maximum amount of disk space used.
- **Avg Used.** The average amount of disk spaced in use during the time period.
- **Min Utilization %.** The minimum disk utilization percentage experienced.
- **Max Utilization %.** The maximum disk utilization percentage experienced.
- **Avg Utilization %.** The average disk utilization percentage across all sample data for this time period.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

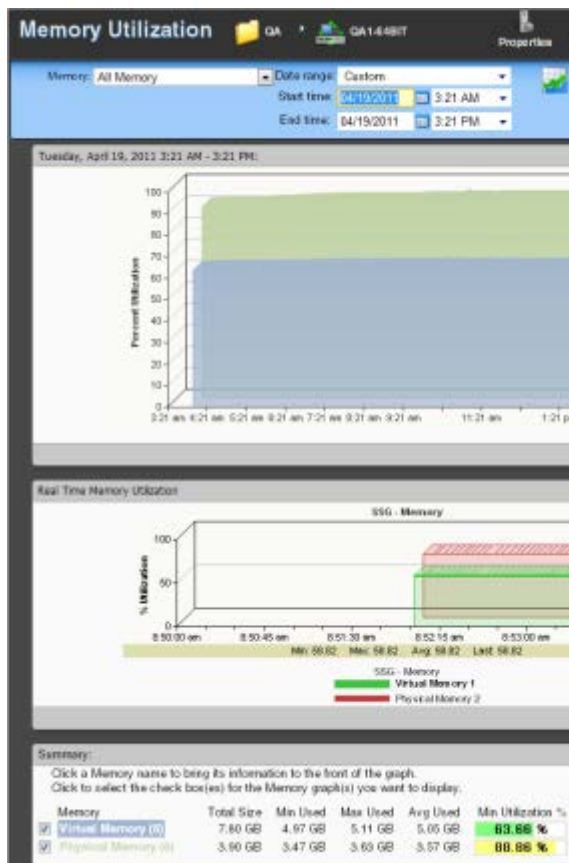
Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Memory Utilization

This performance monitor report displays memory utilization collected during the selected time period from the device displayed at the top of the report.

- Configure the data collection for a device by right-clicking a device in the Device list and selecting **Properties > Performance Monitors > Memory Utilization**.
- Configure the data collection for a group by selecting a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Memory** menu.

Device Report:**Group Report:**

Memory Utilization GA

Date range: Yesterday Start time: 04/19/2011 12:00 AM End time: 04/20/2011 12:00 AM

Page 1 of 1 (1 - 11 out of 11 rows) Showing 10 rows per page

| Device | Description | Size |
|------------------------|---------------------|------------|
| GA-3750 | Drive test (10) | 4.00 MB |
| GA-3750 | I/O (2) | 16.00 MB |
| GA-2901.yourdomain.com | I/O (2) | 36.00 MB |
| GA-2921.ipswitch.com | I/O (2) | 12.00 MB |
| GAMAINCONTROL1 | Physical Memory (4) | 1015.38 MB |
| GA-1-64BIT | Physical Memory (6) | 3.90 GB |
| GA-2901.yourdomain.com | Processor (1) | 315.19 MB |
| GA-3750 | Processor (1) | 179.00 MB |
| GA-2921.ipswitch.com | Processor (1) | 133.90 MB |
| GA-1-64BIT | Virtual Memory (5) | 7.80 GB |
| GAMAINCONTROL1 | Virtual Memory (3) | 2.39 GB |

Page 1 of 1 (1 - 11 out of 11 rows) Showing 10 rows per page



Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, be sure to change the Determine uniqueness by option in the Advanced Data Collection settings for this performance monitor to description.

Monitor report body for group reports

The group report displays a list of all devices in the group and the current memory utilization for each memory type in each monitored device. To view the Memory Utilization monitor report for a specific device, click the memory type displayed in the Description column. WhatsUp Gold opens the CPU Utilization device report for that device.

Monitor report body for devices

Below the date/time picker is a graph showing the memory utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

When multiple memory types are present in the selected device, the following selections are available from the **Memory** menu:

- The Memory menu lists all available memory types in the device. You can select any type and view utilization information for that memory.
- **All Memory.** A combined graph displaying utilization for all memory types.

Split Second Graphs - Real-Time Memory Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time memory utilization data.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the average memory utilization collected during the time period:

- **Total Size.** The total amount of memory on the device being monitored.
- **Min Used.** The minimum amount of memory in use on the device.
- **Max Used.** The maximum amount of memory in use on the device.
- **Avg Used.** The average amount of memory in use on the device during the time period.
- **Min Utilization %.** The minimum disk utilization percentage experienced.
- **Max Utilization %.** The maximum disk utilization percentage experienced.
- **Avg Utilization %.** The average disk utilization percentage across all sample data for this time period.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

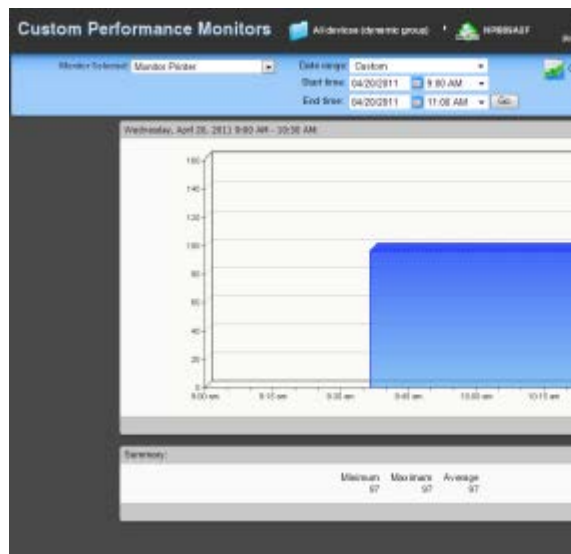
To view the properties of the current group or device, click **Properties** in the toolbar.

Custom

This performance monitor report graphs custom performance monitor values over a selected period of time.

- Configure the data collection for a device by selecting a device from the Device list and selecting **Properties > Performance Monitors**, then selecting the monitor you want to apply to the device.
- Configure the data collection for a group by selecting a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then selecting the monitor you want to apply to the group.

Device Report:



Group Report:

| Devices with Custom Performance Monitors | |
|--|----------|
| Device | Monitors |
| GA-2821 ipswitch... | APC UPS |
| GA-2901 yondora... | APC UPS |
| GA-3750 | APC UPS |
| GAMAINCONTROL1 | APC UPS |

Monitor report body for group reports

The group report displays a list of all devices in the group and the custom monitor applied to each device. To view the custom monitor data for each device, click the link to the right of the device name in the Monitors column.

Monitor report body for device reports

- Below the date/time picker, Monitor, and Chart size boxes is a graph showing the chosen monitor for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

Split Second Graph - Real Time

Under the main report graph is a Split Second Graph that displays real-time data for the WMI or SNMP custom performance monitor.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.



Note: Split Second Graphs are not available with Active Script performance monitors.

At the bottom of the graph, the report displays the average monitor percentages collected during the time period:

- Minimum.** The minimum monitor percentage experienced.
- Maximum.** The maximum percentage experienced.
- Average.** The average monitor percentage across all sample data for this period.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via *Program Options > Report Data* (on page 815).

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Device Properties

To view the properties on the current device, click the **Device Properties** button in the application at the top of the page.

Network monitor reports

Learning about network monitors

The Network monitor group provides data about network traffic. This group includes the following monitor reports:

Interface. Displays the percent utilization or traffic for a selected interface on a device, or for all interfaces for a group of devices.

Ping Availability. Displays ping availability data collected during the selected time period for the device or group displayed in the page title bar.

Ping Response. Displays ping response time data collected during the selected period from the device or group displayed in the page title bar.

Interface Discards. Displays the percentage of interface utilization discards for inbound and outbound packet data for a device interface, or group of device interfaces, during a selected time period.

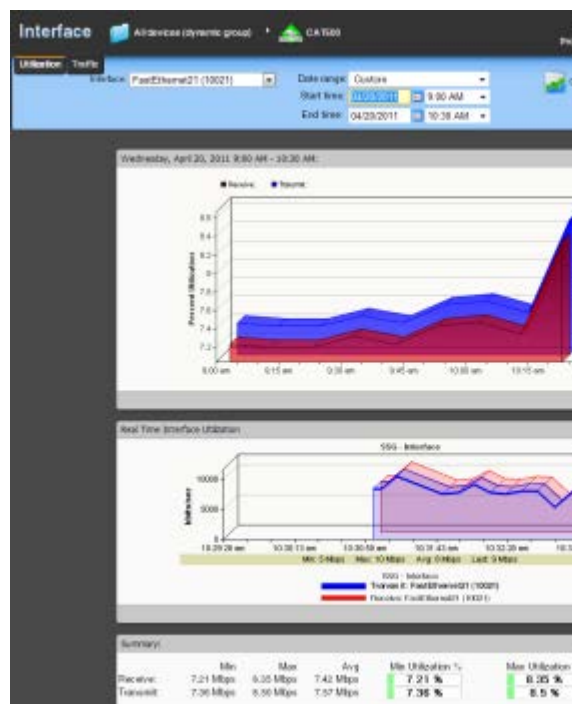
Interface Errors. Displays a line graph showing the percentage of interface utilization errors for inbound and outbound packet data for a specific device interface, or group of device interfaces, during a selected time period.

Interface Utilization

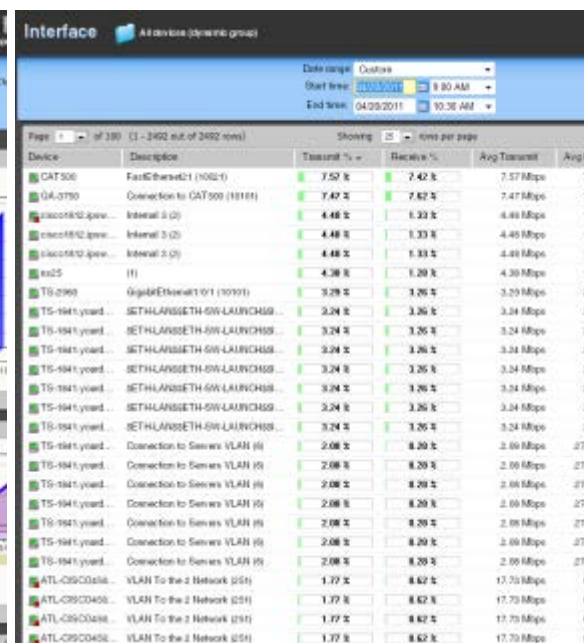
This monitor report displays the percent utilization for device interfaces.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.
- Configure the data collection for a group by right-clicking a group in the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Interfaces** menu.

Device Report:



Group Report:



Monitor report body for device reports

When a device is selected, the percent utilization for the currently selected interface displays. Each point on the graph corresponds with an entry in the graph data table below. In Octets are graphed with a red line, while Out Octets are graphed using blue.

When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graphs - Real-Time Interface Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time interface utilization data.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the Summary report displays the average interface utilization collected during the time period:

- **Min.** The minimum bits per second rate recorded for the interface.
- **Max.** The maximum bits per second rate recorded for the interface.
- **Avg.** The average bits per second rate recorded for the interface during the time period.
- **Min Utilization %.** The minimum interface utilization percentage recorded.
- **Max Utilization %.** The maximum interface utilization percentage recorded.
- **Avg Utilization %.** The average interface utilization percentage across all sample data for this time period.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).

Monitor report body for groups

Below the date/time picker is a table showing interface utilization across the current group for the selected time period.

- **Device.** The name and IP address of the device.
- **Description.** The label for the interface being shown.
- **Transmit %.** The percentage of available bandwidth used by this interface in transmitting data.

- **Receive %.** The percentage of available bandwidth used by this interface in receiving data.
- **Avg. Transmit.** The average number of bytes transmitted through the interface.
- **Avg. Receive.** The average number of bytes received through the interface.
- **Bytes Transmitted.** The total number of bytes transmitted through the interface.
- **Bytes Received.** The total number of bytes received by the interface.

Split Second Graphs in group reports

To see a real-time graph for the utilization of a device, hover over the interface description in the Description column.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.

Change to another device monitor report by selecting a different report button.

Viewing Properties

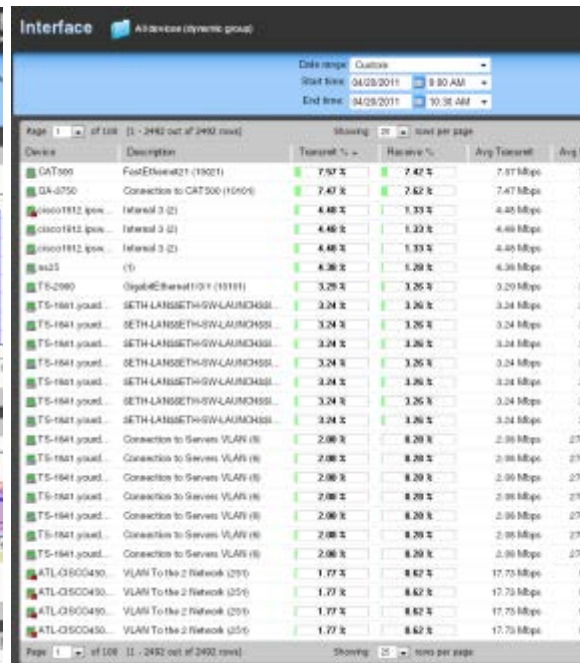
To view the properties of the current group or device, click **Properties** in the toolbar.

Interface Traffic

This monitor report displays the traffic in automatically selected units for device interfaces.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.
- Configure the data collection for a group by right-clicking a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Interfaces** menu.

Group Report:



Split Second Graphs - Real-Time Interface Utilization for devices

Under the main report graph is a Split Second Graph that displays real-time interface traffic data.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the Summary report displays the average interface utilization collected during the time period:

- **Min.** The minimum bits per second rate recorded for the interface.
- **Max.** The maximum bits per second rate recorded for the interface.
- **Avg.** The average bits per second rate recorded for the interface during the time period.
- **Min Utilization %.** The minimum interface utilization percentage recorded.
- **Max Utilization %.** The maximum interface utilization percentage recorded.
- **Avg Utilization %.** The average interface utilization percentage across all sample data for this time period.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).

Monitor report body for groups

Below the date/time picker is a table showing interface utilization across the current group for the selected time period.

- **Device.** The name and IP address of the device.
- **Description.** The label for the interface being shown.
- **Transmit %.** The percentage of available bandwidth used by this interface in transmitting data.

- **Receive %.** The percentage of available bandwidth used by this interface in receiving data.
- **Avg. Transmit.** The average number of bytes transmitted through the interface.
- **Avg. Receive.** The average number of bytes received through the interface.
- **Bytes Transmitted.** The total number of bytes transmitted through the interface.
- **Bytes Received.** The total number of bytes received by the interface.

Split Second Graphs in group reports

To see a real-time graph for the utilization of a device, hover over the interface description in the Description column.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.

Change to another device monitor report by selecting a different report button.

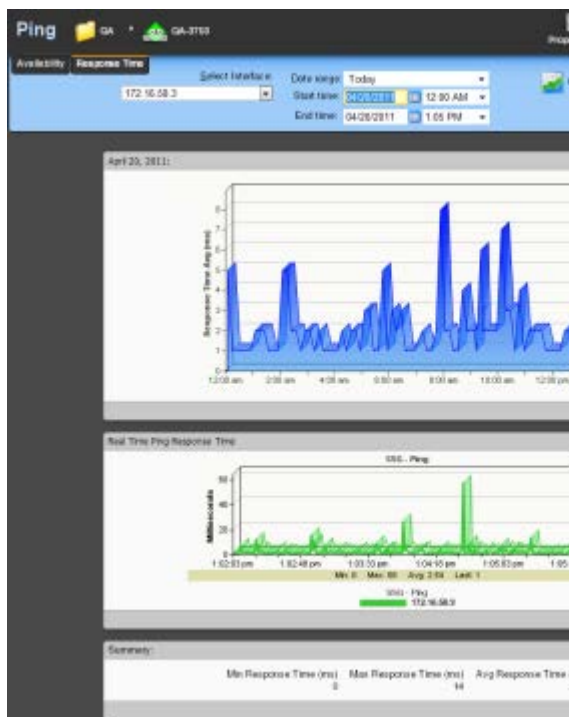
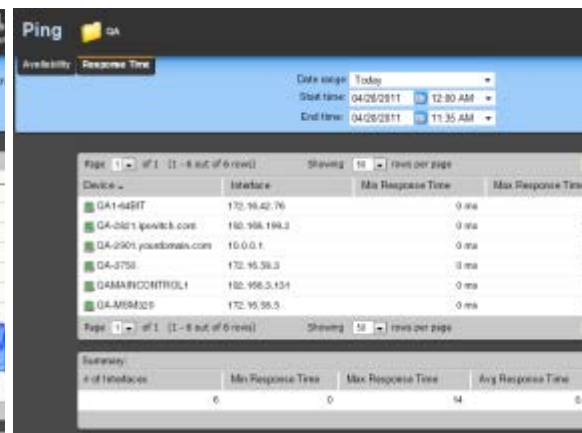
Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Ping Response Time

This monitor report displays ping response time data collected during the selected period from the device or group displayed in the page title bar. This is the amount of time it takes a packet to be returned from the device after an ICMP (Internet Control Message Protocol) poll. It is enabled when the Ping performance monitor is applied to a device.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Ping Latency and Availability > Configure**.
- Configure the data collection for a group by right-clicking a group in the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Ping** menu.

Device Report:**Group Report:****Monitor report body for device reports**

Below the date/time picker is a graph showing ping response times for the selected time period. Each point on the graph corresponds to an entry in the graph data table below.

When multiple interfaces are present in the selected device, change the selected interface using the **Select an Interface** menu.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graph - Real Time Ping Response Time for devices

Under the main report graph is a Split Second Graph that displays real-time ping response data.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays the summary for ping response time during the selected time period:

- **Min. Response Time.** The minimum amount of time (in milliseconds) that it took for the interface to respond to a ping over the selected time period.
- **Max Response Time.** The maximum amount of time (in milliseconds) that it took for the interface to respond to a ping over the selected time period.
- **Avg. Response Time.** The average amount of time (in milliseconds) that it took for the interface to respond to a ping over the selected time period.

Monitor report body for groups

Below the list of devices in the current group, the Summary table shows the average response time for all interfaces in the group.

- **Device.** The device the ping monitor is active on.
- **Interface.** The specific interface the ping monitor is active on.
- **Min response time (ms).** The minimum ping response time (in milliseconds) for the device during the selected time period
- **Max response time (ms).** The maximum ping response time (in milliseconds) for the device during the selected time period.
- **Avg response time (ms).** The average ping response time (in milliseconds) for the device across all sample data for this time period.

Split Second Graphs in group reports

To see a real-time graph for a device's ping response time, hover over a device interface in the Interface column.

Below the report body is an information summary:

- **# of Interfaces.** The number of monitored interfaces.
- **Min Response Time.** The minimum response time from the monitored interfaces over the selected time period.
- **Max Response Time.** The maximum response time from the monitored interfaces over the selected time period.
- **Avg Response Time.** The average response time from the monitored interfaces over the selected time period.



Note: Split Second Graphs are not available in VMware host reports.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).



Note: Click the device name to access the *Device Status report* (on page 354), and click the interface.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

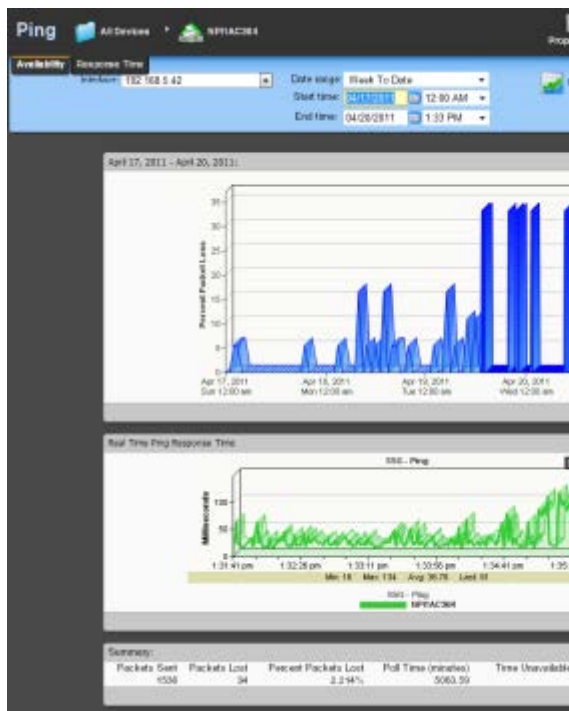
To view the properties of the current group or device, click **Properties** in the toolbar.

Ping Availability

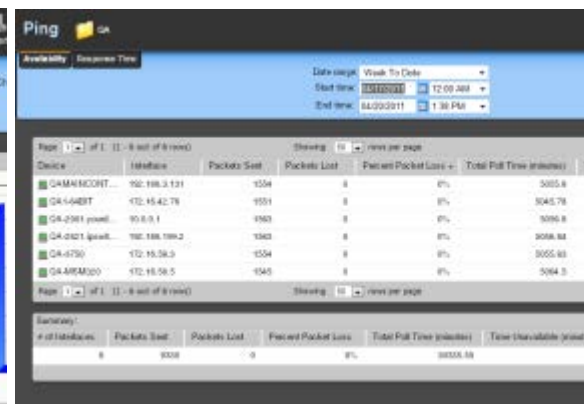
This performance report displays ping availability data collected during the selected time period for the device or group displayed at the top of the report.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Ping Latency and Availability > Configure**.
- Configure the data collection for a group by right-clicking a group in the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Ping** menu.

Device Report:



Group Report:



Monitor report body for device reports

Below the date/time picker is a graph showing device ping availability for the selected time period. Each point on the graph corresponds with an entry in the graph data table below.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Split Second Graph - Real Time Ping Availability for devices

Under the main report graph is a Split Second Graph that displays real-time ping availability data.



Note: Split Second Graphs are not available in WhatsUp Gold Standard Edition.



Note: Split Second Graphs are not available in VMware host reports.



Note: When viewing information for devices running Microsoft Windows, information gathered via WMI is displayed in real time. Information gathered by SNMP, however, may reflect a delay of one minute or more. This delay is caused by a limitation in how often Microsoft Windows updates SNMP values.

Below the Split Second Graph, the report displays general ping availability information for the device collected during the selected time period:

- **Packets Sent.** The total number of packets sent from the device during the selected time period.
- **Packets Lost.** The total number of packets lost from the device during the selected time period.
- **Percent Packets Lost.** The percentage of packets lost from the device during the selected time period.
- **Poll Time (minutes).** Amount of total time (in minutes) that passed during the time period selected.
- **Time Unavailable (minutes).** Amount of total time (in minutes) that the device was unavailable in the group.
- **Percent Available.** The total availability percentage for the device.

Monitor report body for groups

Below the date/time picker is a table showing ping availability across the current group for the selected time period.

- **Device.** The network device.
- **Interface.** The network interface.
- **Packets Sent.** The total number of packets sent throughout the current group during the selected time period.
- **Packets Lost.** The total number of packets lost throughout the current group during the selected time period.
- **Percent Packet Loss.** A percentage of packet loss throughout the current group for the selected time period.
- **Total Poll Time (minutes).** Amount of total time (in minutes) that passed during the time period selected..
- **Time Unavailable (minutes).** Amount of total time (in minutes) that a device was unavailable in the group.
- **Percent Available.** The total availability percentage averaged over all samples during the selected time period.

The Device Data table displays the same information as above, but on a per device basis.



Note: The Percent Available is a weighted average of availability for all data entries. It is not a simple average of percent availability for each entry. The value for the total availability percentage is reached by: multiplying the availability percentage with the amount of time that passed between polls to get a sum for each entry. Add those sums and divide by the sum of all time periods between polls.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data** (on page 815).



Note: Click the device name to access the *Device Status report* (on page 354), and click the interface name in the Interface column to view the availability report for that interface.

Split Second Graphs in group reports

To see a real-time graph for the availability of a device, hover over the interface name in the **Interface** column.

Below the body text is a summary of the above information:

- **# if Interfaces.** The total number of monitored network interfaces.
- **Packets Sent.** The total number of packets sent over the selected time period by the monitored interfaces.
- **Packets Lost.** The total number of packets lost over the selected time period by the monitored interfaces.
- **Percent Packet Lost.** The percentage of packets lost over the selected time period by the monitored interfaces.
- **Total Poll Time.** The total amount of time in minutes the monitored interfaces were polled.
- **Time Unavailable.** The total amount of time the monitored interfaces were unavailable.
- **Percent Available.** The percentage of the amount of time the monitored interfaces were available.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

- To view the properties of the current group or device, click **Properties** in the toolbar.

Interface Discards

This network monitor report displays the percentage of interface utilization discards for inbound and outbound packet data for a device interface, or group of device interfaces, during a selected time period. This report allows you to monitor and troubleshoot interfaces experiencing packet discard problems.

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.



Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, click **Advanced** and change the **Determine uniqueness by** list option to **Interface description**.

- Configure the data collection for a group by right-clicking a group from the Device list, selecting **Bulk Field Change** > **Performance Monitors**, and then making a selection from the **Interface** menu.

Device report:



Group report:

Interface Discards and Errors

Discards

Errors

Date range: Week To Date
Start time: 09/26/2011 12:08 AM
End time: 09/26/2011 1:01 PM

Page: 1 of 2 (1 / 33 out of 33 rows)
Showing 21 items per page

| Device | Description | Avg Transmit | Total Transmits | Avg Recv |
|----------------|--------------------------------|--------------|-----------------|----------|
| GA-2821 speed. | Mtu Network (5) | 0.00 m/s | 0 | 0 |
| GA-2821 speed. | Mtu Network (2) | 0.00 m/s | 0 | 0 |
| GA-2821 speed. | Natlo (4) | 0.00 m/s | 0 | 0 |
| GA-2901 yoad. | Connection to GA-0750 (1) | 0.00 m/s | 0 | 0 |
| GA-2901 yoad. | Connection to GA-2904 d (2) | 0.00 m/s | 0 | 0 |
| GA-2901 yoad. | Gigaset Huawei3G (3) | 0.00 m/s | 0 | 0 |
| GA-2901 yoad. | Natlo (4) | 0.00 m/s | 0 | 0 |
| GA-3750 | Vlan F (3) | 0.00 m/s | 0 | 0 |
| GA-3750 | Connection to CAT300 (10/10) | 0.00 m/s | 0 | 0 |
| GA-3750 | Gigaset Huawei1 102 (10/102) | 0.00 m/s | 0 | 0 |
| GA-3750 | Gigaset Huawei1 102 (10/102) | 0.00 m/s | 0 | 0 |
| GA-3750 | Gigaset Huawei1 1020 (10/1020) | 0.00 m/s | 0 | 0 |
| GA-3750 | Natlo (140/1) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* (2) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* 4 (8) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* 4 (8) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* 6 (7) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* 7 (8) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* 9 (8) | 0.00 m/s | 0 | 0 |
| GA1-guest | Local Area Connection* 10 (10) | 0.00 m/s | 0 | 0 |

Monitor report body for device reports

Below the date/time picker is a graph showing interface utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below. ifInDiscards (Receive) are graphed as a red line, while ifOutDiscards (Transmit) are graphed as a blue line. When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Summary

Under the main report graph, the report displays a summary of data for the interface collected during the time period:

Receive

- **Min.** The minimum number of interface discard packets received (ifInDiscards) per minute.
- **Max.** The maximum number of interface discard packets received (ifInDiscards) per minute.
- **Avg.** The average number of interface discard packets received (ifInDiscards) per minute.

Transmit

- **Min.** The minimum number of interface discard packets transmitted (ifOutDiscards) per minute.
- **Max.** The maximum number of interface discard packets transmitted (ifOutDiscards) per minute.
- **Avg.** The average number of interface discard packets transmitted (ifOutDiscards) per minute.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Monitor report body for groups

Below the date/time picker is a table showing device interface packet discard information for the selected time period:

- **Device.** The network device name.
- **Description.** The network device interface description.
- **Avg Transmit.** The average number of discarded packets transmitted from each interface per minute.
- **Total Transmit.** The total number of discarded packets transmitted for each interface.

- **Receive.** The average number of discarded packets received from each interface per minute.
- **Total Receive.** The total number of discarded packets received for each interface.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

- To view the properties of the current group or device, click **Properties** in the toolbar.

Interface Errors

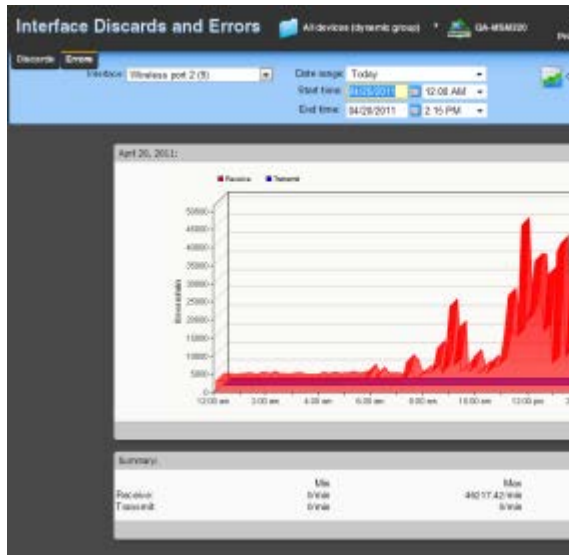
This network monitor report displays a line graph showing the percentage of interface utilization errors for inbound and outbound packet data for a specific device interface, or group of device interfaces, during a selected time period. This report allows you to monitor and troubleshoot interfaces experiencing packet error problems

- Configure the data collection for a device by right-clicking the device in the Device list and selecting **Properties > Performance Monitors**, then selecting **Interface Utilization > Configure**.



Note: To ensure that your data collection is uninterrupted in the occurrence of a re-index, click **Advanced** and change the **Determine uniqueness by** list option to **Interface description**.

- Configure the data collection for a group by right-clicking a group from the Device list, selecting **Bulk Field Change > Performance Monitors**, and then making a selection from the **Interface** menu.

Device report:**Group report:**

| Device | Description | Avg Transmit | Total Transmit | Avg R |
|----------------|-------------------|--------------|----------------|-------|
| GA-2521 ipw... | 192.168.1.1 (1) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.2 (2) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.3 (3) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.4 (4) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.5 (5) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.6 (6) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.7 (7) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.8 (8) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.9 (9) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.10 (10) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.11 (11) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.12 (12) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.13 (13) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.14 (14) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.15 (15) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.16 (16) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.17 (17) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.18 (18) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.19 (19) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.20 (20) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.21 (21) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.22 (22) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.23 (23) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.24 (24) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.25 (25) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.26 (26) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.27 (27) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.28 (28) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.29 (29) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.30 (30) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.31 (31) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.32 (32) | 0.00/min | 0 | 0 |
| GA-2521 ipw... | 192.168.1.33 (33) | 0.00/min | 0 | 0 |

Monitor report body for device reports

Below the date/time picker is a graph showing interface utilization for the selected time period. Each point on the graph corresponds with an entry in the graph data table below. ifInErrors (Receive) are graphed as a red line, while ifOutErrors (Transmit) are graphed as a blue line.

When multiple interfaces are present in the selected device, change the selected interface using the **Interface** menu.

Summary for device reports

Under the main report graph, the report displays a summary of data for the interface collected during the time period:

Receive

- **Min.** The minimum number of interface error packets received (ifInErrors) per minute.
- **Max.** The maximum number of interface error packets received (ifInErrors) per minute.
- **Avg.** The average number of interface error packets received (ifInErrors) per minute.

Transmit

- **Min.** The minimum number of interface error packets transmitted (ifOutErrors) per minute.
- **Max.** The maximum number of interface error packets transmitted (ifOutErrors) per minute.

- **Avg.** The average number of interface error packets transmitted (ifOutErrors) per minute.



Note: Values displayed in the graph are the average values for the selected time period. Values displayed in the summary are the minimum, maximum, and average values for the selected time period. If raw polling data has been averaged into hourly or daily summarized data, the values for min and average, or maximum and average can be different. In some cases, they may be very different if there was a period of time when polled values were much higher or lower than normal.



You can verify your report rollup settings on the WhatsUp Gold console via **Program Options > Report Data**.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Monitor report body for groups

Below the date/time picker is a table showing device interface packet error information for the selected time period:

- **Device.** The network device name.
- **Description.** The network device interface description.
- **Avg Transmit.** The average number of packets transmitted with errors from each interface per minute.
- **Total Transmit.** The total number of packets transmitted with errors for each interface.
- **Receive.** The average number of packets received with errors from each interface per minute.
- **Total Receive.** The total number of packets received with errors for each interface.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

- To view the properties of the current group or device, click **Properties** in the toolbar.

Using Device monitor reports

Learning about Device monitors

The Device monitor group includes monitors which provide information about specific devices that you select to monitor. This group includes the following monitor reports:

- **Active Monitor Availability.** Displays a graph that outlines the availability of the Active Monitors for a device or group of devices.
- **Active Monitor Outages.** Displays a table showing the downtime of all active monitors in the currently selected group.
- **Device Uptime.** Displays a table showing the uptime status for monitored devices in the selected group.
- **Device Health.** Displays the current status of monitored devices in the selected group, along with each monitor applied to those devices.
- **State Change Acknowledgement.** Displays a table of devices in the selected group that have changed state and have not received acknowledgement.
- **State Change Timeline.** Displays a table showing when a monitor on a device, or all monitors on all devices in a group, changed from one state to another during a selected time period.
- **Top 10.** Displays a dashboard containing lists of top 10 devices based on a variety of monitor reports.

Active Monitor Availability

This device monitor report displays an area graph that outlines the availability of the Active Monitors for a device or group of devices.

Active Monitor Availability

All devices (dynamic group)

2008RDCR02.HANDC

Active Monitor: Ping

Diff range: Today

Start time: 04/20/2011 12:00 AM

End time: 04/20/2011 1:32 PM

April 20, 2011:

Monitor Status

Up

Down

12:00 am 2:00 am 4:00 am 6:00 am 8:00 am 10:00 am 12:00 pm 2:00 pm

Summary:

| Up | Maintenance | Unknown | Down | Availability |
|--------|-------------|---------|-------|--------------|
| 98.74% | 0.00% | 0.00% | 1.56% | 98.74% |

Active Monitor Availability

Adventica (dynamic group)

Date page: Today
 Start time: 04/29/2011 12:00 AM
 End time: 04/29/2011 2:28 PM

| Page | 117 | of 120 | (2005 - 2009 out of 2009 rows) | Showing | 25 | rows per page |
|---------------------|-----------------|---------|--------------------------------|---------|---------|---------------|
| Device | Monitor | Up | Maintenance | Unknown | Down | |
| 200RFX-CHANGE | Plug | 98.738% | 0.000% | 0.000% | 1.262% | |
| MART06a | Plug | 98.399% | 0.000% | 0.000% | 1.601% | |
| RWS175 | Plug | 98.182% | 0.000% | 0.000% | 1.818% | |
| d-wm200crt | Plug | 91.306% | 0.000% | 0.000% | 8.694% | |
| spongyteacher.jp... | Plug | 90.855% | 0.000% | 0.000% | 9.145% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.249% | 0.000% | 0.000% | 9.750% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.249% | 0.000% | 0.000% | 9.750% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.237% | 0.000% | 0.000% | 9.763% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.237% | 0.000% | 0.000% | 9.763% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.227% | 0.000% | 0.000% | 9.773% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.227% | 0.000% | 0.000% | 9.773% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| ATL-GIGOC4300.g... | Interface (...) | 91.219% | 0.000% | 0.000% | 9.781% | |
| 192.168.6.213 | Plug | 84.537% | 0.000% | 0.000% | 15.463% | |
| DEM-AIIC2 | Plug | 89.793% | 0.000% | 0.000% | 10.207% | |
| DEM-AIIC21 | Plug | 30.408% | 0.000% | 0.000% | 69.591% | |
| atl-sayonaraipow... | Plug | 30.695% | 0.000% | 0.000% | 69.305% | |
| 192.168.2.19 | Plug | 90.134% | 0.000% | 0.000% | 9.866% | |
| ATL-5500G2.ipw... | Interface (...) | 47.584% | 0.000% | 0.000% | 52.416% | |
| vethelp-61958.g... | Plug | 45.464% | 0.000% | 0.000% | 54.536% | |

Page: 117 of 120 (2005 - 2009 out of 2009 rows) Showing 25 rows per page

A graph at the top of the monitor report displays the state of the selected active monitor for the device.

At the bottom of the graph, the summary section displays:

- **Up.** The percentage for the amount of time the Active Monitors were up.
- **Maintenance.** The percentage for the amount of time the Active Monitors were in maintenance.
- **Unknown.** The percentage for the amount of time the Active Monitors status was unknown.
- **Down.** The percentage for the amount of time the Active Monitors were down.
- **Availability.** The overall availability for the Active Monitor by color for the selected time period.
- **Green.** Percentage of the time device was available.
- **Red.** Percentage of time the device was unavailable.
- **Orange.** Percentage of time the device was in maintenance mode.
- **Gray.** Percentage of time the device was in an unknown state. The state of a device is unknown when the monitors for that device are disabled or deleted, or if a device has an "up" dependency and the device it is dependent upon is down.

Changing how the chart looks

Click the **Chart Properties** button to change how the report chart is displayed.

Monitor report body for group reports

This group report displays a summary of availability times for all Active Monitors within a device group. The following information is displayed within the report:

- **Device.** The network device. Click one of the device entries to view the Device Active Monitor Availability Report for that device.
- **Monitor.** The type of Active Monitor.
- **Up.** The percentage for the amount of time the Active Monitor was up.
- **Maintenance.** The percentage for the amount of time the Active Monitor was in maintenance.
- **Unknown.** The percentage for the amount of time the Active Monitor was in an unknown state.
- **Down.** The percentage for the amount of time the Active Monitor was down.
- **Availability.** The overall availability for the Active Monitor by color for the selected time period.
- **Green.** Percentage of the time device was available.
- **Red.** Percentage of time the device was unavailable.
- **Orange.** Percentage of time the device was in maintenance mode.
- **Gray.** Percentage of time the device was in an unknown state. The state of a device is unknown when the monitors for that device are disabled or deleted, or if a device has an "up" dependency and the device it is dependent upon is down.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Active Monitor Outages

This device report shows the downtime of all active monitors in the currently selected group.

| Device | Monitor | Down time | Down count |
|------------------------|--------------|-----------|------------|
| QA-290t.yourdomain.com | Fan | 6m | 1 |
| QA-290t.yourdomain.com | Power supply | 6m | 1 |
| QA-290t.yourdomain.com | Temperature | 6m | 1 |
| QA-64BIT | Ping | 5m | 4 |

Monitor report body

- **Device.** Lists the device state icon, host name, and IP address.
- **Monitor.** Lists the active monitor as it appears in the Active Monitor Library.
- **Down time.** Specifies how long the active monitor has been in the down state.
- **Down count.** Specifies how many times the active monitor has gone into the down state during the down time.

Navigation

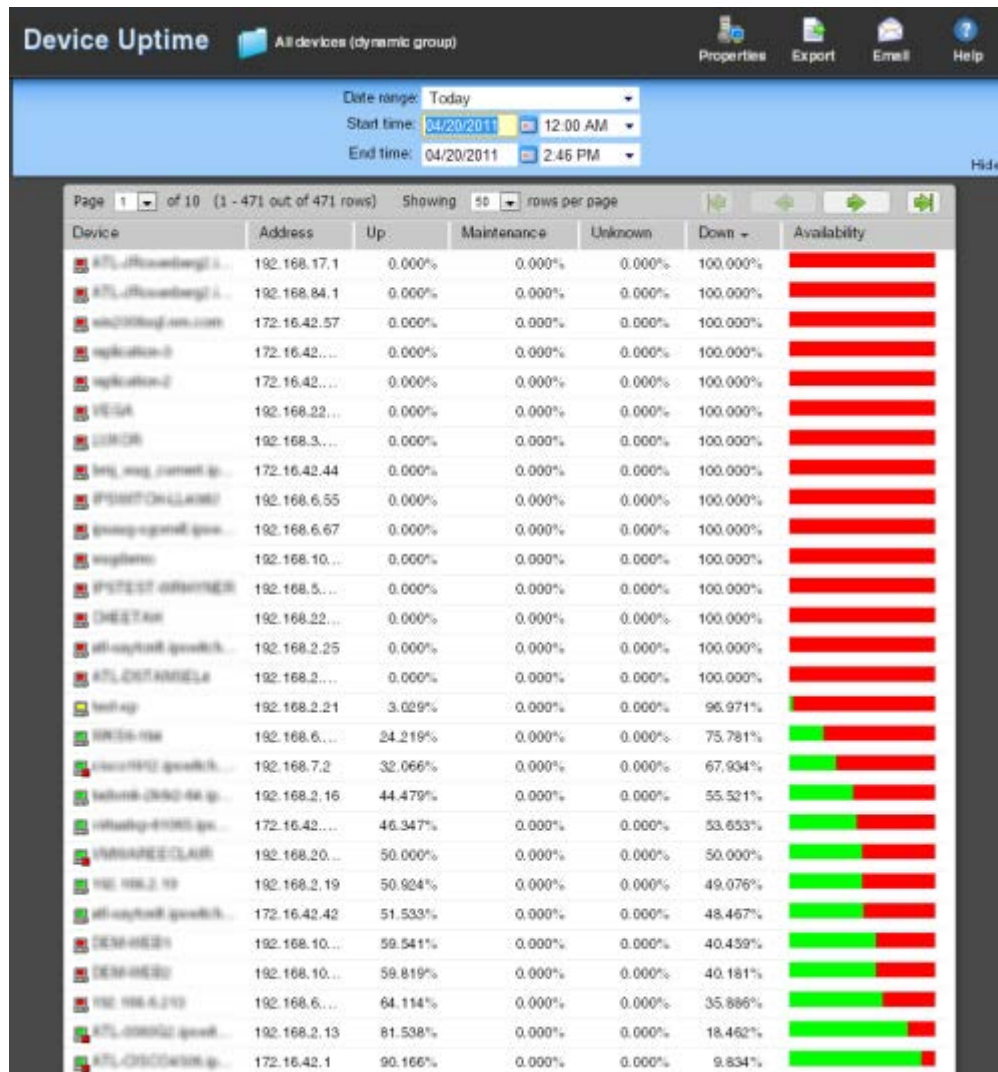
- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Device Uptime

This device report displays the uptime status for monitored devices in the selected group.



- For more information about what each icon state means, see Device State Legend.

Monitor report body

Below the date/time picker is a table showing the devices in the group collecting data for the time period chosen, and the uptime status information for the each device in the group:

- Device.** The group device's display name (or IP address if a display name isn't specified in its Device Properties) and device state icon.
- Address.** The device IP address monitor.
- Up.** The percentage for the amount of time the device was up during the selected time period for all devices.

- **Maintenance.** The percentage for the amount of time the device was in maintenance during the selected time period for all devices.
- **Unknown.** The percentage for the amount of time the device status was in an unknown state during the selected time period for all devices.
- **Down.** The percentage for the amount of time the device was down during the selected time period for all devices.
- **Availability.** The overall availability for the device during the selected time period, by color. The percentage of the bar shaded red in the Availability column indicates the percentage of time the device was not available, while the percentage shaded green indicates the percentage of time the device was available.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Device Health

This group report displays the current status of monitored devices in the selected group, along with each monitor configured to those devices.

Health

All devices (dynamic group)

Properties

Export

Email

Help

| Device | Monitor | Status | How long | When |
|------------------------------|--------------------------------|-------------------|-----------|------------------------------|
| qti_8087_56.goweth.itn.ap... | Ping | Up at least 5 min | 10h 30m | Wed Apr 20 04:24:41 EDT 2011 |
| ATL_018004086.goweth.itn... | Ping | Up at least 5 min | 1d 4h 25m | Tue Apr 19 10:29:53 EDT 2011 |
| TEL_198_198.32 | Ping | Up at least 5 min | 1d 4h 25m | Tue Apr 19 10:29:53 EDT 2011 |
| TEL_198_198.34 | Ping | Up at least 5 min | 1d 4h 25m | Tue Apr 19 10:29:53 EDT 2011 |
| TEL_198_198.36 | Ping | Up at least 5 min | 1d 4h 25m | Tue Apr 19 10:29:53 EDT 2011 |
| TEL_198_198.38 | Ping | Up at least 5 min | 1d 4h 25m | Tue Apr 19 10:29:53 EDT 2011 |
| TEL_198_198.40 | Ping | Up at least 5 min | 1d 4h 25m | Tue Apr 19 10:29:53 EDT 2011 |
| ATL_018004086.goweth.itn... | Temperature | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Power supply | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Fan | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Ping | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:40:54 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@274 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@275 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@272 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@271 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@270 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@269 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@268 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@267 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@266 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@265 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@264 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@263 - unrooted VL... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@262 - Nexus-Mara... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@261 - Nexus-Pack... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |
| ATL_018004086.goweth.itn... | Interface@260 - Nexus-Cont... | Up at least 5 min | 5d 3h 14m | Fri Apr 15 11:41:12 EDT 2011 |

For more information about what each icon state means, see [Device State Legend](#).

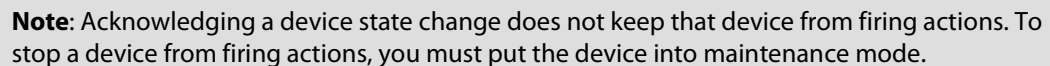
Monitor report body

Below the date/time picker is a table showing the total number of devices in the group collecting data for the time period chosen, and the status of the monitors configured for the devices in that group. The following information displays:

- **Device.** The network device.
- **Monitor.** The specific monitor.
- **State.** The state of the monitor at the time of the last poll.
- **How long.** The period of time that the monitor has been in the current state.
- **When.** The date and time the monitor went in to the current state.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.



- **In Maintenance.** Indicates whether or not the device is in maintenance mode. The state is either yes or no.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

State Change Timeline

Device report:

The screenshot shows the 'State Change Timeline' for a single device. The toolbar includes a 'Date range' dropdown set to 'Today', 'Start time' (04/28/2011 12:00 AM), and 'End time' (04/28/2011 3:53 PM). The table below lists state changes for a single monitor.

| Start time | Monitor | State | Duration |
|--------------------------------------|---------|-------------------|----------|
| Wednesday, April 20, 2011 03:45:1... | Ping | Up at least 5 min | 5m |
| Wednesday, April 20, 2011 03:41:1... | Ping | Up | 4m |
| Wednesday, April 20, 2011 03:40:1... | Ping | Down | 56s |
| Wednesday, April 20, 2011 11:30:5... | Ping | Up at least 5 min | 4h 7m |
| Wednesday, April 20, 2011 11:28:5... | Ping | Up | 4m |
| Wednesday, April 20, 2011 11:27:5... | Ping | Down | 56s |
| Wednesday, April 20, 2011 10:34:2... | Ping | Up at least 5 min | 52m |
| Wednesday, April 20, 2011 10:30:2... | Ping | Up | 4m |
| Wednesday, April 20, 2011 10:29:2... | Ping | Down | 50s |
| Wednesday, April 20, 2011 10:07:1... | Ping | Up at least 5 min | 22m |
| Wednesday, April 20, 2011 10:02:1... | Ping | Up | 5m |
| Wednesday, April 20, 2011 10:01:1... | Ping | Down | 56s |
| Wednesday, April 20, 2011 02:33:5... | Ping | Up at least 5 min | 7h 27m |
| Wednesday, April 20, 2011 02:28:5... | Ping | Up | 4m |
| Wednesday, April 20, 2011 02:27:5... | Ping | Down | 1m |
| Wednesday, April 20, 2011 01:01:1... | Ping | Up at least 5 min | 1h 26m |
| Wednesday, April 20, 2011 12:58:0... | Ping | Up | 5m |
| Wednesday, April 20, 2011 12:54:1... | Ping | Down | 1m |

Group report:

The screenshot shows the 'State Change Timeline' for a group of devices. The toolbar is identical to the device report. The table lists state changes for multiple monitors across the group.

| Start time | Device - Monitor | State | Duration |
|--------------------------------------|----------------------------|----------------------|----------|
| Wednesday, April 20, 2011 03:55:2... | cisco1842.ipswitch.com ... | Down at least 2 min | 56s |
| Wednesday, April 20, 2011 03:55:1... | test-p - Ping | Down at least 20 min | 1m |
| Wednesday, April 20, 2011 03:53:2... | cisco1842.ipswitch.com ... | Down | 2m |
| Wednesday, April 20, 2011 03:52:3... | cisco1842.ipswitch.com ... | Up | 1m |
| Wednesday, April 20, 2011 03:49:2... | URAM35 - Ping | Up at least 5 min | 7m |
| Wednesday, April 20, 2011 03:49:2... | TELEVANTAGE - Ping | Up at least 5 min | 7m |
| Wednesday, April 20, 2011 03:49:2... | ipsoq-ohart.ipswitch.m... | Up at least 5 min | 8m |
| Wednesday, April 20, 2011 03:47:1... | WRS2005P264 - Ping | Up at least 5 min | 9m |
| Wednesday, April 20, 2011 03:45:2... | URAM35 - Ping | Up | 4m |
| Wednesday, April 20, 2011 03:45:1... | WRS216 - Ping | Up at least 5 min | 11m |
| Wednesday, April 20, 2011 03:45:1... | TELEVANTAGE - Ping | Up | 4m |
| Wednesday, April 20, 2011 03:42:2... | URAM35 - Ping | Down | 9m |
| Wednesday, April 20, 2011 03:42:2... | ipsoq-ohart.ipswitch.m... | Up | 4m |
| Wednesday, April 20, 2011 03:44:1... | TELEVANTAGE - Ping | Down | 3m |
| Wednesday, April 20, 2011 03:43:3... | ipsoq-ohart.ipswitch.m... | Down | 3m |
| Wednesday, April 20, 2011 03:43:3... | lad-ws2106ahd.ipswitch... | Up at least 5 min | 13m |
| Wednesday, April 20, 2011 03:43:1... | WRS2005P264 - Ping | Up | 2m |
| Wednesday, April 20, 2011 03:42:1... | WRS2005P264 - Ping | Down | 3m |
| Wednesday, April 20, 2011 03:41:1... | WRS231 - Ping | Up at least 5 min | 15m |
| Wednesday, April 20, 2011 03:41:1... | WRS216 - Ping | Up | 4m |
| Wednesday, April 20, 2011 03:42:1... | WRS216 - Ping | Down | 5m |
| Wednesday, April 20, 2011 03:42:1... | test-p - Ping | Down at least 5 min | 15m |
| Wednesday, April 20, 2011 03:39:2... | URAM35 - Ping | Up at least 5 min | 9m |
| Wednesday, April 20, 2011 03:39:1... | lad-ws2106ahd.ipswitch... | Up | 4m |
| Wednesday, April 20, 2011 03:38:2... | lad-ws2106ahd.ipswitch... | Down | 57s |

Monitor report body for devices

This device monitor report shows a timeline of when a monitor on a device, or all monitors on all devices in a group, changed from one state to another during a selected time period.

- **Start time.** The date and time of the state change.
- **Monitor.** The device name and the type of monitor that experienced the state change.
- **State.** The state of the condition at the time of the poll. The thin gray bar on a state indicator color block means that the device state change has not been acknowledged.

- **Duration.** The amount of time the state remained unchanged.
- **Message.** The actual result message returned to WhatsUp Gold at the time of the poll.

Monitor report body for groups

This group report shows a timeline of when each monitor on a device in the selected group changed from one state to another during the selected time period.

- **Start time.** The date and time of the state change.
- **Device-Monitor.** The device name and the type of monitor that experienced the state change.
- **State.** The state of the condition at the time of the poll. The thin gray bar on a state indicator color block means that the device state change has not been acknowledged.
- **Duration.** The amount of time the state remained unchanged.
- **Message.** The actual result message returned to WhatsUp Gold at the time of the poll.

Click a device name to access the *Device Status Report* (on page 354) for that device.

Click the current state to access the State Change Timeline for that device.

Navigation

- Change the device you are viewing by clicking the group or device name currently in context and then selecting a new device in the device picker.
- Change to another device monitor report by selecting a different report button.

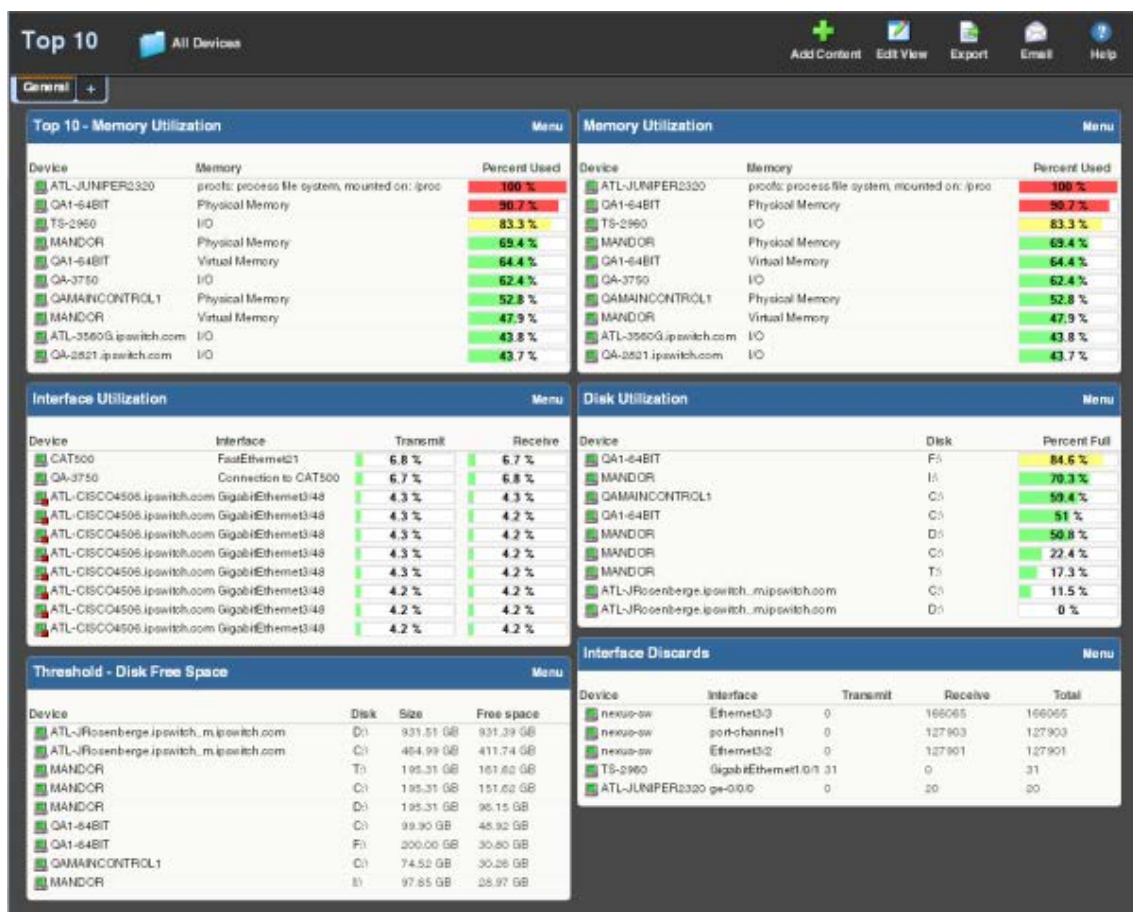
Viewing Properties

To view the properties of the current group or device, click **Properties** in the toolbar.

Top 10 Dashboard

The WhatsUp Gold Top 10 dashboard displays Top 10 reports for your network devices. The Top 10 dashboard shows devices, at a glance, that may be potential problems and to provide information on the current health of your network devices. It is pre-configured to include reports that display data on the top network devices by:

- Interface Errors
- Interface Discards
- Interface Utilization
- Interface Traffic
- Ping Response Time
- Disk Utilization
- CPU Utilization
- Memory Utilization



You can add any of the *Top 10 reports* (on page 561) to the Top 10 dashboard.

Unlike the Home and Device dashboards, the Top 10 dashboard is designed with only the General dashboard view. You can customize the general view in the same way you can other dashboard views by removing the default dashboard reports and/or adding other Top 10 and Threshold dashboard reports.

- Add the reports you want to see here by clicking **Add Content**. For more information, see *Adding dashboard reports to a dashboard view* (on page 342).

- Change options for individual reports by clicking **Menu > Configure** for each report.
- Add additional views by clicking the +. Remove views by dragging them to the trash. For more information, see *Working with dashboard views* (on page 345).

The Top 10 dashboard also displays threshold reports. These reports let you set a threshold to filter out items that do not match a specified criteria. For example, the Interface Utilization Threshold report could have been used (in the example above) instead of the Interface Top 10 report, to filter out the interfaces that are not above 50% utilization. Using this approach, only interfaces with significant usage would be shown.

Thresholds

Report percentages are displayed in colors that represent the utilization thresholds:

- **Red.** Above 90%
- **Yellow.** Above 80%
- **Green.** 80% or less

Remote Site Log

This system report lists all error messages generated by remote site connection attempts.

You can change the order of the information displayed in each column by clicking a column header.

Report body

Below the date/time picker is a table showing all remote site errors that occurred during the selected time period.

The following information is displayed in the log:

- **Date.** The date on which the error occurred.
- **Type.** The type of the error message received.
- **Status.** The error message received.
- **Remote Site.** The remote site on which the failed connection took place.



Note: If this report's data exceeds the maximum number of records set for full reports, use the Zoom Tool to view more records for the report. The maximum number of records any full report displays is specified in the Preferences dialog.

Remote Site Status

This system problem areas report displays a summary status of devices and monitors on all remote sites configured for WhatsUp Gold remote reports at the time of the last refresh.

Report Body

The report body contains the following pieces of information:

- **Location.** The location, or remote site's display name and HTTP address.
- **Devices up.** The number of devices on the remote site that are in the Up state at the time of the last refresh.
- **Devices down.** The number of devices on the remote site that are in the Down state at the time of the last refresh.
- **Devices in maintenance.** The number of devices on the remote site that are in Maintenance at the time of the last refresh.
- **Monitors up.** The number of monitors on the remote site that are in the Up state at the time of the last refresh.
- **Monitors down.** The number of monitors on the remote site that are in the Down state at the time of the last refresh.
- **Last refresh time.** The time WhatsUp Gold gathered the data from the remote site.

Diagnostic Report

This system problem areas report allows the user to perform and view a series of diagnostic checks on the WhatsUp Gold application, the database, and the computer where the application is running. When this report is viewed for the first time, you must click **Execute Diagnostics Now** to have WhatsUp Gold perform the checks. When the checks are complete, the information is displayed in the body of the report. With subsequent visits to the report, you can view previous checks, or click **Execute Diagnostics Now** again to update that information.

Click the **View Latest Report** button to only display the results of the last diagnostic check, or click **View All Results** to show all checks that have been performed on the system.

Report Body

- **Date.** The date and time the diagnostic was run.
- **Diagnostic.** The specific diagnostic check that was performed.
- **Status.** Displays either Issue or Success for each diagnostic.
- **Result.** This column shows the text results of the diagnostic checks. If an issue is found during one of the checks, a link appears in the row for that diagnostic check, directing you to more information about the issue.

Maximum report records



Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance.



Note: WhatsUp Gold v14.1 and prior used a default value of 10,000 max records; WhatsUp Gold v14.2 and later use a default value of 1,000 max records. For more information, see *Manage Web Server* (on page 681).

Business Hours report settings

You can select **Standard Business Hours** in many WhatsUp Gold and Flow Monitor reports. Click the **Date range** list and select **Standard Business Hours** to limit report views to business operation hours. Standard business hours default to Monday - Friday from 9:00 am - 5:00 pm. You can add, edit, and delete business hour settings in the Business Hours dialog.



Note: The Business Hours setting is available for group reports only.

- **Add Hours.** Click to add a new set of business hours for report time ranges.
- **Name** list. Click to select an existing business hours setting to edit or delete it.
- **Delete.** Select a business hours setting you want to remove from the list, then click **Delete** to remove it.
- **Link days.** Select this option to use the same start and end time for each scheduled day.

To change/edit Standard Business Hours:

- 1 Select the days you want to include in your business hours, then use the slider bar to adjust the start and end times for each day.
- 2 If you want to stop creating or editing a business hours setting, click **Cancel**.
- 3 Click **OK** to complete the Business Hours report setting.

WhatsConnected Device Info

The WhatsConnected Device Info full report provides a tabular view that displays detailed network device information gathered by WhatsConnected.



Note: Data for the WhatsConnected Device Info report appears only when the selected device is a device imported from WhatsConnected.

You can access this report using one of the following methods:

- **Device view right-click menu.** From the WhatsUp Gold Device View, right-click on a WhatsConnected device and select **Device Viewer**.
- **Device Reports.** On the Reports tab, click **Device Reports**. The reports overview screen appears. In the General section of the Device Reports section, click **WhatsConnected Device Information**.
- **More Device Reports.** From any device report, select **WhatsConnected Device Info** from the More Device Reports list box.

The WhatsConnected Device Info report has several information types whose availability is based on the type of device on which you invoke the report. The following is a list of all of the possible information types:

- **System.** Provides IP Address/MAC Address, MIB II information, product vendor, and other system information.
- **IP Addresses.** Provides IP Address configuration information.
- **Interfaces.** Provides name entries (IF information) for each device interface and other interface information.
- **Bridge Ports.** Provides Bridge Port and VLAN name and index information.
- **VLANs.** Provides Virtual LAN configuration information.
- **LAG Trunks.** Provides Link Aggregation Group information.
- **Assets.** Provides inventory information about the device components.
- **Links.** Provides physical connectivity information from this device to other network devices.
- **IP Routes.** Provides IP route configuration data information.
- **Spanning Tree (STP).** Provides spanning tree configuration and status information.
- **ARP Cache.** Provides Address Resolution Protocol (ARP) table information.
- **Forwarding.** Provides Layer 2 forwarding information.
- **Protocol Profile.** Provides information about successful protocol matches for this device.
- **HSRP.** Provides information about the Hot Standby Router Protocol (HSRP) on the device. The information relates to the standby nature of routers.
- **IP Phone.** Provides information about the selected (individual) IP phone.
- **IP Phone Manager.** Provides information about the IP phones that are registered or are communicating with a call manager.
- **IP Routes.** Provides information about the IP routes configured for this device.
- **VRRP.** Provides information about the Virtual Router Redundancy Protocol (VRRP) on the device. The information relates to the standby nature of routers.
- **STP.** Provides information about Spanning Tree Protocol entries discovered on this device.
- **Software.** Provides information about installed software discovered on this device.

Navigation

You can change the device you are viewing by clicking the device name in the application bar at the top of the page.

You can change to another device report by selecting it from the **More Device Reports** list.

Device Properties

To view the properties on the current device, click the **Device Properties** button in the application at the top of the page.

Device State Legend

The following shows the default device states used by WhatsUp Gold. You can make additions to these on the Device States section of Program Options.



Unknown (Unknown - 0)



Down (Not Responding - 0)



Down at least 2 min (Not Responding - 2)



Down at least 5 min (Not Responding - 5)



Down at least 20 min (Not Responding - 20)



Maintenance (Maintenance - 0)



Up (Responding - 0)



Up at least 5 min (Responding - 5)

Logs

In This Chapter

| | |
|--|-----|
| Working with logs | 676 |
| Using WhatsUp Gold System Logs..... | 686 |
| Using WhatsUp Gold Group / Device Logs | 704 |

Working with logs

In This Chapter

| | |
|---|-----|
| Learning about Logs | 676 |
| Selecting a device to view logs | 677 |
| Changing the report or log date range | 678 |
| Changing the date range..... | 678 |
| Using paging options..... | 679 |
| Navigating between logs | 680 |
| Printing reports and logs | 680 |
| Using the WhatsUp Gold toolbar buttons..... | 680 |
| Using Manage Web Server | 681 |
| Managing Action Policies | 682 |
| Viewing payload details | 683 |
| Changing preferences | 683 |

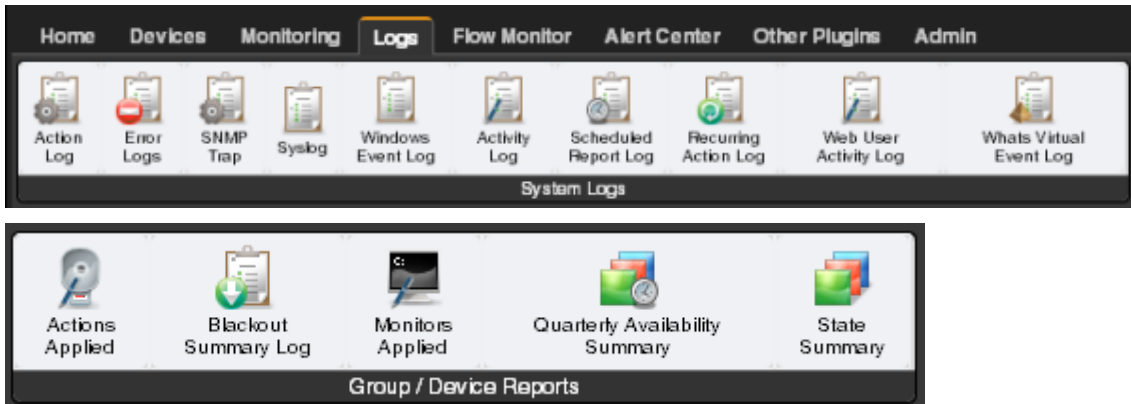
Learning about Logs

The WhatsUp Gold Logs tab provides device information to help you monitor and troubleshoot device performance and historical data that WhatsUp Gold and WhatsUp Gold plug-in products collect. The logs provide a view of: activity that has occurred on devices and device groups, actions and monitors applied, and summary reports so you have a view of network performance. This information provides insight into network issues and trends so you can tune and troubleshoot WhatsUp Gold server and network performance.

Most of the data in the logs can be exported to a formatted text file, Microsoft Excel, or a PDF. You can also email reports as a PDF, or send on scheduled intervals.

The Logs tab includes the following groups:

- **System Logs.** Display system-wide information and information about the WhatsUp Gold server. System log reports usually do not focus on a specific device nor a specific device group. For example, the Action Log displays all actions for all network devices.
- **Group/Device Reports.** Group reports display information relating to a specific device group. For example, the Quarterly Availability and the State Summary reports are group reports. Device reports display information relating to a specific device. For example, the Monitors Applied report for a single device is a device report.



Selecting a device to view logs

Many of the logs in the Logs tab are general logs that do not require a specific device selection to view the log. However, some of the logs require that you select a device to view the log. Following are common methods to select a device.

To select a device from the Device tab:

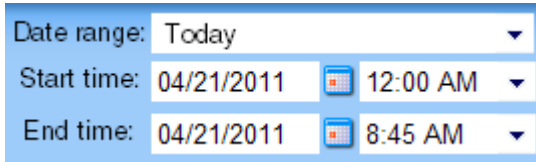
- 1 Select a device from the **Devices** tab by double-clicking a device in the Details View or Map View. The Device Status appears.
- 2 Click the **Logs** tab, then select the log you want to view for that device. The log data for the device currently in context displays.

To select a device from the Logs tab:

- 1 Click the **Logs** tab, then click the log you want to view for the selected device.
- 2 Click **View All Entries/Select a Device**. The Select a Device dialog box appears.
- 3 Select the device for which you want to view a log.
- 4 Click **OK**. The log data for the selected device displays.

Changing the report or log date range

Use the *date/time picker* (on page 602) at the top of a report or log to select a date range and time frame.

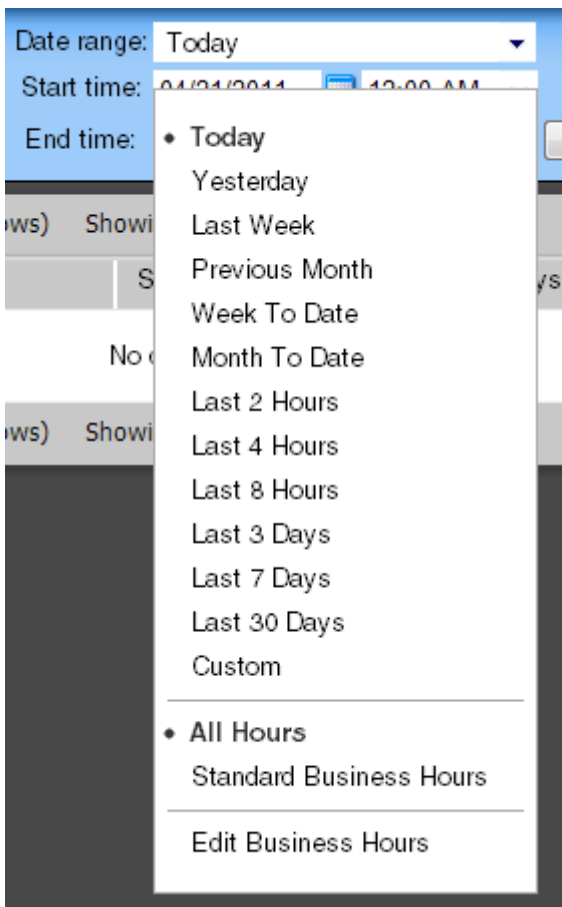


The screenshot shows a date/time picker interface with three rows. The first row is labeled 'Date range:' and has a dropdown menu currently showing 'Today'. The second row is labeled 'Start time:' and has two fields: a date field showing '04/21/2011' and a time field showing '12:00 AM'. The third row is labeled 'End time:' and has two fields: a date field showing '04/21/2011' and a time field showing '8:45 AM'. Each date and time field has a small calendar icon to its left.

In the **Date range** list, many group reports also allow you to specify and customize the business hour report times for reports to display. Selecting this option allows you to view the network activity only for specified business hours.



Note: The Business Hours setting is available for group reports only.



The screenshot shows the 'Date range:' dropdown menu open. The menu lists several options: 'Today' (selected with a bullet point), 'Yesterday', 'Last Week', 'Previous Month', 'Week To Date', 'Month To Date', 'Last 2 Hours', 'Last 4 Hours', 'Last 8 Hours', 'Last 3 Days', 'Last 7 Days', 'Last 30 Days', 'Custom', 'All Hours' (selected with a bullet point), 'Standard Business Hours', and 'Edit Business Hours'. The menu is divided into sections by horizontal lines.

Changing the date range

Use the time and date menus in the control bar to select the time period you want to view the data for. You can select a pre-configured time period from the **Date Range** list, or select

Custom and enter the start and end time manually. If no data exists for that time period, the following message displays: **No data available for the selected date range.**

To change the date range for a report or log:

- Click the calendar icon next to the date field to select the specific date from the calendar.
- Click the left and right arrows on the calendar to browse through the months.
- In the Date range list, click **Today** to navigate back to the current date. When you click a date, the calendar closes and the field is populated with the selected date.



Note: The date and time format on this report or log matches the format specified in the WhatsUp Gold console (**Configure > Program Options > Regional**).

You can also use the report *zoom tool* (on page 603) to select a date and time for monitor reports.

To control the date/time picker display:





- Hide the control bar by clicking the **Hide** link in the control bar. The selected date/time range displays instead and allows more rows of the report or log to display.
- To redisplay the date/time picker, click anywhere in the control bar summary.

Using paging options

At both the bottom and the top of the monitor report or log table are paging controls that allow you to move through large amounts of data.

Use the **Page** list to select the specific page to view. Next, use the **Showing ___ rows per page** list to specify the number of rows to display in the report. You can choose to display 25, 50, 100, 250, or 500 rows. The default maximum is 50 rows.

The paging buttons allow you to move from page to page, or go to the first or last page:

| Click: | To view: |
|---|---|
|  | <ul style="list-style-type: none"> ▪ The first page of values |
|  | <ul style="list-style-type: none"> ▪ The previous page of values |
|  | <ul style="list-style-type: none"> ▪ The next page of values |
|  | <ul style="list-style-type: none"> ▪ The last page of values |








Navigating between logs

Change the log you are viewing by selecting a different log from the **Logs** tab.

Printing reports and logs

- 1 Open the report you want to export.
- 2 Right-click anywhere inside the report window, then select **Print**.
- or -
Click **File** > **Print** from the browser menu options.

Using the WhatsUp Gold toolbar buttons

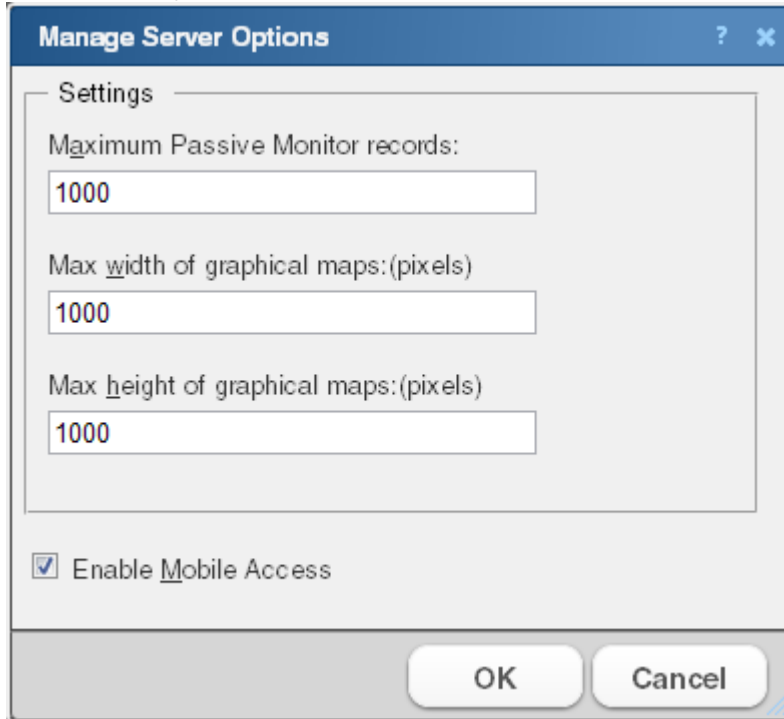
| Click: | To: |
|---|--|
|  Email | <ul style="list-style-type: none"> Email a report or log as a PDF attachment. Schedule the report or log to be emailed at regular intervals. |
|  Add Content | <ul style="list-style-type: none"> Add additional dashboard reports to the current dashboard view using the Add Content panel. |
|  Edit View | <ul style="list-style-type: none"> Edit settings for the currently displayed dashboard view. |
|  Properties | <ul style="list-style-type: none"> View group or device properties. |
|  Status | <ul style="list-style-type: none"> Display the Device Status of the device currently in context. This icon does not appear when a group is in the current context. |
|  Export | <ul style="list-style-type: none"> Export a report or log: <ul style="list-style-type: none"> To a text file To an Excel file To a PDF file |
|  Help | <ul style="list-style-type: none"> View help for the current page. |



Note: Different sets of icons appear on different types of pages.

Using Manage Web Server

- 1 Click the **Admin** tab.
- 2 Click **Manage Server Options** in the System Administration group. The Manage Server Options dialog appears.



- 3 Make changes to the fields as necessary. Available options include:
 - **Maximum Passive Monitor records.** Enter the maximum number of device and system level passive monitor records to collect for full reports. The default value is 1000 max records for WhatsUp Gold v14.2 and later.



Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance.

- **Max width of graphical maps.** Enter the maximum width of maps viewed through the web browser. The size is in pixels and the default is 1000.
 - **Max height of graphical maps.** Enter the maximum height of maps viewed through the web browser. The size is in pixels and the default is 1000.
 - **Enable Mobile Access.** Select this option to enable WhatsUp Gold Mobile access, which allows you to connect to WhatsUp Gold from a mobile device.
- 4 Click **OK** to save the changes.

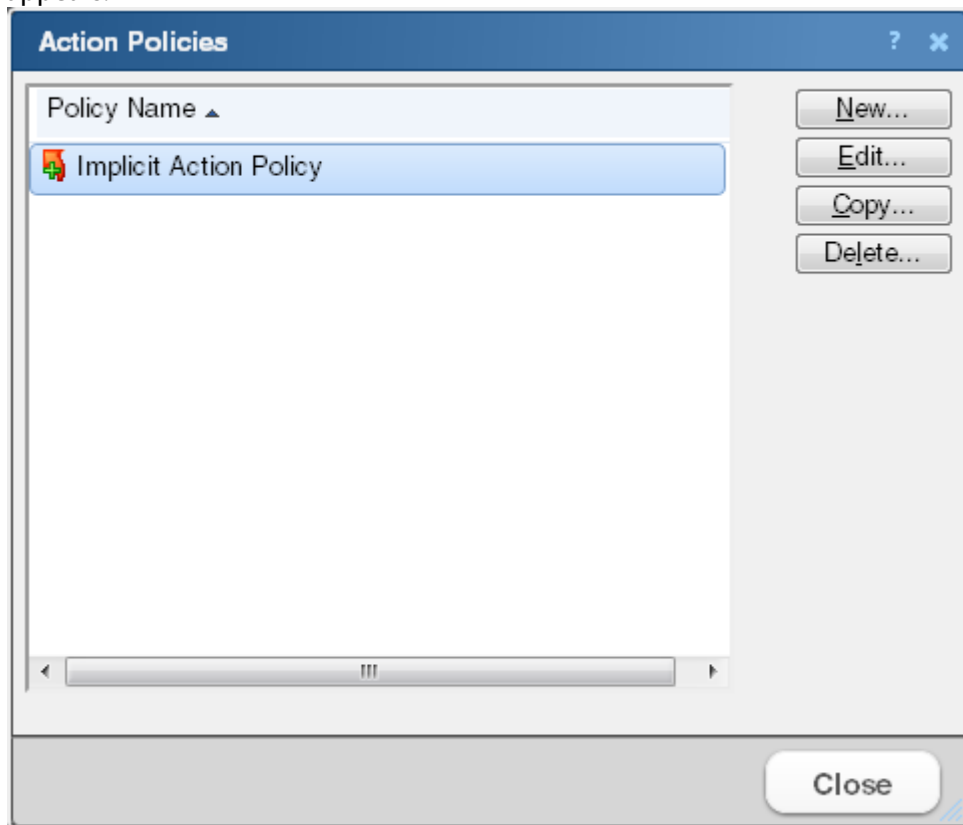
Managing Action Policies

The Action Policy dialog shows the action policies that you can assign to any device or monitor. Use this dialog to create a new action policy, modify or copy an existing policy, or delete a policy.

For more information, see *Using Action Policies* (on page 299).

To create an action policy:

- 1 Click the **Admin tab**, then click **Action Policy Library**. The Action Policies dialog appears.



- 2 Click **New** and enter a name for the new policy in the **Policy name** box. Give the policy a descriptive name that helps you remember its function.
- 3 Click **Add**. The Action Builder wizard appears.
- 4 Follow the directions in the wizard.
- 5 Click **Finish** at the end of the wizard to add the action to the policy.
- 6 Add as many actions as you need to complete the policy. You can move actions up and down in the list by clicking **Up** and **Down** above the action list.



Note: If you select **Only execute first action**, WhatsUp Gold executes the actions in the list for each state, starting at the top, and stops as soon as an action successfully fires.

- 7 After you have added all of the actions you want to use for the policy, click **OK** to create the policy and add it to the active list.

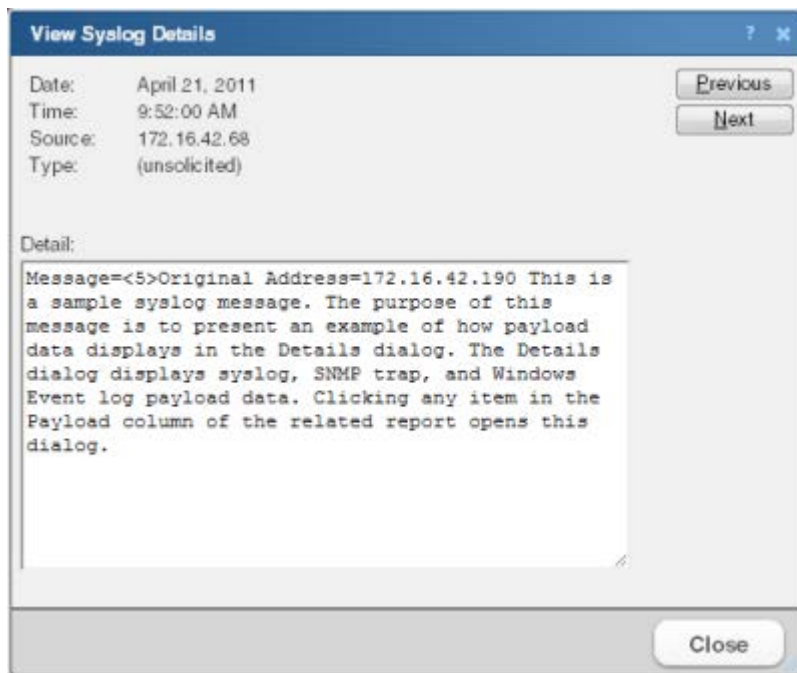


Note: During Device Discovery, you can assign an existing action policy (if one has been created previously), create a simple action policy through a wizard, or access the Action Policy Editor to create an action policy yourself.

Viewing payload details

Click any link in the Payload column of a log to access payload details.

Use this dialog to view the full payload of the entries in the SNMP Trap Log, Syslog, or WinEvent Log.



The following information is displayed for the currently viewed payload:

- **Date.** The date the payload reached WhatsUp Gold.
- **Time.** The time the event occurred or the message was received.
- **Source.** The device or monitor that sent the message.
- **Type.** The type of payload.
- **Detail.** The complete details of the message payload.

Use the **Previous** and **Next** buttons to browse through the log payloads in the same column. Click **Close** to exit the dialog and return to viewing the log.

Changing preferences

Access the Preferences dialog by clicking **Admin > Preferences**, or through your user account link in the upper right corner of any page. Use this dialog to change various Web user options. Changes made in this dialog only change settings for the current user Web account.

General

- **Language.** Select a language for the application.
- **Change your password.** Click this option to change your account password.
- **Show Getting Started Pane.** Select this option to display the Getting Started pane. The Getting Started pane includes links to resources to help you resolve issues and learn more about WhatsUp Gold.



Note: If you have an evaluator license, this field displays as **Show Evaluator Pane**. This option is not selectable with an evaluator license.

Refresh intervals

- **Dashboard report.** Enter a time (in seconds) for how often *dashboard reports* (on page 340) should refresh.
- **Full report.** Enter a time (in seconds) for how often *monitor reports* (on page 619) should refresh.
- **Devices list.** Enter a time (in seconds) for how often the content Devices tab should refresh.

Reports

- **Default records per page for long reports.** Enter a number to control the maximum number of rows reports and logs display. If a report contains a number of rows greater than the maximum number specified, you can use either the page controls to view the data. The default max records setting is 50.
- **Collapse legends on split second graph dashboard reports.** Select this option to hide the legends on split second graph dashboard reports until the mouse pointer moves over a graph. When multiple split second graph dashboard reports display in a dashboard view, selecting this option can help reduce the percentage of the screen area used by reports. This option affects split second graph dashboard reports only; legends are always displayed in popups.

Web Alarms

- **Enable web alarms.** Select this option to enable *Web alarms* (on page 117).



Note: Web alarms are enabled by default.

- **Check every.** If you enable Web alarms, enter a time (in seconds) for how often WhatsUp Gold should check for Web alarms.

Instant Info (popups)

- **Show popups on device list.** Select this option to enable popups on the device list. If this option is cleared, popups are not displayed when you hover device or group names in the device list.
- **Show popups on dashboard reports.** Select this option to enable popups on dashboard reports. If this option is cleared, popups are not displayed on dashboard reports.
- **Show popups on full reports.** Select this option to enable popups on monitor reports. If this option is cleared, popups are not displayed on monitor reports.



Note: By default, popups are enabled on both dashboard and reports.



Note: Popups are not available in WhatsUp Gold Standard Edition.

Using WhatsUp Gold System Logs

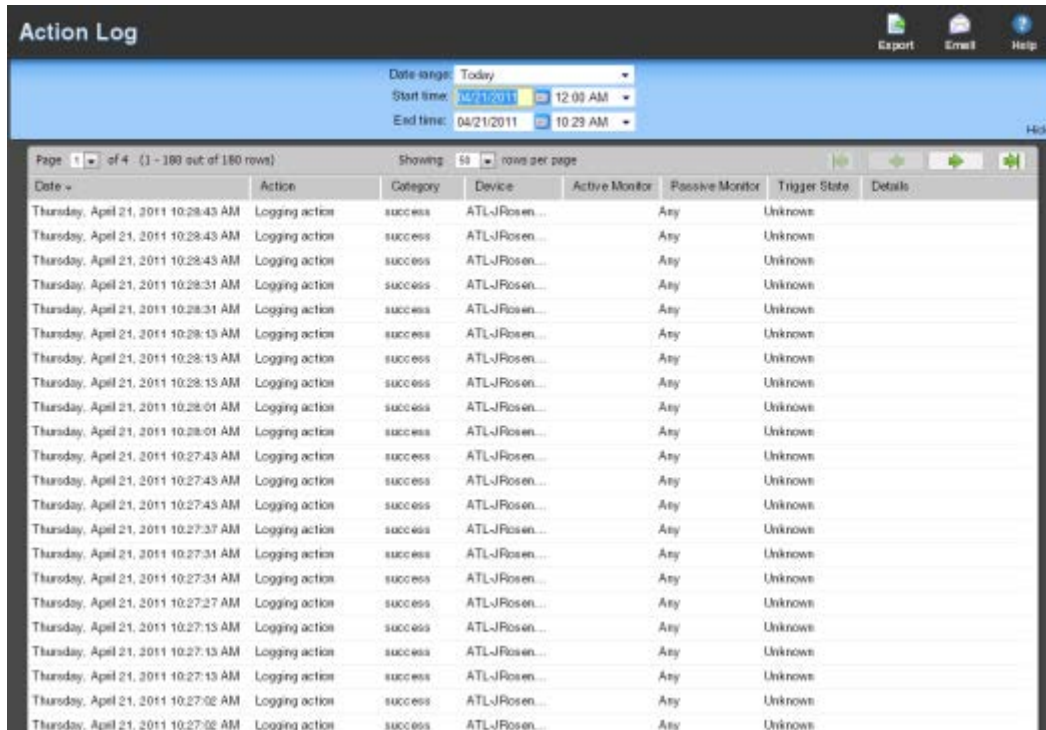
In This Chapter

| | |
|------------------------------|-----|
| Action Log | 687 |
| Error Logs | 688 |
| SNMP Trap Log | 692 |
| Syslog | 693 |
| Windows Event Log | 696 |
| Activity Log | 698 |
| Scheduled Report Log | 699 |
| Recurring Action Log | 700 |
| Web User Activity Log | 701 |
| WhatsVirtual Event Log | 702 |

The *system logs* display passively collected information on the WhatsUp Gold server or on selected devices. Logs contain information and display the data in the order in which it was received. You can sort log information by clicking the headings of the different log columns.

Action Log

The Action Log shows all actions that WhatsUp Gold has attempted to fire, based on the configuration of the action.



| Date | Action | Category | Device | Active Monitor | Passive Monitor | Trigger State | Details |
|--------------------------------------|----------------|----------|---------------|----------------|-----------------|---------------|---------|
| Thursday, April 21, 2011 10:28:43 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:43 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:43 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:31 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:31 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:13 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:13 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:13 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:01 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:28:01 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:43 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:43 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:43 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:37 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:31 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:31 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:27 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:15 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:13 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:13 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:02 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |
| Thursday, April 21, 2011 10:27:02 AM | Logging action | success | ATL-JRosen... | | Any | Unknown | |

Log body

The following information is displayed in the log:

- **Date.** The date the action was fired.
- **Action.** The specific action type that was fired. This corresponds to the name of the action in the Actions Library.
- **Category.** Shows the category that the action fits in here in the log. Either success, failure, cancel, retry, or blacked out.
- **Device.** The device that the action is assigned to.
- **Active Monitor.** The Active Monitor that the action is assigned to.
- **Passive Monitor.** The Passive Monitor that the action is assigned to.
- **Trigger State.** The state that caused the action to fire. The trigger state is determined when the Action is configured on the device.
- **Details.** Text that shows the reason for the category that is used in the log.



Note: A *skipped due to priority* message displays in the Action Log when an action is NOT executed because the **Only execute first action (for each state)** option is enabled in the Action Policy. For more information, see *Add/Edit Action Policy* (on page 682).

Error Logs

In This Chapter

| | |
|-------------------------------------|-----|
| General Error Log..... | 688 |
| Passive Monitor Error Log..... | 690 |
| Performance Monitor Error Log | 691 |

General Error Log

This log shows a list of error messages generated by WhatsUp Gold for the selected time period.

| Date | Category | Source | Details |
|---------------------------------------|----------|-----------------------|--|
| Thursday, April 21, 2011 07:31:16 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Thursday, April 21, 2011 07:27:02 AM | Failure | NmEngine | There is no registered license for W... |
| Wednesday, April 20, 2011 02:08:18... | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Wednesday, April 20, 2011 01:02:31... | Error | Whats/VirtualServi... | Error initializing VCenter server mon... |
| Wednesday, April 20, 2011 08:04:23... | Error | Whats/VirtualServi... | Error initializing VCenter server mon... |
| Wednesday, April 20, 2011 07:12:31... | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Wednesday, April 20, 2011 07:06:12... | Failure | NmEngine | There is no registered license for W... |
| Tuesday, April 19, 2011 03:04:22 PM | Error | Whats/VirtualServi... | Error initializing VCenter server mon... |
| Tuesday, April 19, 2011 07:05:04 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Tuesday, April 19, 2011 07:02:40 AM | Failure | NmEngine | There is no registered license for W... |
| Monday, April 18, 2011 09:54:54 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Monday, April 18, 2011 09:54:15 AM | Failure | NmEngine | There is no registered license for W... |
| Monday, April 18, 2011 09:43:46 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Monday, April 18, 2011 07:12:37 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Monday, April 18, 2011 07:11:45 AM | Failure | NmEngine | There is no registered license for W... |
| Monday, April 18, 2011 07:00:02 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Friday, April 15, 2011 11:39:54 AM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Friday, April 15, 2011 07:12:39 AM | Failure | NmEngine | There is no registered license for W... |
| Thursday, April 14, 2011 03:36:13 PM | Error | Whats/VirtualServi... | NmService notifications connect fail... |
| Thursday, April 14, 2011 03:33:03 PM | Failure | NmEngine | There is no registered license for W... |

Log body

The following information is displayed in the log:

- **Date.** The date the error occurred.
- **Category.** The category of error.
- **Source.** Where the error originated.
- **Details.** The details of the error.

The following is a list of the types of errors that are logged:

- All errors due to SQL statement failure
- Recurring Report load error
- Engine startup errors (Device load error, Group load error)
- Statistics update error
- State update error
- Roll-up activity and failure
- Device or Monitor deletion error
- Exception thrown (check service, process internal event)
- Passive Monitor startup errors

Passive Monitor Error Log

This log shows all Passive Monitor errors that occur during the operation of WhatsUp Gold. The table below the date/time picker shows all passive monitor errors that occurred during the selected time period.

Error Logs

General **Passive Monitor** Performance Monitor

Date range: Month To Date

Start time: 04/01/2011 12:00 AM

End time: 04/26/2011 7:47 AM

Page 1 of 1 (1 - 24 out of 24 rows) Showing 25 rows per page

| Date | Passive ... | Device | Category | Details |
|-------------------------------------|-------------|------------|------------|-------------------------------------|
| Tuesday, April 26, 2011 07:16:0... | Any | CHEETAH | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:16:0... | Any | 192.168... | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:15:5... | Any | ATL-CIS... | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:15:5... | Any | qa_win7... | connection | Cannot connect passive monito... |
| Tuesday, April 26, 2011 07:15:5... | Any | QA1-64BIT | connection | Cannot connect passive monito... |
| Tuesday, April 26, 2011 07:15:4... | Any | QA-2901... | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:10:4... | Any | CHEETAH | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:10:4... | Any | ATL-JRo... | cancel | Unregister for events on [172.16... |
| Tuesday, April 26, 2011 07:10:3... | Any | 192.168... | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:10:3... | Any | ATL-CIS... | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:10:2... | Any | QA1-64BIT | connection | Cannot connect passive monito... |
| Tuesday, April 26, 2011 07:10:2... | Any | qa_win7... | connection | Cannot connect passive monito... |
| Tuesday, April 26, 2011 07:10:1... | Any | QA-2901... | connection | The RPC server is unavailable. |
| Tuesday, April 26, 2011 07:04:2... | Any | ATL-JRo... | cancel | Unregister for events on [172.16... |
| Thursday, April 21, 2011 02:34:4... | Any | ATL-CIS... | connection | The RPC server is unavailable. |
| Thursday, April 21, 2011 02:33:4... | Any | CHEETAH | connection | The RPC server is unavailable. |
| Thursday, April 21, 2011 02:31:5... | Any | 192.168... | connection | The RPC server is unavailable. |
| Thursday, April 21, 2011 02:30:5... | Any | ATL-CIS... | connection | The RPC server is unavailable. |
| Thursday, April 21, 2011 02:26:3... | Any | QA1-64BIT | connection | Cannot connect passive monito... |
| Thursday, April 21, 2011 02:26:3... | Any | QA1-64BIT | connection | Cannot connect passive monito... |
| Thursday, April 21, 2011 02:18:0... | Any | qa_win7... | connection | Cannot connect passive monito... |
| Thursday, April 21, 2011 02:09:3... | Any | QA-2901... | connection | The RPC server is unavailable. |
| Thursday, April 21, 2011 10:07:0... | Any | ATL-JRo... | cancel | Unregister for events on [172.16... |
| Thursday, April 21, 2011 09:38:2... | Any | ATL-JRo... | cancel | Unregister for events on [172.16... |

Page 1 of 1 (1 - 24 out of 24 rows) Showing 25 rows per page

Log Body

The following information is displayed in the log:

- **Date.** The date of the error.
- **Passive Monitor.** The name of the passive monitor that received the error.
- **Device.** The host name of the device that the Passive Monitor is assigned to.
- **Category.** The category code of the error: Con. Established (Connection Established), Con. Failed (Connection Failed), or Auth Error (Authorization Error).

- **Details.** Text that describes the error.

Performance Monitor Error Log

This log shows all Performance Monitor errors that occur during the operation of WhatsUp Gold.

| Date | Device | Category | Source | Details |
|---------------------------------------|-------------------|----------|-----------------|---|
| Thursday, April 21, 2011 11:01:52 AM | ATL-CHAMPS | Error | RDC Memory | Timeout |
| Thursday, April 21, 2011 11:01:52 AM | ATL-CHAMPS | Error | RDC CPU | Timeout |
| Thursday, April 21, 2011 09:53:09 AM | ATL-CHAMPS | Error | RDC Interface | Timeout |
| Thursday, April 21, 2011 09:41:49 AM | ATL-CHAMPS | Error | RDC Memory | Timeout |
| Thursday, April 21, 2011 09:41:49 AM | ATL-CHAMPS | Error | RDC CPU | Timeout |
| Thursday, April 21, 2011 07:31:46 AM | WINNOREE-CLAB | Error | RDC CPU | Timeout |
| Thursday, April 21, 2011 07:31:46 AM | WINNOREE-CLAB | Error | RDC Memory | Timeout |
| Thursday, April 21, 2011 07:31:46 AM | WINNOREE-CLAB | Error | RDC Interface | Timeout |
| Thursday, April 21, 2011 07:31:42 AM | GA-6480T | Error | RDC Smp (SN... | No Such object |
| Thursday, April 21, 2011 07:31:42 AM | GA-6480T | Error | RDC APC UPS ... | No Such object |
| Thursday, April 21, 2011 07:31:42 AM | GA-2001 powermate | Error | RDC Disk | The remote device does not support the h... |
| Thursday, April 21, 2011 07:31:42 AM | GA-2001 powermate | Error | RDC APC UPS ... | No Such object |
| Thursday, April 21, 2011 07:31:42 AM | GA-2001 powermate | Error | RDC Disk | The remote device does not support the h... |
| Thursday, April 21, 2011 07:31:42 AM | GA-2001 powermate | Error | RDC APC UPS ... | No Such object |
| Thursday, April 21, 2011 07:31:42 AM | GA-2750 | Error | RDC APC UPS ... | No Such object |
| Thursday, April 21, 2011 07:31:42 AM | GA-2750 | Error | RDC Disk | The remote device does not support the h... |
| Thursday, April 21, 2011 07:31:42 AM | GA-400000 | Error | RDC APC UPS ... | No Such object |
| Thursday, April 21, 2011 07:31:42 AM | GA-400000 | Error | RDC Disk | The remote device does not support the h... |
| Thursday, April 21, 2011 07:31:42 AM | GA-400000 | Error | RDC CPU | No Such object |
| Thursday, April 21, 2011 07:31:41 AM | GA-400000 | Error | RDC APC UPS ... | No Such object |
| Wednesday, April 20, 2011 02:09:05 PM | WINNOREE-CLAB | Error | RDC CPU | Timeout |
| Wednesday, April 20, 2011 02:09:05 PM | WINNOREE-CLAB | Error | RDC Memory | Timeout |
| Wednesday, April 20, 2011 02:09:05 PM | WINNOREE-CLAB | Error | RDC Interface | Timeout |
| Wednesday, April 20, 2011 02:09:01 PM | GA-2001 powermate | Error | RDC APC UPS ... | No Such object |
| Wednesday, April 20, 2011 02:09:01 PM | GA-2750 | Error | RDC APC UPS ... | No Such object |

Log body

The following information is displayed in the log:

- **Date.** The date of the error.
- **Device.** The host name of the device that the Performance Monitor is assigned to.
- **Category.** The category of the error.
- **Source.** Where the error came from (such as Ping, CPU, Memory, Disk, Interface, and Custom Performance Monitors).
- **Details.** Description of the error that was received.

SNMP Trap Log

The SNMP Trap Log provides a history of SNMP traps that have occurred for all devices in the selected group during a time period. If the SNMP Trap Listener is configured to listen for messages, any messages received are recorded in the SNMP Trap Log.

SNMP Trap Log Export Email Help

The SNMP trap listener is currently **OFF**. Date range: Month To Date
 Start time: 04/01/2011 12:00 AM
 End time: 04/26/2011 7:53 AM

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

| Date | Source | Trap | Payload |
|-------------------------------------|-----------|---------------|--|
| Tuesday, April 26, 2011 03:36:27 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:36:23 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:36:19 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:21:03 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:21:02 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:21:01 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:21:00 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:59 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:58 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:57 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:56 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:55 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:54 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:53 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:52 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:51 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:50 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:49 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:48 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:47 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:46 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:45 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:44 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:43 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |
| Tuesday, April 26, 2011 03:20:42 AM | 172.16... | (unsolicited) | TrapName=authenticationFailure TrapMajor=4 TrapMinor=... |

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

- To add an SNMP monitor for a specific device, select the device from the Devices list and select **Properties > Passive Monitors > SNMP Trap**.
- To accept SNMP messages from any device, access the console and select **Program Options > Passive Monitor Listeners > SNMP Trap**. Select **Configure** and choose **Accept unsolicited SNMP traps**.



Note: In order for entries to be added to this log, the SNMP Trap Listener must be enabled. For more information, see *Enabling the SNMP Trap Listener* (on page 873). Additionally, if the trap receiving port is not on the list of firewall exceptions, traps may not be receivable and as a result will not be added to the SNMP Trap Log. Please ensure that the trap receiving port is on the firewall exceptions list.



Tip: If you experience page load delays for device or system passive monitor logs (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records displaying for the selected time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report and log display performance. For more information, see *Managing server options* (on page 681).

This log includes the time the message was received as well as its source, the trap that triggered it, and its payload.

Log body

The following information is displayed in the log:

- **Date.** The date the trap occurred.
- **Source.** The device or program that originated the trap.
- **Trap.** The type of trap received.
- **Payload.** The vital data (such as trap name, the IP address from which the trap came, date of the trap, etc.) that passed within a packet or other transmission unit.



Tip: Move your mouse over the payload entry to view more of the payload information.



Note: The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to *view the payload details* (on page 683).



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the log. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Syslog

This log shows Syslog events recorded for selected devices on the network during the time period displayed at the top of the log. WhatsUp Gold can accept Syslog messages from specific devices or from all devices, depending on the selected options.

A Syslog event is used to examine Syslog messages forwarded from other devices for a specific record and/or specific text within a record. Usually Syslog messages are forwarded from the "Syslog" on a system that runs UNIX, but they can also come from non-UNIX devices as well. They might contain anything that you want permanently logged, such as a device failure, or an attempt to log in to the system.

Syslog Entries Export Email Help

The Syslog Listener is currently **ON** Date range: Month To Date
 Start time: 04/01/2011 12:00 AM
 End time: 04/26/2011 8:30 AM Hide

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

| Date | Source | Syslog Type | Payload |
|--------------------------------------|-----------|---------------|---|
| Thursday, April 21, 2011 02:21:32 PM | 172.16... | (unsolicited) | Message=<173>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:31 PM | 172.16... | (unsolicited) | Message=<103>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:30 PM | 172.16... | (unsolicited) | Message=<52>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:29 PM | 172.16... | (unsolicited) | Message=<43>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:28 PM | 172.16... | (unsolicited) | Message=<107>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:27 PM | 172.16... | (unsolicited) | Message=<11>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:26 PM | 172.16... | (unsolicited) | Message=<64>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:25 PM | 172.16... | (unsolicited) | Message=<176>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:24 PM | 172.16... | (unsolicited) | Message=<50>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:23 PM | 172.16... | (unsolicited) | Message=<131>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:22 PM | 172.16... | (unsolicited) | Message=<55>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:21 PM | 172.16... | (unsolicited) | Message=<3>Original Address=172.16.4... |
| Thursday, April 21, 2011 02:21:20 PM | 172.16... | (unsolicited) | Message=<21>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:19 PM | 172.16... | (unsolicited) | Message=<79>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:17 PM | 172.16... | (unsolicited) | Message=<90>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:16 PM | 172.16... | (unsolicited) | Message=<100>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:15 PM | 172.16... | (unsolicited) | Message=<32>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:14 PM | 172.16... | (unsolicited) | Message=<88>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:13 PM | 172.16... | (unsolicited) | Message=<14>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:12 PM | 172.16... | (unsolicited) | Message=<39>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:11 PM | 172.16... | (unsolicited) | Message=<145>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:10 PM | 172.16... | (unsolicited) | Message=<133>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:09 PM | 172.16... | (unsolicited) | Message=<171>Original Address=172.1... |
| Thursday, April 21, 2011 02:21:08 PM | 172.16... | (unsolicited) | Message=<44>Original Address=172.16... |
| Thursday, April 21, 2011 02:21:07 PM | 172.16... | (unsolicited) | Message=<57>Original Address=172.16... |

Page 1 of 40 (1 - 25 out of 1000 rows) Showing 25 rows per page

If the Syslog Listener is configured to listen for messages, any messages received are recorded in WhatsUp Gold Syslog.

- To add a Syslog monitor for a specific device, select the device from the Devices list and select **Properties > Passive Monitors > Syslog**.

- To accept Syslog messages from any device, access the console and select **Program Options > Passive Monitor Listeners > Syslog**. Select **Configure** and choose **Accept unsolicited passive monitors**.



Note: In order for this log to receive syslog messages, the Syslog Listener must be enabled. For more information, see *Enabling the Syslog Listener* (on page 875). Additionally, if the receiving port is not on the list of firewall exceptions, messages may not be receivable and as a result will not be added to Syslog. Please ensure that the syslog receiving port is on the firewall's list of exceptions.



Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance. For more information, see *Managing server options* (on page 681).

This report includes the time the message was received, the syslog type, and its payload.

Report body

The following information is displayed in the log:

- **Date.** The date the message was received.
- **Source.** The device where the message originated.
- **Syslog Type.** The type of syslog message received.
- **Payload.** The information contained in the syslog message.



Tip: Move your mouse over the entry to see more of the payload.



Note: The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to *view the payload details* (on page 683).



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Windows Event Log

This report shows Windows events logged for the selected device during the time period displayed at the bottom of the report.

| Date | Source | WinEvent Type | Payload |
|-------------------------------------|-----------------|---------------|-------------------------------|
| Tuesday, April 26, 2011 09:30:46 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:46 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:38 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:38 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:36 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:36 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:16 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:08 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:30:06 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:18 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:10 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:08 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:08 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:08 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:06 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:29:04 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:50 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:50 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:42 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:42 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:40 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:40 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |
| Tuesday, April 26, 2011 09:27:40 AM | ATL-Firewall... | Any | Computed from ATL-Firewall... |

- To add a Windows Event Log monitor for a specific device, select the device from the Devices list and select **Properties > Passive Monitors > Windows Event Log**.



Note: In order for entries to be added to this report, the Windows Event Log listener must be enabled and a Windows Event passive monitor must be added to the device. For more information on the Windows Event Log listener, see *Enabling the Windows Event Log Listener* (on page 874).



Tip: If you experience page load delays for device or system passive monitor reports (SNMP Trap, Syslog, and Windows Event Log), this may be caused by too many records to display for this report time range. Change the time range or reduce the Maximum Passive Monitor Records setting to display fewer records. Reducing the maximum number of passive monitor records will improve WhatsUp Gold report display performance.



Note: WhatsUp Gold v14.1 and prior used a default value of 10,000 max records; WhatsUp Gold v14.2 and later use a default value of 1,000 max records. For more information, see *Managing server options* (on page 681).

A Windows log event is a Windows Event Viewer entry monitored by WhatsUp Gold. This could be monitoring when a service is started or stopped, if there was a logon failure, or any other entry in the Windows Event Viewer.

Log report body

The following information is displayed in the log:

- **Date.** The time event was received by WhatsUp Gold.
- **WinEvent Type.** The type of message received.
- **Payload.** The vital data (such as the event name, the IP address that the event came from, date of the event, etc.) that is passed within a packet or other transmission unit. Move your mouse over the entry to see more of the payload. The data is limited to the first 100 bytes in the payload. To view the full payload, click the payload entry to *view the payload details* (on page 683).



Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Activity Log

This report is a history of system-wide configuration and application initialization messages generated by WhatsUp Gold for the time period selected at the top of the report. All messages found in this Log are also written to the Windows Event log.

| Date | Type | Source | Category | Message |
|--------------------------------------|-------------|-------------|-----------|--|
| Tuesday, April 26, 2011 09:29:56 AM | Information | PasSyslog | startup | Syslog server stopped. |
| Tuesday, April 26, 2011 09:29:56 AM | Information | PasSyslog | startup | Syslog server started on port 514. Unsolicited syslog mes... |
| Tuesday, April 26, 2011 07:15:41 AM | Information | PasSNMP | startup | SNMP server is disabled |
| Tuesday, April 26, 2011 07:15:41 AM | Information | PasSyslog | startup | Syslog server is disabled |
| Tuesday, April 26, 2011 07:15:41 AM | Information | PasWinEvent | startup | WinEvent server started. Generate payload is On |
| Tuesday, April 26, 2011 07:15:41 AM | Information | NmEngine | NmService | Engine started |
| Tuesday, April 26, 2011 07:15:35 AM | Information | NmEngine | NmService | Actions have been enabled. |
| Tuesday, April 26, 2011 07:10:40 AM | Information | PasWinEvent | startup | WinEvent server stopped |
| Tuesday, April 26, 2011 07:10:40 AM | Information | PasSNMP | startup | SNMP server stopped |
| Tuesday, April 26, 2011 07:10:40 AM | Information | NmEngine | NmService | Engine stopped |
| Tuesday, April 26, 2011 07:10:17 AM | Information | PasSyslog | startup | Syslog server stopped. |
| Tuesday, April 26, 2011 07:10:15 AM | Information | NmEngine | NmService | Engine started |
| Tuesday, April 26, 2011 07:10:12 AM | Information | PasSNMP | startup | SNMP server is disabled |
| Tuesday, April 26, 2011 07:10:12 AM | Information | PasSyslog | startup | Syslog server is disabled |
| Tuesday, April 26, 2011 07:10:12 AM | Information | PasWinEvent | startup | WinEvent server started. Generate payload is On |
| Tuesday, April 26, 2011 07:10:05 AM | Information | NmEngine | NmService | Actions have been enabled. |
| Tuesday, April 26, 2011 07:04:29 AM | Information | PasSyslog | startup | Syslog server stopped. |
| Tuesday, April 26, 2011 07:04:29 AM | Information | PasWinEvent | startup | WinEvent server stopped |
| Tuesday, April 26, 2011 07:04:29 AM | Information | PasSNMP | startup | SNMP server stopped |
| Tuesday, April 26, 2011 07:04:29 AM | Information | NmEngine | NmService | Engine stopped |
| Thursday, April 21, 2011 09:38:26 AM | Information | PasWinEvent | startup | WinEvent server stopped |
| Thursday, April 21, 2011 09:38:26 AM | Information | PasWinEvent | startup | WinEvent server started. Generate payload is On |
| Thursday, April 21, 2011 09:13:50 AM | Information | PasSNMP | startup | SNMP server stopped |
| Thursday, April 21, 2011 09:13:50 AM | Information | PasSNMP | startup | SNMP server started on port 162. Unsolicited traps are as... |
| Thursday, April 21, 2011 09:13:50 AM | Information | PasSyslog | startup | Syslog server stopped. |

Each entry shows the type of activity logged as well as the date, source, category and actual message of the activity.

- Click the link above the **Type** column to group the entries by message severity (Information, Warning, or Error).

Log Body

The following information is displayed in the log:

- Date.** The date the activity took place.
- Type.** The type of activity, for example *Information*.
- Source.** Where the activity originated, for example, *NmEngine*.
- Category.** The category of the activity, for example, *startup*.
- Message.** The activity message, for example, *Engine started*.



Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Scheduled Report Log

This log shows a log of all recurring and scheduled reports that have occurred during the selected time period.

Recurring / Scheduled Report Log

Date range: Month To Date
 Start time: 04/01/2011 12:00 AM
 End time: 04/26/2011 9:49 AM

Page 1 of 4 (1 - 25 out of 81 rows) Showing 25 rows per page

| Date | Recurring Report | Category | Details |
|-------------------------------------|------------------------|--------------|--|
| Tuesday, April 26, 2011 09:48:47 AM | Disk Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:48:37 AM |
| Tuesday, April 26, 2011 09:48:47 AM | Interface | Scheduled | Scheduled for execution at: 4/26/2011 9:50:18 AM |
| Tuesday, April 26, 2011 09:48:46 AM | Disk Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:48:37 AM |
| Tuesday, April 26, 2011 09:48:46 AM | Interface Discards ... | Scheduled | Scheduled for execution at: 4/27/2011 9:45:31 AM |
| Tuesday, April 26, 2011 09:48:46 AM | Interface Utilization | Scheduled | Scheduled for execution at: 4/26/2011 9:50:32 AM |
| Tuesday, April 26, 2011 09:48:46 AM | CPU Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:46:50 AM |
| Tuesday, April 26, 2011 09:48:46 AM | Memory Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:45:37 AM |
| Tuesday, April 26, 2011 09:48:46 AM | Disk Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:45:18 AM |
| Tuesday, April 26, 2011 09:48:46 AM | Disk Utilization | Complete | Finished. |
| Tuesday, April 26, 2011 09:48:45 AM | Disk Utilization | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:45 AM | CPU Utilization | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:45 AM | Disk Utilization | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:45 AM | Interface Utilization | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:45 AM | Interface | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:45 AM | Memory Utilization | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:45 AM | Interface Discards ... | Initializing | Initializing... |
| Tuesday, April 26, 2011 09:48:43 AM | Disk Utilization | Running | PDF generated successfully. |
| Tuesday, April 26, 2011 09:48:43 AM | Disk Utilization | Running | Sending email to joesm@ipswitch.com |
| Tuesday, April 26, 2011 09:48:37 AM | Disk Utilization | Running | Generating PDF for the URL: http://172.16.42.36/NimCons... |
| Tuesday, April 26, 2011 09:48:11 AM | Interface Discards ... | Scheduled | Scheduled for execution at: 4/27/2011 9:45:31 AM |
| Tuesday, April 26, 2011 09:48:11 AM | CPU Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:46:50 AM |
| Tuesday, April 26, 2011 09:48:11 AM | Disk Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:45:18 AM |
| Tuesday, April 26, 2011 09:48:11 AM | Disk Utilization | Scheduled | Scheduled for execution at: 4/26/2011 9:48:37 AM |
| Tuesday, April 26, 2011 09:48:11 AM | Interface Utilization | Scheduled | Scheduled for execution at: 4/26/2011 9:50:32 AM |
| Tuesday, April 26, 2011 09:48:11 AM | Memory Utilization | Scheduled | Scheduled for execution at: 4/27/2011 9:45:37 AM |

Page 1 of 4 (1 - 25 out of 81 rows) Showing 25 rows per page

Log body

The following information is displayed in the log:

- **Date.** The date that the report was run.
- **Recurring Report.** The name of the recurring report as it appears on the Recurring Report dialog.
- **Category.** The result of the report attempt: Success, Failure, Disabled.
- **Details.** Describes the results of the report.



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Recurring Action Log

This log shows a log of recurring actions that were scheduled to fire.

| Date | Recurring Action | Category | Details |
|-------------------------------------|------------------------|----------|---------------------------------|
| Tuesday, April 26, 2011 01:06:08 PM | Monitors for the we... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:07 PM | Recurring alerts | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:07 PM | Scheduled action | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:07 PM | General check | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:07 PM | Check | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:07 PM | Check monitors | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:07 PM | Check these mont... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:13 PM | Monitors for the we... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:13 PM | General check | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:13 PM | Check these mont... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:13 PM | Scheduled action | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:13 PM | Check monitors | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:06:13 PM | Recurring alerts | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:43 PM | Check these mont... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:43 PM | Scheduled action | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:40 PM | General check | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:40 PM | Recurring alerts | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:40 PM | Check monitors | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:40 PM | Monitors for the we... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:20 PM | Recurring alerts | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:17 PM | Scheduled action | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:17 PM | Monitors for the we... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:17 PM | Check these mont... | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:17 PM | General check | success | SMTP message sent successfully. |
| Tuesday, April 26, 2011 01:05:17 PM | Check monitors | success | SMTP message sent successfully. |

Log body

The following information is displayed in the log:

- **Date.** The date and time the attempt to fire the action occurred.
- **Recurring Action.** The name of the recurring action that was scheduled to fire.
- **Category.** The result of the attempt to fire the action (success, failure, information, or cancel).

- **Details.** This column displays information about the specific action that was scheduled to fire. If the category is information, details show that the scheduled action occurred during a blackout period. If the category is cancel, details show that the action was stopped while it was in the process of being fired, either manually by the user, or by the shutdown of the Ipswitch WhatsUp Engine service.



Note: If this report's data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Web User Activity Log

This log records when a user logs on or off the web interface, and the actions taken while logged on.

| Date range: Custom | | Export | Email | Help |
|--|---------------------|----------|---|------|
| Start time: | 03/27/2011 12:00 AM | | | |
| End time: | 04/26/2011 1:30 PM | | | |
| Page 1 of 13 (1 - 25 out of 309 rows) Showing 25 rows per page | | | | |
| Date | Category | Web User | Details | |
| Tuesday, April 26, 2011 11:25:26 AM | Recurring Action | admin | Created recurring action 'A third recurring action' | |
| Tuesday, April 26, 2011 11:25:14 AM | Recurring Action | admin | Created recurring action 'Recurring action 2' | |
| Tuesday, April 26, 2011 11:22:53 AM | Recurring Action | admin | Modified recurring action 'Recurring Action 1' | |
| Tuesday, April 26, 2011 11:21:20 AM | Recurring Action | admin | Created recurring action 'Recurring Action 1' | |
| Tuesday, April 26, 2011 10:47:17 AM | Device Properties | admin | Modified critical polling order on 'QA1-64BIT' | |
| Tuesday, April 26, 2011 10:47:17 AM | Device Properties | admin | Added the 'Interface' active monitor on 'QA1-64BIT' | |
| Tuesday, April 26, 2011 10:47:17 AM | Device Properties | admin | Modified critical polling order on 'QA1-64BIT' | |
| Tuesday, April 26, 2011 10:47:17 AM | Device Properties | admin | Added the 'Temperature' active monitor on 'QA1-64BIT' | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'atl-sayonbi.i... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'bmj_wug_cur... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'qa-sql2.ipswi... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'atl-adyb2.ips... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'atl-dshoskins.i... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'ATL-SE1.ips... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'JJ-TEST2' | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on '172.16.42.9' | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'gateem2k3-6... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'tgasq2k8r2... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'atl-dshambha... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'ATL-JHENUJ... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'win-islzhtsq... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on '172.16.42.7' | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'ATL-CISCO4... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on '3qs2k8sp2v... | |
| Tuesday, April 26, 2011 10:23:41 AM | Bulk Field Change | admin | Action Policy bulk field changes on 'ATL-JRosen... | |
| Page 1 of 13 (1 - 25 out of 309 rows) Showing 25 rows per page | | | | |

Log body

The following information is displayed in the log:

- **Date.** The date the activity took place.

- **Category.** The category of activity, for example, *login*.
- **Web user.** The web user account.
- **Details.** The details of the activity, for example, *Logged in*.



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

WhatsVirtual Event Log

The WhatsVirtual Events log provides a record of the events generated by virtual devices managed by a vCenter server.

| Date | Target | User | Message |
|------------------------------|--|---------------|--|
| Fri Apr 22 14:23:14 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - QA... | IPSWITCH_M... | Migration of QA_Win7_64 from atl-esxi1.ipswitch... |
| Tue Apr 19 13:29:23 EDT 2011 | Atlanta - atl-esxi2.ipswitch_m.ipswitch.com - bmq... | | DRS migrated bmq_FreeBSD from atl-esxi1.ipswit... |
| Tue Apr 19 13:27:45 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - bmq... | | Migrating bmq_FreeBSD from atl-esxi1.ipswitch... |
| Mon Apr 18 10:49:41 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - QA... | | DRS migrated QA_Win2k3_R2_64 from atl-esxi2... |
| Mon Apr 18 10:48:32 EDT 2011 | Atlanta - atl-esxi2.ipswitch_m.ipswitch.com - QA... | | Migrating QA_Win2k3_R2_64 from atl-esxi2.ipswi... |
| Mon Apr 18 02:19:42 EDT 2011 | Atlanta - atl-esxi2.ipswitch_m.ipswitch.com - AT... | | DRS migrated ATL-ELM from atl-esxi1.ipswitch... |
| Mon Apr 18 02:18:31 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - AT... | | Migrating ATL-ELM from atl-esxi1.ipswitch_m.ips... |
| Mon Apr 18 01:19:37 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - bmq... | | DRS migrated bmq_FreeBSD from atl-esxi2.ipswit... |
| Mon Apr 18 01:18:31 EDT 2011 | Atlanta - atl-esxi2.ipswitch_m.ipswitch.com - bmq... | | Migrating bmq_FreeBSD from atl-esxi1.ipswitch... |
| Mon Apr 18 01:09:26 EDT 2011 | Atlanta - atl-esxi2.ipswitch_m.ipswitch.com - bmq... | | DRS migrated bmq_FreeBSD from atl-esxi1.ipswit... |
| Mon Apr 18 01:08:32 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - bmq... | | Migrating bmq_FreeBSD from atl-esxi1.ipswitch... |
| Sun Apr 17 15:55:38 EDT 2011 | Atlanta - atl-esxi1.ipswitch_m.ipswitch.com - AT... | | DRS migrated ATL-SE2 from atl-esxi2.ipswitch... |
| Sun Apr 17 15:53:30 EDT 2011 | Atlanta - atl-esxi2.ipswitch_m.ipswitch.com - AT... | | Migrating ATL-SE2 from atl-esxi2.ipswitch_m.ips... |



Note: To gather events for this report, you must have enabled WhatsVirtual event collection on the General tab of the WhatsUp Gold Program Options dialog.



Tip: The types of events gathered for this report can be configured on the Virtualization tab of the Device Properties dialog for the vCenter server.

Log Body

The following information is displayed in the log:

- **Date.** Displays the date and time that the event occurred.
- **Target.** Displays the target of the event. The target can be a virtual machine, a virtual host, a cluster, a datacenter, or a vCenter server.
- **User.** Displays the VMWare user associated with the event.



Note: Many events are the result of automatic actions within the VMware system. The user field will only display a VMware user when the event is the result of user action.

- **Message.** The message sent from the vCenter server to WhatsVirtual.



Note: If the log data exceeds the maximum number of records set for full reports, use the *Paging Options* (on page 603) to view more records for the report. The maximum number of records any full report displays is specified in the *Preferences* (on page 604) dialog.

Using WhatsUp Gold Group / Device Logs

In This Chapter

| | |
|--------------------------------------|-----|
| Actions Applied..... | 704 |
| Blackout Summary Log | 705 |
| Monitors Applied..... | 707 |
| Quarterly Availability Summary | 708 |
| State Summary..... | 710 |

The Group / Device logs provide information on the devices in your network.

Groups are user-defined logical collections of devices. Groups let you put devices of interest together, and group logs provide information on these logical groups. *Device logs* provide information on individual devices.

Actions Applied


This log shows actions that are applied to devices and monitors in the group currently in context (displayed in the log title bar). Each entry shows an action and the device, monitor and state that triggered it. To view a different group, click the group currently in context. Select a different group from the dialog.

| Device | State | Action Type | Action | Monitor |
|----------------------|-------|---------------|----------|-------------|
| GA1-44BIT | Down | E-mail Action | Email me | |
| GA1-44BIT | Up | E-mail Action | Email me | Interface |
| GA1-44BIT | Up | E-mail Action | Email me | Temperature |
| GA1-44BIT | Down | E-mail Action | Email me | |
| GA-CLUSTER | Down | E-mail Action | Email me | |
| GA-CLUSTERFC | Down | E-mail Action | Email me | |
| GAMAINCOMTR | Up | E-mail Action | Email me | |
| GA-MINRES | Up | E-mail Action | Email me | |
| ga-rightipswitch_... | Down | E-mail Action | Email me | |
| ga-rightipswitch_... | Down | E-mail Action | Email me | |
| GA-SOLCLUSTER | Down | E-mail Action | Email me | |

- **Device.** The IP address or name of the network device.
- **State.** The state of the action at the time of the last poll, relative to the time selected in the date/time picker.
- **Action Type.** The type of action applied to the device.
- **Action.** The action applied to the device.
- **Monitor.** The type of monitor.

This log displays a detailed list of actions that were not fired as a result of a scheduled blackout period. The information in the report can be filtered by date, device, action, triggering type, state, and blackout start and end time.

Below the date/time picker is a table detailing the action and its coinciding blackout period.

-  **Tip:** Click an **Action** to view the Action Log.

- **Trigger Type.** The type of trigger that initiated the action; either State Change, Passive Monitor, or All Types.
- **State.** The state of the device at the time of the action.



Tip: Click a **State** to view the State Change Timeline report.



Note: The State column displays N/A for Passive Monitor entries. No Passive Monitor entries appear in the State column unless you have configured the log to display All States.

- **Blackout Start.** The date and time the blackout period began.
- **Blackout End.** The date and time the blackout period ended.

Filtering the log

You can refine the log in several ways:

- **Select a Triggering Type.** Use the **Triggering Type** list at the top left of the page to select the triggering type for which to view log data. You can select either All Types, State Change, or Passive Monitor.
- **Select a device.** Use the **Device** list to select the specific device(s) for which to view log data. You can select a specific device, or view data for all devices in the group.

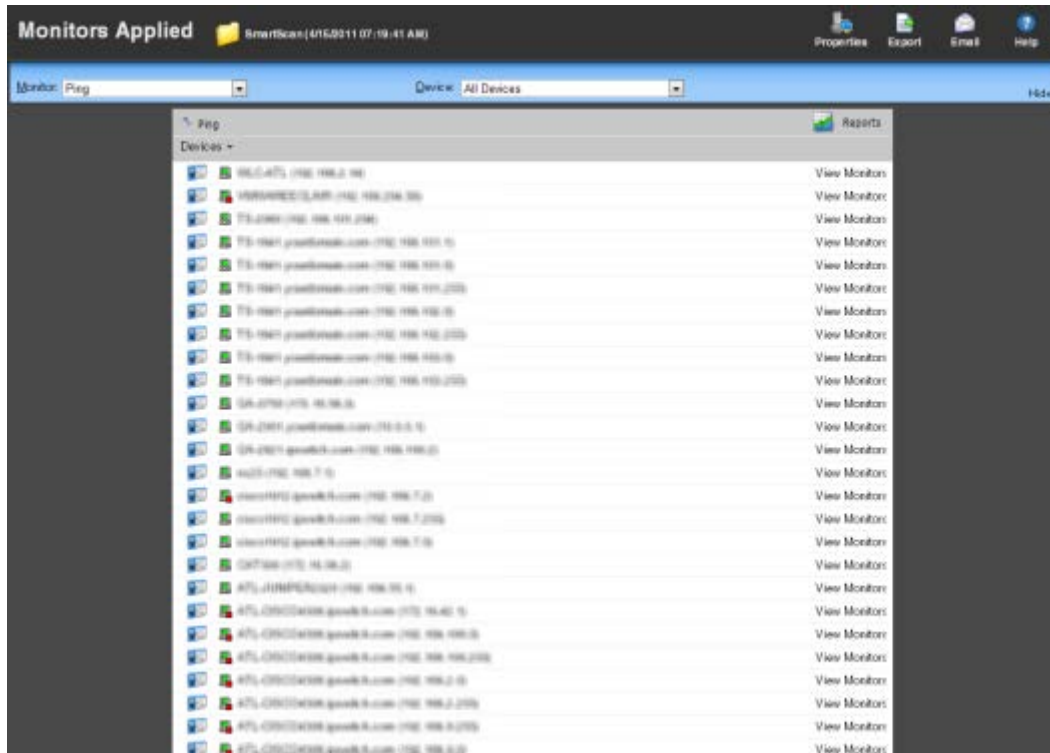


Tip: To change device groups, use the **Device Group** link at the top of the page to the right of the web interface tabs. The name of the device group for which you are currently viewing log data is displayed as the title for this link.

- **Select a different date range.** Use the **Date range** list at the top of the log to change the time frame for which log data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range.
- **Select a device state.** Use the **State** list to select the state(s) for which to view log data. You can select All States, or a specific device state.
- **Select an action.** Use the **Action** list to select the action(s) for which to view log data. You can select a specific action, or view data for all actions.

Monitors Applied

This log displays a list of all monitors applied to devices in the selected device group. The information displayed in the log depends on the device(s) and monitor you select.



Monitor. Use this list to select the specific monitor for which you would like to view data. You can select from the following types of monitors:

- Active
- Performance
- Passive



Note: The list of monitors is populated with monitors currently configured for the device(s) you have selected.

Device. Use this list to select the specific group device for which to view data.



Note: The list of devices is populated with the devices that reside in the group for which you have selected to view log data. To change the the device group, click the Device Group icon located to the right of the web interface tabs.

Log Body

A table displays below the Monitor and Device lists containing data specific to your log selections. For example, if you have selected to view all devices in the group for which a Ping monitor has been configured and assigned, you will see a list of devices on the left-hand side of the log, and a series of View Monitors links on the right-hand side of the log.



Tip: Click the **View Monitor** link for a device for which you would like to view all of the monitors that have been configured and assigned to that specific device.

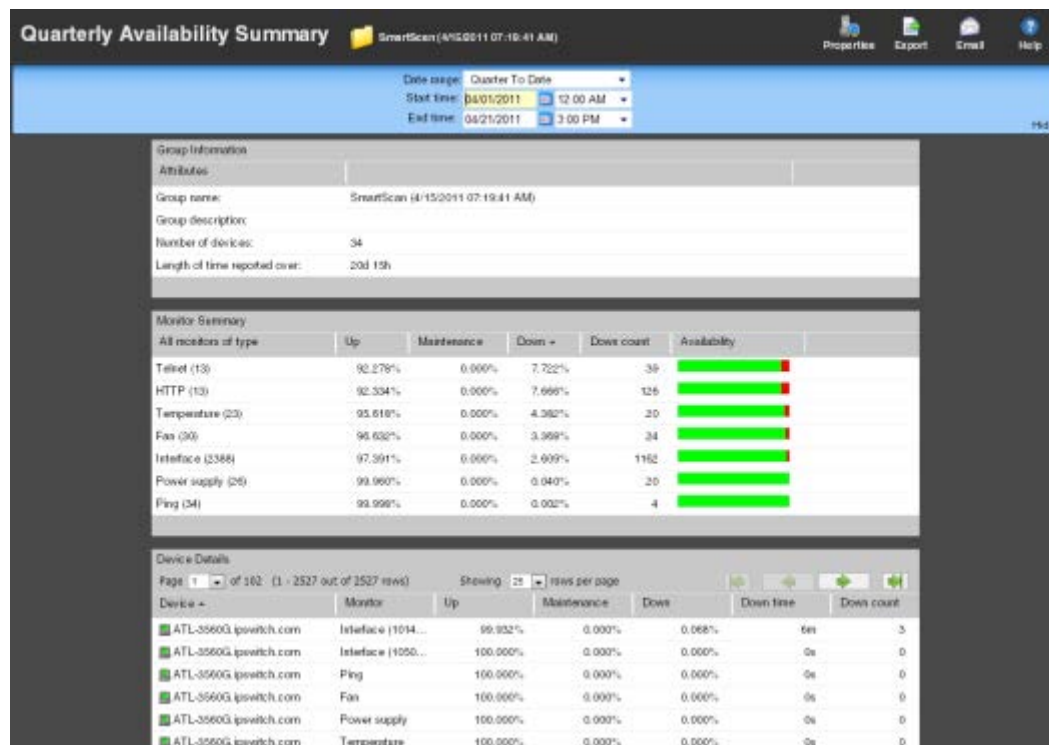


Tip: Click the **Device Properties** icon to the left of each device to view the properties for a specific device.



Quarterly Availability Summary

This Service Level Agreement report shows the state of all Active Monitors within a device group for the selected time period. The Quarterly Availability Summary is a combination of the WhatsUp Gold Active Monitor Outage and Active Monitor Availability monitors, located under the Monitors tab.



Report body

Group Information

- **Group name.** The device group for which the report displays activity data. You can change the group by clicking the group context at the top of the log to the right of the log title.
- **Group description.** A short description for the device group.
- **Number of devices.** The number of monitored devices in the selected group.
- **Length of time reported over.** The amount of time the information displayed represents.

Monitor Summary

- **All monitors of type.** The type of Active Monitor. The number in parenthesis next to the monitor name depicts the total number of that type of monitor in the device group.
- **Up.** The percentage of time the Active Monitor was up during the selected time period for all devices.
- **Maintenance.** The percentage of time the Active Monitor was in maintenance during the selected time period for all devices.
- **Down.** The percentage of time the Active Monitor was down during the selected time period for all devices.
- **Down count.** The number of times the Active Monitor was in the down state during the selected time period for all devices.
- **Availability.** The overall availability for the Active Monitor during the selected time period, by color. The colors in this section match the Device States colors (configured in **Program Options > Device States**).



Note: When hovering over any percentage data listed, a popup appears displaying the total number of seconds the monitor has been in the listed state.

Device Details

- **Device.** The group device's display name (or IP address if a display name isn't specified in its Device Properties) and device state icon.
- **Monitor.** The Active Monitor configured for this device.
- **Up.** The percentage of time the Active Monitor on this device was up during the selected time period.
- **Maintenance.** The percentage of time the Active Monitor on this device was in maintenance during the selected time period.
- **Down.** The percentage of time the Active Monitor on this device was down during the selected time period.
- **Down time.** Specifies how long the Active Monitor on this device was in the down state during the selected time period.

- **Down count.** Specifies the number of times the Active Monitor on these devices went down during the selected time period.



Note: When hovering over any percentage data listed, a popup appears displaying the total number of seconds the monitor has been in the listed state.

Rounded percentages

When calculating percentages of uptime for a monitor, WhatsUp Gold rounds values to the nearest thousandth of one percent (three decimal places). If this rounded value is greater than 99.999 percent, the uptime is displayed as 100% with an asterisk notation to indicate the displayed value is slightly larger than the actual value. The precise downtime value is always visible in the **Down time** column for the monitor.

State Summary

This log is a summary of device states in the current selected group.

| Group | Devices Up | Devices Down | Devices in Maintenance | Monitors Up | Monitors Down |
|-----------------------------------|------------|--------------|------------------------|-------------|---------------|
| SmartScan (4/15/2011 07:19:41 AM) | 19 | 0 | 0 | 2445 | 81 |
| 192.168.0.0/24 | 1 | 0 | 0 | 10 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 71 | 9 | 0 | 252 | 15 |
| 192.168.0.0/24 | 37 | 1 | 0 | 216 | 7 |
| 192.168.0.0/24 | 11 | 0 | 0 | 190 | 5 |
| 192.168.0.0/24 | 17 | 0 | 0 | 65 | 0 |
| 192.168.0.0/24 | 32 | 6 | 0 | 34 | 6 |
| 192.168.0.0/24 | 9 | 1 | 0 | 76 | 1 |
| 192.168.0.0/24 | 5 | 0 | 0 | 37 | 0 |
| 192.168.0.0/24 | 14 | 0 | 0 | 46 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 8 | 0 | 0 | 8 | 0 |
| 192.168.0.0/24 | 1 | 0 | 0 | 545 | 16 |
| 192.168.0.0/24 | 55 | 5 | 0 | 690 | 25 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 2 | 0 | 0 | 4 | 6 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 79 | 1 | 0 | 268 | 6 |
| 192.168.0.0/24 | 0 | 0 | 0 | 0 | 0 |
| 192.168.0.0/24 | 0 | 0 | 0 | 177 | 6 |
| 192.168.0.0/24 | 0 | 0 | 0 | 533 | 16 |
| 192.168.0.0/24 | 1 | 0 | 0 | 547 | 16 |

Log body

The top section of the log displays the following information:

- Devices Up
- Devices Down
- Devices in Maintenance
- Monitors Up
- Monitors Down

To use the log:

- Click a number in the Summary area to view a list of devices that match the selected device state.
- Click **expand** or **collapse** in the Group Summary to show or hide the subgroups within the current groups shown.
The bottom section shows a list of the items that correspond to the number at the top of the log.
- Click the device name to open the *Device Properties* (on page 119) dialog for that device.

Alert Center

In This Chapter

Working with Alert Center reports713

Using the Alerts Home reports720

Configuring notifications.....731

Configuring thresholds747

Working with Alert Center reports

In This Chapter

| | |
|---|-----|
| Using Alert Center reports..... | 713 |
| Filtering the Items Report..... | 713 |
| Using the Item History report | 714 |
| Updating Alert Center items | 715 |
| A note about notifications | 717 |
| Understanding resolving items - examples | 717 |
| Filtering the Log Report | 718 |
| Configuring Alert Center records to expire..... | 719 |

Using Alert Center reports

Alert Center reports are used to troubleshoot and monitor Alert Center data.

There are three Alert Center reports:

- Running Notifications Policies
- Log Report
- Items Report

Filtering the Items Report

Filter the Items Report by threshold and/or state.

To filter by threshold:

Using the **Filter by threshold** list, select the desired threshold(s).



Note: This list is populated with thresholds currently configured in the Threshold Library.

- To view items for all thresholds, select **No Filter**.
- To view items for a specific threshold, select that threshold.
- To view items for specific threshold type, such as Flow, select that threshold type.

To filter by state:

Using the Filter by state list, select the desired item state(s).

- To view items in all states, select **No Filter**.

To view items that have been updated to a specific state, select that state. You can select Acknowledged, Resolved, or Acknowledged and Resolved.

To filter by date:

Use the *date/time picker* (on page 602) at the top of the report to select a date range and time frame.

In the **Date range** list, many reports also allow you to specify and customize the business hour report times for reports to display. This allows you to view the network activity only for specified business hours. The date and time format for the date on this report matches the format specified in **Program Options > Regional** set in the WhatsUp Gold console.




Note: The Business Hours setting is available for group reports only.

Using the Item History report

To access the Item History report, click an item in the first column in the Items Report. The history of the selected item displays.

Alert Center Item History

ExportEmailHelp

Item history for Web service down created by Alert 1

Aspect: Service stopped for too long

Threshold description: This threshold monitors the overall health of your WhatUp Gold installation and will alert you to any modifications your system needs.

| State | Notification Progress | Value | Comment | Entry Time | Duration |
|------------------|-----------------------|-----------|---------|------------------------------------|-----------|
| Out of threshold | Pending | 5 minutes | | Wednesday, April 27, 2011 10:47:30 | - |
| Out of threshold | Step 1 | 5 minutes | | Wednesday, April 27, 2011 10:47:35 | 0.00 h... |
| Out of threshold | Step 2 | 5 minutes | | Wednesday, April 27, 2011 10:48:36 | 0.02 h... |
| Out of threshold | Step 3 | 5 minutes | | Wednesday, April 27, 2011 10:52:36 | 0.09 h... |
| Out of threshold | Repeating step 3 | 5 minutes | | Wednesday, April 27, 2011 10:53:36 | 0.10 h... |
| Out of threshold | Repeating step 3 | 5 minutes | | Wednesday, April 27, 2011 10:54:37 | 0.12 h... |
| Out of threshold | Repeating step 3 | 5 minutes | | Wednesday, April 27, 2011 10:55:39 | 0.14 h... |

The Items report tracks an item through the system from creation to completion.

The report heading displays the item name, the threshold that triggered the item, the monitored device activity, and the threshold description.

Report body

Below the heading, the report displays the following information for the selected item:

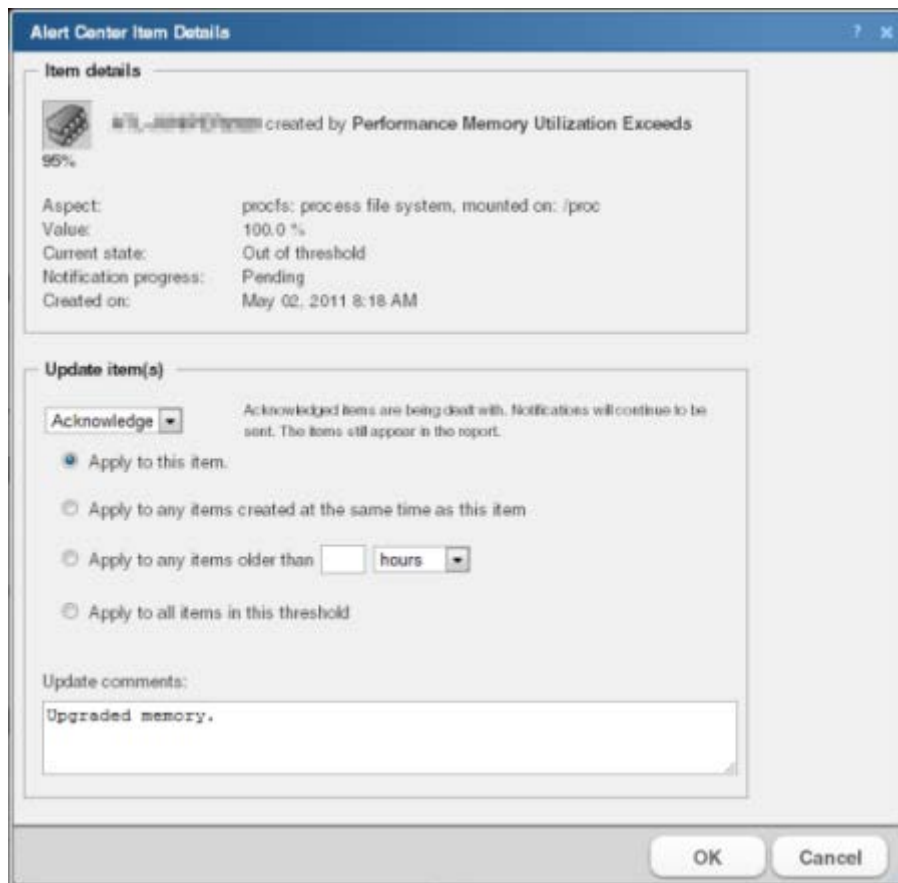
- **State.** Displays the current state of the item. Possible states include *Out of threshold*, *In threshold*, or *Disabled*.
- **Notification progress.** Displays the progress status of an assigned notification policy. Possible progress statuses include *Pending*, *Step 1*, *Step 2*, *Step 3*, *Done*, *Acknowledged*, *Resolved*, or *Repeating Step 3*.
- **Value.** Displays the logged value that caused the item to go out of threshold.
- **Comment.** Displays any comments entered by the user or the system at the time the item was updated.
- **Entry time.** Displays the time the item was updated.
- **Duration.** Displays how long the item spent in the displayed state after it went out of threshold.

Updating Alert Center items

When a monitored device property begins to operate outside of the defined threshold, it appears as an item in a threshold dashboard report on the Alerts Home page. You can update items to either indicate that the issue is known, or remove them from the dashboard report.

To update an item:

- 1 In a threshold dashboard report, click a device name. The Alert Center Item Details dialog appears.



The dialog box is titled "Alert Center Item Details". It contains two main sections: "Item details" and "Update item(s)".

Item details:

- Icon: A small icon representing a hardware component.
- Alert: "Alert created by Performance Memory Utilization Exceeds 95%".
- Aspect: "procfs: process file system, mounted on: /proc".
- Value: "100.0 %".
- Current state: "Out of threshold".
- Notification progress: "Pending".
- Created on: "May 02, 2011 8:18 AM".

Update item(s):

At the top of this section is a dropdown menu set to "Acknowledge". To its right is a note: "Acknowledged items are being dealt with. Notifications will continue to be sent. The items still appear in the report."

Below the dropdown are four radio button options:

- ☒ Apply to this item.
- ☐ Apply to any items created at the same time as this item.
- ☐ Apply to any items older than hours.
- ☐ Apply to all items in this threshold.

At the bottom of the "Update item(s)" section is a text area labeled "Update comments:" containing the text "Upgraded memory."

At the bottom right of the dialog are "OK" and "Cancel" buttons.

- 2 In the Update Items area, select how you would like to update the item(s).
 - **Acknowledge.** Select to indicate that the issue with the item is known. Alert Center continues to send any related notifications regarding the item. The item continues to appear in the dashboard report.
 - **Resolve.** Select to indicate that any actions required to address the item are complete. Notifications regarding the item stop. The item is removed from the dashboard report.
- 3 Select the item(s) to which you would like to apply the update. Options include:
 - **Apply to this item.** Select this option to update only the currently viewed item.
 - **Apply to any items created at the same time as this item.** Select this option to apply the update to any matching items that were created during the same poll.
 - **Apply to any items older than ____ hours/minutes/days.** Select this option to apply the update to all alerts older than the time you select. This option is useful when one device fails and impacts numerous other devices, such as when attempting to ping devices on the other side of a failed router. Selecting to resolve all items that were added at the same time as the router failure saves the time it would otherwise take to acknowledge each item individually.


- **Apply to all items in this threshold.** Select this option to update any items that currently exist for this threshold.
- 4 After selecting the appropriate update, enter a brief comment in the **Update comment** box explaining the actions taken to address the issue.



Note: Comments are optional but recommended for your records.

- 5 Click **OK** to save changes.



Note: Items that have been acknowledged display a green check mark  next to their name on Alert Center Home threshold dashboard reports.

A note about notifications

Notifications are affected depending upon how you choose to acknowledge items. There are two basic scenarios when resolving items:

Single-item threshold

One item exists in a threshold and you acknowledge or resolve that item. The corresponding notification is also deleted and no more notifications for the item are sent.

Multiple-item threshold

Several items fall out of threshold at the same time and one notification is sent for the group of items. If you acknowledge or resolve only one item, a corresponding notification persists for all other unacknowledged and unresolved items.

However, if you select one item from the group, acknowledge or resolve it, and then select **Apply to any items created at the same time as this item**, the corresponding notification stops for all items that were created at the same time as the selected item.

Understanding resolving items - examples

When you mark an out-of-threshold item as resolved, the Alert Center ignores the item until the sample period does not include the time the item was resolved. This gives you one full sample period to fix the problem.

Example #1 - Marking an item as resolved without fixing the underlying problem will cause the item to appear again during the next sampling interval

Threshold: Disk Utilization exceeds 90%

Sample period: 1 day

Polling interval: 1 hour

Scenario:

Tuesday, 1:00 pm - Device exceeds disk utilization threshold and appears in the Items Report.

Tuesday, 1:05 pm - Item is marked as resolved, but no additional resources are provided to the device to solve the disk utilization issue.

Wednesday, 2:00 - During the next sample period, WhatsUp Gold checks the database and finds the device is out-of-threshold again. The device appears in the Items Report a second time.

Example #2 - Marking an item as resolved and fixing the issue before the next poll causes Alert Center to ignore the device during the next poll

Threshold: SNMP Trap exceeds 500 traps per hour

Sample period: 1 day

Polling interval: 30 minutes

Scenario:

Tuesday, 1:00 pm - Alert Center checks the WhatsUp Gold database for the previous 30 minutes and finds a device exceeding the threshold for SNMP traps.

Tuesday, 1:10 pm - You see the device listed as out-of-threshold, and you mark it resolved.

Tuesday, 1:30 pm - Alert Center checks the WhatsUp Gold database. The device is marked "resolved," so Alert Center ignores the device.

Tuesday, 1:35 pm - You turn off the SNMP trap agent on the device that is sending so many messages to the receiving device.

Tuesday, 2:00 pm - The device does not appear in the out of threshold items list.



Note: If you did not address the SNMP agent before the next poll, the device would again appear in the list of out of threshold devices.



Note: This method of resolving items does not apply to the WhatsUp Health threshold.

Filtering the Log Report

You can filter the log report using the following methods:

Filter by date:

Use the **Date range** list at the top of the report to select a time frame for the report. By default, the report displays log entries for the previous hour.

Filter by severity level:

Use the **Filter by severity level** list to select a logging level for the report.

- **No Filter** displays messages for every entry level.
- **Critical** displays only critical messages.
- **Error** displays only error messages.
- **Warning** displays only warning messages.
- **Information** displays only information messages.

Configuring Alert Center records to expire

You can configure the length of time to keep Alert Center data in your database on the Configure Database Record Expiration dialog.

To configure Alert Center data expiration settings:

- 1 From the Alert Center tab, click **Record Maintenance**. The **Configure Database Record Expiration** dialog appears.
- 2 Specify expiration settings:
 - **Alert Center Log**. Enter a number of days and/or hours after which you would like to expire data for this report. Data that is expired is deleted from the database.
 - **Alert Center Items**. Enter a number of days and/or hours after which you would like to expire data for this report.
- 3 Click **OK** to save changes.

Using the Alerts Home reports

In This Chapter

| | |
|---|-----|
| Using the Performance CPU threshold report | 720 |
| Using the Performance Custom threshold report | 721 |
| Using the Performance Disk threshold report | 721 |
| Using the Performance Interface threshold report | 722 |
| Using the Interface Errors and Discards threshold report | 722 |
| Using the Performance Memory threshold report | 723 |
| Using the Performance Ping Availability threshold report | 723 |
| Using the Ping Response Time threshold report | 724 |
| Using the SNMP Trap threshold report | 724 |
| Using the Syslog threshold report | 724 |
| Using the Windows Event Log threshold report | 725 |
| Using the Flow Monitor Conversation Partners threshold report .. | 725 |
| Using the Flow Monitor Custom threshold report | 726 |
| Using the Flow Monitor Failed Connections threshold report | 726 |
| Flow Monitor Interface Traffic threshold report | 727 |
| Using the Flow Monitor Top Sender/Receiver threshold report | 727 |
| Using the Blackout Summary threshold report | 728 |
| Using the WhatsUp Health threshold report | 728 |
| Failover threshold report | 729 |
| Using the WhatsConfigured Threshold report | 729 |
| WhatsVirtual events threshold report | 730 |

Using the Performance CPU threshold report

This Alert Center Home report displays the following threshold information for a CPU utilization threshold:

- **Device.** The network device that has gone out of the parameters of the CPU utilization threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- **CPU.** The specific CPU that has gone out of the parameters of the CPU utilization threshold.
- **Average utilization.** The average utilization of the CPU during the sample time period.



Tip: Click an average utilization value to view the *CPU Utilization* (on page 631) report for that device.

- **Time alerted.** The time the Alert Center discovered the CPU out of threshold.

Using the Performance Custom threshold report

This Alert Center Home report displays the following threshold information for a custom performance monitor threshold:

- **Device.** The network device that has gone out of the parameters of the custom performance monitor threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Custom performance monitor.** The specific custom performance monitor on this device that has gone out of the parameters of this threshold.
- **Value.** The value of the custom performance monitor.
- **Time alerted.** The time the Alert Center discovered the monitor out of threshold.

Using the Performance Disk threshold report

This Alert Center Home report displays the following threshold information for a disk utilization threshold:

- **Device.** The network device that has gone out of the parameters of the disk utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Disk.** The disk that has gone out of the parameters of the disk utilization threshold.
- **Average utilization.** The average utilization of the disk during the sample time period.



Tip: Click an average utilization value to view the *Disk Utilization* (on page 633) report for that device.

- **Time alerted.** The time the Alert Center discovered the disk out of threshold.

Using the Performance Interface threshold report

This Alert Center Home report displays the following threshold information for an interface utilization threshold:

- **Device.** The network device that has gone out of the parameters of the interface utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Interface.** The specific interface that has gone out of the parameters of the interface utilization threshold.
- **Average utilization.** The average utilization of the interface during the sample time period.



Tip: Click an average utilization value to view the *Interface Utilization* (on page 641) report for that device.

- **Time alerted.** The time the Alert Center discovered the interface was out of threshold.

Using the Interface Errors and Discards threshold report

This Alert Center Home report displays the following threshold information for inbound and outbound device interface discards or errors response time thresholds.

- **Device.** The network device that has gone out of the threshold parameters.



Tip: Click a device to view the Alert Center Item Details for that device.

- **Interface.** The specific interface on which the inbound and/or outbound interface discards or errors response time is out of threshold.
- **Discards or Errors.** The number of inbound and/or outbound interface discards or errors per minute during the sample time period.



Tip: Click an average response time to view the *Ping Response Time* (on page 647) report for that device.

- **Time Alerted.** The time the Alert Center discovered the inbound and outbound interface discards or errors out of threshold.

Using the Performance Memory threshold report

This Alert Center Home report displays the following threshold information for a memory utilization threshold:

- **Device.** The network device that has gone out of the parameters of the memory utilization threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Memory.** The specific memory that has gone out of the parameters of the memory utilization threshold.
- **Average utilization.** The average utilization of the memory during the sample time period.



Tip: Click an average utilization value to view the *Memory Utilization* (on page 636) report for that device.

- **Time alerted.** The time the Alert Center discovered the memory out of threshold.

Using the Performance Ping Availability threshold report

This Alert Center Home report displays the following threshold information for a ping availability threshold.

- **Device.** The network device that has gone out of the parameters of the ping availability threshold.



Tip: Click a device to view the Alert Center Items Report for that device.

- **Interface.** The specific interface on which the ping packet loss is occurring.
- **Percent Packet Loss.** The percentage of packets lost during the sample time period.



Tip: Click a packet loss value to view the *Ping Availability* (on page 650) report for that device.

- **Time Alerted.** The time the Alert Center discovered the ping availability out of threshold.

Using the Ping Response Time threshold report

This Alert Center Home report displays the following threshold information for a ping response time threshold.

- **Device.** The network device that has gone out of the parameters of the ping response time threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Interface.** The specific interface on which the ping response time is out of threshold.
- **Response Time Average.** The average ping response time during the sample time period.



Tip: Click an average response time to view the *Ping Response Time* (on page 647) report for that device.

- **Time Alerted.** The time the Alert Center discovered the ping response time out of threshold.

Using the SNMP Trap threshold report

This Alert Center Home report displays the following threshold information for an SNMP Trap threshold.

- **Device.** The network device that has gone out of the parameters of the SNMP trap threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Trap.** The specific trap that has gone out of the parameters of the threshold.
- **Trap Count.** The number of traps received for this specific trap during the sample time period.



Tip: Click a trap count value to view the *SNMP Trap Log* (on page 692) for that device.

- **Time Alerted.** The time the Alert Center discovered the number SNMP traps out of threshold.

Using the Syslog threshold report

This Alert Center Home report displays the following threshold information for a Syslog threshold.

- **Device.** The device that has gone out of the parameters of the Syslog threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Syslog.** The specific Syslog that has gone out of the parameters of the threshold.
- **Message Count.** The number of Syslog messages received for that specific Syslog.



Tip: Click a message count value to view the *Syslog* (on page 693) report for that device.

- **Time Alerted.** The time the Alert Center discovered the number of Syslog messages out of threshold.

Using the Windows Event Log threshold report

This Alert Center Home report displays the following threshold information for a Windows Event threshold.

- **Device.** The network device that has gone out of the parameters of the SNMP trap threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Windows Event.** The specific Windows event that has gone out of the parameters of the threshold.
- **Windows Event Count.** The number of Windows events received for this specific event type during the sample time period.



Tip: Click an event count value to view the *Windows Event Log* (on page 696) for that device.

- **Time Alerted.** The time the Alert Center discovered the number of Windows events out of threshold.

Using the Flow Monitor Conversation Partners threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor conversation partners threshold.

- **Host.** The host that has gone out of the parameters of the conversation partners threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Conversation Partners.** The number of conversation partners sending or receiving data with the host.



Tip: Click a conversation partners value to view the Interface Details report.

- **Time Alerted.** The time the Alert Center discovered the host's number of conversation partners out of threshold.

Using the Flow Monitor Custom threshold report

This Alert Center Home report displays the following threshold information for a Flow custom threshold.

- **Host.** The Flow Monitor host that has gone out of the parameters of the custom threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Bytes.** The number of bytes transferred.



Tip: Click a bytes value to view the Interface Details report.

- **Time Alerted.** The time the Alert Center discovered the number of bytes out of threshold.

Using the Flow Monitor Failed Connections threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor failed connections threshold.

- **Host.** The host that has gone out of the parameters of the failed connections threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Failed connections.** The number of failed connections the host has sent or received.



Tip: Click a failed connections value to view the Interface Details report.

- **Time Alerted.** The time the Alert Center discovered the host's number of failed connections out of threshold.

Flow Monitor Interface Traffic threshold report

This Alert Center Home report displays the following threshold information for a Flow Monitor interface traffic threshold.

- **Interface** displays the source interface over which traffic is transmitting.



Tip: Click a host to view the *Alert Center Item Details* (on page 801) for that interface.

- **Interface traffic** displays the amount of traffic that has been transmitted over the sample time period.



Tip: Click an interface value to view the Interface Details report.

- **Time Alerted** displays the time Alert Center discovered the interface's traffic amount out of threshold.

Using the Flow Monitor Top Sender/Receiver threshold report

This Alert Center Home report displays the following threshold information for the Flow Monitor top sender/receiver threshold.

- **Host.** The host that has gone out of the parameters of the top sender/receiver threshold.



Tip: click a device to view the Alert Center Items Report for that device.

- **Bytes transferred.** The number of bytes sent or received by a host.



Tip: Click a bytes value to view the Interface Details report.

- **Time Alerted.** The time the Alert Center discovered the host's total number of bytes sent or received out of threshold.

Using the Blackout Summary threshold report

This Alert Center Home report displays the following threshold information for a blackout summary threshold.

- **Device.** The device for which the action would have been triggered.
- **Action.** The action that was not fired due to the blackout.
- **Occurrences.** The number of times the action would have fired had the action not been in a blackout period.



Tip: Click an entry in the **Occurrences** column to view the *Blackout Summary Log* (on page 705).

- **Time Alerted.** The time the Alert Center was alerted; Alert Center is notified of action activity when the blackout period ends.

Using the WhatsUp Health threshold report

This Alert Center Home report displays the following threshold information for a WhatsUp Health threshold.

- **System Aspect.** The aspect of your system that has gone out of threshold. For example, Flow service, Total expired records, or WUG service.



Tip: click a device to view the Alert Center Items Report for that device.

- **Value.** The length of time in which the service has met the threshold parameters.
- **Help Link.** Click this link for a list of ways you can resolve problems associated with the out of threshold item.
- **Time Alerted.** The time the Alert Center discovered the system aspect out of threshold.

Failover threshold report

This Alert Center Home report displays the following threshold information for a Failover threshold.

- **Source.** The machine on which the failover event took place.



Tip: Click a device to view the Alert Center Item Details for that device.

- **Category.** The category of activity and message; either information or error.
- **Message.** The message generated as a result of the failover event.



Tip: Hover over a message with your mouse to view the message in its entirety.



Tip: Click an entry in the Message column to view the *General Error Log* (on page 688).

- **Time Alerted.** The time the Alert Center discovered the failover event.

Using the WhatsConfigured Threshold report

This Alert Center Home report displays the following threshold information about a WhatsConfigured task.

- **Description.** Describes the task threshold.
- **Device.** The device where the WhatsConfigured task ran.
- **Configuration result.** The WhatsConfigured task result.
- **Time Alerted.** The time Alert Center received the tasks configuration results.

WhatsVirtual events threshold report

The WhatsVirtual events threshold report displays events collected from the vCenter server that are of the type selected in the threshold definition. The events appear in reverse chronological order, so that the last event received appears at the top of the list.

- **Target.** Displays the virtual server, host or virtual device that was the target of the event. The display format is either *<Datacenter - VMware Host name - virtual machine name>*, or *<vCenter server name>*.
- **User.** Displays the user that initiated the event.
- **Message.** Displays the message received from the vCenter server that describes the event.
- **Date.** Displays the date and time that the event was received by the Alert Center.



Note: The WhatsVirtual events threshold can be created for any of the event groups that WhatsVirtual can collect from the vCenter server.

Configuring notifications

In This Chapter

- Using Alert Center and actions.....731
- Alert Center Percent Variables.....732
- Using Alert Center Notification Policy options733
- Configuring a notification policy734
- Configuring an Alert Center email notification736
- Configuring an Alert Center SMS Direct notification738
- Configuring an Alert Center SMS Action notification740
- Configuring email notification message settings.....743
- Stopping a running notification policy743
- Using the Email Action745
- Using the SMS Direct Action.....745
- Using the SMS Action.....746

Using Alert Center and actions

Alert Center lets you receive alerts for performance monitors, the WhatsUp Gold system, and WhatsUp Gold Flow Monitor plug-in addition to email alerts you can receive for active and passive monitors.

The table below shows the system you use to receive alerts of a particular type.

| | Actions | Alert Center |
|-------------------------------------|---------|--------------|
| Alerts on active monitors | ● | |
| Alerts on passive monitors | ● | ● |
| Alerts on performance monitors | | ● |
| Alerts on the WhatsUp Gold database | | ● |
| Alerts on WhatsUp Gold services | | ● |
| Alerts on WhatsUp Gold Flow Monitor | | ● |

Alert Center and actions are different systems and have different functions.

While Alert Center displays alerts on the Alerts Home page and in email notifications, there are many different types of tasks you can perform using actions. Actions allow you to restart services, reboot systems, send text messages, and perform many other tasks. Used together, Alert Center and actions help you more thoroughly support and manage your network.

For more information on alerting through actions, see *Using Actions* (on page 271).

For more information on alerting through Alert Center, see *Using Notification Policies*.

Alert Center Percent Variables

The Email, SMS, and SMS Direct Actions can include four categories of percent variables in Alert Center notification message:

- Threshold
- Notification Policy
- System

Use Alert Center percent variables in the Alert Center message body for SMS Direct and SMS action notifications, and in the subject line of Email notifications.

Threshold percent variables

| Name | Description |
|---|---|
| %AlertCenter.Threshold.ID | The threshold ID listed in the ProActiveAlert table. |
| %AlertCenter.Threshold.Name | The threshold name. |
| %AlertCenter.Threshold.Description | The threshold description. |
| %AlertCenter.Threshold.PollingInterval | The threshold polling interval. |
| %AlertCenter.Threshold.TotalItems | The total new new and current items out of threshold. |
| %AlertCenter.Threshold.TotalNewItem | The total of newly alerted items. |
| %AlertCenter.Threshold.TotalCurrentItems | The total of existing items out of threshold (not including new items). |
| %AlertCenter.Threshold.TotalMonitoredItems | The count of items that can be evaluated in the threshold, i.e. there are 22 devices that have a Disk Performance Monitor configured. |
| %AlertCenter.Threshold.TotalAutoResolvedItems | The number of items automatically resolved. |
| %AlertCenter.Threshold.NewItemNames | The display name of each new item in an alert. |
| %AlertCenter.Threshold.CurrentItemNames | The display name of each current item in an alert. |

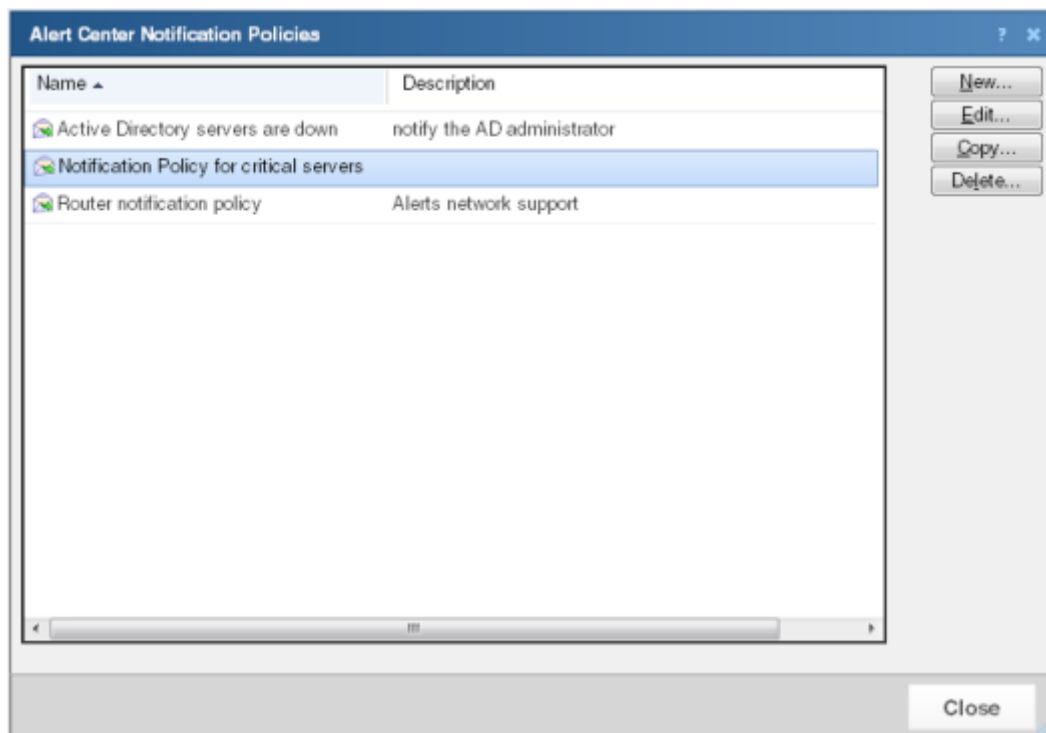
Notification policy percent variables

| Name | Description |
|--|---|
| %AlertCenter.NotificationPolicy.ID | The notification policy ID. |
| %AlertCenter.NotificationPolicy.Name | The notification policy name. |
| %AlertCenter.NotificationPolicy.Description | The notification policy description. |
| %AlertCenter.NotificationPolicy.Recipients | The list of actions included in the policy. |
| %AlertCenter.NotificationPolicy.NextEscalationTime | When the next step is to be sent. |
| %AlertCenter.NotificationPolicy.EscalationStep | The current escalation step. |

System percent variables

| Name | Description |
|--------------|--------------------------|
| %System.Date | The current system date. |
| %System.Time | The current system time. |

Using Alert Center Notification Policy options



To access notification policy options:

- 1 Click the **Alert Center** tab.

- 2 Click **Notification Policies**. The Alert Center Notification Policies dialog appears.
 - Click **New** to configure a new policy.
 - Select a policy, then click **Edit** to modify the policy configuration.
 - Select a policy, then click **Copy** to make a duplicate of the selected policy.
 - Select a policy, then click **Delete** to remove the policy from the dialog.



Caution: When you delete a policy from the list, it is removed from any threshold to which it is assigned.

Configuring a notification policy



Note: It is not required that you select a notification policy for use with every threshold. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report with the out of threshold items appears on the Alerts Home page.

To create a notification policy:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Policies**. The Alert Center Notification Policies dialog appears.
- 3 Click **New**. The New Alert Center Notification Policy dialog appears.

New Alert Center Notification Policy

Name:

Description:

Select which notifications will be delivered by each step of this policy:

| Notification | Type | Step 1 | Step 2 | Step 3 |
|----------------------------|---------------|--------------------------|--------------------------|--------------------------|
| Alert tech support | E-mail Action | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Email support | E-mail Action | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Email the AD administrator | E-mail Action | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Email the administrator | E-mail Action | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Escalation Steps

Step 2 begins hours after the notification starts

Step 3 begins hours after the notification starts

☐ Repeat step 3 every hours until the notification is stopped

☐ Show me a graph of this notification policy in action

OK Cancel

- 4 Complete the identifying information for the policy.
 - **Name.** Type a name for the notification policy. The name identifies the policy in the Alert Center Notification Policies dialog.
 - **Description.** Enter a description of the policy. The description appears next to the policy name in the Alert Center Notification Policies dialog.
- 5 Select the notifications you would like delivered for each of the 3 steps in the policy. You can select multiple notifications for each policy step. To select a notification, click the box for the step of the policy that you would like the notification to be sent. For example, if you would like an email sent to Bob for the policy's first step, select the **Step 1** box for the Email Bob notification. Continue the same for Step 2 and Step 3.

New Alert Center Notification Policy

Name:

Description:

Select which notifications will be delivered by each step of this policy:

| Notification | Type | Step 1 | Step 2 | Step 3 |
|--------------------------|---------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Alert tech support | E-mail Action | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Email support | E-mail Action | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Email the AD administ... | E-mail Action | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Email the administrator | E-mail Action | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Escalation Steps

Step 2 begins hours after the notification starts

Step 3 begins hours after the notification starts

☐ Repeat step 3 every hours until the notification is stopped

Show me a graph of this notification policy in action

OK Cancel


Step 1 of the notification policy begins as soon as an item falls out of threshold. You can specify when steps 2 and 3 begin in the Escalation Steps section of the dialog. If you do not see an appropriate notification, or if the list is empty, click browse (...) to open the Notification Library and configure a new notification.

- 6 Select the how the policy notifications proceed after Step 1 in the **Escalation Steps** section.
 - Specify a start time for steps 2 and 3 of the policy. By default, step 2 is set to begin 1 hour after the first notification occurs, and step 3 is set to begin 2 hours after the first notification.
 - You can choose to repeat step 3 of the policy at a regular interval until the notification is stopped. By default, the policy is set to repeat step 3 every hour until the notification is stopped.



Note: In order for this repeat function to work properly, step 3 must be enabled for at least one notification in the policy.



Tip: You can view a graph of the notification policy in action by clicking  **Show me a graph of this notification policy in action.**

- 7 Click **OK** to save changes.

Configuring an Alert Center email notification

Alert Center email notifications and WhatsUp Gold email actions use the same configuration dialog.

For more information about Email Actions, see *Using the Email Action* (on page 284).

To configure an email notification:

- 1 Click the **Alert Center** tab, then click **Notification Library**. The Alert Center Notification Library dialog appears.
- 2 Click **New**. The Select Notification Type dialog appears.

- 3 Select **E-mail Action**, then click **OK**. The New Email Action dialog appears.

- 4 Complete the appropriate information in the dialog fields.
- **Name.** Type a name for the action. This name identifies the action in the Notification Library.
 - **Description.** Enter a few words to describe the action. This description displays beside the action name in the Notification Library.
- 5 Click the **Alert Center** tab to complete the appropriate Alert Center settings for the Email notification.

The **Alert Center Settings** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.

- **Alert Center Message Subject.** Enter a subject for the message. This text appears as the subject in the email that is sent by the Alert Center notification. This subject can include percent variables.



Tip: To include *Alert Center percent variables* (on page 732), right click inside the above field.

- **Alert Center Link.** Select **Include hyperlink to Alert Center in the email content** to include a link to the Alerts Home page in the email message sent by the Alert Center notification.
 - **Use HTTP or Use HTTPS.** Select the appropriate protocol to use in the link address.
 - **Use dynamic address or Use static hostname or IP address.** If you select to use the dynamic address, WhatsUp Gold automatically renders the hostname or IP address at the time the action runs.
 - **Hostname or IP address.** If you selected Use static hostname or IP address, type the server address in the box.
 - **Port.** Specify the specific port to include in the link address.



Important: The address you enter here must be the exact address of the Alerts Home page to which you want to connect. Verify the address and enter its exact contents in the above options.



Note: Click the **Configuration** tab to edit the email action settings and specify a destination address for the notification.

- 6 Click **OK** to save changes.

Configuring an Alert Center SMS Direct notification

Alert Center SMS Direct notifications and WhatsUp Gold SMS Direct actions use the same configuration dialog.

For more information about SMS Direct Actions, see Using the SMS Direct Action.

To configure an SMS Direct notification:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Library**.

- 3 Click **New**. The Select Notification Type dialog appears.
- 4 Select **SMS Direct**. The New SMS Direct Action dialog appears.

- 5 Specify or select the appropriate information in the dialog boxes.
 - **Name.** Enter a name for this notification. This name is for your reference only and will never be displayed to the notification recipient.
 - **Description.** Create or modify the description. This description appears in the Action Library and is for your reference only.
 - **Phone number.** Type the cell phone number(s) of the intended SMS message recipients. You can enter multiple phone numbers, separated by a comma. For example: 555-555-5555, 55 555 55 55, (555) 555 5555



Note: All non-numeric characters other than the comma, such as "-" and ".", will be ignored.



Note: There is a 2,000 character limit in this field, so you can enter many numbers.

- **COM Port.** Select the COM port you want to use with this notification.



Note: The list displays all ports associated with the GSM modem, including virtual and hard-wired, serial ports. You must select the port that is assigned to the modem in the Windows Device Manager.

- 6** Select the **Alert Center Message** tab to specify the appropriate settings for the SMS notification message.
The **Alert Center Message** tab contains options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.
Enter a text message plus any necessary percent variable codes. Keep in mind that using percent variables can greatly increase the character count.



Tip: To enter *Alert Center percent variables* (on page 732), right-click inside the message box.



Note: The size limit for the message is 160 characters (140 bytes).

- 7** Click **OK** to save changes.
Enter a text message plus any desired percent variable codes. Keep in mind that if you use percent variables, this will greatly increase the character count.



Tip: To enter Alert Center percent variables, right click inside the message box.



Note: If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).

- 8** Click **OK** to save changes.

Configuring an Alert Center SMS Action notification

Alert Center SMS notifications and WhatsUp Gold SMS actions use the same configuration dialog.

For more information about SMS Actions, see Using the SMS Action.

To configure an SMS notification:

- 1 Click the **Alert Center** tab.
- 2 Click **Notification Library**. The Alert Center Notification Library dialog appears.
- 3 Click **New**. The Select Notification Type dialog appears.
- 4 Select **SMS Action** and click **OK**. The New SMS Action dialog appears.

New SMS Action

Name:

Description:

Country:

Provider:

Mode:
☐ Email ☐ Diglu

Phone number:

Alert Center Message

WhatsUp Gold Alert Center: Threshold '%
 AlertCenter.Threshold.Name' has %
 AlertCenter.Threshold.TotalNewItem
 new items. %System.Date - %System.Time

Message characters remaining: 14

Right Click in the message box for percent variable support.

Message Alert Center Message

OK Cancel

- 5 Specify or select the appropriate information in the dialog boxes.
 - **Name.** Type a unique display name to identify the SMS notification.
 - **Description.** Type a short description of the action. This description is displayed in the Action Library along with the action name.
 - **Country.** Select the country for the SMS provider from the list.
 - **Provider.** Select the appropriate SMS provider from the list.



Note: If the provider list is incomplete and/or incorrect, you can click browse (...), then click **New** or **Edit** to add or edit an SMS provider.

- **Mode.** Select either Email or Dialup, depending on the Provider configuration in the system.
- **Email to.** If Email is selected as the Mode, type the SMS device email address.
- **Phone Number.** If Dialup is selected as the Mode, type the phone number to call with the message. You can enter multiple phone numbers, separated by a comma. There is a 2,000-character limit in this field, so you can enter many numbers.



Note: Non-numeric characters such as "-" and "." are ignored.

- 6** In the **Alert Center Message** box, specify the options pertaining to the message that is to be sent from an WhatsUp Gold Alert Center notification.
Enter a text message plus any necessary percent variable codes. Keep in mind that using percent variables can greatly increase the character count.



Tip: To add *Alert Center percent variables* (on page 732), right-click inside the message box and make selections from the lists.



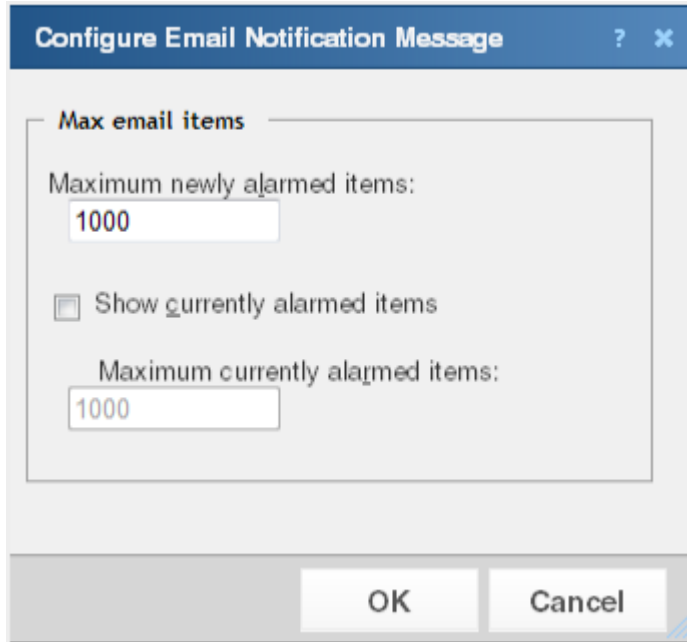
Note: The size limit for the message is 160 characters (140 bytes).

- 7** Click **OK** to save the changes.

Configuring email notification message settings

To configure email notification message settings:

- 1 Click the **Alert Center** tab.
- 2 Click **Email Notification Message Settings**. The Configure Email Notification Message dialog appears.



The screenshot shows a dialog box titled "Configure Email Notification Message". It contains a section titled "Max email items" with the following settings:

- Maximum newly alarmed items: 1000
- ☐ Show currently alarmed items
- Maximum currently alarmed items: 1000

At the bottom of the dialog are "OK" and "Cancel" buttons.

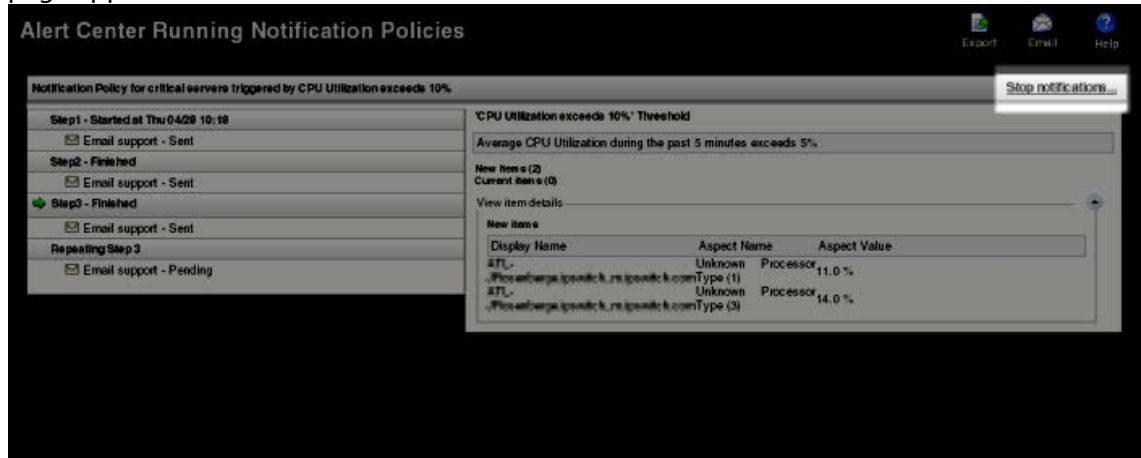
- 3 Select or specify the appropriate settings:
 - **Maximum newly alarmed items.** Enter the maximum number of new, previously unreported alerts to display in notification email messages.
 - **Show currently alarmed items.** Select to include previously reported items that are still generating alerts in addition to newly alarmed items.
 - **Maximum currently alarmed items.** Enter the maximum number of previously reported alerts to display in notification email messages.
- 4 Click **OK** to save changes.

Stopping a running notification policy

After resolving a problem, you can stop proceeding steps in a notification policy using the Stop Notification dialog.

To stop a notification policy:

- 1 Click the **Alert Center** tab.
- 2 Click **Running Notification Policies**. The Alert Center Running Notification Policies page appears.



- 3 Next to the notification policy that you want to stop, click **Stop notification**. The Stop Notification dialog appears.

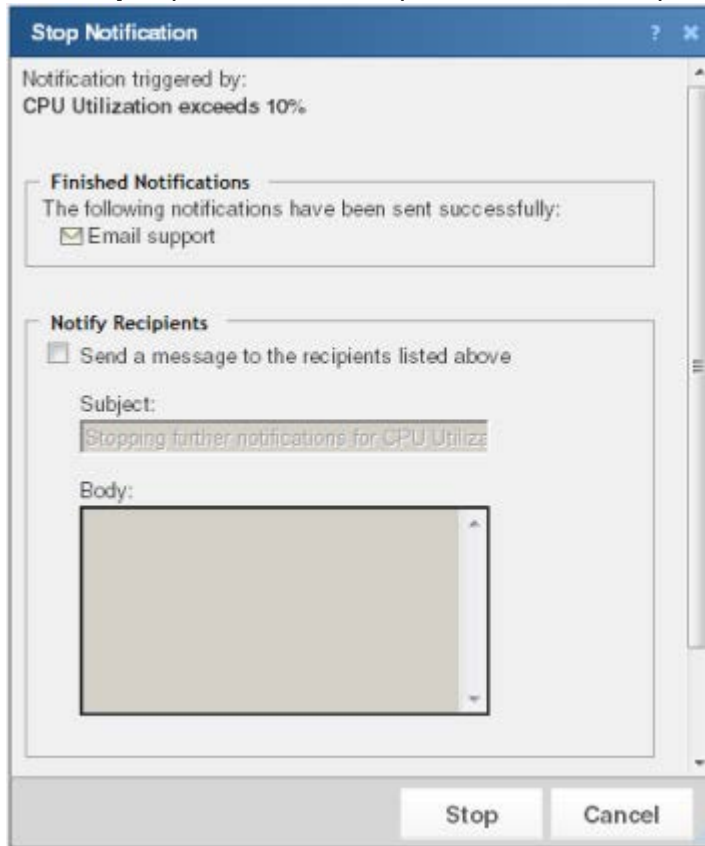


Tip: You can send an optional message to the recipients listed in this dialog to notify them that you have resolved the problem and are stopping the notification policy from this point forward.



If you choose to do so, select **Send a message to the recipients listed above**, and enter a **Subject** and **Body** for the message.

- 4 Click **Stop** to prevent further steps in the notification policy from firing.



Note: SMS message recipients only receive the message body contents; the message subject is not included.

Using the Email Action

The Email Action sends an SMTP mail message to a specific email account. An Email Action can also be used as an email notification in the WhatsUp Gold Alert Center. While you can configure this action on both the console and web interface, you can only configure the Alert Center notification message on the web. For more information, see *Configuring an Alert Center email notification* (on page 736).

Using the SMS Direct Action

The SMS Direct Action send SMS messages directly through an SMS modem, unlike SMS actions, which use email gateways or dial-up modems. For more information, see *Configuring an Alert Center SMS Direct Notification* (on page 738). If you want to send an SMS message and do not have an SMS modem, see *Configuring an Alert Center SMS Action notification* (on page 740).

Using the SMS Action

The SMS Action sends a Short Message Service (SMS) notification to a pager or cell phone using an email gateway or dial-up modem. An SMS Action can also be used as an SMS notification in the WhatsUp Gold Alert Center. While you can configure this action on both the console and web interface, you can only configure the Alert Center notification message on the web. For more information, see *Configuring an Alert Center SMS Action notification* (on page 740).

Configuring thresholds

In This Chapter

| | |
|---|-----|
| Configuring Alert Center thresholds | 748 |
| Selecting threshold devices..... | 749 |
| Configuring performance thresholds | 753 |
| Configuring passive thresholds..... | 770 |
| Configuring Flow Monitor thresholds..... | 777 |
| Configuring system thresholds | 790 |
| Notification Policy Graph View | 799 |
| Threshold Devices | 800 |
| Alert Center Item Details..... | 801 |
| Netflow database record types | 802 |
| Reducing the WhatsUp database size..... | 802 |
| Reducing the number of raw, hourly, or daily data records | 803 |
| Reducing the number of host records..... | 803 |
| Restarting the Flow Collector service..... | 803 |
| Reducing performance monitors..... | 804 |
| WhatsUp discovery service is down..... | 804 |
| WhatsUp web service SQL queries exceed threshold | 804 |
| WhatsUp web service is down..... | 806 |
| WhatsUp web service HTTP responses exceed threshold | 806 |
| WhatsUp polling service SQL queries exceed threshold..... | 808 |
| WhatsUp polling service is down..... | 809 |
| Troubleshooting the WhatsUp Health Threshold | 809 |
| Changing how long report data is stored | 810 |
| Reducing passive monitor records..... | 811 |
| Reducing expired records | 814 |
| Database Tools Table Maintenance..... | 814 |
| Program Options - Report Data..... | 815 |

| | |
|---|-----|
| Configure CPU Utilization..... | 816 |
| Configure Disk Utilization..... | 816 |
| Configure Memory Utilization | 816 |
| Configure Ping Latency and Availability | 817 |
| Configure Data Collection Advanced Settings | 817 |
| Creating global custom performance monitors..... | 818 |
| Creating device-specific custom performance monitors..... | 818 |
| Reducing ActiveMonitorStateChangeLog | 818 |
| Reducing StatisticalInterface..... | 819 |
| Bulk Field Change - Performance Monitor | 820 |
| Configure Interface Data Collection | 822 |
| Monitored devices exceeds license limit | 824 |
| Flow Threshold Hosts..... | 825 |
| Select Notification Type | 826 |
| Reducing performance monitor records | 826 |
| Reducing PassiveMonitorActivityLog | 827 |
| Configure VMware event listener | 829 |

Configuring Alert Center thresholds

To configure any of the four types of Alert Center thresholds, click the Alert Center tab, then click **Threshold Library**.

On the Select Threshold Type dialog, select the type of threshold you want to configure, then click **OK**.

You can select from the following thresholds:

- Performance
- *CPU* (on page 753)
- *Custom* (on page 755)
- *Disk* (on page 757)
- *Interface* (on page 759)
- *Interface Errors and Discards* (on page 761)
- *Memory* (on page 763)
- *Ping Availability* (on page 765)
- *Ping Response Time* (on page 767)

- Passive
- *SNMP trap* (on page 770)
- *Syslog* (on page 772)
- *Windows Event Log* (on page 774)
- Flow Monitor
- *Flow Monitor Conversation Partners* (on page 780)
- *Flow Monitor Custom Threshold* (on page 781)
- *Flow Monitor Failed Connections* (on page 783)
- *Flow Monitor Interface Traffic* (on page 785)
- *Flow Monitor Top Sender/Receiver* (on page 787)
- System
- *Blackout Summary* (on page 790)
- *Failover* (on page 794)
- *WhatsUp Health* (on page 795)
- *VMware* (on page 792)

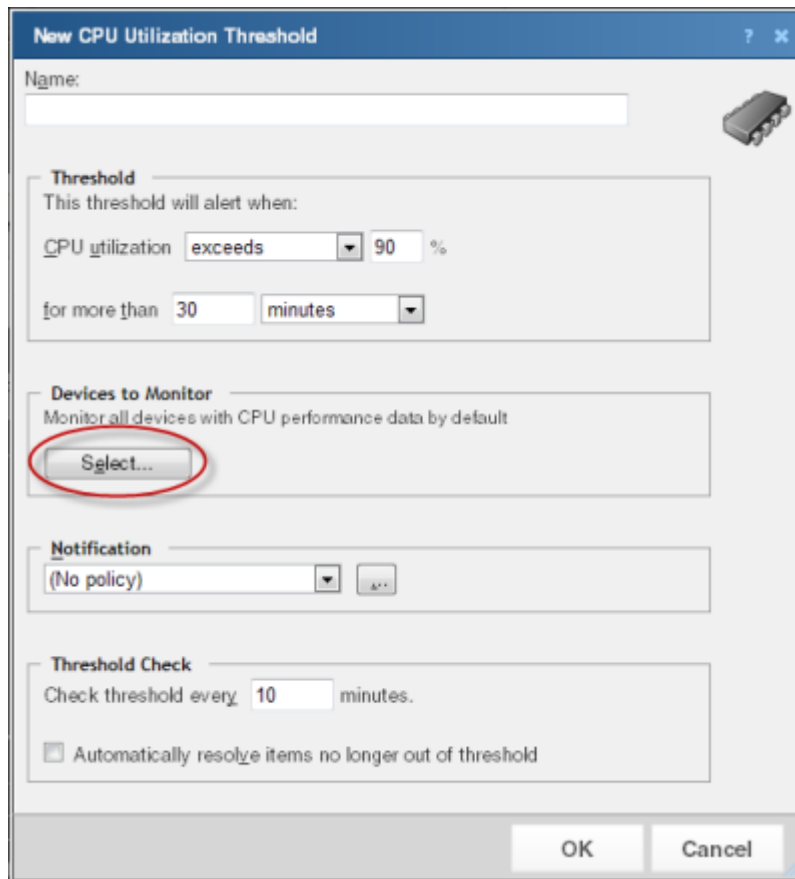
Selecting threshold devices

For each performance or passive threshold that you configure you can include a list of devices or device group exceptions to which the threshold will apply. If you choose not to select specific devices to include or to exclude, by default, the threshold monitors all devices on which the applicable monitor is enabled.

To select threshold devices:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.

- 4 Select the desired threshold type, then click **OK**. The dialog where you configure threshold properties appears.

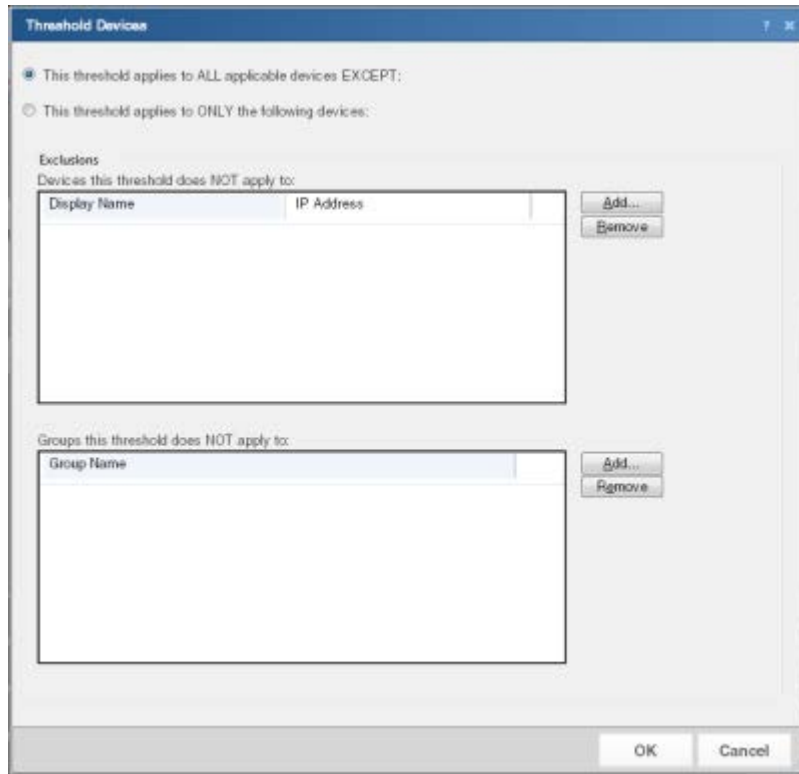


The image shows a dialog box titled "New CPU Utilization Threshold". It contains several sections for configuring a threshold:

- Name:** A text input field.
- Threshold:** A section with the text "This threshold will alert when:". It includes a dropdown menu for "CPU utilization" set to "exceeds", a text input for "90", and a percentage sign "%". Below this is another dropdown menu for "for more than" set to "30" and a dropdown menu for "minutes".
- Devices to Monitor:** A section with the text "Monitor all devices with CPU performance data by default". It features a button labeled "Select..." which is circled in red.
- Notification:** A section with a dropdown menu set to "(No policy)" and a button labeled "...".
- Threshold Check:** A section with the text "Check threshold every" followed by a text input set to "10" and the word "minutes.". Below this is a checkbox labeled "Automatically resolve items no longer out of threshold".

At the bottom of the dialog are "OK" and "Cancel" buttons.

- 5 In the **Devices to Monitor** section, click **Select**. The Threshold Devices dialog appears.



- 6 Select the devices to which the threshold will apply:
- To apply the threshold to all devices except for the device(s) or group of devices that you specify, select **This threshold applies to ALL applicable devices EXCEPT**. After you select this option, you will choose the devices to exclude from the threshold.
 - To apply the threshold to only the device(s) or group of devices that you specify, select **This threshold applies to ONLY the following devices**. After you select this option, you will choose the devices to include in the threshold.
- 7 Select the specific devices to include or exclude from the threshold.
- To specify a device to exclude or include in the threshold, in the upper section of the dialog, click **Add**.
 - To specify a group of devices to exclude or include in the threshold, in the lower section of the dialog, click **Add**.



Note: You can select Dynamic Groups.



Note: When you add a device group to the list of exceptions, all devices within the device group, as well as any sub-groups contained within the group (and devices in those sub-groups), are excluded from the threshold. Additionally, if you add a device group to the list of exceptions that contains a device shortcut, then that device is excluded from the threshold—even if that device is also a member of another group which is not part of the list of excluded groups.



Tip: To delete a device or device group from the list, select it, then click **Remove**.

- 8 Click **OK** to save changes.

Configuring performance thresholds

In This Chapter

| | |
|---|-----|
| Configuring performance thresholds | 753 |
| Configuring a CPU utilization threshold | 753 |
| Configuring a custom performance monitor threshold..... | 755 |
| Configuring a disk utilization threshold..... | 757 |
| Configuring an interface utilization threshold | 759 |
| Configuring an interface errors and discards threshold..... | 761 |
| Configuring a memory utilization threshold | 763 |
| Configuring a ping availability threshold | 765 |
| Configuring a ping response time threshold | 767 |

Configuring performance thresholds

Alert Center performance thresholds notify you about WhatsUp Gold performance monitors that have exceeded or dropped below threshold limits. You can create the following performance threshold types:

- *CPU* (on page 753)
- *Custom Performance Monitor* (on page 755)
- *Disk* (on page 757)
- *Interface* (on page 759)
- *Interface Errors and Discards* (on page 761)
- *Memory* (on page 763)
- *Ping Availability* (on page 765)
- *Ping Response Time* (on page 767)

Configuring a CPU utilization threshold

To configure a CPU utilization threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Performance CPU**, then click **OK**. The New/Edit CPU Utilization Threshold dialog appears.

New CPU Utilization Threshold

Name:

Threshold

This threshold will alert when:

CPU utilization %

for more than

Devices to Monitor

Monitor all devices with CPU performance data by default

Notification

Threshold Check

Check threshold every minutes.

☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when CPU utilization exceeds 90% for more than 30 minutes.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a custom performance monitor threshold

To configure a custom performance monitor threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Performance Custom**, then click **OK**. The New Custom Performance Monitor Threshold dialog appears.

New Custom Performance Monitor Threshold

Name:

Show: ☒ Global Monitors ☐ Device Specific Monitors

Custom performance monitor type:
 SNMP

| Global Monitor | Monitor Name |
|--|--------------|
| No global monitors of this type available... | |

Threshold
 This threshold will alert when the custom performance monitor's
 average value exceeds for more than minutes

Devices to Monitor
 Monitor all devices with this custom performance data by default.

Notification

Threshold Check
 Check threshold every minutes.
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Show.** Select either **Global Monitors** or **Device Specific Monitors** for the custom performance monitor type that you choose.
 - **Custom performance monitor type.** Select the custom performance monitor type from the menu. Select APC UPS, Printer, Active Script, SNMP, or WMI.

- **Monitor.** The configured monitors of the selected type. These are the monitors used to determine if the measured parameters have dropped below or exceeded threshold limits.



Note: When you select Global Monitors, this list is populated with custom performance monitors currently configured in the *Performance Monitor Library* (on page 247). When you select Device Specific Monitors, this list is populated with custom performance monitors currently configured for specific devices.

- **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the custom performance monitor average value exceeds 10 for 30 minutes.
- **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a disk utilization threshold

To configure a disk threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Performance Disk**, then click **OK**. The New/Edit Disk Utilization Threshold dialog appears.

New Disk Utilization Threshold

Name:

Threshold
The threshold will alert when:
disk utilization exceeds 95 %
for more than 1 days

Devices to Monitor
Monitor all devices with disk performance data by default

Notification
(No policy)

Threshold Check
Check threshold every 60 minutes.
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is exceeded when disk utilization exceeds 95% for more than 1 day.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold applies to all devices where the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database for items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold.

Configuring an interface utilization threshold

To configure an interface utilization threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Performance Interface**, then click **OK**. The New Interface Utilization Threshold dialog appears.

New Interface Utilization Threshold

Name:

Threshold
The threshold will alert when:

Devices to Monitor
Monitor all devices with interface performance data by default

Notification

Threshold Check
Check threshold every minutes
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the threshold criteria variables and values. The default threshold is configured to alert when inbound or outbound utilization exceeds 90% for more than 60 minutes.
 - **Devices to Monitor.** Click Select to choose the devices to which the threshold applies. By default, the threshold monitors all devices where the applicable monitor is enabled.

- **Notification.** Select the notification policy you would like to apply to this threshold. This policy kicks off when an item falls out of the threshold you configure above. If you do not see an appropriate threshold policy, or if the list is empty, browse (...) to the Notification Policy dialog to configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring an interface errors and discards threshold

To configure an interface utilization discard and error threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Performance Interface Errors and Discards**, then click **OK**. The New/Edit Interface Error and Discard Threshold dialog appears.

New Interface Error and Discard Threshold

Name:

Threshold
The threshold will alert when either:

☐ Discards for interface traffic
exceed discards per minute
for more than minutes

☐ Errors for interface traffic
exceed errors per minute
for more than minutes

Devices to Monitor
Monitor all devices with interface error and discard data by default

Notification
(No policy)

Threshold Check
Check threshold every minutes.
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.

- **Threshold.** Select and enter the threshold criteria variables and values. You can choose to create a threshold based on discards, errors, or a combination of the two. The default threshold is configured to alert when inbound or outbound interface utilization exceeds 100 discards per minute for more than 20 minutes.
- and / or -
when errors for inbound or outbound interface utilization exceeds 100 errors per minute for more than 20 minutes.



Note: If you select both error and discard thresholds, each error and discard are reported as separate items (rows) in the dashboard report.

- **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices where the applicable monitor is enabled.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters. The default threshold check is 10 minutes.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a memory utilization threshold

To configure a memory utilization threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Performance Memory**, then click **OK**. The New/Edit Memory Utilization Threshold dialog appears.

New Memory Utilization Threshold

Name:

Threshold
The threshold will alert when:

memory utilization exceeds 95 %

for more than 1 hours

Devices to Monitor
Monitor all devices with memory performance data by default

Notification
(No policy)

Threshold Check
Check threshold every 10 minutes
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when disk utilization exceeds 95% for more than 1 hour.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a ping availability threshold

To configure a ping availability threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Ping Availability**, then click **OK**. The New/Edit Ping Availability Threshold dialog appears.

New Ping Availability Threshold

Name:

Threshold
This threshold will alert when:
Ping availability average falls below 95 %
for more than 30 minutes

Devices to Monitor
Monitor all devices with ping availability performance data by default
Select...

Notification
(No policy)

Threshold Check
Check threshold every 3 minutes.
☐ Automatically resolve items no longer out of threshold

OK Cancel

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when ping availability average falls below 95% for more than 30 minutes.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold Check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a ping response time threshold

To configure a ping response time threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Ping Response Time**, then click **OK**. The New Ping Response Time Threshold dialog appears.

New Ping Response Time Threshold

Name:

Threshold
This threshold will alert when:
Ping Response Time average exceeds ms
for more than

Devices to Monitor
Monitor all devices with ping response time performance data by default

Notification
(No policy)

Threshold Check
Check threshold every minutes
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when ping response time average exceeds 2 ms for more than 30 minutes.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring passive thresholds

In This Chapter

| | |
|--|-----|
| Configuring passive thresholds..... | 770 |
| Configuring an SNMP trap threshold..... | 770 |
| Configuring a Syslog threshold..... | 772 |
| Configuring a Windows Event Log threshold..... | 774 |

Configuring passive thresholds

Alert Center passive thresholds notify you when WhatsUp Gold passive monitors fall out of the parameters of the thresholds you configure. You can create three passive threshold types:

- *SNMP trap* (on page 770)
- *Syslog* (on page 772)
- *Windows Event Log* (on page 774)

Several things to keep in mind when configuring thresholds for passive monitors:

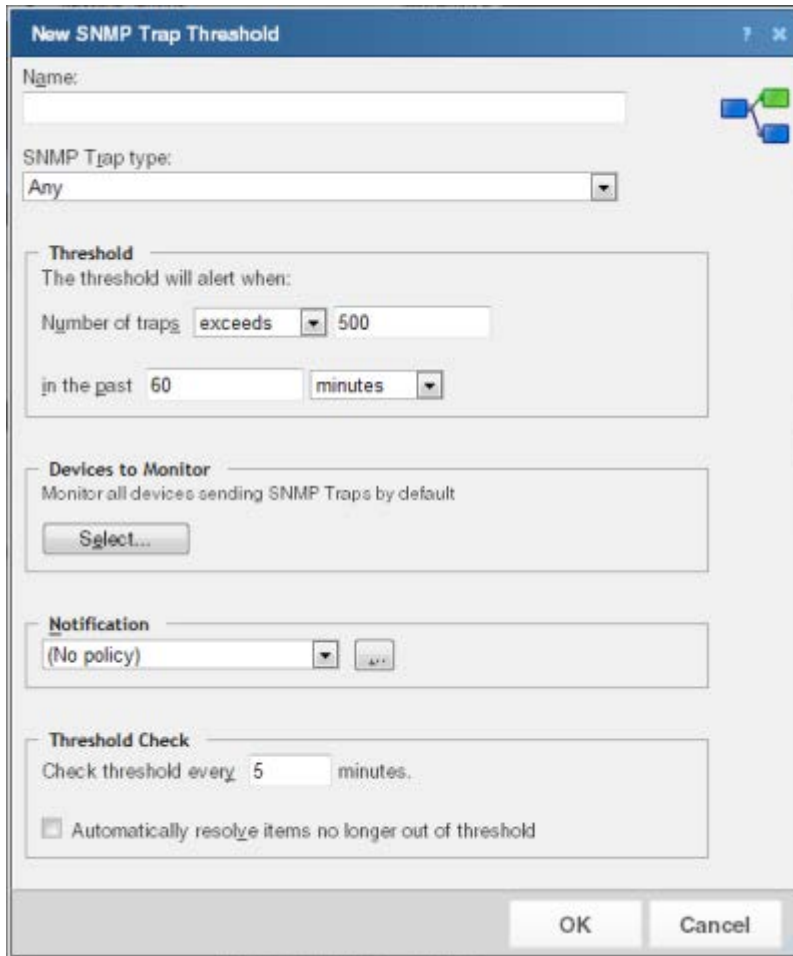
- Each Alert Center threshold is associated with a specific passive monitor. The passive monitor associated with the threshold you are creating must be assigned to at least one device. Otherwise, the threshold will not work.
- When creating a passive threshold, you must select a passive monitor from a list to associate with the threshold. This list contains the passive monitors already configured in the Passive Monitor Library. These monitors are not necessarily assigned to devices, however. To determine which devices have passive monitors assigned to them, you can create a dynamic group. For more information, see *Configuring Dynamic Groups* (on page 80).
- It is not possible to monitor unsolicited traps using Alert Center.

Configuring an SNMP trap threshold

To configure an SNMP trap threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.

- 4 Select **SNMP Trap**, then click **OK**. The New SNMP Trap Threshold dialog appears.

The image shows a Windows-style dialog box titled "New SNMP Trap Threshold". It contains several sections: "Name:" with a text input field; "SNMP Trap type:" with a dropdown menu currently set to "Any"; "Threshold" section with the text "The threshold will alert when:" followed by "Number of traps" (dropdown set to "exceeds"), a text input field with "500", and "in the past" (dropdown set to "60") followed by "minutes" (dropdown); "Devices to Monitor" section with the text "Monitor all devices sending SNMP Traps by default" and a "Select..." button; "Notification" section with a dropdown menu set to "(No policy)" and a small icon button; and "Threshold Check" section with the text "Check threshold every" followed by a text input field with "5" and "minutes", and a checkbox labeled "Automatically resolve items no longer out of threshold". At the bottom right are "OK" and "Cancel" buttons.

- 5 Specify or select the appropriate information in the dialog fields:
- **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **SNMP Trap type.** Select the SNMP trap type from the list that you want to associate with this threshold. The list is populated with SNMP traps currently configured in the Passive Monitor Library.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of traps exceeds 500 in the past 60 minutes.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters. By default, the threshold check is set to every five minutes.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a Syslog threshold

To configure a Syslog threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Syslog**, then click **OK**. The New Syslog Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Syslog type.** Select the Syslog monitor to use with the threshold. This list is populated with Syslog monitors currently configured in the Passive Monitor Library.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of messages exceeds 500 in the past 60 minutes.
 - **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a Windows Event Log threshold

To configure a Windows Event Log threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Windows Event Log**, then click **OK**. The Windows Event Log Threshold dialog appears.

New Windows Event Log Threshold

Name:

Windows Event Log type:

Threshold
The threshold will alert when:
Number of events
in the past

Devices to Monitor
Monitor all devices sending Windows events by default

Notification

Threshold Check
Check threshold every
☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Windows event type.** Select the Windows Event Log monitor to use with this threshold. The list is populated with Windows Event Log monitors currently configured in the Passive Monitor Library.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when the number of events exceeds 500 in the past 60 minutes.

- **Devices to Monitor.** Click **Select** to choose the devices to which the threshold applies. By default, the threshold monitors all devices on which the applicable monitor is enabled.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.
- 6 Click **OK** to save the threshold settings.

Configuring Flow Monitor thresholds

In This Chapter

| | |
|--|-----|
| Configuring Flow Monitor thresholds..... | 777 |
| Selecting Flow Monitor threshold hosts | 777 |
| Configuring a conversation partners threshold | 780 |
| Configuring a Flow Monitor Custom Threshold..... | 781 |
| Configuring a failed connections threshold | 783 |
| Configuring a Flow Monitor Interface Traffic threshold | 785 |
| Configuring a top sender/receiver threshold..... | 787 |

Configuring Flow Monitor thresholds

Alert Center Flow Monitor thresholds notify you on WhatsUp Gold Flow Monitor plug-in aspects that fall out of the parameters of the thresholds you create.

You can create five Flow Monitor threshold types:

- *Flow Monitor Conversation Partners* (on page 780)
- *Flow Monitor Custom Threshold* (on page 781)
- *Flow Monitor Failed Connections* (on page 783)
- *Flow Monitor Interface Traffic* (on page 785)
- *Flow Monitor Top Sender/Receiver* (on page 787)

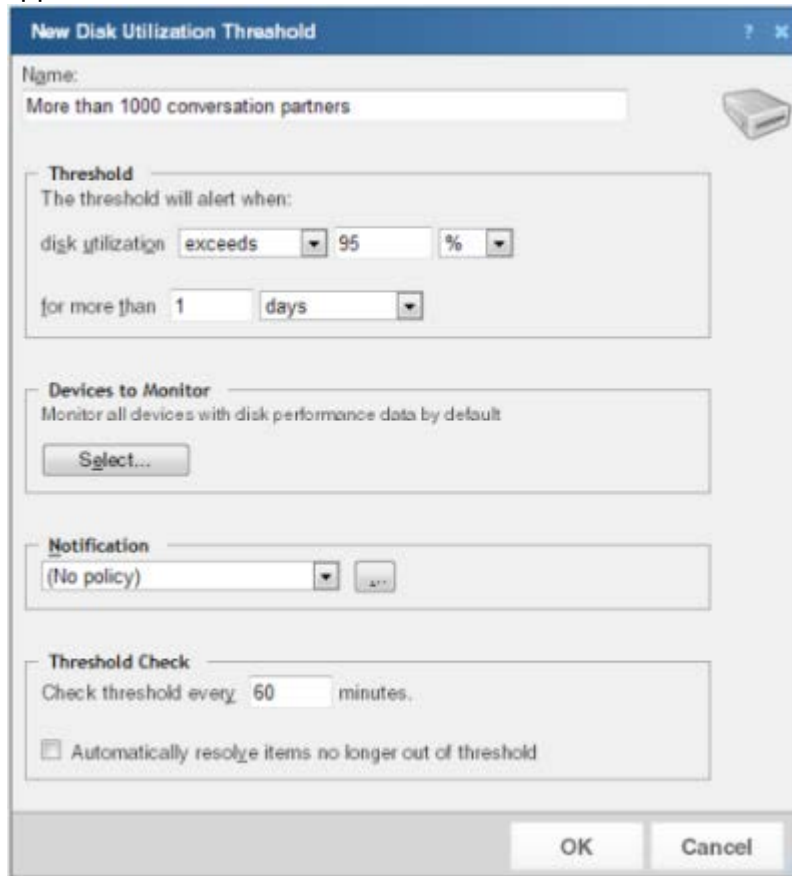
Selecting Flow Monitor threshold hosts

For each Flow threshold that you configure you can include a list of Flow Monitor groups, hosts, or a range of IP addresses to which the threshold will not apply.

To configure a list of Flow threshold exceptions:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.

- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select the desired Flow threshold type, then click **OK**. The threshold properties dialog appears.

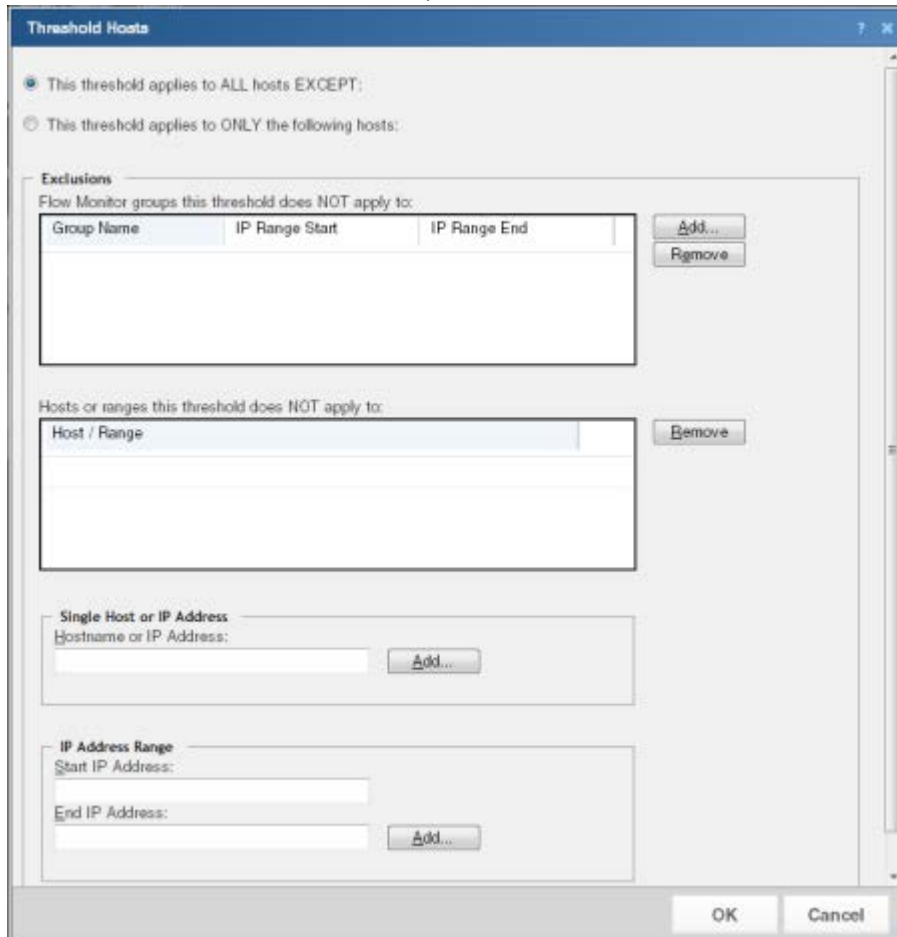


The image shows a Windows-style dialog box titled "New Disk Utilization Threshold". It contains several sections for configuring a threshold:

- Name:** A text field containing "More than 1000 conversation partners".
- Threshold:** A section with the text "The threshold will alert when:". It contains two rows of settings:
 - Row 1: "disk utilization" followed by a dropdown menu set to "exceeds", a text field with "95", and a dropdown menu set to "%".
 - Row 2: "for more than" followed by a text field with "1" and a dropdown menu set to "days".
- Devices to Monitor:** A section with the text "Monitor all devices with disk performance data by default" and a "Select..." button.
- Notification:** A section with a dropdown menu set to "(No policy)" and a small icon button.
- Threshold Check:** A section with the text "Check threshold every" followed by a text field with "60" and the word "minutes". Below this is a checkbox labeled "Automatically resolve items no longer out of threshold".

At the bottom right of the dialog are "OK" and "Cancel" buttons.

- 5 In the **Devices to monitor** section, click **Select**. The Threshold Hosts dialog appears.



The Threshold Hosts dialog box is shown with the following sections:

- Threshold Options:**
 - ☒ This threshold applies to ALL hosts EXCEPT:
 - ☐ This threshold applies to ONLY the following hosts:
- Exclusions:**

Flow Monitor groups this threshold does NOT apply to:

| Group Name | IP Range Start | IP Range End |
|------------|----------------|--------------|
| | | |

Buttons: Add..., Remove
- Hosts or ranges this threshold does NOT apply to:**

| Host / Range |
|--------------|
| |

Button: Remove
- Single Host or IP Address:**

Hostname or IP Address: Add...
- IP Address Range:**

Start IP Address: End IP Address: Add...

Buttons: OK, Cancel

- 6 Select the hosts to which the threshold applies.
- To apply the threshold to all hosts except the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ALL hosts EXCEPT**. After you select this option, you will choose the hosts to exclude from the threshold.
 - To apply the threshold to only the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ONLY the following hosts**. After you select this option, you will choose the hosts to include in the threshold.
- 7 Select the specific hosts to include or exclude from the threshold.
- To specify a Flow Group to include or exclude from this threshold, in the upper section of the dialog, click **Add**.



Tip: To delete a Flow group, host, or IP range from the list, select it, and then click **Remove**.

- To specify a single host or IP address to include or exclude from this threshold, enter a **Hostname or IP Address**, and then click **Add**.
 - To specify an IP address range to include or exclude from this threshold, enter a **Start IP Address** and an **End IP Address**, and then click **Add**.
- 8 Click **OK** to save changes.

Configuring a conversation partners threshold

To configure a Flow Monitor conversation partners threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Click the menu, select **Flow Conversation Partners**, and then click **OK**. The New Flow Conversation Partners Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when a host has sent to or received from more than 1000 conversation partners in the past 15 minutes.
 - **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a time interval for Alert Center to check the WhatsUp Gold database for items that are out of the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they return to the parameters inside the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a Flow Monitor Custom Threshold

To configure a Flow Monitor custom threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Flow Monitor Custom Threshold**, then click **OK**. The New Flow Monitor Custom Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Description.** As you configure threshold criteria settings, the description automatically updates to include your selections.
 - **Threshold.** Select the threshold filters and limits, and enter the values to use for each. You can define up to three filters for each Flow Monitor custom threshold.

An example threshold involving multiple filters could state, "This threshold will alert when any host with Protocol matching TCP and Application matching pop3 sent or received more than 100 MB of data in the past 15 minutes."

The default threshold time value is data in the past 15 minutes.

- **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.

When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.

By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a failed connections threshold

To configure a Flow failed connections threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Flow Monitor Failed Connections**, then click **OK**. The New Flow Monitor Failed Connections Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is exceeded when when a host has sent or received more than 1000 failed connections in the past 15 minutes.



Note: WhatsUp Gold Flow Monitor can only find failed connections on sources that are not sending sampled data.

- **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.



Note: Sources sending sampled data are not displayed as a selection option in the Traffic to monitor list because Flow Monitor cannot determine that traffic has failed on sampled data.

- **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold.

Configuring a Flow Monitor Interface Traffic threshold

To configure a Flow Monitor interface traffic threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Flow Monitor Interface Traffic**, then click **OK**. The New Flow Monitor Interface Traffic Threshold dialog appears.

New Flow Monitor Interface Traffic Threshold

Name:

Threshold
The threshold will alert when:

%

minutes

Traffic to monitor

Notification

Threshold Check
Check threshold every minutes.

☐ Automatically resolve items no longer out of threshold

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variables and values. The default threshold is configured to alert when incoming or outgoing interface traffic exceeds 90% for more than 60 minutes.
 - **Traffic to monitor.** Select the Flow Monitor sources from which to monitor traffic; all interfaces on a Flow source are monitored. By default, the threshold is set to monitor traffic from all Flow sources.

- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a top sender/receiver threshold

To configure a Flow Monitor top sender/receiver threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Flow Monitor Top Sender/Receiver**, then click **OK**. The New Flow Monitor Top Sender/Receiver Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields:
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select and enter the desired threshold criteria variable and values. The default threshold is configured to alert when a host has sent or received more than 500 MB in the past 15 minutes.
 - **Traffic to monitor.** Select the Flow Monitor source or interface from which to monitor traffic.
When you select a *source*, traffic for all interfaces on the source is monitored. When you select an *interface*, only traffic for the selected interface is monitored.
By default, the threshold is set to monitor traffic from all Flow Monitor sources.

- **Hosts to monitor.** Click **Select** to choose the hosts to which the threshold applies. By default, the threshold monitors all applicable hosts.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are out of the threshold's parameters. The default polling interval is 5 minutes.
- Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring system thresholds

In This Chapter

| | |
|--|-----|
| Configuring system thresholds | 790 |
| Configuring a Blackout Summary threshold | 790 |
| Configuring a VMware threshold | 792 |
| Configuring a Failover threshold | 794 |
| Configuring a WhatsUp Health threshold | 795 |

Configuring system thresholds

Alert Center system thresholds alert you on aspects of your WhatsUp Gold system according to the threshold parameters you configure. You can create four system threshold types:

- *Blackout Summary* (on page 790)
- *VMWare* (on page 792)
- *Failover* (on page 794)
- *WhatsUp Health* (on page 795)



Note: The thresholds listed in the Threshold Library may vary, depending on your WhatsUp Gold license.

Configuring a Blackout Summary threshold

To configure a Blackout Summary threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.

- 4 Select **Blackout Summary** from the menu, then click **OK**. The New/Edit Blackout Summary Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields:
- **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** The threshold alerts you when a blackout period has ended and an action would have been triggered by a passive monitor or state change.



Note: You cannot configure threshold criteria for the Blackout Summary threshold.

- **Devices to Monitor.** Click Select to select the devices to which the threshold applies. By default, the threshold applies to all devices. Use this dialog to select groups to which this threshold does not apply.
- **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.

- **Threshold check.** Enter a time interval for Alert Center to check the WhatsUp Gold database for actions that were not triggered because of a scheduled blackout period that has finished.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold settings.

Configuring a VMware threshold

To configure a VMware threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **VMware** from the menu, then click **OK**. The New/Edit Blackout Summary Threshold dialog appears.

- 5 Complete the fields with the appropriate information:
 - **Name.** Enter a name for the VMware threshold. The name entered here is displayed as the threshold's dashboard report title on the Alert Center Home page.
 - **Virtualization Events type.** Select the event type for which you want to create a threshold. The following options are available:
 - **All HA (High Availability) error events**
 - **All Virtual machine migration events**
 - **All security related events**
 - **Other events**



Note: When **Other events** are collected from the vCenter server, and you select **Other events** in the threshold configuration, you only see those events that were selected when event collection was configured in the Device Properties - Virtualization menu.



Note: For more information about event types and event type selection, see the Configure VMware event listener dialog help.

- 6 Select one of the following alert criteria:
 - **The threshold will alert immediately if an event occurred within the last Threshold Check of <Threshold_Check_Period> minutes.** Select this option if you want alerts to occur immediately when an event has occurred within the threshold check period, where <Threshold_Check_Period> is the value defined in the Threshold Check area of this dialog.
 - **The threshold will alert when:** Select this option if you want to define a number of events and time range for the threshold alert.
 - **Number of events** <exceeds_or_falls_below> <number>. Use this setting to configure the number of events of the selected event type that must be received before firing the alert, where <exceeds_or_falls_below> determines if the number should **Exceed** or **Fall Below** the threshold value, and <number> is the threshold value.
 - **in the past** <number> <unit_of_time>. Use this setting to configure the number and units of time that the threshold check should check for events, where <number> is the number of units of time, and <unit_of_time> is the unit of time.
- 7 Select the policy you want to apply to the threshold from the **Notification** box. Use the browse (...) button to access the Alert Center Notification Policies dialog. You can create new policies or edit existing policies from the Alert Center Notification Policies dialog.
- 8 Enter the number of minutes to wait between threshold checks in the **Threshold Check** area of the dialog.
- 9 Click **OK** when you have completed your configuration.

Configuring a Failover threshold

To configure a failover threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **Failover**, then click **OK**. The New Failover Threshold dialog appears.

- 5 Specify or select the appropriate information in the dialog fields.
 - **Name.** Specify a name for the threshold. This name helps you identify the threshold in the Threshold library and displays as the report title on the Alert Center Home page.
 - **Threshold.** Select the desired threshold criteria variables and values. You can configure the threshold to alert you when any event occurs, when an error occurs, or when an informational event occurs. By default, the threshold is configured to alert you when any event has occurred in Failover.
 - **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alert Center Home page.

- **Threshold check.** Enter a value for the threshold check interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items that are outside the threshold parameters.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 6 Click **OK** to save the threshold.

Configuring a WhatsUp Health threshold

To configure a WhatsUp Health threshold:

- 1 Click the **Alert Center** tab.
- 2 Click **Threshold Library**. The Alert Center Threshold Library dialog appears.
- 3 Click **New**. The Select Threshold Type dialog appears.
- 4 Select **WhatsUp Health**, then click **OK**. The New WhatsUp Health Threshold dialog appears.

New WhatsUp Health Threshold

Name:

Threshold

This threshold will alert when:

- ☒ Database size exceeds % (Size limit: 4 GB)
- ☒ Total performance monitors exceed
- ☒ Total performance monitor records exceed
- ☒ Total passive monitor records exceed
- ☒ Total expired records exceed
- ☒ Total devices being monitored exceeds % of license limit

View WhatsUp database

Database Services Flow Monitor

Notification

(No policy)

Threshold Check

Check threshold every minutes.

☐ Automatically resolve items no longer out of threshold

OK **Cancel**

- 5 Enter a **Name** for the threshold. This name is displayed as the threshold dashboard report title on the Alerts Home page.
- 6 Click the **Database** tab. Enter the appropriate threshold information:
 - **Database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the database size exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- **Total performance monitors exceed ____.** Select this option to have the threshold alert when the total number of performance monitors exceeds the number you specify. The default number of total performance monitors is 3,000.
- **Total performance monitor records exceed ____.** Select this option to have the threshold alert when the total number of performance monitor records exceeds the number you specify. The default number of total performance monitor records is 2,000,000.
- **Total passive monitor records exceed ____.** Select this option to have the threshold alert when the total number of passive monitor records exceeds the number you specify. The default number of total passive monitor records is 1,000,000.
- **Total expired records exceed ____.** Select this option to have the threshold alert when the total number of expired records exceeds the number you specify. The default number of total expired records is 500,000.
- **Total devices being monitored exceeds ____ % of license limit.** Select this option to have the threshold alert when the total number of devices being monitored exceeds the percentage of the license limit you specify. The default percentage of the license limit is 90%.



Tip: Click **View WhatsUp database** to view a graph of the current WhatsUp database usage.

- 7 Click the **Services** tab. Enter the appropriate threshold information:
 - **WhatsUp polling service is down ____ minutes.** Select this option to have the threshold alert when the WhatsUp service has been down for the number of minutes you specify. The default threshold value is 5 minutes.
 - **WhatsUp polling service SQL queries exceed ____ ms on average.** Select this option to have the threshold alert when SQL queries exceed the number of ms on average that you specify. The default number is 750 ms.
 - **WhatsUp discovery service is down ____ minutes.** Select this option to have the threshold alert when the WhatsUp discovery service is down the number of minutes that you specify. The default number is 5 minutes.



Note: Web service threshold checks do not apply to users running IIS.



Note: If you are experiencing a high volume of errors from your WhatsUp Health threshold service checks, please see Troubleshooting the WhatsUp Health Threshold.

- 8 Click the **Flow Monitor** tab. Enter the appropriate threshold information pertaining to the WhatsUp Gold Flow Monitor.
 - **Netflow database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the Netflow database exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- **NfArchive database size exceeds ____ %/GB/MB.** Select this option to have the threshold alert when the NfArchive database size exceeds the value you specify. The default threshold value is 80%.



Note: If you have an unlimited-size database, WhatsUp Gold uses a 4GB cap to calculate the size of your database.

- **Flow collector service is down ____ minutes.** Select this option to have the threshold alert when the Flow collector service is down for the number of minutes you specify. The default threshold value is 5 minutes.
- **Any bounce traffic occurs.** Select this option to have the threshold alert when bounce traffic occurs on a Flow Monitor source.
- **Host records exceed ____.** Select this option to have the threshold alert when the number of host records exceeds the amount you specify. The default threshold value is 2,000,000 records.
- **Raw, hourly, or daily records exceed ____.** Select this option to have the threshold alert when the number of raw data records exceeds the amount you specify. The default threshold value is 10,000,000 records.
- **Total sources sending data exceeds ____ % of license limit.** Select this option to have the threshold alert when the total sources sending data exceeds the percentage of license limit that you specify. The default threshold value is 90% of license limit.



Tip: Click View Netflow database usage to view a graph of the current Netflow database usage. Click View NfArchive database usage to view a graph of the current NfArchive database usage.

- 9 After selecting the desired options for each tab and entering the appropriate threshold variables and values, specify your choices for the Notification and Polling sections of the dialog.
 - **Notification.** Select the notification policy to apply to this threshold. This policy begins sending notifications when an item is outside the configured threshold limits. If you do not see an appropriate threshold policy, or if the list is empty, click browse (...) to open the Notification Policy dialog and configure a new policy.



Note: Notification policies are optional for most thresholds. If you do not select a notification policy, no notifications are generated for the threshold, but a dashboard report listing the out of threshold items still appears on the Alerts Home page.

- **Threshold check.** Enter a value for the polling interval, or the interval at which the Alert Center checks the WhatsUp Gold database to see if there are items out of the threshold's parameters. The default polling interval is 5 minutes.
Select **Automatically resolve items no longer out of threshold** to have Alert Center automatically resolve items when they go back inside the parameters of the threshold.



Note: Configure the threshold check interval for a longer time than the sampling interval for thresholds relating to trends, such as percent utilization. Configure it for a time the same as (or similar to) the sampling interval when configuring a threshold for a health check.

Avoid setting the threshold check interval to a very short time as this can degrade system performance. In general, setting the threshold check interval to less than five minutes is inadvisable.

- 10 Click **OK** to save the threshold settings.

Notification Policy Graph View

This graph displays a visual representation of the notification policy you are configuring on the *New/Edit Notification Policy* (on page 734) dialog.

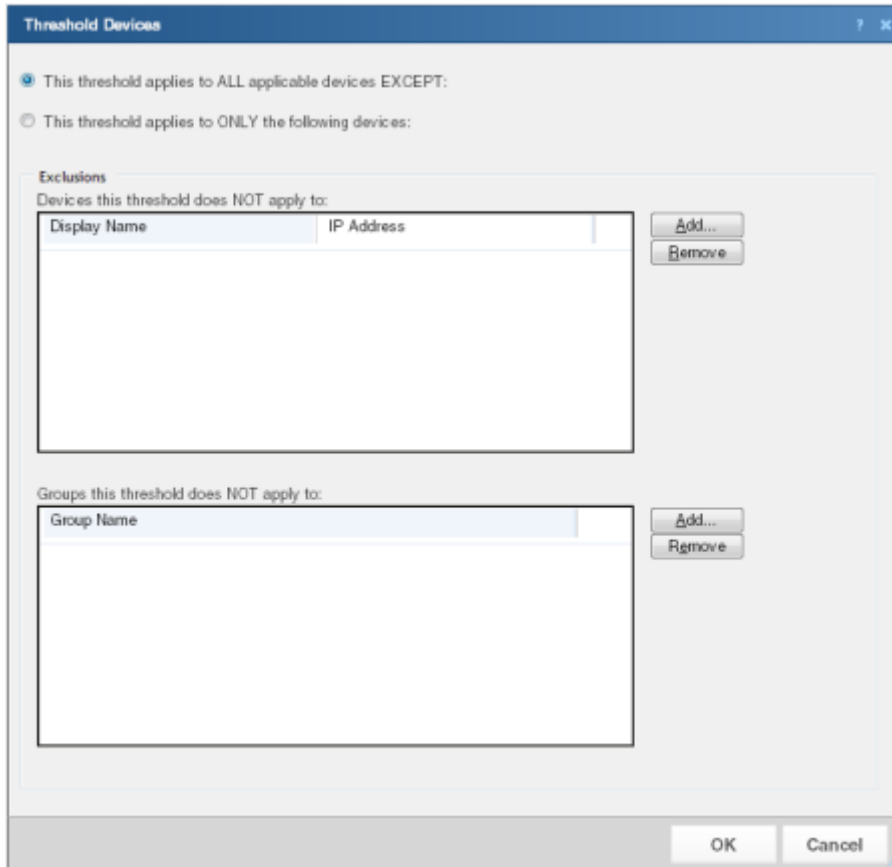


The y (vertical) axis displays the email notifications that are sent for each step of the policy. The x (horizontal) axis displays the time each policy step executes.

Click **Return** to go back to the New/Edit Notification Policy dialog.

Threshold Devices

Use this dialog to specify the devices or device groups to which an Alert Center threshold does or does not apply.



The dialog box is titled "Threshold Devices". It contains two radio buttons at the top: "This threshold applies to ALL applicable devices EXCEPT:" (selected) and "This threshold applies to ONLY the following devices:". Below the first radio button is a section titled "Exclusions" with the text "Devices this threshold does NOT apply to:". It contains a table with two columns: "Display Name" and "IP Address". To the right of the table are "Add..." and "Remove" buttons. Below the table is a section titled "Groups this threshold does NOT apply to:" with a table containing a "Group Name" column. To the right of this table are also "Add..." and "Remove" buttons. At the bottom of the dialog are "OK" and "Cancel" buttons.

- To apply the threshold to all devices except for the device(s) or group of devices that you specify, select **This threshold applies to ALL applicable devices EXCEPT**. After you select this option, you will choose the devices to exclude from the threshold.
- To apply the threshold to only the device(s) or group of devices that you specify, select **This threshold applies to ONLY the following devices**. After you select this option, you will choose the devices to include in the threshold.
- To specify a device to exclude or include in the threshold, in the upper section of the dialog, click **Add**.
- To specify a group of devices to exclude or include in the threshold, in the lower section of the dialog, click **Add**.



Note: When you add a device group to the list of exceptions, all devices within this device group, as well as any sub-groups contained within the group (and devices in those sub-groups), are excluded from, or include in the threshold. Additionally, if you add a device group to the list of exceptions that contains a device shortcut, then that device is excluded from the threshold—even if that device is also a member of another group which is not part of the list of excluded groups.



Tip: To delete a device or device group from the list, select it, then click **Remove**.

Alert Center Item Details

Use this dialog to view the details of and to update an item that is out of the parameters of an Alert Center threshold.

The **Item details** area includes the following information:

- **Aspect** lists the specific device aspect on which the item has gone out of threshold. For example, the specific CPU or interface.
- **Value** displays the length of time in which the service has met the threshold parameters.
- **Current state** lists the state of the item; can be either *Out of threshold*, *In threshold*, or *Disabled*.
- **Notification progress** lists the current step of the applied notification policy.
- **Created on** lists the time the Alert Center initially found the item out of threshold.
- **Last updated** lists the most recent time the item was updated. This item does not appear unless the item has been previously updated.

To update item(s)

- 1 From the list, select how you would like to update the item(s).
 - **Acknowledge.** Select to indicate that the issue with the item is known. Alert Center continues to send any related notifications regarding the item. The item continues to appear in the dashboard report.
 - **Resolve.** Select to indicate that any actions required to address the item are complete. Notifications regarding the item stop. The item is removed from the dashboard report.
- 2 Select the item(s) to which you would like to apply the update. Options include:
 - **Apply to this item.** Select this option to update only the currently viewed item.
 - **Apply to any items created at the same time as this item.** Select this option to apply the update to any matching items that were created during the same poll.
 - **Apply to any items older than ____ hours/minutes/days.** Select this option to apply the update to all alerts older than the time you select. This option is useful when one device fails and impacts numerous other devices, such as when attempting to ping devices on the other side of a failed router. Selecting to resolve all items that were added at the same time as the router failure saves the time it would otherwise take to acknowledge each item individually.
 - **Apply to all items in this threshold.** Select this option to update any items that currently exist for this threshold.


- 3 After selecting the appropriate update, enter a brief **Update comment** that explains what was done to take care of the problem.



Note: It is not required that you enter an explanatory comment, though we suggest that you do so for record keeping purposes.

- 4 Click **OK** to save changes.



Note: Items that have been acknowledged display a green check mark  next to their name on Alert Center Home threshold dashboard reports.

Netflow database record types

This graph displays the Netflow database tables by number of records, gathered over the sample time period.

The top database tables are displayed, along with the number of records existing for each.



Tip: Mouse over a table bar to view the number of records for that table.

Click **Return** to go back to the WhatsUp Health Threshold dialog.

Reducing the WhatsUp database size

The first step to troubleshooting a large WhatsUp database is to identify which table or tables are consuming the bulk of the used database space. To do this, open the WhatsUp Database tables by size home dashboard report (accessible from the WhatsUp Gold Home tab, click **Add Content > General > Database Table Usage**) and note the tables that are consuming the most space. A list of common large database tables is listed below. Click on a table name for more information on how to reduce that table.

PassiveMonitorActivityLog (on page 827)

StatisticalInterface (on page 819)

ActiveMonitorStateChangeLog (on page 818)



Tip: You can use the Alert Center to set database threshold alerts for WhatsUp Gold and Flow Monitor. For more information, see *Configuring a WhatsUp Health threshold* (on page 795).

Reducing the number of raw, hourly, or daily data records

This threshold is designed to alert you to a potential performance problem in the Flow Monitor caused by a large quantity of flow data. This can happen if your flow-enabled sources are sending large numbers of flows to you, or you are keeping flow data for long periods of time. As more data is kept in Flow Monitor's databases, you may encounter performance problems, or even timeouts, when loading Flow Monitor reports. Consider reducing the **Report Data** settings for Flow Monitor on the Flow Monitor Settings dialog (click the **Flow Monitor** tab, then click **Settings**), or even moving to a SQL Server with greater resource capacity. For more information, see the WhatsUp Gold Database Migration Guide on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/wugtechsupport>).

Reducing the number of host records

This threshold is designed to alert you to a potential performance problem in Flow Monitor. As Flow Monitor receives flow information from your network devices, the IP addresses of traffic senders and receivers are recorded in WhatsUp. If your systems communicate with a large variety of hosts, this can cause the table which contains these IP addresses to become large. For example, if you have NetFlow enabled on the public interface of your border firewall, potentially you could receive traffic from a large portion of Internet hosts. This could cause the number of recorded hosts seen in Flow Monitor to be very high.

In some cases, changing the interfaces from which you receive flow information can help (such as only sending flow information from the private side of the firewall instead of the public), but moving to a SQL instance with greater resource capacity can also improve performance. For more information, see the WhatsUp Gold Database Migration Guide on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/wugtechsupport>).

Restarting the Flow Collector service

If the WhatsUp Health Threshold reports that the Flow Collector Service has stopped, you must restart the Ipswitch Flow Collector service. This service must be running at all times in order for your network devices to send flow information to WhatsUp. For more information, see *Stopping or restarting the collector*.

If this service has stopped unexpectedly, it may have crashed. To assist Technical Support in locating the source of the failure, please perform the following:

- 1 Open the Windows Event Viewer from Administrative Tools or the Computer Management console.
- 2 Locate an Error entry with BWCollector.Net.exe listed as the Source.
- 3 Use the Technical Support request form on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/support/technical-support.aspx>) to submit the details of this error, along with the version of Windows installed on the WhatsUp computer, including any service pack and CPU architecture (32-bit or 64-bit). Please also include the version of WhatsUp Gold installed. You can find version information on the WhatsUp Gold About box (on the WhatsUp Gold console at **Help > About**).

Reducing performance monitors

This option examines the number of performance monitors applied to devices in WhatsUp Gold. There are several issues that can arise if you have too many performance monitors assigned to your WhatsUp Gold devices.

- More database space is needed to store the monitor configuration as well as the data collected from polling.
- Increased CPU and memory usage from both the WhatsUp Gold and SQL processes during polling.
- Increased network resource usage during polling, increasing the change for packet loss and latency issues.
- Polling delays; for example, devices not being polled on schedule because there are other monitors in the task queue.

Consider reducing the number of Performance Monitors applied to your WhatsUp devices or increasing the polling interval for less-critical performance monitors.

WhatsUp discovery service is down

If the WhatsUp Health Threshold reports that the WhatsUp discovery service is down, you need to restart the Ipswitch Discovery service. This service must be running at all times to allow devices to be discovered and for scheduled discoveries run. If this service has stopped unexpectedly, it may have crashed. To assist Technical Support in locating the source of the failure, please perform the following task:

- 1 Open the Windows Event Viewer from Administrative Tools or the Computer Management console.
- 2 Locate an Error entry with DiscoveryService.exe listed as the Source.
- 3 Use the Technical Support request form on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/support/technical-support.aspx>) to submit the details of this error, along with the version of Windows installed on the WhatsUp computer, including any service pack and CPU architecture (32-bit or 64-bit). Please also include the version of WhatsUp Gold installed. You can find version information on the WhatsUp Gold About box (on the WhatsUp Gold console at **Help > About**).

WhatsUp web service SQL queries exceed threshold

If the WhatsUp Health Threshold reports that the WhatsUp web service SQL queries have exceeded the threshold number, there are several steps you can take to resolve the problem, dependent on the SQL database you are using.

If you are using the default SQL Express database included with WhatsUp Gold:

- Ensure that a full 1 GB of memory is available to the SQL Server process.



Note: SQL Server Express is limited to 1 GB of memory and 1 CPU.

- Defragment the SQL Server data directory hard-drive.

If the WhatsUp database file becomes fragmented, this can decrease database performance. Before defragmenting, you need to stop the WhatsUp services and applications as well as the SQL Server services to allow defragmentation utilities to operate on SQL's database files.

- Move the WhatsUp Gold database files.

If you have a hard drive on a separate disk from your operating system drive, you can improve file performance by relocating the WhatsUp database files to this separate hard drive.



Note: Moving files between different partitions on the same hard drive will not increase file system performance.

- Install a faster hard drive.

Because SQL Express does not benefit from memory improvements (beyond the 1GB limit), increasing file I/O performance provides a decrease in SQL statement execution time.

If you are using a non-default SQL configuration, such as SQL Standard installed on another computer:

- Add additional memory.

The single biggest performance improvement available to any database application is additional memory.



Important: Be sure to consider the memory limitation of the edition of SQL you have installed as well as any limitations imposed by the operating system.

- Reduce resource contention.

If the WhatsUp database is located in a SQL instance shared by other databases, WhatsUp has to compete with other applications for database resources. Consider moving WhatsUp Gold's databases to a dedicated SQL instance.

- Improve network efficiency.

If SQL is installed on a remote computer, ensure that network traffic between the WhatsUp application and the SQL Server is optimized. This includes both packet loss and latency between the WhatsUp computer and the SQL Server.



Note: If you are using IIS as your web server, this counter will not report results.

WhatsUp web service is down

If the WhatsUp Health Threshold reports that the WhatsUp web service is down, you need to restart the Ipswitch WhatsUp Web Server. This service must be running at all times to allow access to report data and the WhatsUp web interface. If this service has stopped unexpectedly, it may have crashed. To assist Technical Support in locating the source of the failure, please perform the following:

- 1 Open the Windows Event Viewer from Administrative Tools or the Computer Management console.
- 2 Locate an Error entry with `NMWebService.exe` listed as the Source.
- 3 Use the Technical Support request form on the *WhatsUp Gold* web site (<http://www.whatsupgold.com/support/technical-support.aspx>) to submit the details of this error, along with the version of Windows installed on the WhatsUp computer, including any service pack and CPU architecture (32-bit or 64-bit). Please also include the version of WhatsUp Gold installed. You can find version information on the WhatsUp Gold About box (on the WhatsUp Gold console at **Help > About**).



Note: Even if you are using IIS as your web server, the Ipswitch Web Server\$WhatsUp service should still be started. Be sure to disable the web server via its configuration dialog in Program Options.

Related Topics

Managing Services using the WhatsUp Services Controller880

WhatsUp web service HTTP responses exceed threshold

This threshold measures the amount of time elapsed between an incoming HTTP request and the completion of the request back to the browser. It does not account for any time required by the browser to render the information returned from the web server. While the largest factor in response time is the database query itself, there may be other issues which are negatively impacting performance. To isolate whether a slow response time from the WhatsUp web interface is because of database latency, follow these steps first:

Windows Vista

- 1 On the WhatsUp computer, from open the Reliability and Performance Monitor (perfmon.exe) (**Control Panel > System and Maintenance > Performance and Information Tools > Advanced Tools** - or - run `perfmon.exe`).
- 2 From the left side of the dialog, select Performance Monitor. The Performance Monitor appears.
- 3 Below the graph, clear the selection of any default counters, then click the Add Counter (+) button on the toolbar. The Add Counters dialog appears.
- 4 From the list of **Available counters**, scroll to *Ipswitch Web Server* and expand the counter.
- 5 Select *AvgHttpRespTimeMilliSecs*, then click **Add** to add the counter to the list of **Added counters**.
- 6 Select *AvgSqlExecTimeMs*, then click **Add** to add the counter to the list of **Added counters**.
- 7 Click **OK** to add these counters to the Performance Monitor graph.

Windows XP or 2003

- 1 On the WhatsUp computer, open the Performance tool (perfmon.exe) (**Control Panel > Administrative Tools** - or - run `perfmon.exe`).
- 2 Remove any default counters by selecting the counters and then clicking the Delete (X) button on the toolbar.
- 3 Click the Add Counter (+) button on the toolbar. The Add Counters dialog appears.
- 4 From **Performance Object** list, select *Ipswitch Web Server*.
- 5 Select the **Select counters from list**.
- 6 Select *AvgHttpRespTimeMilliSecs*, then click **Add**.
- 7 Select *AvgSqlExecTimeMs*, then click **Add**.
- 8 Click **Close**.

Next, perform the web interface request that is performing poorly and note its effect on these counters. You have to wait for the page to completely load for its results to be display here. Similar values between the counters likely indicate a SQL query performance problem. See (***) link to the below "web service SQL queries exceed topic (***) for information on investigating this issue.

If the problem is not database performance, here are some items to examine:

- Configure antivirus applications.

Many antivirus applications install "script scanning" components to ensure that malicious script-based malicious software cannot be executed. In order to display web page content, we load a script host in our web server process. When processing web pages and requests, we must wait for the antivirus application to scan the contents before we can deliver the page to the requesting browser. Consider disabling the scanning of our script engine component. For more information, contact your antivirus software vendor.

- Eliminate packet loss.

Ensure that any packet loss between the WhatsUp computer and the browser is kept to a minimum.

- Decrease network latency.

Ensure that any latency between the WhatsUp computer and the browser is kept to a minimum.

- Bypass proxy servers.

Web application responsiveness improves if the traffic can pass directly from the web server to the browser and vice versa. Routing the requests and responses through a proxy server will result in slower load times for pages.



Note: If you are using IIS as your web server, this counter will not report results.

WhatsUp polling service SQL queries exceed threshold

If the WhatsUp Health Threshold reports that the WhatsUp polling service SQL queries have exceeded the threshold number, there are several steps you can take to resolve the problem, dependent on the SQL database you are using.

If you are using the default SQL Express database included with WhatsUp Gold:

- Ensure that a full 1 GB of memory is available to the SQL Server process.



Note: SQL Server Express is limited to 1 GB of memory and 1 CPU.

- Defragment the SQL Server data directory hard-drive.

If the WhatsUp database file becomes fragmented, this can decrease database performance. Before defragmenting, you need to stop the WhatsUp services and applications as well as the SQL Server services to allow defragmentation utilities to operate on SQL's database files.

- Move the WhatsUp Gold database files.

If you have a hard drive on a separate disk from your operating system drive, you can improve file performance by relocating the WhatsUp database files to this separate hard drive.



Note: Moving files between different partitions on the same hard drive will not increase file system performance.

- Install a faster hard drive.

Because SQL Express does not benefit from memory improvements (beyond the 1GB limit), increasing file I/O performance provides a decrease in SQL statement execution time.

If you are using a non-default SQL configuration, such as SQL Standard installed on another computer:

- Add additional memory.

The single biggest performance improvement available to any database application is additional memory.



Important: Be sure to consider the memory limitation of the edition of SQL you have installed as well as any limitations imposed by the operating system.

- Reduce resource contention.

If the WhatsUp database is located in a SQL instance shared by other databases, WhatsUp has to compete with other applications for database resources. Consider moving WhatsUp Gold's databases to a dedicated SQL instance.

- Improve network efficiency.

If SQL is installed on a remote computer, ensure that network traffic between the WhatsUp application and the SQL Server is optimized. This includes both packet loss and latency between the WhatsUp computer and the SQL Server.

WhatsUp polling service is down

If you the WhatsUp Health Threshold reports that your WhatsUp polling service is down, you need to restart the Ipswitch WhatsUp Engine service. This service must be running at all times so that polling of your network devices and alerting can take place. If this service has stopped unexpectedly, it may have crashed. To assist Technical Support in locating the source of the failure, please perform the following task:

- 1 Open the Windows Event Viewer from Administrative Tools or the Computer Management console.
- 2 Locate an Error entry with NMService.exe listed as the Source.
- 3 Use the Technical Support request form on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/support/technical-support.aspx>) to submit the details of this error, along with the version of Windows installed on the WhatsUp computer, including any service pack and CPU architecture (32-bit or 64-bit). Please also include the version of WhatsUp Gold installed. You can find version information on the WhatsUp Gold About box (on the WhatsUp Gold console at **Help > About**).

Troubleshooting the WhatsUp Health Threshold

If you are encountering errors in the Alert Center Log after configuring and running the WhatsUp Health Threshold's service checks, there are several steps you can take to troubleshoot the occurrence of these errors.

First, from a CMD window, run the following commands:

Windows XP and later

```
wmiadap/clearadap
```

```
wmiadap/resyncperf
```

Windows 2000

```
winmgmt/clearadap
```

```
winmgmt/resyncperf
```



Note: These commands may take some time to execute.

If after running these commands the errors persists, run the Microsoft WMI Diagnosis Utility, found on Microsoft's web site:

<http://www.microsoft.com/downloads/details.aspx?familyid=d7ba3cd6-18d1-4d05-b11e-4c64192ae97d&displaylang=en>

Terminal Services

Additionally, you may encounter problems with your service-level threshold checks if you are using Microsoft Terminal Services (Remote Desktop Services) to run the WhatsUp Gold web server. If more than one person is logged in to Terminal Services at a time, the following WhatsUp Health Threshold service checks/performance counters may fail:

- WhatsUp polling service SQL query check
- WhatsUp web service HTTP response check
- WhatsUp web service SQL query check

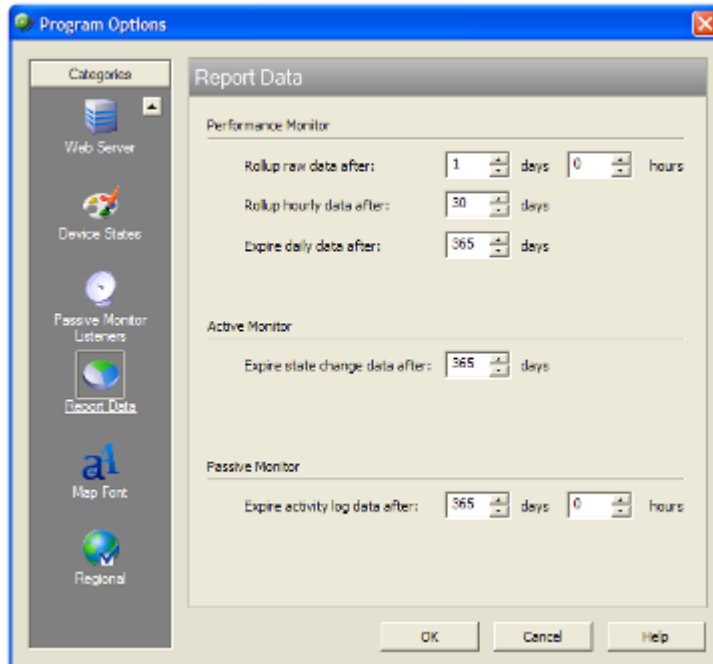
You may experience a high volume of errors logged to the Alert Center Log from these service checks until the number of Terminal Service users drops to one or none.

Changing how long report data is stored

Data is stored in the WhatsUp Gold database to populate the performance reports available in the application.

To configure WhatsUp Gold report data:

- 1 From the main menu, select **Configure > Program Options**.
- 2 In Program Options, select **Report Data**.



- 3 In the Report Data section, you can change the data settings for performance monitors, active monitors, and passive monitors.
- 4 Click **OK** to save the changes.

You can see how many rows in the database that the data takes up by viewing the numbers under the time settings.

Reducing passive monitor records

The PassiveMonitorActivityLog table stores Passive Monitor data collected by SNMP Trap, Syslog, and Windows Event Log monitoring.

When WhatsUp Gold collects large quantities of unnecessary or unwanted passive monitor data, a very large table can result.

- 1 Verify Passive Monitor Listener configuration.
The first step is to ensure you are only collecting data for passive monitors you have explicitly configured for your devices. To do this, ensure that for the both the SNMP Trap Listener and the Syslog Listener, you are not accepting unsolicited messages. You can verify this configuration in Program Options.

To verify Passive Monitor Listener configuration:

- 1 From the main menu of the WhatsUp Gold console, select **Configure > Program Options**. The Program Options dialog appears.
 - 2 Click **Passive Monitor Listeners**. The Program Options - Passive Monitor Listeners dialog appears.
 - 3 Select **SNMP Trap**, then click **Configure**. The SNMP Listener Configuration dialog appears.
 - 4 Ensure that **Accept unsolicited SNMP Traps** is not selected, then click **OK**. The Program Options - Passive Monitor Listeners dialog appears.
 - 5 Select **Syslog**, then click **Configure**. The Syslog Listener Configuration dialog appears.
 - 6 Ensure that **Accept unsolicited passive monitors** is not selected, then click **OK**. The Program Options - Passive Monitor Listeners dialog appears.
 - 7 Click **OK** to exit Program Options.
- 2 Remove unnecessary data from the database
- After you tell WhatsUp Gold to collect data from only passive monitors that are assigned to devices, the next step is to clear the unneeded data already collected from the database.
- This can be done in one of two ways.
- The fastest way is to remove all passive monitor data collected by the application. This removes all passive monitor data that appears in the *SNMP Trap Log* (on page 692), *Syslog Entries* (on page 693), and *Windows Event Log* (on page 696) reports. Any actions triggered by an incoming passive monitor event will still appear in the *Action Log* (on page 687).



Important: We recommend making a backup of your WhatsUp Gold database should you need to reverse any of the following changes.

To remove all passive monitor data from the WhatsUp database:

- 1 Stop all Ipswitch services and applications:
 - Ipswitch WhatsUp Engine
 - Ipswitch Web Server\$WhatsUp
 - Ipswitch Discovery
 - Ipswitch Alert Center
 - Ipswitch Flow Collector

- 2 From a command prompt on the WhatsUp Gold computer, execute the following case-sensitive command on a single line:

```
>sqlcmd -E -S  
"%COMPUTERNAME%\WHATSUP" -Q "TRUNCATE TABLE  
[WhatsUp].[dbo].[PassiveMonitorActivityLog]"
```



Note: Replace %COMPUTERNAME% with the name of the WhatsUp Gold computer.

The command listed above assumes you are using the SQL Server 2005 Express Edition database that is installed with WhatsUp Gold. If you are using an alternate database configuration, contact your database administrator to determine what information should be included with the "-S" switch.

After you have removed all the Passive Monitor data from the WhatsUp database, you can optionally shrink the WhatsUp database files to reclaim disk space on the SQL server.

To shrink the WhatsUp Gold database:

- 1 Ensure that all of the Ipswitch service and applications listed above are still stopped.
- 2 From a command prompt on the WhatsUp computer, execute the following case-sensitive command on a single line:

```
>sqlcmd -E -S "%COMPUTERNAME%\WHATSUP" -Q "DBCC SHRINKDATABASE  
( 'WhatsUp' , 20 )"
```



Note: Replace %COMPUTERNAME% with the name of the WhatsUp Gold computer.

The database shrink could take quite some time depending on the size of the database and system resources, but reports a short database space analysis after completion.



Note: You can abort the shrink process at any time by using the [CTRL] + [C] keystroke sequence.

More information on the "DBCC SHRINKDATABASE" command can be found on Microsoft's web site at:

<http://msdn.microsoft.com/en-us/library/ms190488.aspx>



Important: After you reclaiming database space, you should examine your passive monitors' configuration. You can do this easily by viewing the the *Total Passive Monitors by Type* (on page 443) dashboard report (available on any Home dashboard), and the system-level *SNMP Trap Log* (on page 692), *Syslog Entries* (on page 693), and *Windows Event Log* (on page 696) reports. If you have passive monitors assigned to "talkative" devices, or you have monitors which are not exclusive enough in their search criteria assigned to your WhatsUp devices, you may re-encounter this problem as more passive monitor data is collected by the system.

Reducing expired records

This option examines the number of expired in the performance monitor data tables. An expired record is defined as a record which is marked as overwritable, but has yet to be overwritten by a new record. Typically, the percentage of expired records to total records is small (less than 10%); if a large configuration change is made (some examples are below), the ratio of expired records may be different. In practice, we recommend this ratio not exceed 25% for any of the performance monitor tables (see below). You can purge all expired records for a given performance monitor table from the Table Maintenance property page in the Database Tools dialog. For more information, see the *Database Tools - Database Maintenance* (on page 814) dialog help.

Example changes:

- Removing a 400-port switch from WhatsUp Gold that was collecting Interface Utilization performance monitor data.
- Changing **Keep hourly data** from 30 days to 14 days. For more information, see *Changing how long report data is stored* (on page 810) and the *Program Options - Report Data* (on page 815) dialog help.

Performance monitor data tables:

This part of the WhatsUp Health Threshold checks these specific database tables when looking for expired records.

StatisticalCpu (on page 816)

StatisticalDisk (on page 816)

StatisticalInterface (on page 822)

StatisticalMemory (on page 816)

StatisticalNumeric (on page 260)

StatisticalPing (on page 817)

StatisticalPingPacketLoss (on page 817)

Database Tools Table Maintenance

How to get here

This feature lets you purge expired data from data tables in your database. Be very careful when using this dialog, as data that is purged through this process is lost and cannot be restored.

- **Select tables to purge.** The data tables are grouped by the purpose they serve (active monitors, report data collection, and other). Select the tables you want to purge from the three lists.

- **Total Rows.** The total number of data rows in this table that currently holds data. This includes live and expired rows.
- **Expired Rows.** The total number of expired data rows in this table. Expired data is data that has been rolled up, and has not yet been purged by the application or has not been reused. These are rows that are marked for deletion, or have been kept longer than needed, according to your data roll-up settings. See Program Options - Report Data for more information on setting your data roll-up settings.

Click **Purge Expired Rows** to remove those records from the database.

Program Options - Report Data

This dialog controls how the storage of data is handled in the WhatsUp Gold database. This data is used to populate the various performance reports available in the application.

Performance Monitor

- **Rollup raw data after.** Raw data is data that is gathered during each reporting interval configured through *Device Properties - Performance Monitors* (on page 246). Until raw data is rolled up, it takes up one row per poll in the database, and cannot be deleted from the database. When raw data is rolled up, it is consolidated into one row per hour. It is recommended to set this value as low as possible (as low as 1 hour), to avoid database overgrowth. Select the number of days and/or hours in the time boxes. By default, WhatsUp Gold rolls up raw data after 1 day. This means that between the 24th and 25th hour, WhatsUp Gold rolls up raw data into hourly data.
- **Rollup hourly data after.** After hourly data is rolled up to daily data, hourly entries are flagged as "deleted," and are overwritten with new performance monitor data. The number in the hourly data box must be greater than the number of raw data days. By default, WhatsUp Gold rolls up hourly data after 30 days. This means that between the 24th hour on the 30th day and the 1st hour on the 31st day, WhatsUp Gold rolls up hourly data into daily data.
- **Expire daily data after.** After daily data is expired, it is flagged as "deleted" and is overwritten with new performance monitor data. The number in the daily box must be greater than the number of hourly data days. By default, WhatsUp Gold expires daily data after 365 days, or 1 year. This means that in between the 24th hour on the 365th day and the 1st hour on the 366th day, WhatsUp Gold expires daily data.



Note: After a database entry is flagged as "deleted," although it still exists in the database, it is no longer included in report data. As new performance monitor data is gathered, database entries flagged as "deleted" are overwritten with new data.

- **Active Monitor**

Select the number of days you want to keep active monitor state change data in your database. This is historical data that shows when devices changed state during the monitoring of your network. By default, WhatsUp Gold keeps state change data in your database for 365 days, or 1 year.

- **Passive Monitor**

Select the number of days you want to keep passive monitor data in your database. This is data gathered by the passive monitors assigned to your devices. By default, WhatsUp Gold keeps passive monitor data in your database for 365 days, or 1 year.

- **WhatsConfigured**

Select the number of days you want to keep WhatsConfigured data in your database. This is data gathered by WhatsConfigured about devices it is monitoring. By default, WhatsUp Gold keeps WhatsConfigured data in your database for 365 days, or 1 year.

- **WhatsVirtual**

Select the number of days you want to keep WhatsVirtual data in your database. This is data gathered by WhatsVirtual about virtual devices monitored by a vCenter server. By default, WhatsUp Gold keeps WhatsConfigured data in your database for 365 days, or 1 year.

Configure CPU Utilization

Through this data stream, you can monitor and report on the CPU utilization on the current device. Data collected is displayed in the *CPU Utilization Report* (on page 631).

- **Collect data for.** Select which CPU you want to gather data on. If you select All CPUs from the pull-down menu, all items in the list are selected automatically.
- **Data collection interval.** Enter how often you want data to be collected for the selected item or items. This number represents the number of minutes between each collection.

Click **Advanced** to access Configure Data Collection Advanced Setting. Configure Data Collection Advanced Settings

Configure Disk Utilization

Through this data stream, you can monitor and report on the available disk space for the selected device. Data collected is displayed in the *Disk Utilization Report* (on page 633).

- **Collect data for.** Select which disk you want to gather data on. If you select All Disks from the pull-down menu, all items in the list are selected automatically.
- **Data collection interval.** Enter how often you want data to be collected for the selected item or items. This number represents the number of minutes between each collection.

Click **Advanced** to access Data Collection Advanced Settings.

Configure Memory Utilization

Through this data stream, you can monitor and report on memory utilization on the current device. Data collected is displayed in the *Memory Utilization Report* (on page 636).

- **Collect data for.** Select which specific memory items you want to gather data on. If you select All memory items from the pull-down menu, all items in the list are selected automatically. This list shows the type of memory available, and the total memory capacity (in MB.)
- **Data collection interval.** Enter how often you want data to be collected for the selected item or items. This number represents the number of minutes between each collection.

Click **Advanced** to access Data Collection Advanced Settings.

In addition to the five default performance monitors, WhatsUp Gold gives you the option to create custom performance monitors to track specific APC UPS, Printer, Active Script, SNMP, and WMI performance counters.

You can *create global monitors* (on page 260) for system-wide use through the Performance Monitor Library, or *create device-specific monitors* (on page 264) through device Properties.

Configure Ping Latency and Availability

Through this data stream, you can monitor and report on how often and quickly the device responds to a Ping check. Data collected is displayed in the *Ping Availability* (on page 650) report.

- **Ping timeout.** Enter how long (in seconds) you want WhatsUp Gold to wait for a response from the device when the Ping occurs.
- **Pings per sample.** Enter how many times the device is pinged per sample collection attempt.
- **Data collection interval.** Enter how often you want data to be collected for this device. This number represents the number of minutes between each collection.

Configure Data Collection Advanced Settings

Use the following data collection settings for WhatsUp Gold to use as it attempts to collect data on the current device.

- **Timeout.** Enter the time (in seconds) that you want WhatsUp Gold to wait before it throws an error while attempting to collect data on a device.
- **Retry.** Enter the number of times you want WhatsUp Gold to attempt collecting data, when the device does not respond.
- **Determine uniqueness by.** This option is relevant to the Disk, Memory, and Interface performance monitors. Select to determine uniqueness by:
- **Interface index.** Select to determine uniqueness by the interface index.

- **Interface description.** Select to determine uniqueness by the interface description. This prevents interruptions in data gathering if a re-index occurs. This option is not relevant for CPUs because most Windows machine CPUs are named "Intel."
- **Poll interface traffic counters.** This option allows you to select either the default 32-bit counters, or high capacity 64-bit counters. Most devices support 32-bit counters, but a device with SNMP v2 or v3 counters can use the high capacity counters.



Important: If you monitor high capacity counters for a device, make sure that the device has a v2 or v3 credential assigned to it.



Note: If you do not select the Interface Utilization Performance Monitor to be used during the discovery scan for the device, 64-bit high capacity counters will not be used to poll interface traffic counters. After the discovery scan has completed, you will have to manually change the device's polling properties in the device properties to use the high capacity counters.

Creating global custom performance monitors

Global custom performance monitors are stored in the Performance Monitor Library and can be enabled on any device with the proper credentials that supports the performance counters utilized in the monitor.

You can create global custom monitors for APC UPS, Active Script, SNMP, and WMI performance counters.

Creating device-specific custom performance monitors

Device-specific custom performance monitors are configured for use only on the devices for which they are configured.

You can create device-specific custom monitors for APC UPS, Printer, Active Script, SNMP, and WMI performance counters.

Reducing ActiveMonitorStateChangeLog

The ActiveMonitorStateChangeLog table stores a record of all of the state changes that occurred for all of the active monitors attached to devices in WhatsUp Gold. When a device goes from *up* to *down*, or *down at least 2 minutes* to *down at least 5 minutes*, a record of this event is recorded in the ActiveMonitorStateChangeLog table. This table's records are viewed in the *State Change Timeline* (on page 667) and *Active Monitor Availability* (on page 659) reports in the WhatsUp Gold web interface.

You can control how long state change records are stored in the database by adjusting the **Expire state change data after** setting on the Program Options - Report data dialog. For more information, see *Changing how long report data is stored* (on page 810) and the *Program Options - Report Data* (on page 815) dialog help.



Note: Decreasing this value can take up to 24 hours to take effect.

Reducing StatisticalInterface

The StatisticalInterface table stores data collected by the Interface Utilization performance monitor when enabled on a device.

There are several options to reduce the size of this table, listed in order of least impact to the monitoring system.

- 1** Enable monitoring only for the important interfaces in your network.

By default, WhatsUp Gold monitors all the *active* interfaces on every device that supports SNMP and has interfaces. An active interface is defined as an interface which is both enabled and has a link. This can include Windows workstations, connected but unused ports on switches, and other devices. You should collect interface utilization information from only those interfaces for which bandwidth availability is a concern. You can set WhatsUp Gold to poll only the specific interfaces you identify by configuring the Interface Utilization performance monitor on the device to only poll Specific interfaces. You can do this from the *Device Properties - Performance Monitors* (on page 121) dialog. Also, consider only monitoring interface utilization for one side of a connection. For example, if Port1 on SwitchA is connected to Port2 on SwitchB, monitoring interface utilization on both ports displays the same information, just in opposite directions. Monitoring interface utilization on both ports is redundant. You should also consider disabling data collection on workstations and servers whose interface speeds are greater than the switches to which they are connected. For example, a desktop workstation with a Gigabit interface that is connected to a 100Mbps switch will never reach capacity at the workstation side of the connection. Instead, monitor for interface utilization on the switch. For more information, see the *Configure Interface Data Collection* (on page 822) dialog help.
- 2** Increase the polling interval for the Interface Utilization performance monitor on non-critical devices.

By changing how often WhatsUp Gold collects data from devices, you can decrease the amount of storage needed in the database for the monitor's records. This can be done on a per-device basis from within the *Device Properties - Performance Monitors* (on page 121) dialog or for all devices using the Bulk Field Change feature. We recommend setting each device manually as this allows for separate intervals and will not change the collection type for the monitor on the device. For more information, see *Configuring the Interface Utilization Monitor collection settings* (on page 256) and the *Bulk Field Change - Performance Monitor* (on page 820) dialog help.



Note: By setting a longer polling interval, you are decreasing the granularity of the performance monitor data on a device. For example, a device is set to collect utilization data every ten minutes for an hour. If there is a sustained period of 100% utilization for 10 minutes, while the rest of the hour shows 0% utilization, the period of 100% utilization is visible in the device's reports, followed by 0% utilization for the rest of the hour. But, if that same device is only collecting data once every 20 minutes, you only see 50% utilization of the interface during that 20-minute sample period.

3 Change the data retention settings for all Performance Monitors configured in WhatsUp Gold.

By default, WhatsUp Gold keeps raw performance monitor records for 1 day, hourly records for 30 days, and daily data for 1 year. *Raw* data is records in the database that contain actual values retrieved from a device during the poll of a performance monitor. This is the most granular data this table contains about performance monitor information on a device. *Hourly* records are an aggregate of an hour's worth of raw records, summarized and averaged into a single record. Instead of seeing each poll as a separate data point, the individual data points are reduced to a single, hourly summary. *Daily* records are a summarization of the 24 hourly records for that day. As time progresses, information in the database about a particular performance monitor gets less and less granular or specific until reaching the daily record expiration limit at which point the data is lost and replaced by new, incoming data. By adjusting the retention settings for performance monitor data, you can affect how much space is occupied by the StatisticalInterface table data. As you decrease the time period that records are kept, you decrease the amount of space needed to store those records.

For information on changing data retention settings, see *Changing how long report data is stored* (on page 810) and the *Program Options - Report Data* (on page 815) dialog help.



Note: Changing these settings affects all the performance monitor data collected by WhatsUp Gold. This includes CPU, Disk, Memory, Ping Latency & Availability, Interface Utilization (collecting data for All Interfaces, Active Interfaces, Specific Interfaces, Custom Active Interfaces, and Interface Errors and Discards), Printer, VoIP, and any data collected by custom performance monitors you have created.



Tip: You can use the Alert Center to set database threshold alerts for WhatsUp Gold and Flow Monitor. For more information, see *Configuring a WhatsUp Health threshold* (on page 795).

Bulk Field Change - Performance Monitor

For each of the default performance monitors you want to configure for the selected devices, select a value for **Collect data for** and specify how often (in minutes) you want to collect data in the **Data collection interval (mins)** field.

There are different options to **Collect data for** for each default performance monitor. The following performance monitors (**CPU**, **Disk**, **Memory**, and **Ping**) offer the following options:

- **(No Change)**. Select this option to retain the current settings for a performance monitor.
- **(All)**. Select this option to change all instances of the monitor on the selected devices.
- **(Default)** (available for Ping monitors only). Select this option to set the performance monitor to collect data from the interface designated as the default interface in the device properties.
- **(None)**. Select this option to remove a performance monitor from the selected devices.

The following monitors have additional options available:

- **Interface**
- **(No Change)**. Select this option to retain the current settings for a performance monitor.
- **(All)**. Select this option to change all instances of the monitor on the selected devices.
- **(Active)**. Select this option to set the performance monitor to collect data from interfaces that are up at the exact time of the poll.
- **(Custom Active)**. Select this option to set the performance monitor to collect data from the interfaces that are configured as custom active interfaces in each performance monitor.
 - **High speed interfaces** (Gigabit or faster). Select this option to collect data from all custom active high speed interfaces. This is the default selection.
 - **Name contains**. Select this option to collect data from all custom active interfaces that contain the variable you enter. For example, if your network naming scheme includes a subgroup named "customer," you would enter `customer` in the field to gather data from all interfaces for the subgroup that contain customer in the interface name.
 - **Type is**. Select this option and choose the interface type to collect data from all custom active interfaces of that type.
- **(None)**. Select this option to remove a performance monitor from the selected device interface.
- **Errors and discards data collection for enabled interfaces**. Select this option to collect device interface data on devices that have the Interface Utilization option selected:
 - **ifInErrors**. Lists the number of inbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.14.
 - **ifOutErrors**. Lists the number of outbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.20.

- **ifInDiscards.** List the number of inbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.13.
- **ifOutDiscards.** List the number of outbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.19.



Note: All of the above OIDs point to values of type "counter," and therefore their raw value by itself is not meaningful. The difference between the values obtained from two consecutive polls provides meaningful data.



Important: The **Interface Utilization** option must be enabled for each device for which you want to **Enable errors and discards data collection** through a bulk field change. You can select the Interface Utilization option in the **Device Properties > Performance Monitors** properties dialog for each device. For more information, see *Configure Interface Data Collection* (on page 822).

- **(No Change).** Select this option to retain the current performance monitor settings for device interface utilization.
- **(Yes).** Select this option to enable errors and discards data collection on the selected interface.
- **(No).** Select this option to disable errors and discards data collection on the selected interface.

Custom Performance Monitors

On the WhatsUp Gold web interface, you can also modify custom performance monitors that you add to the Performance Monitor Library using Bulk Field Change.

For each custom performance monitor listed, select a value for **Collect data for** and specify how often (in minutes) you want to collect data in the **Data collection interval (mins)** field.



Note: Only global custom performance monitors can be modified with Bulk Field Change. Custom performance monitors created directly on a device (and, therefore, not included in the Performance Monitor Library), cannot be modified by Bulk Field Change.

Configure Interface Data Collection

Through this data stream, you can monitor and report on the SNMP interfaces on the current device. Data collected is displayed in the *Interface Utilization* (on page 641) report.

- **Collect data for** list. Select the interfaces from which you want to gather data.
- **All Interfaces** or **Active interfaces**. *All interfaces* selects and gathers data for all interfaces in the list. *Active interfaces* collects data only for those interfaces that are currently in use.
- **Specific interfaces**. Lets you select interfaces from the Interface list.
- **Custom active interfaces**. Lets you select custom interfaces from which to collect data. A custom dialog opens to select custom interface options.
 - **High speed interfaces** (Gigabit or faster). Select this option to collect data from all custom active high speed interfaces. This is the default selection.
 - **Name contains**. Select this option to collect data from all custom active interfaces that contain the variable you enter. For example, if your network naming scheme includes a subgroup named "customer", you would enter `customer` in the field to gather data from all interfaces for the subgroup that contain customer in the interface name.
 - **Type is**. Select this option and choose the interface type to collect data from all custom active interfaces of that type.



Important: Be aware when you use the **Collect errors and discards data for selected interfaces** feature, it has potential to increase the database size quickly because there is potential for a significant amount of errors and discards data. You can set WhatsUp Health thresholds, in the Alert Center, to stay informed when the database size exceeds specified thresholds. For more information, see *Configuring system thresholds* (on page 790).



Tip: To disable the errors and discards data collection, you can disable for the individual device (**Device Properties > Performance Monitor**) or disable for multiple devices with the bulk field change option:

1. Select multiple devices that have the Interface Utilization performance monitor enabled, right-click, then select **Bulk Field Change > Performance Monitors**. The Bulk Field Change dialog appears.
2. In the Interface section of the dialog, under the **Collect errors and discards data for enabled interfaces** list, click **Yes**.

For more information, see *Editing multiple devices with the Bulk Field Change feature* (on page 116).

- **Collect errors and discards data for all selected interfaces**. Select this option to collect the following device interface data:
 - **ifInErrors**. Lists the number of inbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.14.

- **ifOutErrors.** Lists the number of outbound packets with errors, on the selected interface, that prevent the packets from being delivered to a higher-layer protocol. The associated OID is 1.3.6.1.2.1.2.2.1.20.
- **ifInDiscards.** List the number of inbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.13.
- **ifOutDiscards.** List the number of outbound packets, on the selected interface, that were discarded though no errors were detected to prevent their transmission. One possible reason for discarding such a packet could be to free up buffer space. The associated OID is 1.3.6.1.2.1.2.2.1.19.



Note: All of the above OIDs point to values of type "counter," and therefore their raw value by itself is not meaningful. The difference between the values obtained from two consecutive polls provides meaningful data.

- **Data collection interval** (minutes). Enter how often you want data to be collected for the selected item or items. This value represents the number of minutes between each collection.

Click **Advanced** to access Data Collection Advanced Settings.

Click **Speed** to override the interface speed. This option is only available when you have selected **Specific interfaces**.



Important: You cannot change the speed for an interface unless you have selected **Specific Interfaces**.



Note: If the Interface Utilization Performance Monitor was not used during Device Discovery, 64-bit high capacity counters are not used to poll interface traffic counters. You need to manually change the device's polling properties in the device properties to use high capacity counters.

Monitored devices exceeds license limit

This option compares the number of devices allowed by your WhatsUp Gold license against the number of devices configured in the application. If you reach the device count limit allowed by your WhatsUp Gold license, you will not be able to add any additional devices to the WhatsUp Gold configuration.

You can either purchase an upgrade to a license with a higher device count limit, or remove un-needed or non-critical devices from your WhatsUp Gold system.

Licensing and support information is available on the *MyIpswitch licensing portal* (<http://www.myipswitch.com/>). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.

Flow Threshold Hosts

Use this dialog to specify Flow Monitor groups, hosts, or IP ranges to which an Alert Center Flow threshold does or does not apply.

- To apply the threshold to all hosts except the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ALL hosts EXCEPT**. After you select this option, you will choose the hosts to exclude from the threshold.
- To apply the threshold to only the Flow groups, hosts, or IP range that you specify, click **This threshold applies to ONLY the following hosts**. After you select this option, you will choose the hosts to include in the threshold.
- To specify a Flow Group to include or exclude from this threshold, in the upper section of the dialog, click **Add**.



Tip: To delete a Flow group, host, or IP range from the list, select it, then click **Remove**.

- To specify a single host or IP address to include or exclude from this threshold, enter a **Hostname or IP Address**, then click **Add**.

- To specify an IP address range to include or exclude from this threshold, enter a **Start IP Address** and an **End IP Address**, then click **Add**.

Select Notification Type

Select the Alert Center Notification type that you want to create.

You can select either *Email Action* (on page 284), *SMS Action* (on page 746), or *SMS Direct Action* (on page 745).

Reducing performance monitor records

This option examines the number of records in the performance monitor data tables. A large number of records in these tables can potentially cause performance problems in WhatsUp when writing performance monitor polling data and when viewing polling data in the web interface. You can decrease the quantity of records in these tables in several ways:

- 1 Enable monitoring only for the important devices in your network.
You should collect performance monitor information from only those devices that are a concern. You can do this from the *Device Properties - Performance Monitors* (on page 121) dialog.
- 2 Increase the polling interval for performance monitors on non-critical devices.
By changing how often WhatsUp Gold collects data from devices, you can decrease the amount of storage needed in the database for the monitor's records. This can be done on a per-device basis from within the *Device Properties - Performance Monitors* dialog or for all devices using the Bulk Field Change feature. We recommend setting each device manually as this allows for separate intervals and will not change the collection type for the monitor on the device. For more information, see *Configuring the Interface Utilization Monitor collection settings* (on page 256) and the *Bulk Field Change - Performance Monitor* (on page 820) dialog help.



Note: By setting a longer polling interval, you are decreasing the granularity of the performance monitor data on a device. For example, a device is set to collect utilization data every ten minutes for an hour. If there is a sustained period of 100% utilization for 10 minutes, while the rest of the hour shows 0% utilization, the period of 100% utilization is visible in the device's reports, followed by 0% utilization for the rest of the hour. But, if that same device is only collecting data once every 20 minutes, you only see 50% utilization of the interface during that 20-minute sample period.

- 3 Change the data retention settings for all performance monitors configured in WhatsUp Gold.
By default, WhatsUp Gold keeps raw performance monitor records for 1 day, hourly records for 30 days, and daily data for 1 year. *Raw* data is records in the database that contain actual values retrieved from a device during the poll of a performance monitor. This is the most granular data this table contains about performance monitor information on a device. *Hourly* records are an aggregate of an hour's worth of raw records, summarized and averaged into a single record. Instead of seeing each poll as a separate data point, the individual data points are reduced to a single, hourly summary.

Daily records are a summarization of the 24 hourly records for that day. As time progresses, information in the database about a particular performance monitor gets less and less granular, or specific, until reaching the daily record expiration limit at which point the data is lost and replaced by new, incoming data. By adjusting the retention settings for performance monitor data, you can affect how much space is occupied by a table's data. As you decrease the time period that records are kept, you decrease the amount of space needed to store those records.

For information on changing data retention settings, see *Changing how long report data is stored* (on page 810) and the *Program Options - Report Data* (on page 815) dialog help.



Note: Changing these settings affects all the performance monitor data collected by WhatsUp Gold. This includes CPU, Disk, Memory, Ping Latency & Availability, Interface Utilization (collecting data for All Interfaces, Active Interfaces, Specific Interfaces, Custom Active Interfaces, and Interface Errors and Discards), Printer, VoIP, and any data collected by custom performance monitors you have created.



Tip: You can use the Alert Center to set database threshold alerts for WhatsUp Gold and Flow Monitor. For more information, see *Configuring a WhatsUp Health threshold* (on page 795).

Reducing PassiveMonitorActivityLog

The PassiveMonitorActivityLog table stores Passive Monitor data collected by SNMP Trap, Syslog, and Windows Event Log monitoring.

In most cases, a very large table is the result of WhatsUp collecting unnecessary or unwanted passive monitor data.

1. Verify Passive Monitor Listener configuration

The first step is to ensure you are only collecting data for passive monitors you have explicitly configured for your devices. To do this, ensure that for the both the SNMP Trap Listener and the Syslog Listener, you are not accepting unsolicited messages. You can verify this configuration in Program Options.

To verify Passive Monitor Listener configuration:

- 1 From the main menu of the WhatsUp Gold console, select **Configure > Program Options**. The Program Options dialog appears.
- 2 Click **Passive Monitor Listeners**. The Program Options - Passive Monitor Listeners dialog appears.
- 3 Select **SNMP Trap**, then click **Configure**. The SNMP Listener Configuration dialog appears.
- 4 Ensure that **Accept unsolicited SNMP Traps** is not selected, then click **OK**. The Program Options - Passive Monitor Listeners dialog appears.
- 5 Select **Syslog**, then click **Configure**. The Syslog Listener Configuration dialog appears.
- 6 Ensure that **Accept unsolicited passive monitors** is not selected, then click **OK**. The Program Options - Passive Monitor Listeners dialog appears.
- 7 Click **OK** to exit Program Options.

2. Remove unnecessary data from the database

After WhatsUp Gold is configured to collect data from only passive monitors that are assigned to devices, the next step is to clear the unneeded data already collected from the database.

Do this by removing all passive monitor data collected by the application. This removes all passive monitor data that appears in the *SNMP Trap Log* (on page 692), *Syslog Entries* (on page 693), and *Windows Event Log* (on page 696) reports. Any actions triggered by an incoming passive monitor event will still appear in the Action Log.



Important: We recommend making a backup of your WhatsUp database should you need to reverse any of the following changes.

To remove all passive monitor data from the WhatsUp database:

- 1 Stop all Ipswitch services and applications:
 - Ipswitch WhatsUp Engine
 - Ipswitch Web Server\$WhatsUp
 - Ipswitch Discovery
 - Ipswitch Alert Center
 - Ipswitch Flow Collector
- 2 From a command prompt on the WhatsUp computer, execute the following case-sensitive command on a single line:

```
>sqlcmd -E -S "%COMPUTERNAME%\WHATSUP" -Q "TRUNCATE TABLE  
[WhatsUp].[dbo].[PassiveMonitorActivityLog]"
```



Note: Replace %COMPUTERNAME% with the name of the WhatsUp computer.

The command listed above assumes you are using the SQL Server 2005 Express Edition database that is installed with WhatsUp Gold. If you are using an alternate database configuration, contact your database administrator to determine what information should be included with the "-S" switch.

After you have removed all the Passive Monitor data from the WhatsUp database, you can optionally shrink the WhatsUp database files to reclaim disk space on the SQL server.

To shrink the WhatsUp database:

- 1 Ensure that all of the Ipswitch service and applications listed above are still stopped.
- 2 From a command prompt on the WhatsUp computer, execute the following case-sensitive command on a single line:

```
>sqlcmd -E -S "%COMPUTERNAME%\WHATSUP" -Q "DBCC SHRINKDATABASE ('WhatsUp', 20)"
```



Note: Replace %COMPUTERNAME% with the name of the WhatsUp computer.

The database shrink could take quite some time depending on the size of the database and system resources, but reports a short database space analysis after completion.



Note: You can abort the shrink process at any time by using the [CTRL] + [C] keystroke sequence.

More information on the "DBCC SHRINKDATABASE" command can be found on Microsoft's web site at:

<http://msdn.microsoft.com/en-us/library/ms190488.aspx>



Important: After you reclaiming database space, you should examine your passive monitors' configuration. You can do this easily by viewing the the *Total Passive Monitors by Type* (on page 443) dashboard report (available on any Home dashboard), and the system-level *SNMP Trap Log* (on page 692), *Syslog Entries* (on page 693), and *Windows Event Log* (on page 696) reports. If you have passive monitors assigned to "talkative" devices, or you have monitors which are not exclusive enough in their search criteria assigned to your WhatsUp devices, you may re-encounter this problem as more passive monitor data is collected by the system.

Configure VMware event listener

Use this dialog to select the events you want to collect from the vCenter server, and to start and stop the collection of these events.

- **Start/Stop collecting.** Dual mode button that starts and stops event collection.
- Click **Start collecting** to enable event collection. The event collection status message reads, "Event collection is *ENABLED* for this vCenter server".
- Click **Stop collecting** to disable event collection. The event collection status message reads, "Event collection is *DISABLED* for this vCenter server".

Use options in the event selection area to select events you want to collect.

- **All HA (High Availability) error events.** Select this option to select the HA error events. The events in this category are:

- **DAS Agent Unavailable.** Records that the vCenter cannot contact any primary host in the High Availability (HA) cluster.
- **DAS Host Failed.** Records when a host failure has been detected by VMware High Availability (HA).
- **Insufficient Failover Resources.** Records that the cluster resources are insufficient to satisfy the configured HA failover level
- **Host DAS Error.** Records when there is a HA error on a host.
- **Not Enough Resources to Start VM.** Records when the VMware High Availability (HA) does not find sufficient resources to failover a virtual machine.
- **VM DAS Update Error.** Records that an error occurred when updating the HA agents with the current state of the virtual machine.
- **All Virtual machine migration events.** Select this option to receive the virtual machine migration events. The events in this category are:
 - **Migration.** Records the receipt of a migration warning or error.
 - **Migration Error.** Records the receipt of a migration error.
 - **Migration Host Error.** Records a migration error that includes the destination host.
 - **Migration Host Warning.** Records a migration warning that includes the destination host.
 - **Migration Resource Error.** Records a migration error that includes both the destination host and the resource pool.
 - **Migration Resource Warning.** Records a migration warning that includes both the destination host and the resource pool.
 - **Migration Warning.** Records the receipt of a migration warning.
 - **Vm Being Hot Migrated.** Records that a virtual machine is being hot-migrated.
 - **Vm Being Migrated.** Records that a virtual machine is being migrated.
 - **Vm Migrated.** Records a virtual machine migration.
 - **Drs Vm Migrated.** Records a virtual machine migration initiated by Distributed Resource Scheduling (DRS).
- **All security related events.** Select this option to receive security related events. The events in this category are:
 - **Bad Username Session.** Records a failed user log on.
 - **No Access User.** Records a failed user log on due to insufficient access permission.
 - **Other events.** Select this option to select additional events you want to receive.
- **Advanced.** Click **Advanced** to open the event tree. You can expand the tree to select individual events in each category.

CHAPTER 1

Admin

In This Chapter

Using WhatsUp Gold Admin features832

Home.....834

Libraries.....835

Scheduled842

System Administration845

Options.....865

Using WhatsUp Gold Admin features

In This Chapter

Using Admin features832

Using Admin features

From the Admin tab, you can access the following features:

- **Admin Panel.** Use the Admin Panel to start, stop, and restart WhatsUp Gold services. The Admin Panel also provides a list of all your WhatsUp Gold processes, along with a real-time state. The Admin Panel also provides information about the type and size of databases used by WhatsUp Gold.
- **Monitor Libraries** (active, passive, and performance). Use the Monitor Library to configure new or existing monitors. The Monitor Library includes separate libraries for active monitors, passive monitors, and performance monitors. After configuring a monitor, you must apply it to a device.
- **Action Library.** The Action Library displays all actions currently configured for use in WhatsUp Gold. WhatsUp Gold includes five pre-configured actions. These actions also display in the Action Library. As you create new actions, they are added to the Action Library.
- **Action Policy Library.** The Action Policy Library displays a list of action policies.
- **Credentials Library.** The credentials library stores login, community string, and database connection information in a central area for Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), Telnet, SSH, ActiveX Data Objects (ADO), and VMware connections used in WhatsUp Gold.
- **Recurring Actions.** Recurring actions provide the ability to fire actions based on a regular schedule, independent of the status of devices. Among other things, this can be used to send regular heartbeat messages to a pager or cellular phone, letting users know the system is up and running.
- **Scheduled Reports.** The Report Scheduler feature allows you to manage all scheduled reports that the WhatsUp Event Analyst Service is responsible for producing on a regular basis.
- **Server Options.** From the Manage Service Options feature, you can manage WhatsUp Gold server settings, for example, height and width of maps and the maximum number of passive monitor records.
- **SNMP MIB Manager.** The SNMP MIB Manager provides a list of all of the MIB files installed in the WhatsUp Gold MIB directory. Using this tool, you can import new MIB files to the MIB Manager. SNMP MIB Manager validates imported MIB files and flags errors if there is a problem with a file.

- **LDAP Credentials.** Use LDAP credentials to configure LDAP or Active Directory (AD) credentials and to configure WhatsUp Gold to connect with an Active Directory server to import group information from a Microsoft Domain Controller into WhatsUp Gold.
- **Translation.** The WhatsUp Gold translation features allows you to change the language in which WhatsUp Gold appears. You can export the entire UI for translation, or, you can translate one page each time.
- **Manage Users.** User accounts allow users to log in to the web interface of WhatsUp Gold and control access to data and functionality either through direct assignment of user rights or by membership in a user group. You can also access group information from the Manage Users tab.
- **Email Settings.** From here you can manage default global Email settings.
- **Preferences.** Use the Preferences feature to change various Web user options. Changes made here only change settings for the current user Web account.
- **Manage Dashboard Views.** WhatsUp Gold comes with a several pre-configured dashboard views. You can create your own dashboard views to use in addition to the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting.

Home

In This Chapter

| | |
|---|-----|
| Using Admin Console | 834 |
| Opening NM Console from the Web interface | 834 |

Using Admin Console

Access the Admin Panel by clicking **Admin > Admin Panel**. Use the Admin Panel to start, stop, and restart WhatsUp Gold services. The Admin Panel provides a list of all your WhatsUp Gold processes, along with a real-time state. The Admin Panel also provides information about the type and size of WhatsUp Gold databases.

Opening NM Console from the Web interface

The ability to open the WhatsUp Gold NM Console from within the Web interface is only available using Microsoft Internet Explorer; this functionality is not available using Mozilla Firefox, Google Chrome, or other Internet browsers.

To open NM Console from the WhatsUp Gold Web interface, click the **Admin** tab, then click **Open NM Console**.

This functionality uses Remote Desktop. Ensure that the machine on which you have WhatsUp Gold installed has Remote Desktop enabled.

For more information about Remote Desktop, visit *Microsoft's Web site* (<http://www.whatsupgold.com/MicrosoftRDP>), where you can watch videos and learn more about using Remote Desktop.

Libraries

In This Chapter

| | |
|-------------------------------------|-----|
| Using the Monitor Library | 835 |
| Using the Credentials Library | 836 |

Using the Monitor Library

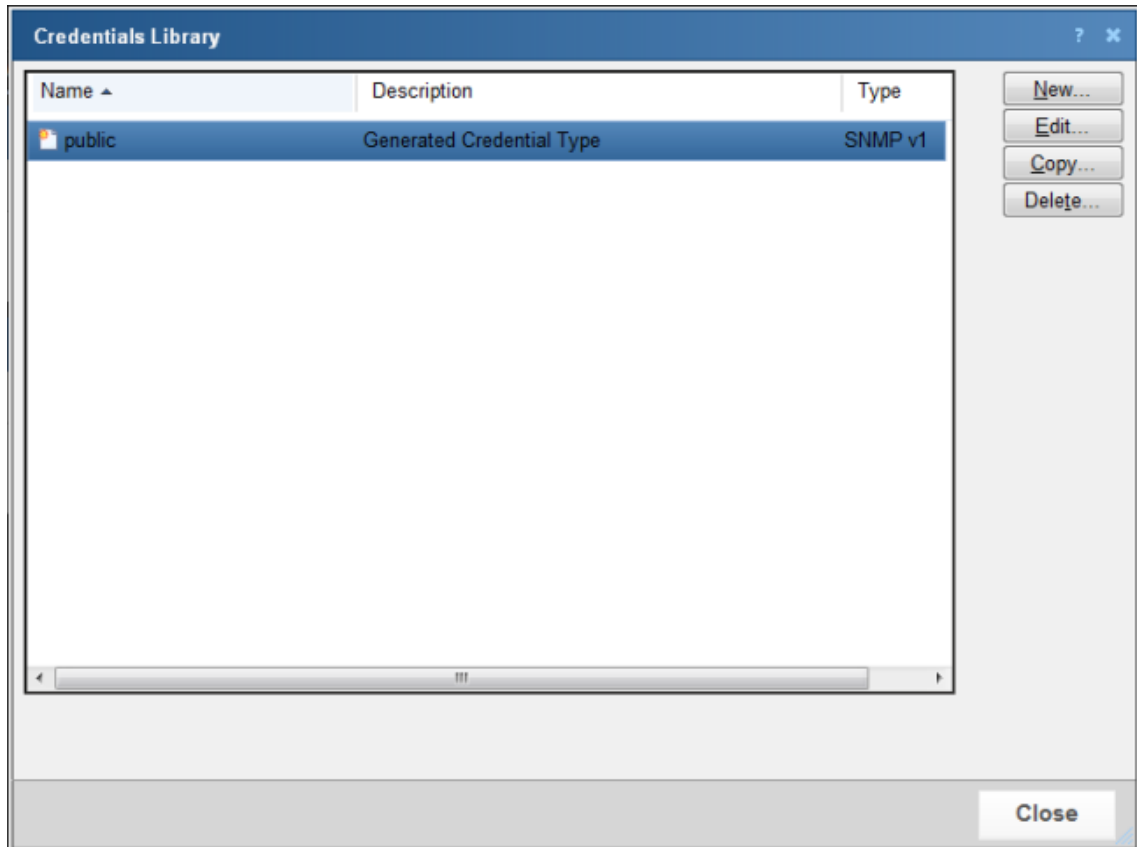
Use the Monitor Library to configure new or existing monitors. The Monitor Library includes separate libraries for active monitors, passive monitors, and performance monitors. From the monitor library, select the appropriate tab to view the other libraries. From the monitor library you can create new monitors, edit existing monitors, or delete existing monitors. After creating monitors, assign them to devices.

For more information, see:

- *Using Active Monitors* (on page 155)
- *Using Passive Monitors* (on page 232)
- *Using Performance Monitors* (on page 246)

Using the Credentials Library

The credentials library stores login, community string, and database connection information in a central area for Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), Telnet, SSH, ActiveX Data Objects (ADO), and VMware connections used in WhatsUp Gold. Use the credentials library to manage the credentials required to connect to devices and read from devices you monitor and databases you query.



- Click **New** to create a new credential to add to the library.
- Select an existing credential from the list and click **Edit** to make changes to that credential.
- Select an existing credential from the list and click **Copy** to make an exact copy of the selected credential.
- Select an existing credential from the list and click **Delete** to remove the credential from the library.

Selecting a credential type

Select the type of credential that you want to create; after selecting the credential type, click **OK** to configure the selected credential type.

- *SNMP v1* (on page 837)
- *SNMP v2* (on page 837)

- *SNMP v3* (on page 838)
- *Windows* (on page 838)
- *ADO* (on page 839)
- *Telnet* (on page 840)
- *SSH* (on page 840)
- *VMware* (on page 841)

Adding and editing a new SNMP v1 credential

The Credentials system stores community string information for SNMP devices in your WhatsUp Gold database to be used whenever a read or write community string is needed to monitor a device. SNMP v1 uses a plain text read and write community string.

To add or edit a new SNMP v1 credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **SNMP read community.** Type the read community string you want to use for this credential. See SNMP Security for more information on community strings.
 - **SNMP write community.** Type the write community string you want to use for this credential, if needed. See SNMP Security for more information on community strings.
- 4 Click **OK** to save changes.

Adding and editing a new SNMP v2 credential

The Credentials system stores community string information for SNMP devices in your WhatsUp Gold database to be used whenever a read or write community string is needed to monitor a device. SNMP v2 uses a plain text read and write community string (also known as SNMP V2c).

To add or edit a new SNMP v2 credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **SNMP read community.** Type the read community string you want to use for this credential. See SNMP Security for more information on community strings.

- **SNMP write community.** Enter the write community string you want to use for this credential. See SNMP Security for more information on community strings.

4 Click **OK** to save changes.

Adding and editing a new SNMP v3 credential

The Credentials system stores community string information for SNMP devices in your WhatsUp Gold database to be used whenever a read or write community string is needed to monitor a device. For more information, see *Using Credentials* (on page 75).

To add or edit a new SNMP v3 credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **Username.** Type the username that is configured for the SNMP agent. This username is included in every SNMP packet in the authentication header. An SNMP device, upon reception of a packet, uses this username to look for configured authentication and encryption parameters and applies them to the received message.
 - **Context.** Type the context needed to identify specific SNMP instances on your network. This box is optional.
 - **Authentication.** If required, select the authentication protocol for this SNMP credential.
 - **Protocol.** Select the algorithm method for authenticating SNMP v3 packets. MD5 creates a 128 bit digital signature and SHA-1 creates a 160 bit digital signature.
 - **Password.** Type the authentication password.
 - **Confirm password.** Re-type the authentication password a second time for confirmation.
 - **Encryption.** If supported, and an authentication protocol was selected for the SNMP v3 device, select the encryption protocol for the SNMP credential.
 - **Protocol.** Select the algorithm method for encrypting SNMP v3 packets. DES56 uses a 56 bit encryption scheme and AES-128 uses a 128 bit encryption scheme.
 - **Password.** Type the encryption password.
 - **Confirm password.** Re-type the authentication password a second time for confirmation.
- 4 Click **OK** to save changes.

Adding and editing a new Windows credential

The credentials system stores Windows account information for monitors and devices in your WhatsUp Gold database. For more information, see *Using credentials* (on page 75).

To add or edit a new Windows credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **Domain\UserID.** Type the domain and user login to use with this credential. To monitor a service on your devices, configure the Windows credential with the correct domain, user name and password and a user account that belongs to the administrators group on the remote machine. If a domain account is used, the expected user name format is *domain\user*. If the device is on a workgroup, there are two possible user names: *workgroup name\user* or *machine name\user*. In any case, the Domain\UserID must contain the backslash (\) character.
 - **Password.** Type the password for the login used above. To monitor NT services on a XP machine with an account that has empty password, the XP Local Security Settings might have to be modified. From Administrative tools > Local Security Settings, click on Security Settings > Local Policies > Security Options. Then right click on the setting: **Account: Limit local account use of blank passwords to console logon only** and click Properties, and select **Disable**.
 - **Confirm password.** Re-enter the authentication password for confirmation.
- 4 Click **OK** to save changes.

Adding and editing a new ADO credential

The credentials system stores ADO database connection string information in your WhatsUp Gold database. For more information, see *Using Credentials* (on page 75).

To add or edit a new ADO credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **Username.** Type a username. This username is used to authenticate to the device.

- **Password.** Type a password. This password is used with the above username to authenticate to the device
 - **Confirm password.** Re-enter the authentication password for confirmation.
- 4 Click **OK** to save changes.

Adding and editing a new Telnet credential

From here you can create a new Telnet credential type for use with WhatsUp Gold and WhatsConfigured plug-in. For more information, see *Using Credentials* (on page 75).

To add or edit a new Telnet credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential or from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **Username.** Enter a username. This username is used to authenticate to the device.
 - **Password.** Type a password. This password is used with the above username to authenticate to the device.
 - **Confirm password.** Re-type the authentication password for confirmation.
 - **Enable/privilege password.** Type the password that enables the router to go to privileged EXEC mode, enabling you to configure the router. If the username and password provided above provide the privilege needed to run the required commands, the enable/privilege password is not needed.
 - **Confirm enable/privilege password.** Re-type the authentication privilege password for confirmation.
 - **Port.** Type the Telnet port associated with the router. The default Telnet port is 23.
 - **Timeout.** Type a timeout (in seconds) for the length of time the connection should be attempted. The default timeout is 10 seconds.
- 4 Click **OK** to confirm changes.

Adding and Editing a New SSH Credential

The WhatsUp Gold credentials system stores SSH authentication data for devices in your WhatsUp Gold database to be used whenever authentication is needed to connect to and gather data from a device. For more information, see *Using credentials* (on page 75).

To add or edit a new SSH credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential or from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.

- **Name.** Type a name for the credential. This name displays in the Credentials Library.
- **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
- **Username.** Type a username. This username is used to authenticate to the device.
- **Password.** Type a password. This password is used with the above username to authenticate to the device.
- **Confirm password.** Re-type the authentication password for confirmation.
- **Enable/privilege password.** Type the password that enables the router to go to privileged EXEC mode, enabling you to configure the router. If the username and password provided above provide the privilege needed to run the required commands, the enable/privilege password is not needed.
- **Confirm enable/privilege password.** Re-type the authentication privilege password for confirmation.
- **Port.** Type the SSH port associated with the router. The default SSH port is 22.
- **Timeout.** Type a timeout (in seconds) for the length of time the connection should be attempted. The default timeout is 10 seconds.

4 Click **OK** to save changes.

Adding and editing a new VMware credential

The credentials system stores VMware authentication data for VMware hosts and vCenter servers in your WhatsUp Gold database to be used whenever authentication is needed to connect to and gather data from the vCenter server or VMware host. For more information, see *Using Credentials* (on page 75).

To add or edit a new VMware credential:

- 1 Access the Credentials Library.
- 2 Click **New** to create a new credential *or* from the list of current credentials, select the credential you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Name.** Type a name for the credential. This name displays in the Credentials Library.
 - **Description.** Type a short description. This description displays next to the credential in the Credentials Library.
 - **Username.** Enter a username. This username is used to authenticate to the device.
 - **Password.** Type a password. This password is used with the above username to authenticate to the device
 - **Confirm password.** Re-type the authentication password for confirmation.
- 4 Click **OK** to save changes.

Scheduled

In This Chapter

| | |
|--|-----|
| Adding and editing a Recurring Action..... | 842 |
| Using Admin Scheduled features | 843 |

Adding and editing a Recurring Action

Recurring Actions provide users with the ability to fire actions based on a regular schedule, independent of the status of devices. Among other things, this can be used to send regular heartbeat messages to a pager or cellular phone, letting users know the system is up and running.



Note: Recurring actions can be configured to adhere to a blackout schedule.

To add or edit a recurring action:

- 1 Click **Admin**, then select **Recurring Actions**.
- 2 Click **New** to create a new recurring action *or* from the list of recurring actions, select the action you want to change, and then click **Edit**.
- 3 Type or select the appropriate information in the following fields.
 - **Recurring action name.** Type a name for the recurring action.
 - **Select an action.** Select an action from the pull-down box. This list displays all actions in your Action Library that you can configure as a recurring action.
 - Click the ... button next to the **Select an action** box to launch the Action Library. In the Action Library, you can create a new action to configure as the recurring action.
- 4 Click **Next**.



Note: Web Alarm actions cannot be used as recurring actions.

Scheduling

In This Chapter

| | |
|-------------------------------------|-----|
| Scheduling a Recurring Action | 843 |
| Scheduling maintenance..... | 843 |

Scheduling a Recurring Action

Complete the following fields, and then click **Finish**.

- **Enable Schedule.** Select this option to activate the recurring action schedule; clear the option to disable the recurring report schedule.
- **Blackout Schedule.** Click this button to access the Weekly Blackout Schedule dialog.
- **Monthly.** Select the time, day, and month or months you want the action to fire. The action only fires during the month selected from this list. Quarterly actions can be created by selecting the last day of each quarter.

If a day is entered that does not exist in a selected month (September 31, February 30, etc.) then the action is fired on the last day of that month.

- **Weekly.** Select the day and time each week you want the action to fire.

To fire an action more frequently than daily, select **Every _ minutes** and enter a number of minutes for WhatsUp Gold to wait before firing the recurring action.



Note: To schedule multiple time periods, you must create another recurring action.

Scheduling maintenance

Select the day and time you want the device to be placed in maintenance mode, and when you want WhatsUp Gold to restart polling. You can select multiple days for a single time period. To schedule multiple time periods, you must create another maintenance entry.

Click **OK** to add the schedule to the device.



Note: When in maintenance mode, device active monitors will not be polled, actions will not be triggered, and logging activity is disabled. To resume polling, actions, and logging, take the device out of maintenance mode.

Using Admin Scheduled features

The Scheduled Reports functionality allows you to manage all scheduled reports that the WhatsUp Event Analyst Service is responsible for producing on a regular basis. You can schedule a new report, edit an existing report's settings, delete a report from the scheduling database, or perform a test run of a scheduled report.

To manage scheduled reports:

- 1** Click **Admin**, then click **Scheduled Reports**.
- 2** Click one of the following options to manage scheduled reports:
 - **Edit.** Select a report you want to modify, then click **Edit**. The scheduled report opens in the Scheduled Report dialog where you can change the report settings.
 - **Disable.** Select a report you want to stop sending at scheduled intervals, then click **Disable**. To return a report to a scheduled interval, select the report, then click **Enable**.
 - **Delete.** Select a report you want to remove, then click **Delete**.
 - **Send Email.** Select a report, then click **Send Email**. The scheduled email report is sent to the intended recipients immediately.

System Administration

In This Chapter

| | |
|---|-----|
| Managing WhatsUp Gold server options..... | 845 |
| Using the SNMP MIB Manager..... | 845 |
| Setting LDAP credentials..... | 848 |
| Translation Groups..... | 851 |
| Managing users and groups..... | 852 |

Managing WhatsUp Gold server options

Type or select the appropriate information to manage the WhatsUp Gold server.

Settings

- **Max width of graphical maps.** Type 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.** Type the maximum height of maps viewed through the web browser. The size is in pixels and the default is 1000.

Enable Mobile Access. Select this option to enable WhatsUp Gold Mobile access, which allows you to connect to WhatsUp Gold from a mobile device.

Click **OK** to save changes.

Using the SNMP MIB Manager

The SNMP MIB Manager provides a list of all of the MIB files installed in the WhatsUp Gold MIB directory. Using this tool, you can import new MIB files to the MIB Manager. SNMP MIB Manager validates imported MIB files and flags errors if there is a problem with a file. For more information, see *Using the SNMP MIB Manager to troubleshoot MIB files* (on page 846).

To use the SNMP MIB Manager:

- 1 Click **Admin**, then click **SNMP MIB Manager**. The SNMP MIB Manager dialog opens.
- 2 Use the following options in the SNMP MIB Manager:
 - **View.** Select a MIB file in the list, then click **View** to open the MIB and view the code.
 - **Add.** Click **Add** to import a MIB file to the MIB Manager. Follow the dialogs to complete the process.

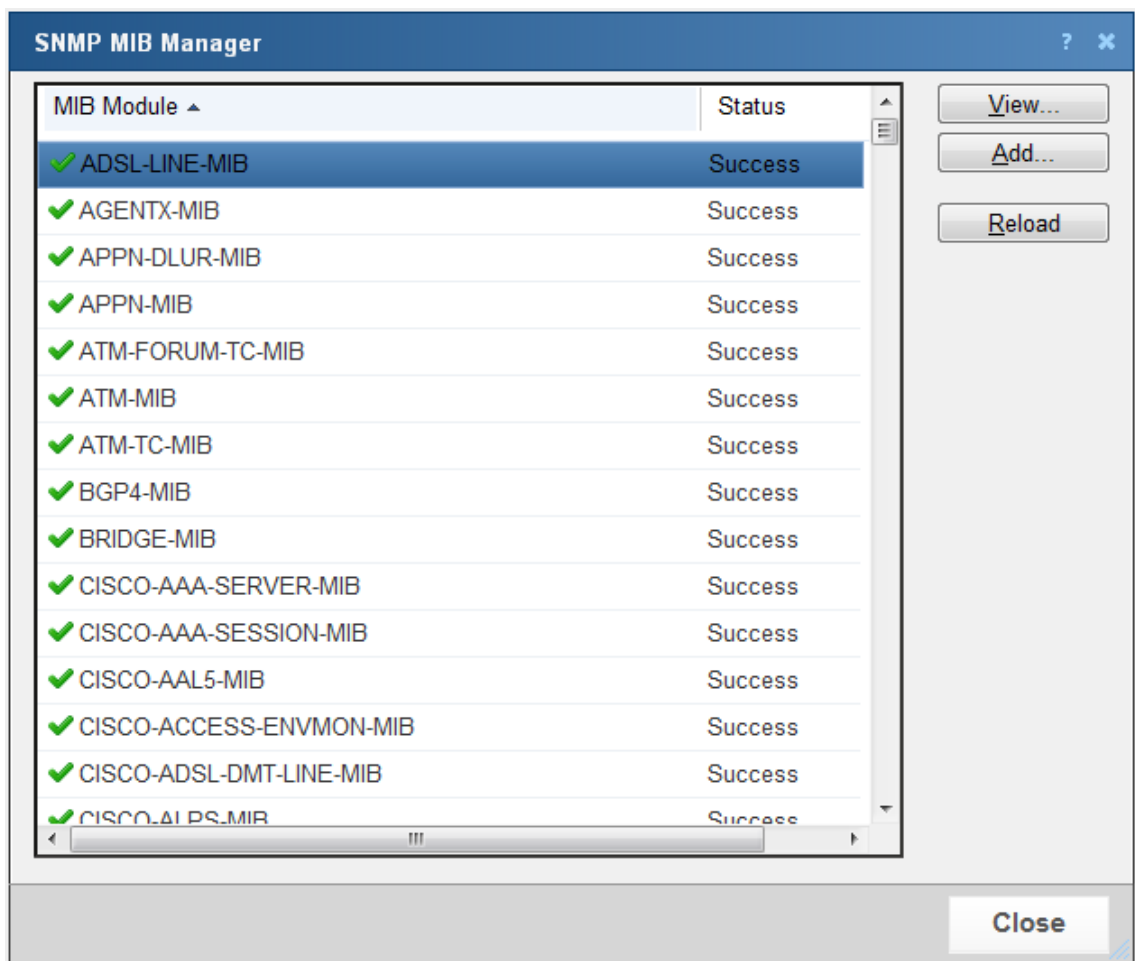


Note: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

- **Reload.** When you import a new MIB file or are troubleshooting code in a MIB file, click **Reload** to refresh the MIB Module list and the Status list.

Using the SNMP MIB Manager to troubleshoot MIB files



The SNMP MIB Manager validates all MIB files that are imported into or already exists in WhatsUp Gold. If an error is identified in a MIB file, the Status column displays the number of errors and warnings in the file. If the MIB file syntax is correct and all MIB file dependencies are fulfilled, then a check mark is displayed next to the MIB file name and a Success message displays in the Status column.



Identifying MIB file problems and errors

If an error exists in a MIB file, you can use the MIB manager to identify where code problems exist, then open the MIB file in a text editor (for example, Notepad) and correct the code. There are a variety of issues that may exist in the code; for example, there may be a simple syntax error in the MIB file or there could be a MIB file that has a dependency on another MIB file. Use the error messages when you view a MIB file to find and correct the problem.

There are two types of errors that may display in the SNMP MIB Manager list:

-  (Warning). This indicates a minor issue with the MIB file (for example, a small syntax problem). A MIB file that contains a warning may continue to work, but it is best to identify and correct the issue in the MIB file.
-  (Error). This indicates there is a problem in the MIB file that prevents it from working. A MIB file that contains an error must have the error corrected in order for the MIB file to function.



Tip: The most common MIB errors are caused by a MIB dependency on another MIB file that is not included in the MIB library. Often, when this issue is corrected, many of the MIB issues are resolved.

Example: If a MIB is missing, the MIB Manager indicates the issue in an error as shown in this example excerpt from a MIB status report:

```
22      ipMRouteGroup, ipMRouteSource,
23      ipMRouteSourceMask, ipMRouteNextHopGroup,
24      ipMRouteNextHopSource, ipMRouteNextHopSourceMask,
25      ipMRouteNextHopIfIndex,
26      ipMRouteNextHopAddress          FROM IPMROUTE-STD-MIB
Error: Cannot find module (IANA-RTPROTO-MIB): At line 26 in
C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs\IPMROUTE-STD-MIB.my
```

The important information in this report is:

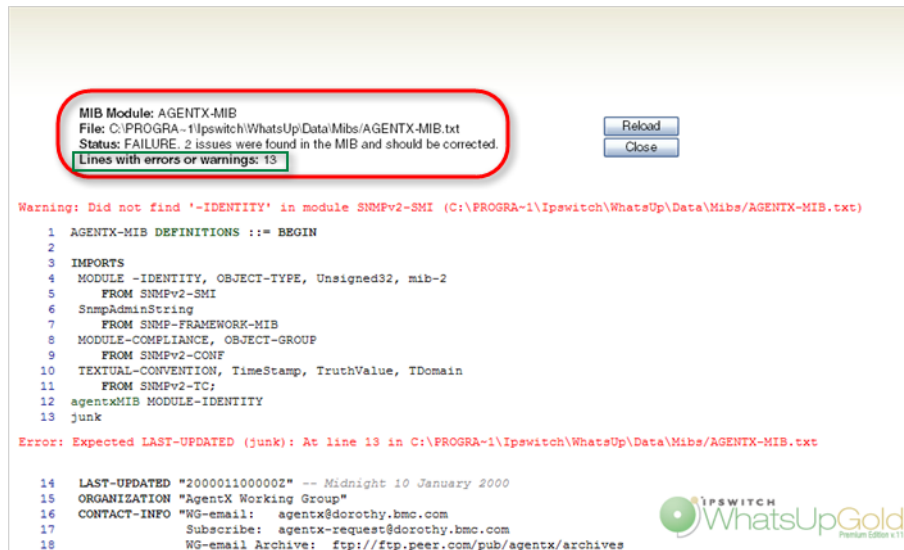
Cannot find module (IANA-RTPROTO-MIB).

This information indicates that the IANA-RTPROTO-MIB is missing from the MIB library in
C:\Program Files\Ipswitch\WhatsUp\Data\Mibs

If you determine that a MIB file is missing, you can manually copy the file to the \Program Files\Ipswitch\WhatsUp\Data\Mibs\ directory or use the *SNMP MIB Manager* (on page 845) to add (import) a new MIB file.

To identify and correct MIB file code:

- 1 Select the MIB file that has an error message in the Status column, then click **View**. The viewer opens with summary information at the top of the page that identifies the number of errors or warnings. In the **Lines with errors or warnings** summary information, you can click the line number to jump directly to a line of code with the error.



- 2 Now that the Viewer has helped you identify the problems in the code, open a text editor and correct the code. The MIB files are located in `.. \Program Files\Ipswitch\WhatsUp\Data\Mibs`.
- 3 After you have made code changes, save the MIB file, then click **Reload** in the SNMP MIB Manager dialog.
- 4 Look for the MIB file, that you made changes to, in the list to determine if all the errors have been corrected. If all the errors have been corrected, click **Close**. If the SNMP MIB Manager dialog (validator) displays errors, continue repeating steps 1 through 3 until you have corrected all of the code issues.

Setting LDAP credentials

Use the LDAP Credentials dialog to configure LDAP or Active Directory (AD) credentials and to configure WhatsUp Gold to connect with an Active Directory server to import group information from a Microsoft Domain Controller into WhatsUp Gold.

To configure WhatsUp Gold to use Windows Active Directory for authentication:

- 1 Navigate to the LDAP Credentials dialog (**Admin > LDAP Credentials**).
- 2 Type the Domain Controller IP address or hostname in **Domain Controller or LDAP server**. If you are authenticating to an Active Directory domain, the LDAP server for your domain is a DC (domain controller).
- 3 Type the port the Active Directory server uses to listen for connections in **Server port** (Default: 389).
- 4 Select **Secure** if you want Active Directory domain or LDAP queries to be encrypted using SSH (Default port: 636).

- 5 In the Server Type area, select **Active Directory** to enable Active Directory domain credentials. The Logon Domain box is activated.
- 6 Enter the Active Directory **Logon Domain** from which you want to access and import AD groups.
- 7 Click **Test** to open the Test dialog. The Test dialog allows you to verify that your credentials are configured correctly. For more information, see *Test LDAP credentials* (on page 850).
- 8 Click **Browse** to open the Browse Active Directory dialog. The Browse Active Directory dialog allows you to select the AD groups you would like to map to existing WhatsUp Gold user groups. For more information, see *Browse Active Directory* (on page 850).
- 9 In the Active Directory group list, select the WhatsUp Gold group you want to map to each AD group.



Note: Before you can map AD groups to WhatsUp Gold groups, you must create the WhatsUp Gold groups using the *Add User Group* (on page 858) dialog. When you have added the WhatsUp Gold user groups you can then select the AD groups you want to map to WhatsUp Gold groups using the *Browse Active Directory* (on page 850) dialog.



Note: When a member of an AD group logs into WhatsUp Gold using their Windows Domain credentials, they will be added as a member of the WhatsUp Gold group mapped to that AD group.

- 10 Click **OK**. WhatsUp Gold saves the Active Directory credentials and the LDAP Credentials dialog closes.

To configure WhatsUp Gold to use an LDAP server for authentication:

- 1 Navigate to the LDAP Credentials dialog (**Admin > LDAP Credentials**).
- 2 Type the LDAP server IP address or hostname in **Domain Controller or LDAP server**.
- 3 Type the port the LDAP server uses to listen for connections in **Server port** (Default: 389).
- 4 Select **Secure** if you want Active Directory domain or LDAP queries to be encrypted using SSH (Default port: 636).
- 5 In the In the Server Type area, select **Standard LDAP** to enable Active Directory domain credentials. The Authorize DN box is activated.
- 6 Type the path to the container which holds the users you want to access the WhatsUp Gold web interface in **Authorize DN**.



Note: The following is an example of how a specific LDAP server might CN=%s, OU=Users, o=yourdomain.net where %s is replaced by the username and password of the user.



Note: If you are not sure about the LDAP attributes to use or the path to specify, contact your LDAP administrator or LDAP vendor.

- 7 Click **Test** to open the Test dialog. The Test dialog allows you to verify that your credentials are configured correctly.

- 8 Click **OK**. WhatsUp Gold saves the LDAP credentials and the LDAP Credentials dialog closes.



Note: After you have entered the LDAP credentials you can create user accounts for those users that you want to allow access by authenticating using the username and passwords that are available on the LDAP server with which you have configured WhatsUp Gold to communicate.

Test LDAP credentials

Use the Test LDAP Credentials dialog to test the LDAP or Active Directory credentials you have entered in the LDAP Credentials dialog.

To Test LDAP or Active Directory credentials:

- 1 Navigate to the LDAP Credentials dialog (**Admin > LDAP Credentials**).
- 2 Type the LDAP Credentials you want to test using the LDAP Credentials dialog.
- 3 Click **Test**. The Test LDAP Credentials dialog appears.
- 4 Type a valid user name that has access to the LDAP or Active Directory server in User name.
- 5 Type the password associated with the user name in Password.
- 6 Click **Test**. WhatsUp Gold attempts to connect using the credentials and returns a test success or failure message.
- 7 Click **OK**. The test message closes.
- 8 Click **Close**. The Test LDAP Credentials dialog closes.

Browse Active Directory

Use the Browse Active Directory dialog to select the Active Directory (AD) groups from which you want to allow users to log in to WhatsUp Gold.

To select groups from the Browse Active Directory dialog:

- 1 Navigate to the LDAP Credentials dialog (**Admin > LDAP Credentials**).
- 2 Ensure the correct Active Directory server is configured (Domain Controller, port and server type). For more information see *Setting LDAP Credentials* (on page 848).
- 3 Click **Browse**. The Browse Active Directory dialog appears.
- 4 Type a valid user name that has access to the LDAP or Active Directory server in User name.
- 5 Type the password associated with the user name in Password.
- 6 Press **Tab**. The list of the most used AD groups appears.



Tip: You can see all of the groups available on the AD server by selecting Show all groups.

- 7 Select the AD groups you want to map to WhatsUp Gold groups.



Tip: Click **Check all** to select all of the displayed AD groups. Click **Clear all** to clear all of the selected AD groups.

- 8 Click **OK**. The Browse Active Directory dialog closes and the selected AD groups appear on the LDAP Credentials dialog in the AD group list.

Translation Groups

The current language is specific to each user and can be configured under **Translation** from the **Admin** tab on the web interface. The language can be temporarily changed by selecting another language from the **Language** list. To choose a language not included in the list, click browse (...) to go to the Language Library.

You can use the Translation Groups dialog box to translate content in one of two ways. You can export the entire UI for translation, or you can translate one page each time.

To use the import/export translation features, you must have translation rights turned on.

To edit a dialog, select it from the list, then click **Edit**.

Select **Show mobile only** to view only dialogs used in WhatsUp Gold Mobile Access.

For more information about translation, see the *WhatsUp Gold Translation Guide* (<http://www.ipswitch.com/Wug15Trans>).

About the Language Library

The Language Library shows the languages that you can use to translate a dialog on the WhatsUp Gold web interface. From here you can add a new language, modify an existing language, or delete a language from the library.

- To create a new language, click **New**.
- To make changes to an existing language, click **Edit**.
- To delete a language from the library, click **Delete**.
- To import a language into the library, click **Import**.
- To export a language from the library, click **Export**.

Managing users and groups

In This Chapter

| | |
|--|-----|
| Managing Users | 852 |
| About user rights | 854 |
| Adding and editing user accounts | 857 |
| Adding and editing user groups | 858 |
| About device group access rights | 859 |

Managing Users

Use this dialog to manage user accounts and user groups.

User Accounts

User accounts allow users to log in to the web interface of WhatsUp Gold and control access to data and functionality either through direct assignment of user rights or by membership in a user group.

User accounts can authenticate using:

- **Internal authentication.** The user account is created using the Add User dialog, and will authenticate using an Internal password.
- **LDAP authentication.** The user account is created using the Add User dialog, however its authentication type is set to LDAP. The user will log in using the credentials they use to authenticate with their LDAP server. The credentials for their LDAP server must be configured in PNS using the LDAP credentials dialog. For more information see *LDAP credentials* (on page 848).
- **Active Directory authentication.** The user account is created when a user that belongs to an AD group that has been mapped to a WhatsUp Gold group initially authenticates with WhatsUp Gold. The user will log in to WhatsUp Gold using their Windows domain credentials which must be configured using the LDAP credentials dialog. For more information see *LDAP credentials* (on page 848).

User accounts gain user rights when:

- Directly assigned those rights using the Add/Edit user accounts dialog. User rights directly assigned to the user account supersede any rights prohibited by membership in a WhatsUp Gold user group.
- The user is a member of a WhatsUp Gold user group. The user will gain those rights assigned to the WhatsUp Gold user group.
- The user is a member of a AD group that has been mapped to a WhatsUp Gold user group. The user will gain those rights assigned to the WhatsUp Gold user group.

There are two default user accounts:

- 1 **admin account.** The **admin** account is given all user rights, including **Manage Users**, which grants the the right to create and edit user accounts. The Administrator is also given all group access rights, so that when enabled, this account will be able to view and edit devices in all device groups.
- 2 **guest.** The Guest account allows users to see the application without giving them the ability to modify any settings. By default, all user rights and all group access rights are disabled for this account. This limits the account to only seeing a limited number of things in the application. The **admin** account (or anyone else with **Manage User** rights) can modify the Guest account rights using the Manage Users dialog.

The **admin** account can be used to create additional user accounts as needed.



Note: We recommend limiting the number of users to whom you grant the **Manage Users** right. If multiple user accounts are given permission to create and delete user accounts, confusion could surface as a result. Open communication between all user accounts with the **Manage Users** right is crucial to a smooth network management operation.

To manage users:

- To add a new user account, click **New**. The Add User dialog appears.
- To change an existing user account, select a user account from the user account list, then click **Edit**. The Edit User dialog appears.
- To remove a user account, select the user account from the user account list, then click **Delete**. A confirmation message will appear. Click **Yes**. The user account will be removed from the user account list.

User Groups

User groups efficiently manage assignment of permissions and rights to user accounts. You can map WhatsUp Gold user groups to Active Directory groups so that users can authenticate and be assigned to WhatsUp Gold groups using their Windows domain credentials.

domain-guests. The domain-guests group is created if you attempt to map AD groups before any WhatsUp Gold user groups have been created, this group is not given any user rights. Any user account with Manage Users can add user group rights to this group.

To manage groups:

- To add a new user group, click **New**. The Add User Group dialog appears.
- To change an existing user group, select a user group from the user group list, then click **Edit**. The Edit User dialog appears.
- To remove a user group, select the user group from the user group list, then click **Delete**. A confirmation message will appear. Click **Yes**. The user account will be removed from the user account list.

To enforce access rights set up in the Device Group Properties dialog:

Click **Enable Group Access Rights** to enforce access rights set up in the Device Group Properties dialog.

About user rights

User rights govern what actions users in WhatsUp Gold can perform. Any user who has been granted the Manager Users right or belongs to a group that has this right can manage user rights.



Caution: When creating an account for a novice user, do not grant all user rights. An inexperienced user with too many user rights may make inappropriate selections that accidentally interrupt network monitoring. In the case of a new user, we recommend that you restrict the account to only those rights that they will need to gain familiarity with the application. Grant additional rights as the user gains confidence and application knowledge.

The table below lists and describes each of the user rights.

| Account Administration | |
|-------------------------------|--|
| Change your Password | Enables users to change their own password from the Preferences dialog (Admin > Preferences). |
| Manage Dashboard Views | Enables users to add, delete and copy dashboard views. Allows users to modify the properties of a specific dashboard view. |
| Mobile Access | Enables users to access the mobile web interface. |
| System Administration | |
| Manage Users | Enables users to create and edit users for the web interface. This option also allows users to specify Group Access Rights. Enabling this right will enable all other rights. |
| Configure LDAP Credentials | Enables user to configure LDAP credentials for connecting to an LDAP server for user authentication in the web interface. |
| Configure Dashboards | Enables users to add dashboard views, as well as configure, move and delete dashboard reports within dashboard views. |
| Translations | Enables users to view the translation system as well as import and export languages. |
| Manage SNMP MIBs | Enables users to download and delete SNMP MIBs through the SNMP MIB Manager. |
| System Administration | Enables users to edit system configuration items, including the maximum number of passive monitor records, maximum dimensions of maps, and enabling and disabling mobile access. |
| Configure Credentials | Enables users to configure SNMP and Windows credentials. |

| | |
|---|---|
| Configure WhatsConfigured Tasks | Enables users to configure WhatsConfigured tasks and task scripts on devices in the groups to which the user has access. |
| Configure Alert Center | Enables users to create, edit and delete WhatsUp Gold Alert Center thresholds and policies. |
| Configure Flow Monitor | Enables users to create, edit and delete WhatsUp Gold Flow Monitor sources, collection intervals and data intervals for reports. |
| Email Settings | Enables users to configure WhatsUp Gold email settings from the Email Settings dialog (Admin > Email Settings). |
| Access Virtualization Actions Menu | Enables users to perform VM actions (stop, pause, restart, etc) on any virtual host within WhatsUp Gold. |
| Monitoring | |
| Configure Active Monitors | Enables users to create, edit, and remove active monitors on devices in the groups to which the user has access. |
| Configure Actions | Enables users to create, edit, and remove actions on devices in the groups to which the user has access. |
| Configure Passive Monitors | Enables users to create, edit, and remove passive monitors on devices in the groups to which the user has access. |
| Manage recurring Actions | Enables users to create, edit, and remove recurring actions on devices in the groups to which the user has access. |
| Configure Performance Monitors | Enables users to create, edit, and remove performance monitors on devices in the groups to which the user has access. |
| Configure Action Policies | Enables users to create, edit, and remove action policies on devices in the groups to which the user has access. |
| Access Group and Device Reports | Enables users to view group and device reports for the groups which the user has access. |
| Access SSG Reports | Enables users to view Split Second Graphs in dashboard and full reports. |
| Manage Scheduled Reports | Enables users to view other user's Scheduled Reports in the WhatsUp Gold web interface (Admin > Scheduled Reports). |
| Create Scheduled Reports | Enables users to configure Scheduled Reports in the WhatsUp Gold web interface (Admin > Scheduled Reports). |
| E-Mail Reports | Enables users to email an exported report to a specific email address. |
| Administer Alert Center Threshold Items | Enables users to resolve or acknowledge Alert Center Threshold alerts. |
| Devices | |
| Manage Devices | Enables users to add new devices and edit existing devices in the groups in which the user has access. Note: A user must have this right to view and hear Web Alarms. |
| Manage Device Groups | Enables users to create, edit, or remove device groups on the network. |

| | |
|-----------------------------|---|
| Access Discovery Console | Enables users to access the Discovery Console. Granting users access to this dialog also enables users to discover network devices, define device roles that help identify specific device features, and add them to the WhatsUp Gold database. |
| Reports | |
| Access System Reports | Enables users to view system reports. |
| Manage Business Hours | Enables users to configure Business Hours filters for group reports. |
| Access Alert Center Reports | Enables users to view WhatsUp Gold Alert Center reports. |
| Access Flow Monitor Reports | Enables users to view WhatsUp Gold Flow Monitor reports. |

About Remote User Rights

| | |
|--|--|
| Remote (WhatsUp Gold Central and Remote Site Editions) - (optional) | |
| Access Remote Reports | Enables users to view reports on WhatsUp Gold remote sites. |
| Configure Remote Sites | Enables users to create, edit, and delete remote sites for use with WhatsUp Gold Central and Remote Site Editions. |

When using WhatsUp Gold Distributed or MSP editions, make sure that **Access Remote Reports** is selected on the Central Site for each user that you want to provide access to the Remote Site reports. Also, make sure that you select **Configure Remote Sites** if you want a user to be able to access and change options in the Configure Remote Sites dialog. This dialog provides a list of all of the Remote Sites that have connected to the Central Site. You can view and edit two important settings in this dialog:

- **Accept remote site connection.** Allows authorized users to enable or disable accepting connections from Remote Sites. This option is checked by default. The primary reason to clear the option is if you need to disable the Central Site from accepting any connections from this Remote Site. For example, this option could be helpful if one of the Remote Sites connected to the Central Site has an unusual amount of activity and is using too much bandwidth between sites. This option lets you temporarily disable a single Central Site from accepting remote site connections until you determine what the problem is.
- **Local device.** Allows authorized users to select a local device to associate with the Remote Site. Click the browse (...) button to select a device. This device is often the computer that is running the WhatsUp software on a Remote Site. Associating a local device allows you to view the device status from the Remote Site, keeping you informed about the connection status with the Remote Site. It also provides easy access to the Network Tools for the local device you selected.

Adding and editing user accounts

Use the Add User or Edit User dialog to create a new user account or edit an existing user account.

When creating or editing a user account you can:

- Determine the authentication method for the user account.
- Select the display language to be used for the user account.
- Set and confirm the password when using internal authentication.
- Select the home device group.
- Set user rights.

You must have the **Manage User** right to add or edit a user account.



Note: You do not need to add users that will be authenticating through an Active Directory server. When a user logs in to WhatsUp Gold using their Windows domain credentials for the first time, a user account will be created for that user. They will be added to the group which was mapped to which the AD group that the user account is a member.

To create or edit a user account:

- 1 Type the name of the user account in **User name**.
- 2 Select the **Authentication type**.



Note: Select **Internal** for internal authentication using a password entered on this dialog. Select **LDAP** for remote authentication using an LDAP server (other than an Active Directory server) configured on the LDAP credentials dialog. When you select **LDAP**, the Internal password and Confirm password boxes are deactivated.



Note: When a user is being edited that has authenticated through an Active Directory server, the Authentication type for that user will appear as **Active Directory**.

- 3 Select the **Language** you want the user interface to display for this user account.
- 4 If your Authentication type is **Internal**, type and confirm the password to be used with this user account.
- 5 Select the **Home device group**. This determines the device group that will be used to provide information for monitoring and dashboard reports.
- 6 Select the user groups to which you want the user account to be a member. These groups are listed in **Member of**. Groups must be added prior to adding a user to a group. For more information on adding user groups, see *Adding and Editing user groups* (on page 858).



Note: When you add a user account to a group it will inherit all of the rights assigned to that group.



Tip: Select **Show rights inherited from group membership + user rights** to show the user rights the user will inherit from membership in the groups selected in the **Member of** box. The first column of check boxes in the User Rights list indicates the user rights acquired through group membership.

- 7 Select the **User rights** that you want to grant to the user account. For more information, see About User Rights.



Tip: You can click **Check all** to select all of the available user rights.



Note: If you grant the **Manage Users** right, the user account will acquire all user rights.

- 8 Click **OK**. The user account is added to the user account list on the Manage Users dialog.

Adding and editing user groups

Use the Add User Group or Edit User Group dialog to create or edit a user group. When creating or editing a user group, you can:

- Name the group.
- Choose the default language which will be displayed in the web interface for members of the group.
- Select group rights.

You must have the Manage User right to add or edit a user group.

To add or edit a user group:

- 1 Navigate to the Add User Group dialog.
 - a) Navigate to the Manage Users dialog (**Admin > Manage Users**). The Manage Users dialog appears.
 - b) In the User Group area, click **New** or select a group and click **Edit**. The Add User Group or Edit User Group dialog appears.
- 2 In the **User group** box, type the name of the user group. This name will appear on the user group list when the group is created.
- 3 In the **Language** box, type the language you would like to use as the default display language for this group.



Note: If the WhatsUp Gold user group has been mapped to an Active Directory group, the AD group will be displayed in the AD groups list. Any user that authenticates from one of the AD groups mapped to the WhatsUp Gold user group will appear as a user in the Members box.



Note: All users that are members of the group will be displayed in the Members box.

- 4 In the **User group rights** area, select the User group rights you want to assign to the members of this group. The user group rights you select will be inherited by all user accounts that are assigned to this group.
- 5 Click **OK** to save the user group. The Add User Group dialog closes and the user group appears on the user group list.

About device group access rights

Device group access rights enable WhatsUp Gold users to see or make changes to specific groups and devices. These rights can be enabled or disabled by the administrator and are disabled by default.

Device group access rights are useful when users need to view and edit only those groups that matter to them, as would be the case with a large network with multiple network administrators. Device group access rights allow an administrator to grant each user rights to only the devices on the network for which that user is responsible.

Types of device group access rights

There are four types of device group access rights:

- 1 **Group Read.** This right allows users to view groups and devices in the selected group. This right allows users to see the group's map and device list. Group-level reports are not affected by group access rights but are affected by user rights.
- 2 **Group Write.** This right allows users to edit group properties and add, edit, and delete devices and subgroups within the selected group.
- 3 **Device Read.** This right allows users to view the device properties of all devices within the selected group. Device-level reports are not affected by group access rights but can be affected by user rights.
- 4 **Device Write.** This right allows users to edit the device properties of any device within the selected group and to delete the device from the group.



Note: To add a device to a group, a user must have Group Write rights to the group. Device Write rights allow users to modify and delete existing rights, but do not allow them to add new devices to the group.



Tip: When enabled, group access rights are applied throughout WhatsUp Gold. Device pickers, group pickers, and group views all respect what a user account is granted permission to view and edit. Reports are not affected by group access rights but are affected by user rights.

The following is a list of operations and the group access rights that must be assigned for the user to perform that task:

- List and Map in the Group Views menu require **Group Read** access.
- Create Group and Group Properties in the Group Operations menu require **Group Read** and **Group Write** access.

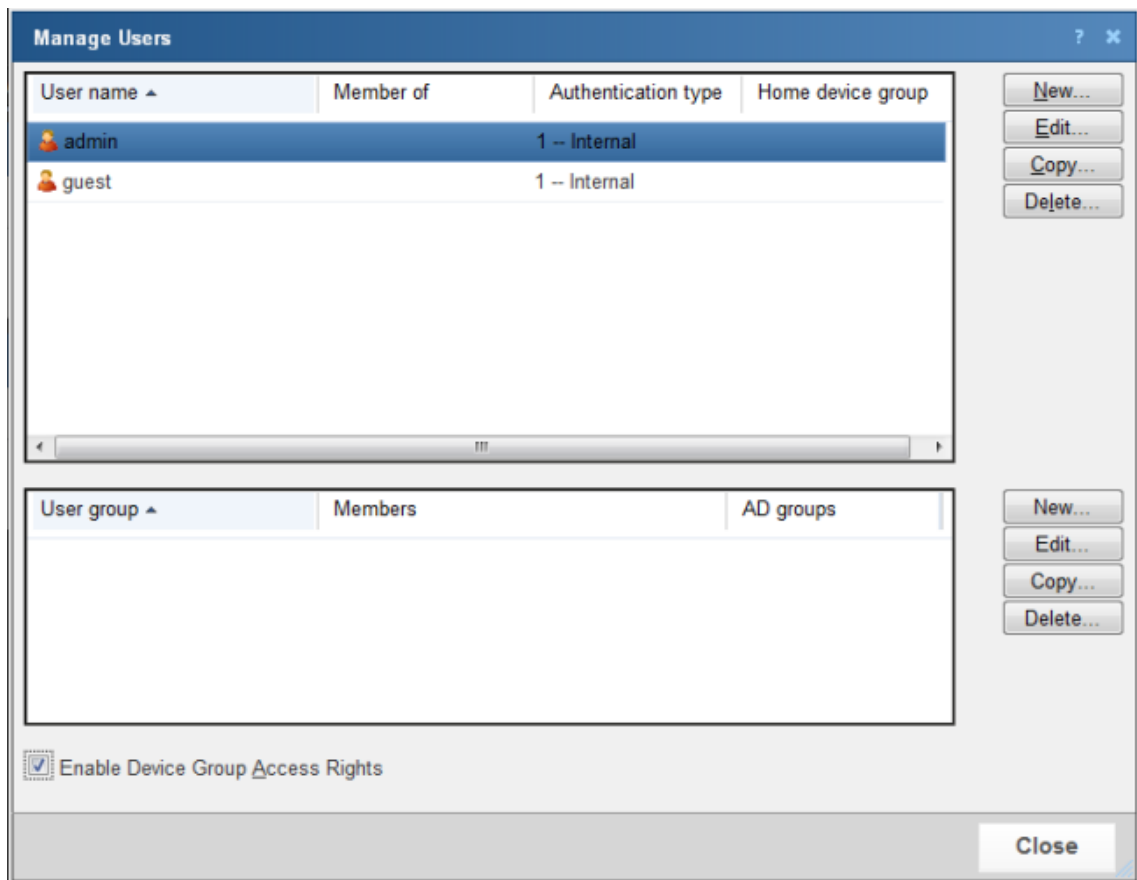
- Copy Group requires **Group Read** in the source group, and **Group Read** and **Group Write** in the destination group. (Permissions to groups and sub-groups are copied, not inherited from the new parent).
- Move Group requires **Group Read** and **Group Write** in both the source and the destination groups. (Permissions of the group and sub-groups remain the same.)
- Delete Group requires **Group Read**, **Group Write**, **Device Read**, and **Device Write** recursively. (Device Read Write may not be required if the group is empty).
- Create Device requires **Group Read**, **Group Write**, **Device Read**, and **Device Write**. If the device already exists in other group(s), you must also have **Group Read**, **Group Write**, **Device Read**, and **Device Write** in one or more of those groups.
- Copy Device requires **Group Read** in the source group and **Group Read** and **Group Write** in the destination group. The level of device permissions must be the same in both groups. Downgrade from **Device Read** and **Device Write** to **Device Read** is also permitted.
- Move Device requires **Group Read** and **Group Write** in both the source and the destination groups. The level of device permissions must be the same in both groups. Downgrade from **Device Read** and **Device Write** to **Device Read** is also permitted.
- Viewing Device Properties requires **Device Read**.
- Modifying Device Properties, Bulk Field Change, and Acknowledgement require **Device Read** and **Device Write**.

Enabling device group access rights

Device group access rights may be enabled and disabled from the Manage Users dialog.



Note: WhatsUp groups can only be managed from the WhatsUp Gold web interface.



To enable device group access rights:

- 1 From the WhatsUp Gold web interface, go to **Admin > Manage Users**. The Manage Users dialog appears.
- 2 Select **Enable Device Group Access Rights** at the bottom of the dialog. The setting is immediately saved.



Note: Simply enabling group access rights does not ensure that the rights are set up the way that you want. You also need to assign group access rights to each group on your network.

Assigning group access rights

From the web interface, select a device group and go to Properties for that group. There are several ways to do this:

- Select a device group from the Devices tab in either Map View or Device View, and right-click. From the right-click menu, select **Properties**.
- Select a device group from the Devices tab in either Map View or Device View. From the Devices Menu bar, go to **Edit > Properties**.

From the Device Group Properties dialog, you can add and edit the access rights for the selected group.

Device Group Properties

Device Group Name: 172.16.58.0/23

Description: Grant Group and Device Read for 172.16.58.0/23 to guest account

Device Group access rights

User name

- admin
- guest

Device Group Access Rights for: admin

| Right | |
|--------------|-------------------------------------|
| Group Read | <input checked="" type="checkbox"/> |
| Group Write | <input type="checkbox"/> |
| Device Read | <input checked="" type="checkbox"/> |
| Device Write | <input type="checkbox"/> |

☒ Apply changes to all sub Device Groups recursively for: guest

OK Cancel



Important: You must enable device group access rights for a user account before a user can add or edit access rights for a device group. To do this, the WhatsUp Gold Administrator must enable group access rights in the Manage Users dialog (on the WhatsUp Gold web interface, go to **Admin > Manage Users**).



Note: Device group access rights cannot be assigned directly to Dynamic Groups. Instead, devices are governed by the group access rights assigned to the other group or groups where the device is located. For more information, please see *About device group access rights* (on page 859).

Propagating group access rights to subgroups

Group access rights are passed from parent group to subgroup: when a new group is created, all of the group access rights that exist in the parent group are copied to the new group. If the rights on a parent group are modified after subgroups have been created, you can propagate the changes to the subgroup by selecting **Apply changes to all sub Device Groups recursively** on the Device Group Properties dialog.

Determining the highest right

Devices can belong to more than one device group, and each group can specify a different set of group access rights. When a device exists in multiple groups, the group access rights from all of the groups are added together to determine the rights granted to a user when accessing the device. This means that if a device is granted a right (Device Read, for example) in one group, it has that right from every group to which the device belongs.

The table below demonstrates the effective rights granted to a user accessing a device that exists in three groups that each have different group access rights.

| | Device Read right | Device Write right |
|---|-------------------|--------------------|
| Rights granted in Group A | X | |
| Rights granted in Group B | | X |
| Rights granted in Group C | | |
| Effective rights when accessing device from any group | X | X |

In this example, the device is granted Device Read by its membership in Group A and Device Write by its membership in Group B. The result is that the user can access the device with full rights from any device group to which the device belongs, even Group C where no explicit rights are set.

Understanding device group access rights and user access rights

When device group access rights are enabled, WhatsUp Gold determines effective rights by first negotiating user rights, then group access rights. This means that, while device group access rights govern access to device groups, a user must first have user access rights to a device or group before group access rights are considered. If a user does not have the Manage Devices user access right, for example, then Device Write group access rights are not honored.



Tip: By disabling the Manage Groups and Manage Devices user access rights, you can prevent a user from modifying any groups or devices in WhatsUp Gold.

About group access rights and users' home groups

Users are given Group Read rights for their Home group by default. If Group Read rights are removed from a user's home group, the user cannot access the Device List until the Group Read right is restored or the user's Home group is changed to a group for which the user has Group Read rights.



Note: Changing a user's Home group does not change the user's Group Access rights for original Home group. Be careful to prevent unintentionally granting access to a device group to which you do not want a user to have access.

For example, an administrator creates a new user account and leaves the Home group as the default My Network. The new user account automatically receives Group Read rights to My Network. At a later date, the administrator changes the user account to use a subgroup as the user's Home group. Unless the administrator deliberately removes the Group Read right from My Network, the user continues to have Group Read rights to My Network, potentially granting the user more visibility into WhatsUp Gold than the administrator intended. Changing the user's Home group is not enough to restrict what he or she can see in WhatsUp Gold.

About group access rights and dynamic device groups

Group access rights cannot be assigned to dynamic device groups. However, every device within a dynamic device group belongs to at least one other group. Therefore, when a user accesses a device accessed through a dynamic device group, the rights he or she is granted to the device are equal to the sum of the rights granted in each of the groups to which the device belongs.

For more information, see *Determining the highest right* (on page 863).

Options

In This Chapter

| | |
|---|-----|
| Configuring Email settings..... | 866 |
| Changing preferences | 867 |
| Managing dashboard views | 868 |
| Using the Program Options | 871 |
| Setting Advanced Options..... | 881 |
| Types of SNMP Trap Monitors..... | 882 |
| Common SNMP Traps..... | 882 |
| Select computer..... | 883 |
| FTP server user permissions..... | 883 |
| WMI..... | 884 |
| Event Viewer..... | 884 |
| Payload Definition..... | 884 |
| SMS Providers | 884 |
| Setting Modem Connection Preferences..... | 884 |
| Configure Memory Threshold..... | 885 |
| Configure Disk Performance - Exchange | 885 |
| Configure System Thresholds | 885 |
| Configure Links Thresholds | 886 |
| Configure Queues Thresholds | 887 |
| Adding Custom Thresholds | 887 |
| FTP server user permissions..... | 887 |
| Configure Disk Performance | 887 |
| Configure Disk space Threshold | 888 |
| Configure System Threshold..... | 888 |
| Configure Buffers Threshold..... | 888 |
| Configure Locks Threshold | 888 |
| Configure Cache Threshold | 889 |

| | |
|---|-----|
| Configure Transactions Threshold | 889 |
| Configure Users Threshold..... | 889 |
| Configure Alerts Threshold | 889 |
| SQL Server Services..... | 890 |
| Selecting a Device | 891 |
| Selecting computers | 891 |
| Configuring CPU Threshold..... | 892 |
| Setting Advanced Properties for a HTTP Content Monitor | 892 |
| Setting Advanced Properties for an Email Active Monitor | 892 |
| Selecting a blackout period | 894 |
| Importing a MIB file | 894 |
| Hub Transport Server Role Thresholds | 894 |
| Select Action Type..... | 896 |
| WinEvent Condition | 896 |

Configuring Email settings

Use this dialog to configure the default global settings for Email actions.

To configure Email settings:

- 1 Click **Admin**, then select **Email Settings**. The Configure Email Settings dialog opens.
- 2 Type or select the appropriate information in the following fields.
 - **Destination email address.** Type the address that the Email action message should be sent.
 - **From email address.** Type the address to be listed as "From" in the email sent by the Email action.
 - **SMTP server.** Type the address of the server on which SMTP is running (email server).
 - **Port.** Type the number of the port on which the SMTP service is listening. The standard SMTP port is 25.
 - **Timeout (sec).** Type the amount of time (in seconds) that WhatsUp Gold should wait for a response from the SMTP server for each command WhatsUp Gold issues. If the time limit is exceeded, the email fails. The default timeout is 30 seconds.
 - **Use SMTP authentication.** Select this option if your SMTP server requires user authentication.
 - **Username.** Type the username to be used with SMTP authentication.
 - **Password.** Type the password of the username to be used with SMTP authentication.

- **Use an encrypted connection (SSL/TLS).** If your SMTP server supports encrypting data over a TLS connection (formerly known as SSL), select this option to encrypt SMTP traffic.
- 3 Click **OK** to save changes.

Changing preferences

Access the Preferences dialog by clicking **Admin > Preferences**, or through your user account link in the upper right corner of any page. Use this dialog to change various Web user options. Changes made in this dialog only change settings for the current user Web account.

General

- **Language.** Select a language for the application.
- **Change your password.** Click this option to change your account password.
- **Show Getting Started Pane.** Select this option to display the Getting Started pane. The Getting Started pane includes links to resources to help you resolve issues and learn more about WhatsUp Gold.



Note: If you have an evaluator license, this field displays as **Show Evaluator Pane**. This option is not selectable with an evaluator license.

Refresh intervals

- **Dashboard report.** Enter a time (in seconds) for how often *dashboard reports* (on page 340) should refresh.
- **Full report.** Enter a time (in seconds) for how often *monitor reports* (on page 619) should refresh.
- **Devices list.** Enter a time (in seconds) for how often the content Devices tab should refresh.

Reports

- **Default records per page for long reports.** Enter a number to control the maximum number of rows reports and logs display. If a report contains a number of rows greater than the maximum number specified, you can use either the page controls to view the data. The default max records setting is 50.
- **Collapse legends on split second graph dashboard reports.** Select this option to hide the legends on split second graph dashboard reports until the mouse pointer moves over a graph. When multiple split second graph dashboard reports display in a dashboard view, selecting this option can help reduce the percentage of the screen area used by reports. This option affects split second graph dashboard reports only; legends are always displayed in popups.

Web Alarms

- **Enable web alarms.** Select this option to enable *Web alarms* (on page 117).



Note: Web alarms are enabled by default.

- **Check every.** If you enable Web alarms, enter a time (in seconds) for how often WhatsUp Gold should check for Web alarms.

Instant Info (popups)

- **Show popups on device list.** Select this option to enable popups on the device list. If this option is cleared, popups are not displayed when you hover device or group names in the device list.
- **Show popups on dashboard reports.** Select this option to enable popups on dashboard reports. If this option is cleared, popups are not displayed on dashboard reports.
- **Show popups on full reports.** Select this option to enable popups on monitor reports. If this option is cleared, popups are not displayed on monitor reports.



Note: By default, popups are enabled on both dashboard and reports.



Note: Popups are not available in WhatsUp Gold Standard Edition.

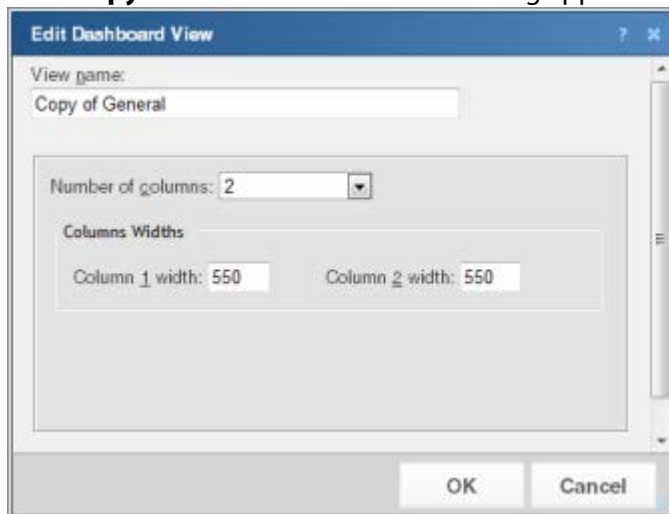
Managing dashboard views

WhatsUp Gold comes with a several pre-configured dashboard *views*. You can create your own dashboard views to use in addition to the pre-configured views. You can create as many as you feel necessary to organize your system for efficient reporting.

To copy an existing dashboard view:

- 1 Click **Admin**, then click **Manage Dashboard Views**. The Manage Dashboard Views dialog appears.
- 2 Select the view you want to copy from the Dashboard Views list.

- 3 Click **Copy**. The Edit Dashboard View dialog appears.

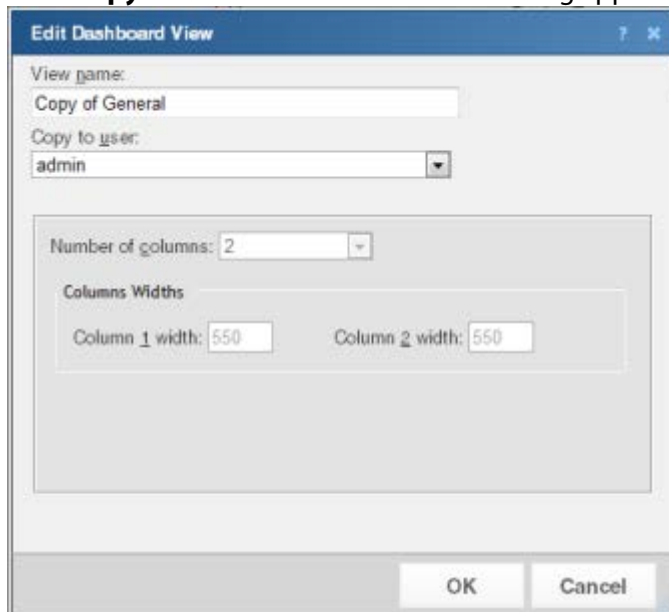
The image shows the 'Edit Dashboard View' dialog box. It has a title bar with a question mark and a close button. The main area contains a 'View name:' text box with 'Copy of General' entered. Below this is a 'Number of columns:' dropdown menu set to '2'. Underneath is a 'Columns Widths' section with two text boxes: 'Column 1 width:' set to '550' and 'Column 2 width:' set to '550'. At the bottom right are 'OK' and 'Cancel' buttons.

Enter the appropriate information in the following fields:

- **View name.** The dashboard view title as it appears in the Manage Dashboard Views dialog.
 - **Number of columns.** The number of columns to include in the view.
 - **Column width.** The width of each column in the view (in pixels).
- 4 Click **OK** to save changes.

To copy a dashboard view to another WhatsUp Gold user:

- 1 Click the **Admin** tab, then click **Manage Dashboard Views**. The Manage Dashboard Views dialog appears.
- 2 Click **Copy to**. The Edit Dashboard View dialog appears.

The image shows the 'Edit Dashboard View' dialog box, similar to the one above but with an additional field. It has a title bar with a question mark and a close button. The main area contains a 'View name:' text box with 'Copy of General' entered. Below this is a 'Copy to user:' dropdown menu with 'admin' selected. Underneath is a 'Number of columns:' dropdown menu set to '2'. Below that is a 'Columns Widths' section with two text boxes: 'Column 1 width:' set to '550' and 'Column 2 width:' set to '550'. At the bottom right are 'OK' and 'Cancel' buttons.

- 3 Enter the appropriate information into the following fields:
 - **View name.** The name of the dashboard view as it will appear in the Manage Dashboard Views dialog.
 - **Copy to user.** Select the user account from where you want to copy the dashboard view.
- 4 Click **OK** to save.

To delete a dashboard view:

- 1 Click the **Admin** tab, then click **Manage Dashboard Views**. The Manage Dashboard Views dialog appears.
- 2 Select the view you want to remove in the Dashboard Views column.
- 3 Click **Delete**.
- 4 Click **Yes** to confirm the deletion. The view is removed from the Manage Dashboard Views dialog.

Using the Program Options

In This Chapter

| | |
|---|-----|
| Enabling the polling engine | 871 |
| Enabling actions..... | 872 |
| Enabling performance monitors..... | 872 |
| Enabling WhatsVirtual event collection | 872 |
| Enabling the Ping Throttle | 873 |
| Enabling the SNMP Trap Listener | 873 |
| Enabling the Windows Event Log listener..... | 874 |
| Enabling the Syslog listener | 875 |
| Enabling FIPS 140-2 mode | 875 |
| About the WhatsUp Gold default SSL certificates | 877 |
| Changing the device state colors or icons | 877 |
| Passive Monitor Listeners | 878 |
| Changing how long report data is stored | 878 |
| Selecting a display font | 878 |
| Changing clock/regional preferences..... | 878 |
| Changing the date and time format..... | 879 |
| Using the WhatsUp Services Controller | 880 |

There are a number of administrative features available in the WhatsUp Gold console Program Options.



Note: Program Options are only available from the WhatsUp Gold console.

To access the WhatsUp Gold console Program Options:

- 1 Click **Start > Programs > Ipswitch WhatsUp Gold > WhatsUp Gold**. The WhatsUp Gold console application appears.
- 2 Click **Configure > Program Options**. The Program Options dialog appears.
- 3 Select options as required.

Enabling the polling engine

To enable or disable the WhatsUp polling engine:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable polling engine** to turn on polling. Clear the selection to turn polling off.
- 4 Click **OK** to save changes.



Tip: In the bottom right corner of the WhatsUp Gold console, the Polling icon shows if the engine is active.

Enabling actions

To enable or disable the WhatsUp Gold actions:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable actions** to enable actions. Clear the selection to disable all actions.



Important: If you disable WhatsUp Gold actions, any configured actions or action policies do not run.

- 4 Click **OK** to save changes.

Enabling performance monitors

To enable or disable WhatsUp Gold performance monitors:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Enable performance monitors** to enable WhatsUp Gold performance monitors. Clear the selection to disable all performance monitors.



Important: If you disable performance monitors, WhatsUp Gold ceases to gather device data using any of the default or custom performance monitors that exist in the Performance Monitor Library.

- 4 Click **OK** to save changes.

Enabling WhatsVirtual event collection

To enable or disable WhatsVirtual event collection:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.

- 3 Select **Enable WhatsVirtual event collection** to enable the collection of events from all of the configured vCenter servers. Clear the selection to disable the collection of events.



Note: The **Enable WhatsVirtual event collection option** is selected by default, enabling event collection for all configured vCenter servers.

- 4 Click **OK** to save your changes, or click **Cancel** to discard your changes.

Enabling the Ping Throttle



Note: Increasing the time between consecutive pings generated by the ping engine lowers the bandwidth required to support the ping engine, but increases the amount of time required to ping monitored devices. Decreasing the time between consecutive pings increases bandwidth requirements, but decreases the amount of time needed to ping monitored devices.



Note: The **Throttle pings by x msec** selection persists only if you have selected an option other than the default. The default setting is 20 msec.

To enable the ping throttle:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon. The General options appear.
- 3 Select **Throttle pings by x msec** option and select the number of milliseconds you want the ping engine to wait between consecutive pings.
- 4 Click **OK**. The Program Options dialog closes.

Enabling the SNMP Trap Listener

You must enable the SNMP Trap listener to collect data for the *SNMP Trap Log* (on page 692) report.



Important: The SNMP Trap Listener cannot be enabled through the web interface; it must be enabled in the WhatsUp Gold console.

Important: The Microsoft SNMP Trap Listener must be disabled to enable the WhatsUp Gold SNMP Trap Listener.

To enable the SNMP Trap listener:

- 1 In the WhatsUp Gold console, select **Configure > Program Options**. The Program Options dialog appears.
- 2 Select **Passive Monitors Listeners**.
- 3 Select **SNMP Trap**, then click **Configure**. The SNMP Trap Listener Configuration dialog opens.
- 4 Select **Listen for messages on port** and enter a port number to enable the SNMP Trap Listener (default port is 162).

- 5 To collect data on unsolicited events as well, select **Accept Unsolicited SNMP Traps**.



Note: Do not select this option when using SNMP v3 credentials.

- 6 Click **OK** to close the SNMP Trap Listener Configuration dialog. Click **OK** again to close the Program Options dialog.

To disable the Microsoft SNMP Trap Listener:

- 1 Click **Start** and type `services.msc` in the search box. The Services console appears.
- 2 Locate **SNMP Trap Service** in the list of services.
- 3 Right-click **SNMP Trap Service**, and select **Properties** from the menu.
- 4 Verify that the service status is **Stopped**. If the service status is Started, click the **Stop** button.
- 5 Verify that the Startup type is **Manual** or **Disabled**. If the startup type is set to another type, select **Manual** from the Startup type menu.
- 6 Click **OK** to close the SNMP Trap Properties dialog.

Enabling the Windows Event Log listener

You must enable the Windows Event Log listener to collect data for the *Windows Event Log* (on page 696).

To configure the Windows Event Log Listener:

- 1 From the WhatsUp Gold console main menu, select **Configure > Program Options**. The Program Options dialog appears.



Note: If the Windows SNMP Trap Service (**Control Panel > Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

- 2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.
- 3 Select the Windows Event Log Listener, then click **Configure**. The Windows Event Log Listener Configuration dialog appears.
- 4 Enter or select the appropriate information in the following fields:
 - **Start Server**. Select this option if you would like WhatsUp Gold to listen for Windows Event logs.
 - **Do not generate payload**. Select this option to only add the event time and message to the Windows Event Log; the payload is withheld from the entry.
 - **Check connections interval**. Select this option to have WhatsUp Gold check for and close inactive connections at the interval you specify. The default interval is 60 seconds.
- 5 Click **OK** to save changes.

Enabling the Syslog listener

You must enable the Syslog listener to collect data for the *Syslog* (on page 693) report.

To configure the Syslog Passive Monitor Listener:

- 1 From the WhatsUp Gold console main menu, select **Configure > Program Options**. The Program Options dialog appears.



Note: If the Windows SNMP Trap Service (**Control Panel > Services**) is running on the WhatsUp Gold console PC, you should stop the service. This is a precaution to prevent any conflict with the WhatsUp Passive Monitor Listener.

- 2 Click **Passive Monitor Listeners**. The WhatsUp Gold Passive Monitor Listeners display in a list.
- 3 Select the Syslog Trap listener, then click **Configure**. The Syslog Listener Configuration dialog appears.
- 4 Enter or select the appropriate information in the following fields:
 - **Listen for messages on port.** Select this option if you want WhatsUp Gold to listen for Syslog messages. The Syslog Listener runs on port 514 by default, but can be changed if necessary, as when another application needs to use the same port.
 - **Accept unsolicited passive monitors.** If option this is cleared, only Syslog entries which are specifically added to devices as passive monitors are logged to the System Syslog report. If you select this option, all incoming Syslog messages are detected and logged to the System Syslog report.



Note: Regardless of this filter setting, only Syslog messages that are solicited are logged to device Syslog reports and are able to trigger actions.

- 5 Click **OK** to save changes.

Enabling FIPS 140-2 mode



Note: For information about operating WhatsUp Gold in FIPS-140-2 mode, please see *About operating WhatsUp Gold in FIPS 140-2 mode* (on page 876).

To enable or disable FIPS 140-2 mode:

- 1 From the console main menu, click **Configure > Program Options**.
- 2 Click the **General** icon.
- 3 Select **Operate in FIPS 140-2 mode** to enable FIPS 140-2 mode. Clear the selection to stop WhatsUp Gold from operating in FIPS 140-2 mode.



Note: WhatsUp Gold automatically enables FIPS 140-2 mode when it detects that it is operating on a FIPS-compliant operating system.



Note: This option is disabled if any of the configured credentials in the Credentials Library are not FIPS-compliant. In order for this option to be available, you must go to the Credentials Library and either modify or remove the non-compliant credentials.

- 4 Click **OK** to save changes.

About operating WhatsUp Gold in FIPS 140-2 mode

There are several *important* things to take into consideration if you plan to operate WhatsUp Gold in FIPS 140-2 mode:

- WhatsUp Gold does not recommend that you enable FIPS if you plan to use SNMPv1, SNMPv2, or SNMPv3 credentials that do not use encryption or authentication.
- WhatsUp Gold detects a FIPS compliant operating system and places the system in FIPS 140-2 mode automatically upon initial start-up.
- WhatsUp Gold recommends that SSHv2 only be used with FIPS 140-2 certified algorithms, because WhatsUp Gold in FIPS 140-2 mode does not support communications using non-certified algorithms.
- SNMPv3 credentials using MD5 and DES56 are prohibited; you are unable to enable FIPS if SNMPv3 credentials using MD5 exist in the Credentials Library. You must modify or remove such credentials in order to enable FIPS.

The following are scenarios may occur when you try to enable FIPS 140-2 mode in the Program Options dialog:

If a message is presented that you have non-compliant SNMPv3 credentials (but you have a compliant SSL certificate):

This option is disabled because the SNMPv3 credentials are not FIPS compliant. Go to the Credentials Library to edit or remove the SNMP credentials. After editing or removing the credentials, you can enable this option in the Program Options dialog.

If a message is presented that you have non-compliant SSL certificate (but you have a compliant SNMP credentials):

This option is disabled because the SSL certificate is not FIPS compliant. Replace your current SSL certificate with a FIPS-compliant SSL certificate. To automatically replace your current SSL certificate with the default FIPS-compliant SSL certificate, click the link in the on-screen message. After replacing the SSL certificate, you can enable this option in the Program Options dialog.

If a message is presented that you have non-compliant SNMPv3 credentials and a non-compliant SSL certificate:

This option is disabled because the SNMPv3 credentials and the SSL certificate are not FIPS compliant. Go to the Credentials Library to edit or remove the SNMP credentials. Also, replace your current SSL certificate with a FIPS-compliant SSL certificate. To automatically replace your current SSL certificate with the default WhatsUp Gold FIPS-compliant SSL certificate, click the link in the on-screen message. After editing or removing the credentials and replacing the SSL certificate, you can enable this option in the Program Options dialog.

If a message is presented that confirms you have used the WhatsUp Gold default SSL certificate:

You have selected to use the default FIPS-compliant SSL certificate in WhatsUp Gold. Your certificate password is not be backed up automatically. Make sure you back up the SSL certificate password before completing this action. The current SSL certificate is backed up as `server.crt.bak` and `server.key.bak`.

For more information about SSL certificates in WhatsUp Gold, see *About the WhatsUp Gold default SSL certificates* (on page 877).

For more information about the FIPS 140-2 specification, see the *U.S. Department of Commerce documentation* (http://www.whatsupgold.com/wug_USDOC_FIPS).

About the WhatsUp Gold default SSL certificates



Important: If you want to implement SSL certificates, refer to Microsoft or other trusted resources for more information. Following are suggested IIS and SSL resources: *SSL and Certificates (IIS 6)* (http://www.whatsupgold.com/wug_SSLcert_IIS6) and *Configuring Server Certificates in IIS 7* (http://www.whatsupgold.com/wug_SSLcert_IIS7).

You should replace the default certificates with new SSL certificates that you generate and sign. These sample files reside in the <WhatsUp Gold Install Directory>\Data\SSL directory. Also, since the sample certificate is issued with Ipswitch as the Common Name, it will generate a Domain Name Mismatch Security Error every time a new browser session is established.



Important: To acquire a valid SSL certificate, refer to an SSL certificate provider such as VeriSign. For more information, see the to WhatsUp Gold *KB article for using a 3rd-party SSL certificate with the WhatsUp Gold web interface* (http://whatsup.custhelp.com/cgi-bin/whatsup.cfg/php/enduser/std_adp.php?p_faqid=231&p_created=1223481560&p_sid=jbX58cek&p_accessibility=0&p_redirect=&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Jvd19jbNq9MywzJnBfcHJvZHM9MCZwX2NhdHM9JnBfcHY9JnBfY3Y9JnBfc2VhcmNoX3R5cGU9YW5zd2Vycy5zZWYy2hfbmwmcF9wYWdlPTEmcF9zZWYy2hfdGV4dD1zc2wgY2VydGlmaWNhdGVz&p_li=&p_topview=1).

Changing the device state colors or icons

To change the device state colors or icons:

- 1 From the main menu, select **Configure > Program Options**.
- 2 In Program Options, select **Device States**.
- 3 To change an existing icon or state, select the entry from the list and click **Edit**.
- 4 Adjust the shape and color of the icon using the settings in the **Device State Editor**.
- 5 Click **OK** to save changes.

If the default settings do not fit your needs, click **Add** to create a new device state, using the internal state and state time that you need.

Passive Monitor Listeners

Passive Monitor Listeners are applications that listen for specific information being passed across your network, or events that occur on one of your devices, then notifies WhatsUp Gold when the information matches what it is listening for. Use this dialog to configure those servers according to your specific needs. For more information, see *Using Passive Monitors* (on page 232).

WhatsUp Gold provides the following Passive Monitor Listeners:

- **SNMP Trap.** This listener monitors SNMP information being passed across your network.
- **Syslog.** This listener monitors a computers Syslog.
- **Windows Event Log.** This listener monitors the Windows Event Log.

Changing how long report data is stored

Ping Active Monitor data is stored in the WhatsUp Gold database to populate the performance logs available in the application.

To configure WhatsUp Gold report data:

- 1 From the main menu, select **Configure > Program Options**.
- 2 In Program Options, select **Report Data**.
- 3 On the Report Data section, you can change the data settings for performance monitors, active monitors, and passive monitors.
- 4 Click **OK** to save the changes.

You can see how many rows in the database that the data takes up by viewing the numbers under the time settings.

Selecting a display font

Use the Map Font to select a font for the device labels in your map views and log graphs. The fonts in the list are fonts that are currently installed and available on your computer.

To select a display font for WhatsUp Gold:

- 1 From the main menu bar on the WhatsUp Gold Console, select **Configure > Program Options**. The Program Options dialog appears.
- 2 Select **Map Font**, then select the font and font size you want to use in WhatsUp Gold.

Changing clock/regional preferences

To use a 24-hour clock instead of the default 12-hour clock:

- 1 From the WhatsUp Gold main menu, select **Configure > Program Options**.
- 2 Select the **Regional** section.
- 3 Select the **Use 24 hour clock** option.
- 4 Click **OK**.

Changing the date and time format

To change the date and time format:

- 1 From the WhatsUp Gold main menu, select **Configure > Program Options**.
- 2 Select the **Regional** section.
- 3 For each of the three date formats, select the one that best suits your needs.
- 4 Click **OK**.

These formats can be seen in use on several of the logs available on the WhatsUp Gold web interface.

Using the WhatsUp Services Controller

In This Chapter

Managing Services using the WhatsUp Services Controller880

Managing Services using the WhatsUp Services Controller

The WhatsUp Gold Services Controller application (`NMServiceManager.exe`) provides a single user interface to manage all Ipswitch WhatsUp Gold services. WhatsUp Gold services controller includes services that you can start, stop, or restart:



Note: Some services are optional. If the associated product is not licensed and enabled you may not be able to start and stop the service with the WhatsUp Services Controller dialog (Ipswitch Services Control Manager). Your license file determines whether or not you can access a plug-in. To update your license to purchase WhatsUp Gold Flow Monitor, VoIP plug-in, WhatsConnected, or WhatsConfigured, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

- Polling Engine (`nm-service.exe`)
- Flow Collector (`bwcollector.net.exe`)
- Alert Center (`alertcenterservice.exe`)
- Trivial File Transfer Protocol Server (`TFTPservice.exe`)
- Whats Configured (`networkconfigservice.exe`)
- Discovery (`discoveryservice.exe`)
- Failover Manager (`nmfailover.exe`)
- API (`nmapi.exe`)
- Whats Connected Data Service (`networkviewerdataservice.exe`)
- Whats Virtual Service (`whatsvirtualservice.exe`)

This application communicates with the Ipswitch Service Control Manager service (`ServiceControlManager.exe`) to issue start, stops, and restarts to the services used by WhatsUp Gold and its plug-in applications.

The following information is displayed in the WhatsUp Services Controller dialog:

- **Description.** Lists the description of the WhatsUp service, as gathered by the Ipswitch Service Control Manager service.
- **Process Name.** Lists the WhatsUp process .exe as listed in the Windows Task Manager Process tab.
- **Status.** Lists the current state of the service.

To stop a WhatsUp Gold or plug-in service:

- 1 Go to the WhatsUp Services Controller dialog.
 - From the console, select **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
- or -
 - From the the Programs menu, click **Ipswitch WhatsUp Gold > Utilities > Service Manager**. The WhatsUp Services Controller dialog appears.
- 2 In the WhatsUp Service Controller, select the service you want to stop by clicking its service **Description**.
- 3 Click **Stop**.

To start a WhatsUp Gold or plug-in service:

- 1 Go to the WhatsUp Services Controller dialog.
 - From the console, select **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
- or -
 - From the the Programs menu, click **Ipswitch WhatsUp Gold > Utilities > Service Manager**. The WhatsUp Services Controller dialog appears.
- 2 In the WhatsUp Service Controller, select the service you want to start by clicking its service **Description**.
 - Click **Start**.

To restart a WhatsUp Gold or plug-in service:

- 1 Go to the WhatsUp Services Controller dialog.
 - From the console, select **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
- or -
 - From the the Programs menu, click **Ipswitch WhatsUp Gold > Utilities > Service Manager**. The WhatsUp Services Controller dialog appears.
- 2 In the WhatsUp Service Controller, select the service you want to restart by clicking its service **Description**.
- 3 Click **Restart**.

Setting Advanced Options

You can set advanced options to configure the timeout and number of retries for the monitor.

Type or select the appropriate information in the following fields.

- **Timeout (seconds).** Type the amount of time (in seconds) you want WhatsUp Gold to attempt collecting data on a device.
- **Number of Retries.** Type the number of times you want WhatsUp Gold to attempt collecting data, when the device does not respond.

- **Use in Rescan.** Select this option to have the monitor appear in the Active Monitor list on the Device Properties dialog. WhatsUp Gold adds the monitor type to the device during a rescan, which is launched using the Rescan button on the Device Properties dialog, if the protocol or service is active on the device.

Click **OK** to save changes.

Types of SNMP Trap Monitors

The SNMP Trap monitors listed in the Passive Monitor Library are based on one of three things:

- **Passive monitors already in the database.** By default, the passive monitor database comes with a few of the most Common SNMP traps already in it.
- **Passive monitors automatically created by WhatsUp Gold Trap Definition Import Tool.** Use the Trap Definition Import Tool to create SNMP Traps from MIB files stored in the `\Program Files\Ipswitch\WhatsUp\Data\Mibs` folder.
- **Passive monitors that you define yourself.** This can be done either by copying and pasting actual trap information directly from your existing logs, or by browsing the MIB for OID values that you are interested in, and adding the **Generic type (Major)** and **Specific type (Minor)** information if required.

Common SNMP Traps

The SNMP standard provides a limited number of unsolicited messages (called traps) that are sent from a device to an SNMP application. These messages can be sent by the SNMP agent on the device to notify an SNMP application of a change in status. There are six standard traps (numbered 0 through 5) as well as vendor-provided traps (6):

| Trap # | Trap | Description |
|--------|-----------------------|---|
| 0 | Cold start | The device is rebooting itself and may change its configuration or the SNMP agent's configuration. |
| 1 | Warm start | The device is rebooting itself but neither the device's nor the SNMP agent's configuration will change. |
| 2 | Link down | One of the communication links for the device is down. |
| 3 | Link up | One of the communication links for the device is back up. |
| 4 | Authorization failure | The device has received a protocol message that is not properly authenticated. |
| 5 | EGP neighbor loss | An EGP neighbor for which the device is an EGP peer is down and the peer relationship no longer exists. |
| 6 | Vendor-provided traps | The SNMP specification lets vendors define enterprise specific traps, for example a trap that occurs on a particular vendor's router. |

Select computer

Use this dialog to connect to another computer on which you have administrator rights in order to browse that computer's WMI or SNMP Performance counters.

- **Select counters from computer.** Enter the computer name or IP address of the computer to which you want to connect.

For WMI (The following options are not available when selecting an WMI counter.)

- **Computer name.** Enter the computer name or IP address for which you want to set up a performance counter. Click browse (...) to select another device.
- **Windows credential.** Select a credential from a list of Windows credentials (pulled from the Credentials Library). Click browse (...) to select, add, or edit credentials in the Credential Library dialog.

For SNMP (The following options are not available when selecting a SNMP counter.)

- **SNMP v1/v2/v3 credentials.** Select valid SNMP credentials for this computer. Click browse (...) to select other credentials.
- **Timeout.** The amount of time (in seconds) you want the system to wait before failing the connection to the computer.
- **Retries.** The number of times you want the computer to attempt to make the connection to the selected computer.

Click **OK** to save changes.

FTP server user permissions

In order for the FTP Monitor to work properly, you must specify a user account that has been granted the appropriate permissions.

Performing file actions

- To **upload** files to the server, the account must have *write* permissions.
- To **download** files from the server, the account must have *read* permissions.
- To **delete** files from the server, the account must have *delete* permissions.



Important: If you configure an FTP Monitor to perform all three tasks, the account must have been granted the write, read, and delete permissions.

WMI

Windows Management Instrumentation (WMI) is a Microsoft Window's standard for retrieving information from computer systems running Windows. Refer to the Micsrosoft web site for information about enabling WMI on a Windows systems.

Event Viewer

Access the WhatsUp Gold Event viewer from `\Program Files\Ipswitch\WhatsUp\EventViewer.exe`.

Payload Definition

The monitor payload is the vital data that is being passed within a packet or other transmission unit. A monitor payload can include things like the event name, the IP address that the event came from, date of the event, etc. The payload does not include the "overhead" data required to get the packet to its destination. Generally speaking, the payload are the bits that get delivered to the end user at the destination.

SMS Providers

Select a country, then select a Provider in that country.

- Select a country, then click **New** to add another provider for that country.
- Select a provider, then click **Edit** to make changes to an existing provider.
- Select a provider, then click **Delete** to remove a provider.

Setting Modem Connection Preferences

- Modem Initialization String (ATE0). The default string is `ATE0Q0V1X4F1`.
- (E0) Command Echo Off
- (Q0) results code
- (V1) verbal results code (as opposed to numeric)
- (X4) result codes for some specific phone/modem conditions (see modem manufacturer for details)
- (F1) local echo off
- **COM Port**. Select the port to which your modem is attached.

- **Baud Rate.** Select the speed (measured in bits per second) at which the serial port communicates with the modem.



Note: Newer modems (e.g. 56K versions) may be utilized if their rate of transfer can be stepped down to a maximum of 2400 bps (TAP specification). However, some newer modems can not be made to transfer below 9600 bps even though you may use an initialization string that specifies a lower rate of transfer.

- **Data bits.** Select the type of data bit transmission used to communicate with the selected port. 6, 7, or 8 data bits.
- **Parity.** Select the type of parity expected by the modem connected to the selected serial port.
- **Stop.** Select the stop bits used to communicate with the selected port. 1 or 2 data bits.

Configure Memory Threshold

Enter the amount of free memory, in kilobytes, that the SQL server needs to have available for optimum performance. If the amount of free memory falls below this threshold, the monitor is considered down.

Configure Disk Performance - Exchange

Set thresholds on disk reads and writes for the Exchange server host.

| Property | Definition |
|-------------|--|
| Bytes read | Enter the maximum number of bytes read per second allowed before the monitor fails. |
| Bytes write | Enter the maximum number of bytes written per second allowed before the monitor fails. |

Configure System Thresholds

Sets the upper limit threshold on system properties that when exceeded causes the monitor to fail.

| Property | Definition |
|------------------|--|
| Context switches | The rate of switches from one thread to another, per second. Thread switches can occur either inside of a single process or across processes. A thread switch can be caused either by one thread asking another for information, or by a thread being preempted by another, higher-priority thread becoming ready to run. Windows NT uses process boundaries for subsystem protection, in addition to user and privileged modes. Thus some work done by Windows NT on behalf of an application appears in other subsystem processes in addition to the privileged time in the application. Switching to the subsystem causes one context switch in the application thread. Switching back causes another context switch in the subsystem thread. |
| CPU queue length | Number of threads in the processor queue. There is a single queue for processor time even on computers with multiple processors. Unlike disk counters, this property counts ready threads only, not threads that are running. A sustained processor queue of greater than two threads generally indicates processor congestion. This property displays the last observed value only; it is not an average. |
| System calls | Combined rate of calls to Windows NT system server routines by all processes running on compute, per second. These routines perform all of the basic scheduling and synchronization of activities on the computer, and provide access to non- graphic devices, memory management, and name space management. This property displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. |

Configure Links Thresholds

You can set thresholds on the following Links properties. For each of these properties, you set the value that is the upper limit, which when exceeded causes the monitor to fail.

| Property | Definition |
|--------------------|--|
| Number of messages | The number of messages that are waiting for transmission across the link. |
| Size of queue | The total size of the messages in the link, in Kilobytes. |
| Increasing time | The amount of time, in seconds, that the number of messages waiting to be transferred by the link has been increasing. |
| Oldest message | The elapsed time, in minutes, since the oldest message that is still waiting to be transmitted was received into the link. |

Configure Queues Thresholds

You can set thresholds on the following Queues properties. For each of these properties, you set the value that is the upper limit, which when exceeded causes the monitor to fail.

| Property | Definition |
|--------------------|---|
| Number of messages | The number of messages that are waiting for transmission in the queue. |
| Size of queue | The total size of all messages in the queue, in Kilobytes. |
| Increasing time | The amount of time, in seconds, that the number of messages waiting to be transferred in the queue has been increasing. |

Adding Custom Thresholds

After selecting the Custom Thresholds parameter, you are presented with the opportunity to specify any performance counter you want to monitor. This dialog shows the performance counters you have selected, as well as the upper and lower thresholds you have selected.

- Click the **Add** button to begin adding your settings.
- Select a performance counter in the list and click **Edit** to make changes to the settings.
- Select a performance counter in the list and click **Remove** to delete the entry.

FTP server user permissions

In order for the FTP Monitor to work properly, you must specify a user account that has been granted the appropriate permissions.

Performing file actions

- To **upload** files to the server, the account must have *write* permissions.
- To **download** files from the server, the account must have *read* permissions.
- To **delete** files from the server, the account must have *delete* permissions.



Important: If you configure an FTP Monitor to perform all three tasks, the account must have been granted the write, read, and delete permissions.

Configure Disk Performance

Set a threshold on the amount of disk reads used by your SQL server.

| Property | Definition |
|-------------|--|
| Bytes read | Enter the maximum number of bytes read per second allowed before the monitor fails. |
| Bytes write | Enter the maximum number of bytes written per second allowed before the monitor fails. |

Configure Disk space Threshold

Sets a threshold on the free disk space for your SQL server host.

| Property | Definition |
|---------------------------------------|--|
| Disk Drive | The drive letter of the drive on which the SQL server is installed. |
| Free space must not be below (MBytes) | The amount of free disk space that the SQL server needs to have or the action fails. |

Configure System Threshold

Enter the maximum number of processes allowed before the monitor fails.

Configure Buffers Threshold

You can set thresholds on the following Buffer properties.

| Property | Definition |
|-------------|--|
| Pages read | Enter the maximum number of physical database page reads issued per second. Any number above this will cause the monitor to fail. |
| Pages write | Enter the maximum number of physical database page writes issued per second. Any number above this will cause the monitor to fail. |

Configure Locks Threshold

You can set thresholds on the following Lock properties.

| Property | Definition |
|---|---|
| The average lock wait time must not be above: | Enter the maximum average wait time (in milliseconds) for each lock request to be allowed before the monitor fails. |
| The number of lock waits must not be more than: | Enter the maximum number of waits requested per second to be allowed before the monitor fails. |

Configure Cache Threshold

You can set thresholds on the following Cache properties.

| Property | Definition |
|---|---|
| The cache hit ratio must be greater than: | Enter the minimum of total uses expected. If the value is less than the threshold, the monitor fails. |
| The cache use count must be greater than: | Enter the minimum number of cache object uses expected (per second.) If the number is lower, the monitor fails. |

Configure Transactions Threshold

You can set thresholds on the following Transaction properties:

| Property | Definition |
|--|---|
| The number of active transactions must not be above: | Enter the maximum number of active transactions allowed before the monitor fails. |
| The number of transactions per second must not be above: | Enter the maximum number of transactions allowed (per second) before the monitor fails. |

Configure Users Threshold

You can set the threshold on the following User properties.

| Property | Definition |
|--|---|
| The number of logins must not be above: | Enter the maximum number of logins allowed (per second) before the monitor fails. |
| The number of connections must not be above: | Enter the maximum number of connections allowed before the monitor fails. |

Configure Alerts Threshold

You can configure WhatsUp Gold to monitor alerts generated by SQL Server.



Note: Before the alert can be monitored, you must configure your System Data Source (ODBC) name for the SQL Server.

- **DSN.** This field controls the connection to the DSN configured for the SQL server. The following show the proper way to structure entries for this field:
- You can enter just the DSN. For example: Whatsup
- You can specify the DSN in the form of DSN=Whatsup as well.

- This field also works as a connection string that you can specify for the connection to the SQL server.

For example: `Provider=sqloledb.2;Server=ARNOR\WHATSUP`

- If you specify the DSN the plug-in will use the field as is. If you leave it blank, the monitor uses the following string to connect:

`Provider=sqloledb;Server=<the device's IP address>\<the specified instance on the main dialog>;`

- If you enter a connection string not a DSN name, the plug-in will try to fill the parts that are missing:
 - If Provider is missing, the plug-in will use `Provider=sqloledb;`
 - If Server is missing the plug-in will use `Server=<the device's IP address>\<the specified instance of the main dialog>;`
- **Use SQL Server Authentication.** Select this option to use SQL Server Authentication to connect to your database for the monitor. If this option is not used, the connection is made by the settings in the DSN, or with the windows credentials configured for the device the monitor is assigned to. Once the option is selected, enter your username and password for the server.
- **Log entry severity range.** WhatsUp Gold will only monitor alerts that match the severity range entered in these boxes.
- **Only track log entries since last poll.** Select this option to have WhatsUp Gold track only those alerts that occurred since the last poll.
- **Log entry threshold.** The maximum number of alerts generated by the SQL Server that WhatsUp Gold allows before considering the monitor will fail.

SQL Server Services

You can monitor the following critical SQL services to determine whether the service is available (Up) or is disabled (Down).

| Select this process: | If you want to: |
|-------------------------------------|--|
| MSSQLSERVER | This is the database engine. It controls processes all SQL functions and manages all files that comprise the databases on the server. |
| SQLSERVERAGENT | This service works with the SQL Server service to create and manage local server jobs, alerts and operators, or items from multiple servers. |
| Microsoft Search | A full-text indexing and search engine. |
| Distributed Transaction Coordinator | The MS DTC service allows for several sources of data to be processed in one transaction. It also coordinates the proper completion of all transactions to make sure all updates and errors are processed and ended correctly. |
| SQL Server Analysis Services | Implements a highly scalable service for data storage, processing, and security. |

| Select this process: | If you want to: |
|------------------------------------|---|
| SQL Server Reporting Services | Used to create/manage tabular, matrix, graphical, and free-form reports. |
| SQL Server Integration Services | A platform for building high performance data integration solutions. |
| SQL Server FullText Search | Issues full-text queries against plain character-based data in SQL Server tables. |
| SQL Server Browser | Listens for incoming requests for SQL Server resources and provides information about SQL Server instances installed on the computer. |
| SQL Server Active Directory Helper | View replication objects, such as a publication, and, if allowed, subscribe to that publication. |
| SQL Server VSS Writer | Added functionality for backup and restore of SQL Server 2005. |

Selecting a Device

You can select a device group from which you want to view a list of devices. Click **+** to expand the preferred device group. The device list displays.

Select a device from the list, then click **OK**.

Selecting computers

You can connect to another computer on which you have administrator rights in order to browse that computer's WMI or SNMP Performance counters.

- **Select counters from computer.** Type the computer name or IP address of the computer to which you want to connect.

For WMI (The following options are not available when selecting an WMI counter.)

- **Computer name.** Type the computer name or IP address for which you want to set up a performance counter. Click browse (...) to select another device.
- **Windows credential.** Select a credential from a list of Windows credentials (pulled from the Credentials Library). Click browse (...) to select, add, or edit credentials in the Credential Library dialog.

For SNMP (The following options are not available when selecting a SNMP counter.)

- **SNMP v1/v2/v3 credentials.** Select valid SNMP credentials for this computer. Click browse (...) to select other credentials.
- **Timeout.** The amount of time (in seconds) you want the system to wait before failing the connection to the computer.

- **Retries.** The number of times you want the computer to attempt to make the connection to the selected computer.

Click **OK** to save changes.

Configuring CPU Threshold

Type the percentage of CPU capacity that, when exceeded, causes the monitor to fail.

Setting Advanced Properties for a HTTP Content Monitor

You can configure the user agent and custom headers for the HTTP Content Monitor.

Type or select the appropriate information in the following fields.

User agent

The user agent string identifies which web browser is making an HTTP request. You can use this to imitate your web site being visited by various browsers. Select a browser from the list. The user agent from the latest version of the browser is populated for the browser you select. You can use this agent string, or enter a different user agent string for the version of the browser that you want WhatsUp Gold to check.

Custom headers

Enter any specific headers for which you want the monitor to check. Enter a header as Field:Value. You can enter up to three custom headers.



Note: Errors can result when using invalid custom headers or when modifying headers that do not allow modification, such as the HTTP Host header. You can test custom headers by clicking Request URL contents on the New/Edit HTTP Content Monitor dialog. If there is a problem with the header, an error message displays the problem. For example,



"An error occurred with the requested website. Error: The 'Host' header cannot be modified directly. Parameter name: name."



In this example, a user entered `Host :myhost.com` as a custom header. However, the Host header cannot be modified and an error generated as a result.

Click **OK** to save changes.

Setting Advanced Properties for an Email Active Monitor

You can configure the advanced properties for the Email Monitor.

Type or select the appropriate information in the following fields.

SMTP Advanced Properties

- **SMTP server requires authentication.** Select this option if your SMTP server requires authentication.



Note: The Email Monitor supports CRAM-MD5, LOGIN and PLAIN authentication methods. The authentication method is not configurable. It is negotiated with the SMTP server automatically using the strongest mutually supported authentication method.

- **Username.** Type the username to be used with SMTP authentication.
- **Password.** Type the password of the username to be used with authentication.
- **Use an encrypted connection (SSL/TLS).** If your SMTP server supports encrypting data over a TLS connection (formerly known as SSL), select this option to encrypt SMTP traffic.



Note: For SMTP connections, WhatsUp Gold only supports explicit SSL sessions negotiated using the STARTTLS command.

- **Timeout.** Type the amount of time (in seconds) to wait for a response from the SMTP server for each command WhatsUp Gold issued. If this time limit is exceeded, the monitor fails.

Incoming server (IMAP or POP3) advanced properties



Note: WhatsUp Gold supports only clear text authentication method for retrieving mail. To protect your username and password while retrieving mail, you must use one of the SSL encryption methods.

- **Port.** Type the port on which your POP3 or IMAP server is running.
- **Use an encrypted connection.** Select this option to connect to a POP3 or IMAP server in an encrypted mode. Select one of the following encryption methods:
 - **Use implicit SSL.** Select this option to login to your POP3 or IMAP server in an encrypted mode.
 - **Use SSL with STLS.** Select this option to login to your POP3 or IMAP server in an unencrypted mode, and then switch to a TLS connection by sending STARTTLS or STLS command to the server.



Important: When connecting using STARTTLS, the connection is encrypted before any authentication information is sent or any mail is retrieved.

- **Timeout.** Type the amount of time (in seconds) to wait for a response from the IMAP/POP3 server for each command WhatsUp Gold issued. If this time limit is exceeded, the monitor fails.



Note: If your IMAP server is configured to move the test message sent by the monitor to a folder other than the Inbox, the monitor fails. WhatsUp Gold only detects messages in the Inbox folder on an IMAP server.

Click **OK** to save changes.

Selecting a blackout period

Select the day and time you want the action placed in blackout period, and when you want WhatsUp Gold to begin using the Action. You can select multiple days for a single time period.

Click **OK** to add the schedule to the device.

Importing a MIB file

- 1 In the **MIB file to upload to the MIB directory** box, type a new MIB file directory path and file name (for example, `\Program Files\Cisco\Mibs\<NewFile-MIB.txt>`), or click **Browse...** to navigate and select the file from the File Upload dialog.
- 2 Click **OK** to import the MIB file into the WhatsUp Gold MIB directory (`\Program Files\Ipswitch\WhatsUp\Data\Mibs\<NewFile-MIB.txt>`). The MIB viewer opens and the MIB file is validated. If errors exist in the MIB, the summary information at the top of the page will identify the number of errors or warnings.



Note: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

Hub Transport Server Role Thresholds

The following table lists the threshold settings available for the Hub Transport Server category:

| Threshold | Description | Value |
|--------------------------|--|------------------------|
| Aggregate Delivery Queue | The Aggregate Delivery Queue holds the aggregate value of all of the messages queued for delivery in all of the queues associated with the Hub Transport Server. | Default: 3000 messages |
| Active Remote Delivery | The Active Remote Delivery queue holds messages that are being | Default: 250 messages |

| Threshold | Description | Value |
|--------------------------------|--|-----------------------|
| Queue | delivered to a remote server using SMTP. | |
| Active Mailbox Delivery Queue | The mailbox delivery queue holds messages that are being delivered to a mailbox server by using encrypted Exchange RPC. | Default: 250 messages |
| Submission Queue | A persistent queue that is used by the categorizer to gather all messages that have to be resolved, routed, and processed by Transport agents | Default: 100 |
| Active Non-SMTP Delivery Queue | The Active Non-SMTP Delivery queue holds messages that are being delivered to a remote server, using a protocol other than SMTP. | Default: 100 |
| Retry Mailbox Delivery Queue | The Retry Mailbox Delivery Queue holds messages with a status of Retry that are being delivered using encrypted Exchange RPC. Messages are given a status of retry when the server cannot connect to the next hop. | Default: 100 |
| Retry Non-SMTP Delivery Queue | The Retry Mailbox Delivery Queue holds messages with a status of Retry that are being delivered using a protocol other than SMTP. | Default: 100 |
| Retry Remote Delivery Queue | The Retry Mailbox Delivery Queue holds messages with a status of Retry that are being delivered using SMTP. | Default: 100 |
| Unreachable Queue | The Unreachable queue is a persistent queue that contains messages that cannot be routed to their destinations. | Default: 100 |
| Largest Delivery Queue | The Largest Delivery queue identifies the largest of all of the delivery queues on the Exchange server. | Default: 200 |
| Poison Queue | The poison message queue is a special queue that is used to isolate messages that are detected to be potentially harmful to the Exchange 2007 system after a server failure. | Default: 0 |

Select Action Type

Select an action type from the list menu. The configuration dialog for that type appears.

Select the type of action you want to create for this device. The menu lists all possible actions that can occur through the WhatsUp Gold action system.

- **Active Script Action.** Write code to perform a customized action.
- **Beeper Action.** Activate a beeper with this type of action.
- **Email Action.** Send an Email to a specific address.
- **Log to Text File.** Write a message to a text file.
- **Pager Action.** Send a message to a pager.
- **Program Action.** Execute an external application.
- **Service Restart Action.** Start or stop a Windows service.
- **SMS Action.** Send a text message to a specific target.
- **SMS Direct.** Send a text message to a wireless phone or other wireless device.
- **SNMP Set.** Use SNMP to set the value of an attribute of a managed object.
- **Sound Action.** Play a specific sound.
- **SSH Action.** Runs a command or script on a remote machine.
- **Syslog Action.** Write a message to a log in the Syslog system.
- **Text to Speech Action.** Plays a voice message on your computer.
- **VMware Action.** Use the VMware API to perform an action on a virtual machine.
- **Web Alarm Action.** Activate a Web Alarm in the WhatsUp Gold Web Interface
- **Windows Event Log Action.** Write an event in the Windows Event Log.
- **Winpopup Action.** Send a Winpopup to a user or specific computer.

WinEvent Condition

- **Not.** Select this option to filter the conditions that match the string.
- **Parameter.** Select a Windows Event Log parameter to match on.
- **Category.** Subcategory for this event. This subcategory is source-specific.
- **CategoryString.** Translation of the subcategory. The translation is source-specific.
- **Computer.** The computer that the event took place on.
- **Event ID.** Identifier of the event. This is specific to the source that generated the event log entry, and is used, together with Source, to uniquely identify a Windows NT event type.
- **Event Type.** Type of event.

Value and Meaning of the Event Type:

- 1 Error
- 2 Warning

3 Information

4 Security audit success

5 Security audit failure

- **Logfile.** Name of Windows NT event log file.
- **Description.** Use this parameter to give a brief description of the logged event.
- **Source.** Name of the source (application, service, driver, subsystem) that generated the entry. It is used, together with EventIdentifier to uniquely identify an Windows NT event type.
- **Type.** Type of event. This is an enumerated string. It is preferable to use the EventType property rather than the Type property, because Type is a string. Strings are localized and using Type will not allow for matching on non-English operating systems.
- **User.** User name of the logged-on user when the event occurred. If the user name cannot be determined, this will be NULL.
- **Operator.** Select the operator that links the parameter to the value.
=, >, <, > =, < =, !=
- **Value.** Enter a value for the selected parameter.
- **And/Or.** You may select and/or to add another condition to the string.

Using SNMP Features

In This Chapter

| | |
|---|-----|
| SNMP overview | 898 |
| Enabling SNMP on Windows devices..... | 899 |
| Monitoring an SNMP Service..... | 899 |
| About the SNMP Agent or Manager | 900 |
| About the SNMP Management Information Base | 900 |
| About SNMP Object Names and Identifiers..... | 901 |
| Using the SNMP MIB Manager..... | 901 |
| Using the SNMP MIB Manager to troubleshoot MIB files..... | 902 |
| About the SNMP operations..... | 904 |
| Using a custom name for SNMP device interfaces | 905 |
| About SNMP Security | 908 |
| Using the Trap Definition Import Tool..... | 908 |

SNMP overview

The Simple Network Management Protocol (SNMP) defines a method by which a remote user can view or change management information for a device (a host, gateway, server, etc.).

A monitoring or management application on the remote user's system uses the protocol to communicate with an SNMP agent on the device to access the management data.

The SNMP agent on each device can provide information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the Management Information Base (MIB). The MIB defines the SNMP objects that can be managed and the format for each object.

The SNMP protocol together with the MIB provide a standard way to view and change network management information on devices from different vendors. Any application that implements SNMP can access MIB data on a specified device. For a detailed description of SNMP, see Request for Comments (RFC) 1157. For a description of the MIB, see RFC 1213. The MIB information used by WhatsUp Gold is contained in MIB files in the MIB directory (`..\Program Files\Ipswitch\WhatsUp\Data\Mibs`).

Enabling SNMP on Windows devices

Before you can collect performance data on a Windows computer using SNMP, you must first install and enable the Microsoft SNMP Agent on the device itself. For more information, see *Using SNMP Features* (on page 898).

To install SNMP Monitoring:

- 1 From the Windows Control Panel, click **Add or Remove Programs**.
- 2 Click **Add/Remove Windows Components**.
- 3 From the Components list, select **Management and Monitoring Tools**.
- 4 Click **Details** to view the list of Subcomponents.
- 5 Make sure Simple Network Management Protocol is selected.
- 6 Click **OK**.
- 7 Click **Next** to install the components.
- 8 After the install wizard is complete, click **Finish** to close the window.

To enable SNMP Monitoring:

- 1 In the Control Panel, click **Administrative Tools**.
- 2 Double-click **Services**. the Services console appears.
- 3 In the Services (Local) list, double-click **SNMP Service** to view the Properties.
- 4 On the **Agent** tab, enter the **Contact** name for the person responsible for the upkeep and administration of the computer, then enter the **Location** of the computer. These items are returned during some SNMP queries.
- 5 On the **Security** tab, click **Add** to add a community string for the device. Community strings are pass codes that allow applications like WhatsUp to read information about the computer. This community string will be later used to create credentials for connecting to this device.
- 6 On the **General** tab, click **Start** to start the service (if necessary).
- 7 Click **OK** to close the dialog.

You can test the device by connecting to it through SNMP View.

Monitoring an SNMP Service

You can add an SNMP active monitor to check that the SNMP service is running on a device. For more information, see *Assigning active monitors* (on page 226).

To assign an SNMP Active Monitor to a device:

- 1 Under the **Devices** tab, on the **Device View** or **Map View** tab, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Active Monitors**. The Device Properties Active Monitor dialog appears.
- 3 Click **Add**. The Select Active Monitor Type dialog appears.

- 4 Select the **SNMP Active Monitor**, then click **Next**. The Set Polling Properties dialog appears.
- 5 Click to select **Enable polling for this Active Monitor**, select the **Network interface to use for poll** from the list, then click **Next**.
- 6 (Optional) Set up an Action for the monitor state changes.
- 7 Click **Finish** to add the monitor to the device.



Note: An SNMP-manageable device is identified on the map by a star in the upper-right corner of the device.

About the SNMP Agent or Manager

SNMP agent software must be installed and enabled on any devices for which you want to receive SNMP information. Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 all provide an SNMP agent in their default installations. Network systems manufacturers provide an SNMP agent for their routers, hubs, and other network boxes.

For more information, see *About the SNMP operations* (on page 904) and *Enabling SNMP on Windows devices* (on page 899).

About the SNMP Management Information Base

The SNMP Management Information Base (MIB) contains the essential objects that make up the management information for a device. The Internet TCP/IP MIB, commonly referred to as MIB-II, defines the network objects to be managed for a TCP/IP network and provides a standard format for each object.

The MIB is structured as a hierarchical object tree divided into logically related groups of objects. For example, MIB-II contains the following groups of objects:

- **System.** Contains general information about the device, for example: sysDescr (description), sysContact (person responsible), and sysName (device name).
- **Interfaces.** Contains information about network interfaces, such as Ethernet adapters, or point-to-point links; for example: ifDescr (name), ifOperStatus (status), ifPhysAddress (physical address), ifInOctets, and ifOutOctets (number of octets received and sent by the interface).
- **IP.** Contains information about IP packet processing, such as routing table information: ipRouteDest (the destination), and ipRouteNextHop (the next hop of the route entry).

- Other groups provide information about the operation of a specific protocol, for example, TCP, UDP, ICMP, SNMP, and EGP.
- The **enterprise** group contains vendor-provided objects that are extensions to the MIB.

Each object of the MIB is identified by a numeric object identifier (OID) and each OID can be referred to by its text label. For example, the system group contains an object named *sysDescr*, which provides a description of the device. The *sysDescr* object has the following object identifier:

```
iso.org.dod.Internet.mgmt.mib.system.sysDescr  
1.3.6.1.2.1.1.1
```

This object identifier is 1.3.6.1.2.1.1.1 to which is appended an instance sub-identifier of 0. That is, 1.3.6.1.2.1.1.1.0 identifies the one and only instance of *sysDescr*.

All of the MIB-II objects (for TCP/IP networks) are under the "mib" sub tree (so all these objects will have an identifier that starts with 1.3.6.1.2.1).

For a detailed description of the MIB, see RFC 1213.

About SNMP Object Names and Identifiers

Each SNMP object has a name and numeric identifier. For example, in the *system* group, the network object named *SysDescr* with object identifier 1.3.6.1.2.1.1.1 contains a description of the device.

An object can have one or more instances, depending on the configuration of the monitored device. For example, a device can have two network adapters, in which case there will be two instances of the *ifPhysAddress* object, which has object identifier 1.3.6.1.2.1.2.2.1.6. In this case, you need to specify an instance number at the end of the object identifier (such as 1.3.6.1.2.1.2.2.1.6.1). If you do not specify an instance, it defaults to zero.

Using the SNMP MIB Manager

The SNMP MIB Manager provides a list of all of the MIB files installed in the WhatsUp Gold MIB directory. Using this tool, you can import new MIB files to the MIB Manager. SNMP MIB Manager validates imported MIB files and flags errors if there is a problem with a file.

To use the SNMP MIB Manager:

- 1 Go to the SNMP MIB Manager.
 - From the web interface, go to **Admin > SNMP MIB Manager**. The SNMP MIB Manager appears.
- 2 Use the following options in the SNMP MIB Manager:
 - **View**. Select a MIB file in the list, then click **View** to open the MIB and view the code.
 - **Add**. Click **Add** to import a MIB file to the MIB Manager. Follow the dialogs to complete the process.

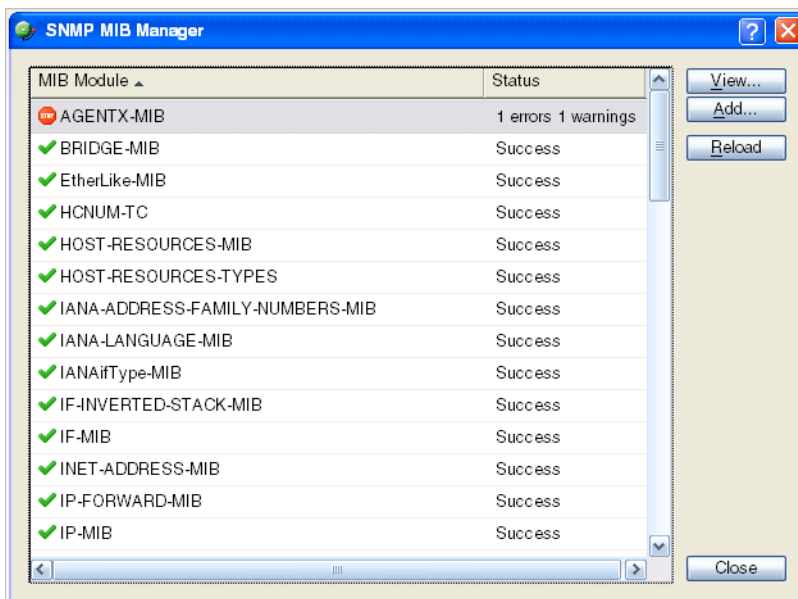


Note: If you need to add a large number of MIB files, you can manually copy them to the `\Program Files\Ipswitch\WhatsUp\Data\Mibs\` directory, then click **Reload** in the SNMP MIB Manager dialog to update and validate their status.

- **Reload**. When you import a new MIB file or are troubleshooting code in a MIB file, click Reload to refresh the MIB Module list and the Status list.

Using the SNMP MIB Manager to troubleshoot MIB files



The SNMP MIB Manager validates all MIB files that are imported into or already exists in WhatsUp Gold. If an error is identified in a MIB file, the Status column displays the number of errors and warnings in the file. If the MIB file syntax is correct and all MIB file dependencies are fulfilled, then a check mark is displayed next to the MIB file name and a Success message displays in the Status column.



Identifying MIB file problems and errors

If an error exists in a MIB file, you can use the MIB manager to identify where code problems exist, then open the MIB file in a text editor (for example, Notepad) and correct the code. There are a variety of issues that may exist in the code; for example, there may be a simple syntax error in the MIB file or there could be a MIB file that has a dependency on another MIB file. Use the error messages when you view a MIB file to find and correct the problem.

There are two types of errors that may display in the SNMP MIB Manager list:

-  (Warning). This indicates a minor issue with the MIB file (for example, a small syntax problem). A MIB file that contains a warning may continue to work, but it is best to identify and correct the issue in the MIB file.
-  (Error). This indicates there is a problem in the MIB file that prevents it from working. A MIB file that contains an error must have the error corrected in order for the MIB file to function.



Tip: The most common MIB errors are caused by a MIB dependency on another MIB file that is not included in the MIB library. Often, when this issue is corrected, many of the MIB issues are resolved.

Example: If a MIB is missing, the MIB Manager indicates the issue in an error as shown in this example excerpt from a MIB status report:

```
22      ipMRouteGroup, ipMRouteSource,
23      ipMRouteSourceMask, ipMRouteNextHopGroup,
24      ipMRouteNextHopSource, ipMRouteNextHopSourceMask,
25      ipMRouteNextHopIfIndex,
26      ipMRouteNextHopAddress          FROM IPMROUTE-STD-MIB
```

Error: Cannot find module (IANA-RTPROTO-MIB): At line 26 in
C:\PROGRA~1\Ipswitch\WhatsUp\Data\Mibs/IPMROUTE-STD-MIB.my

The important information in this report is:

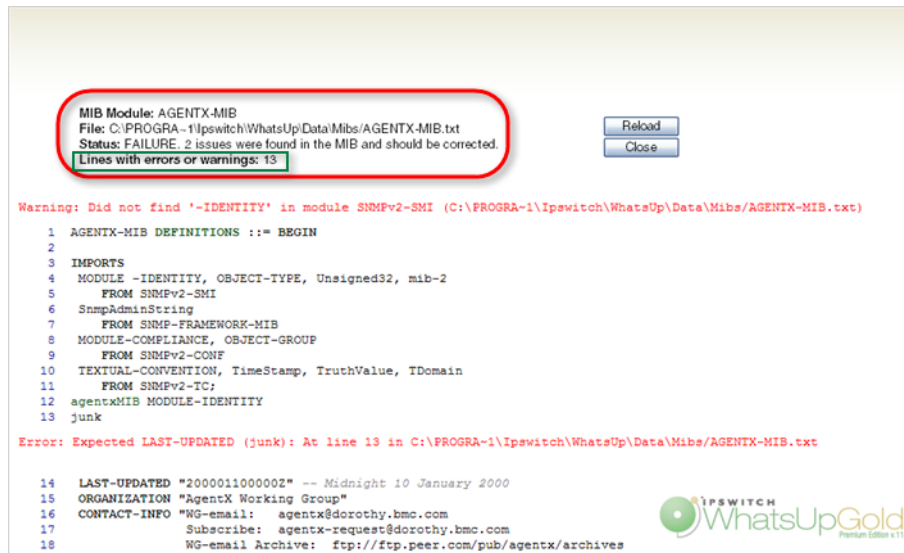
Cannot find module (IANA-RTPROTO-MIB).

This information indicates that the IANA-RTPROTO-MIB is missing from the MIB library in
C:\Program Files\Ipswitch\WhatsUp\Data\Mibs

If you determine that a MIB file is missing, you can manually copy the file to the \Program Files\Ipswitch\WhatsUp\Data\Mibs\ directory or use the SNMP MIB Manager dialog to add (import) a new MIB file.

To identify and correct MIB file code:

- 1 Select the MIB file that has an error message in the Status column, then click **View**. The viewer opens with summary information at the top of the page that identifies the number of errors or warnings. In the **Lines with errors or warnings** summary information, you can click the line number to jump directly to a line of code with the error.



- 2 Now that the Viewer has helped you identify the problems in the code, open a text editor and correct the code. The MIB files are located in `.. \Program Files\Ipswitch\WhatsUp\Data\Mibs`.
- 3 After you have made code changes, save the MIB file, then click **Reload** in the SNMP MIB Manager dialog.
- 4 Look for the MIB file, that you made changes to, in the list to determine if all the errors have been corrected. If all the errors have been corrected, click **Close**. If the SNMP MIB Manager dialog (validator) displays errors, continue repeating steps 1 through 3 until you have corrected all of the code issues.

About the SNMP operations

An SNMP application can read values for the SNMP objects (for monitoring of devices) and some applications can also change the variables (to provide remote management of devices). Basic SNMP operations include:

- **Get.** Gets a specified SNMP object for a device.
- **Get next.** Gets the next object in a table or list.
- **Set.** Sets the value of an SNMP object on a device.
- **Trap.** Sends a message about an event (that occurs on the device) to the management application.

The SNMP agent software on a device listens on port 161 for requests from an SNMP application. The SNMP agent and application communicate using User Datagram Protocol (UDP). Trap messages, which are unsolicited messages from a device, are sent to port 162.



Note: If an SNMP application makes a request for information about a device but an SNMP agent is not enabled on the device, the UDP packets are discarded.

Using a custom name for SNMP device interfaces

This feature lets you rename SNMP device interfaces to help you manage network interfaces more efficiently and intuitively. Without this feature you must reference device interface names, on a router for example, by their default names. Often, the device interface names are not intuitive and it is difficult to determine the specific interface you are selecting when setting up an interface utilization monitor for performance monitors and active monitors. This feature also helps you easily select the interface you want to view in interface utilization logs and other applicable dashboard reports and split second graphs.

Configuring a custom name (ifAlias) for an SNMP device interface

In order to configure a custom name (IfAlias) for a device's SNMP interface, you need to access the device configuration console and rename each interface according to your naming convention preference.

After the interface(s) are renamed, you can add them as performance monitors and active monitors. You can also select the custom interface in various dashboard reports and split second graphs. If the device interface(s) already have performance monitors and/or active monitors set up, the new interface name displays in WhatsUp Gold accordingly.

Use the following example instructions for how to change a Cisco router interface name. If you have other devices, refer to the device documentation for instructions on how to change interface names.

To configure a device custom name for an SNMP interface on a Cisco router:

- Open the Cisco Command Line Interface (CLI) and enter the following commands:

```
Cisco1812# configure
```

```
Cisco1812(config)# interface FastEthernet 9
```

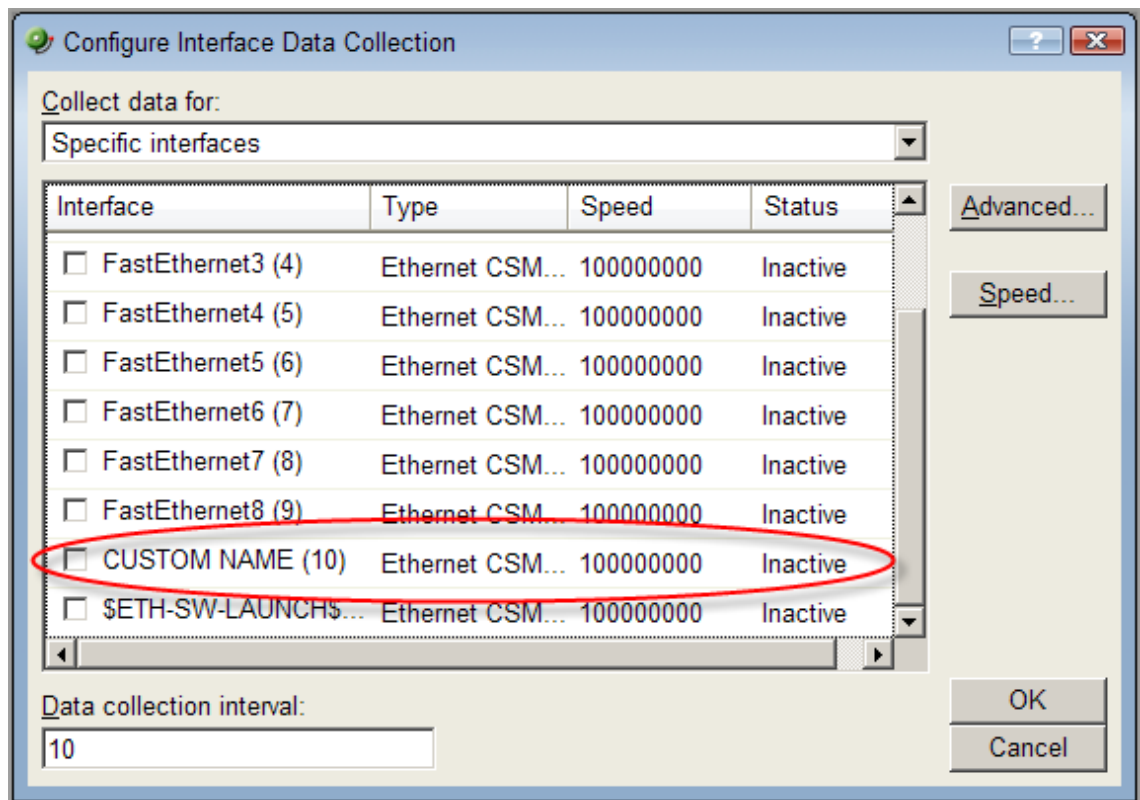
```
Cisco1812(config-if)# description CUSTOM NAME
```

```
Cisco1812(config-if)# ^Z
```

```
Cisco1812#
```

To add a Performance Monitor for a newly renamed device interface:

- 1 On the **Devices** tab, in **Device View** or **Map View**, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Performance Monitors**. The Performance Monitors dialog appears.
- 3 In the **Enable global performance monitors** section, click to select the **Interface Utilization** option, then click **Configure**. The Configure Interface Data Collection dialog appears.
- 4 In the **Collect data for** list, select **Specific Interfaces**. In this example, *CUSTOM NAME* is the interface name created for the Cisco router. Click to select **CUSTOM NAME**, then click **OK**.



- 5 Click **OK**, then click **Close** to close the Device Properties dialog.

To add an Active Monitor for a newly renamed device interface:

- 1 On the **Device View** (Console) or **Details View** (Web) or **Map View** tab, right-click a device, then click **Properties**. The Device Properties dialog appears.

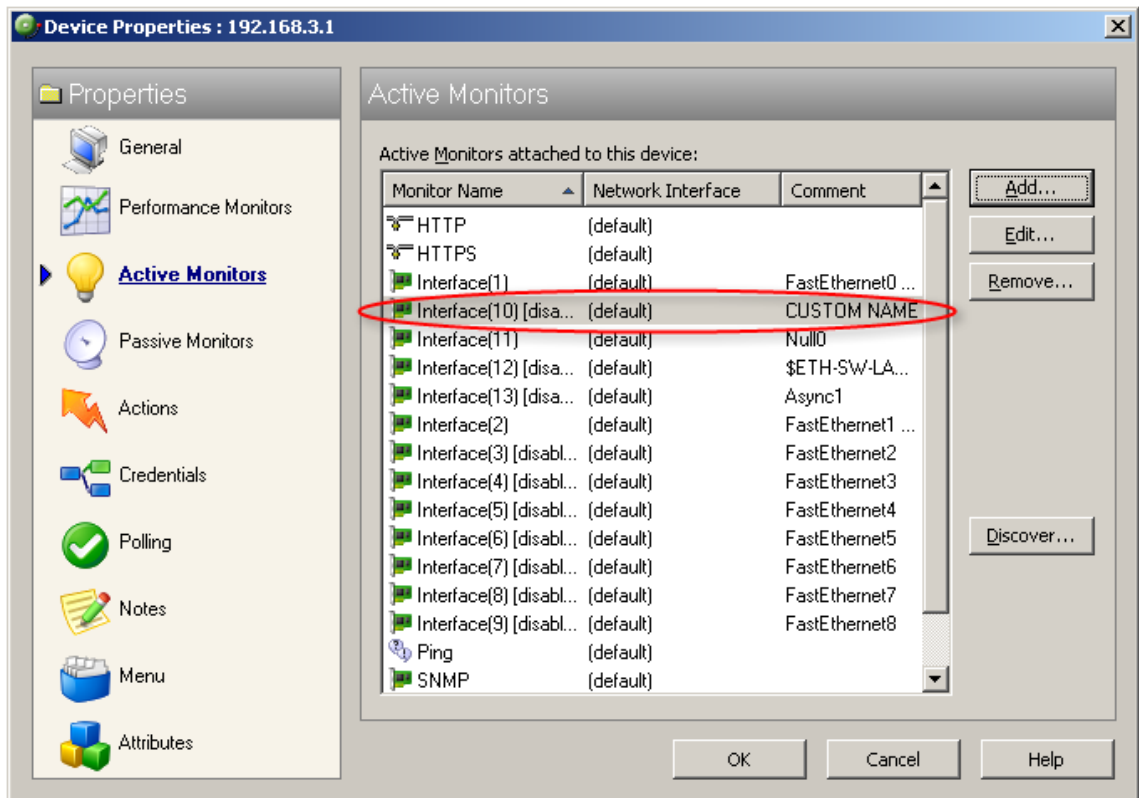
- Click **Active Monitors**. The Active Monitors dialog appears.



Important: If a device has active monitors set up prior to renaming the device's interface(s), then after renaming the device's interface(s), remove the old interface(s) from the Active Monitor dialog, then click **Discover** to refresh the device interface list. Use the console application for the discover process.

If a device has performance monitors set up prior to renaming the device's interface(s), the device interface names are automatically updated.

- (Optional) If a device has active monitors set up for a device prior to renaming the device's interface(s), select the interface(s) that you renamed from the list of interfaces, then click **Remove**.
- (Optional) Click **Discover**. The interface list refreshes and populates with the new interface names in the Comment list.



- Click **OK**, then click **Close** to close the Device Properties dialog.

To select a newly renamed device interface for the Interface Utilization report:

- From the web interface, go to **Monitoring > Interface**. The Interface log appears.
- Click the device name/IP address (shown above) to select the device you want to view. The Select a Device dialog appears.
- Expand the network tree list to view the SNMPScan devices, then select the device for which you want to view the Interface Utilization log. The Interface Utilization log appears.
- In the **Select Interface** list, select the newly named device interface. In this example, the interface is named `CUSTOM NAME`. View the interface utilization log.

About SNMP Security

In WhatsUp Gold, credentials are used like passwords to limit access to a device's SNMP data. The credentials system supports SNMP v1, v2, and v3.

Credentials are configured and stored in Credentials Library (**Configure > Credentials Library**) and used in several places throughout the application. They can be assigned to devices in **Device Properties > Credentials** or through the Credentials Bulk Field Change option.

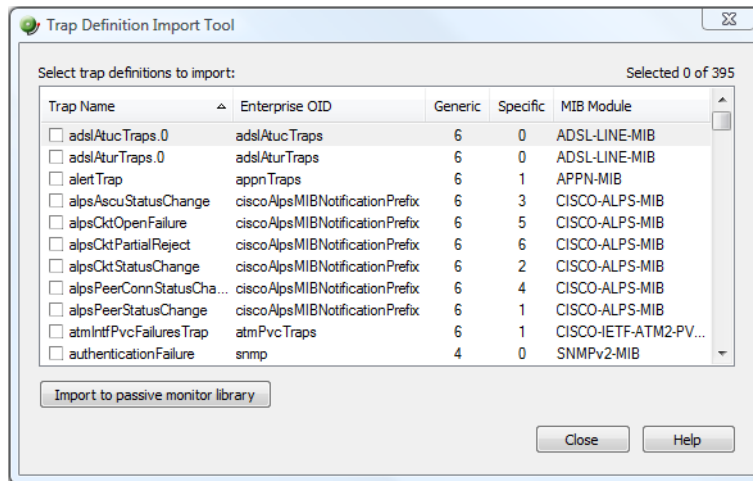
Devices need SNMP credentials assigned to them before SNMP-based Active Monitors will work.

Using the Trap Definition Import Tool

The Trap Definition Import tool is used to import SNMP Trap definitions into the Passive Monitor Library. The list in this dialog is populated by the MIBs typically in your WhatsUp Gold MIB folder (\Program Files\Ipswitch\WhatsUp\Data\Mibs).

To import SNMP trap definitions into the Passive Monitor Library:

- 1 In the WhatsUp Gold console, select **Tools > Import Trap Definitions**. The Trap Definition Import Tool dialog appears.



- 2 Select the traps you want to import, then click **Import to passive monitor library**. The Trap Import Results dialog appears and provides a message about the import results.



Note: Traps that already exist in the database are not imported.



Tip: Use the dialog's scroll bar to scan available traps.

Extending WhatsUp Gold with custom scripting

In This Chapter

| | |
|--|-----|
| Extending WhatsUp Gold with scripting..... | 909 |
| Scripting Active Monitors | 910 |
| Scripting Performance Monitors..... | 926 |
| Scripting Actions..... | 936 |
| Using the SNMP API..... | 942 |

Extending WhatsUp Gold with scripting

This section explains how to use the native development tools included in WhatsUp Gold to extend the product beyond its stock capabilities with Active Script Active Monitors, Performance Monitors, and Actions.

WhatsUp Gold includes three types of Active Scripts, which allow you to write custom JScript and VBScript code to do tasks that WhatsUp Gold cannot natively perform.

- **Active Script Active Monitors** perform specific customized checks on a device. They report their status as a success or failure, and the monitor's status effects the device's status in the same way that stock active monitors do. For more information, see *Scripting Active Monitors* (on page 910).
- **Active Script Performance Monitors** track specific values over time and can be used to generate logs and graphs of historical data. For more information, see *Scripting Performance Monitors* (on page 926).
- **Active Script Actions** can be configured to trigger when an active monitor's state changes. They can be programmed to perform a variety of tasks, from running automated remediation scripts to posting data to external, third party services via API. For more information, see *Scripting Actions* (on page 936).

About Active Script languages

Active scripts can be written in JScript or VBScript. For more information on either of these languages, consult the MSDN Language Reference for that language.

- *MSDN JScript User's Guide* (<http://www.whatsupgold.com/msdnjscript>)
- *MSDN VBScript User's Guide* (<http://www.whatsupgold.com/msdnvbscript>)



Note: Not all aspects of JScript and VBScript can be used in Active Scripts. In general, any function or method that involves the user interface level, such as VBScript's `MsgBox` or JScript's `alert()`, are not allowed.

Scripting Active Monitors

Active Script Active Monitors perform specific customized checks on a device. They report their status as a success or failure, and the monitor's status effects the device's status in the same way that stock active monitors do.

New Active Script Monitor

Name: Database Availability ☐ Use in discovery

Description: Active Script Monitor

Timeout: 10 (seconds) Script type: VBScript

Script text:

```
'Sending log message to the WhatsUp Event Viewer
Context.LogMessage "Checking Address=" & Context.GetProperty("Address")

'Set the result code of the check (0=Success, 1=Error)
Context.SetResult 0, "No error"
Const adOpenStatic = 3
Const adLockOptimistic = 3
Const adUseClient = 3
Set objConnection = CreateObject("ADODB.Connection")
Set objRecordset = CreateObject("ADODB.Recordset")

objConnection.ConnectionString = "Driver={SQL Server};" & _
    "Server=SQLSERVER;" & _
    "Database=DBName;" & _
    "uid=username;" & _
    "pwd=password;"

objConnection.Open
objRecordset.CursorLocation = adUseClient
objRecordset.Open "SELECT * FROM TableName", objConnection

'adOpenStatic, adLockOptimistic
If objRecordset.recordcount < 1 Then
    'Set the result code of the check (0=Success, 1=Error)
    Context.SetResult 1, "Error"
    Context.LogMessage "Checking Address=" & Context.GetProperty("Address")
End If

objRecordset.Close
objConnection.Close
set objRecordset=nothing
set objConnection=nothing
```

OK Cancel Help

Keep In Mind

- You need to include error handling in your monitor script. You must use `Context.SetResult` to report the status of the script to WhatsUp Gold.
- Errors from this active monitor appear in EventViewer.exe.

Using the Context object with Active Monitors

The context object provides an interface for your script to interact with WhatsUp Gold.

All methods and properties are retrieved using the `Context` namespace.

Methods

`LogMessage(sText);`

Method description

This method allows for a message to be written to the WhatsUp Gold debug log.

Example

JScript

```
Context.LogMessage( "Checking Monitor name using  
Context.GetProperty()");
```

VBScript

```
Context.LogMessage "Checking Address using Context.GetProperty()
```

`PutProperty(sPropertyName);`

This method allows you to store a value in the INMSerialize object. This value is retained across polls.

Example

JScript

```
var nCount = parseInt(nNum) +1;  
Context.PutProperty("MyNumeric",nCount);
```

`SetResult(nCode, sText);`

This method allows for a result code and result message to be set. This is how you can tell the WhatsUp Gold system if the monitor succeeded or not.

Every script should call `SetResult`. If `SetResult` is not called, the script is always assumed to have succeeded.

Example

JScript

```
Context.SetResult(0, "Script completed successfully.");  
//Success  
Context.SetResult(1, "An error occurred."); //Failure
```

VBScript

```
Context.SetResult 1, "An error occurred."
```

`GetProperty(sPropertyName) ;` This method offers access to any of the device properties listed below. These names are case sensitive.

| Property | Description |
|-------------------------------|--|
| "ActiveMonitorTypeName" | The active monitor display name |
| "Address" | The IP address of the device |
| "DeviceID" | The device ID |
| "Mode" | 1 = doing discovery 2 = polling 3 = test |
| "ActiveMonitorTypeID" | The active monitor's type ID |
| "CredSnmpV1:ReadCommunity" | SNMP V1 Read community |
| "CredSnmpV1:WriteCommunity" | SNMP V1 Write community |
| "CredSnmpV2:ReadCommunity" | SNMP V2 Read community |
| "CredSnmpV2:WriteCommunity" | SNMP V2 Write community |
| "CredSnmpV3:Username" | SNMP V3 Username |
| "CredSnmpV3:Context" | SNMP V3 Context |
| "CredSnmpV3:AuthPassword" | SNMP V3 Authentication password |
| "CredSnmpV3:AuthProtocol" | SNMP V3 Authentication protocol |
| "CredSnmpV3:EncryptPassword" | SNMP V3 Encrypt password |
| "CredSnmpV3:EncryptProtocol" | SNMP V3 Encrypt protocol |
| "CredWindows:DomainAndUserid" | Windows Domain and User ID |
| "CredWindows:Password" | Windows NT Password |

Example

JScript

```
var sAddress = Context.GetProperty("Address");  
var sReadCommunity =  
Context.GetProperty("CredSnmpV1:ReadCommunity");  
var nDeviceID = Context.GetProperty("DeviceID");
```

Properties

| Property | Description |
|----------|--|
| GetDB; | This property returns an open connection to the WhatsUp Gold database. |

Example Active Script Active Monitors

These scripts demonstrate a few potential uses of Active Script Active Monitors. To view other Active Script Active Monitors created by other WhatsUp Gold users, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

- *Monitoring printer ink level and utilization* (on page 913)
- *Alert when temperature exceeds or drops out of range* (on page 915)
- *Determine invalid user account activity* (on page 916)
- *Monitor bandwidth utilization on an interface* (on page 920)
- *Monitor an SNMP agent running on a non standard port* (on page 923)
- *Monitor for unknown MAC addresses* (on page 924)

Monitoring printer ink level and utilization



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This active monitor polls an object of the printer mib to gather the ink level information and then computes the ink percent utilization of a printer.

The active monitor will fire an alert if the utilization exceeds a value set on the first line of the script.



Note: This script was tested on an HP MIB.

Run the SNMP MIB Walker net tool to check the OIDs of the two polled objects and eventually adjust their instance (1.1 in this example):

1.3.6.1.2.1.43.11.1.1.8.1.1 and 1.3.6.1.2.1.43.11.1.1.9.1.1.



Note: This script is included as a code example only. The Printer Active Monitor should be used to monitor printers.

```
var nMarkerPercentUtilization = 70; // This monitor will fail if the printer ink
utilization is above this value %.
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed) {
    Context.SetResult(1, oComResult.GetErrorMsg);
}
else {
    // poll the two counters
    Context.LogMessage("Polling marker maximum level");
    var oResponse = oSnmpRqst.Get("1.3.6.1.2.1.43.11.1.1.8.1.1");
    if (oResponse.Failed) {
        Context.SetResult(1, oResponse.GetErrorMsg);
    }
    var prtMarkerSuppliesMaxCapacity = oResponse.GetValue;
    Context.LogMessage("Success. Value=" + prtMarkerSuppliesMaxCapacity);

    Context.LogMessage("Polling marker current level");
    oResponse = oSnmpRqst.Get("1.3.6.1.2.1.43.11.1.1.9.1.1");
    if (oResponse.Failed) {
        Context.SetResult(1, oResponse.GetErrorMsg);
    }
    var prtMarkerSuppliesLevel = oResponse.GetValue;
    Context.LogMessage("Success. Value=" + prtMarkerSuppliesLevel);

    var nPercentUtilization = 100 * prtMarkerSuppliesLevel /
    prtMarkerSuppliesMaxCapacity;

    if (nPercentUtilization > nMarkerPercentUtilization) {
        Context.SetResult(1, "Failure. Current Utilization (" + (nPercentUtilization +
        "%") is above the configured threshold (" + nMarkerPercentUtilization) + "%)");
    }
    else {
        Context.SetResult(0, "Success. Current Utilization (" + (nPercentUtilization +
        "%") is below the configured threshold (" + nMarkerPercentUtilization) + "%)");
    }
}
```

Alert when temperature exceeds or drops out of range



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This active monitor polls an SNMP-enabled temperature sensor. If the temperature exceeds or drops below the configured acceptable range, an alert is fired.

```
// This jscript script polls the temperature from an snmp-enabled sensor from "uptime
devices" (www.uptimedevices.com),
// and makes sure the temperature is within an acceptable range configured right below.
// The OID of the temperature object for that device is
1.3.6.1.4.1.3854.1.2.2.1.16.1.14.1
var nMinAllowedTemp = 65;
var nMaxAllowedTemp = 75;
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed) {
    Context.SetResult(1, oComResult.GetErrorMsg);
}
else {
    // poll the two counters
    Context.LogMessage("Polling the temperature");
    var oResponse = oSnmpRqst.Get("1.3.6.1.4.1.3854.1.2.2.1.16.1.14.1");
    if (oResponse.Failed) {
        Context.SetResult(1, oResponse.GetErrorMsg);
    }
    else {
        var nTemperature = oResponse.GetValue / 10.0;
        // comment out the following line to convert the temperature to Celcius degrees
        //nTemperature = (nTemperature - 32) * 5 / 9;
        Context.LogMessage("Success. Value=" + nTemperature + " degrees");

        if (nTemperature < nMinAllowedTemp || nTemperature > nMaxAllowedTemp) {
            Context.SetResult(1, "Polled temperature " + nTemperature + " is outside of
the defined range " + nMinAllowedTemp + " - " + nMaxAllowedTemp);
        }
        else {
            Context.SetResult(0, "Success");
        }
    }
}
}
```


Determine invalid user account activity



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This active monitor will change a device's state to Down if an invalid, or unexpected user account logs on. The monitor will stay up if the valid, expected account is logged on, or if no one is logged on.

```
sComputer = Context.GetProperty("Address")
```

```
nDeviceID = Context.GetProperty("DeviceID")
```

```
'Assuming ICMP is not blocked and there's a ping monitor on the device, we want to
```

```
'perform the actual check only if the Ping monitor is up. ConnectServer method of
```

```
'the SWbemLocator has a long time out so it would be good to avoid unnecessary tries.
```

```
'Please note: there's no particular polling order of active monitors on a device.
```

```
'During each polling cycle, it's possible that this monitor could be polled before
```

```
'Ping is polled. If the network connection just goes down but Ping is not polled yet,
```

```
'and therefore still has an up state, this active monitor will still do an actual
```

```
'check and experience a real down. But for the subsequent polls, it won't be doing a
```

```
'real check (ConnectServer won't be called) as Ping monitor has a down state, and this
```

```
'monitor will be assumed down.
```

```
If IsPingUp(nDeviceID) = false Then
```

```
    Context.SetResult 1,"Actual check was not performed due to ping being down. Automatically set to down."
```

```
Else
```

```
    sAdminName = Context.GetProperty("CredWindows:DomainAndUserid")
```

```
    sAdminPasswd = Context.GetProperty("CredWindows:Password")
```

```
    sLoginUser = GetCurrentLoginUser(sComputer, sAdminName, sAdminPasswd)
```

```
    sExpectedUser = "administrator"
```

```
If Not IsNull(sLoginUser) Then

    If Instr(1,sLoginUser, sExpectedUser,1) > 0 Then

        Context.SetResult 0,"Current login user is " & sLoginUser

    ElseIf sLoginUser = " " Then

        Context.SetResult 0,"No one is currently logged in."

    Else

        Context.SetResult 1,"an unexpected user " & sLoginUser & " has logged in " & sComputer

    End If

End If

End If

'Check if Ping monitor on the device specified by nDeviceID is up.

'If nDeviceID is not available as it's in the case during discovery, then assume

'ping is up.

'If ping monitor is not on the device, then assume it's up so the real check will be

'performed.

Function IsPingUp(nDeviceID)

    If nDeviceID > -1 Then

        'get the Ping monitor up state.

        sSqlGetUpState = "SELECT sStateName from PivotActiveMonitorTypeToDevice as P join " & _

            "ActiveMonitorType as A on P.nActiveMonitorTypeID=A.nActiveMonitorTypeID " & _

            "join MonitorState as M on P.nMonitorStateID = M.nMonitorStateID " & _

            "where nDeviceID=" & nDeviceID & " and A.sMonitorTypeName='Ping' and " & _

            " P.bRemoved=0"

        Set oDBConn = Context.GetDB
```

```
Set oStateRS = CreateObject("ADODB.Recordset")

oStateRS.Open sSqlGetUpState,oDBconn,3

'if recordset is empty then

If oStateRS.RecordCount = 1 Then

    If instr(1,oStateRS("sStateName"),"up",1) > 0 Then

        IsPingUp = true

    Else

        IsPingUP = false

    End If

Else

    'if there's no ping on the device, then just assume up, so regular check will happen.

    IsPingUp= true

End If

oStateRS.Close

oDBconn.Close

Set oStateRS = Nothing

Set oDBconn = Nothing

Else

    'assume up, since there's no device yet. It's for scanning during discovery.

    IsPingUP = true

End If

End Function

'Try to get the current login user name.
```

```
Function GetCurrentLoginUser(sComputer, sAdminName, sAdminPasswd)

    GetCurrentLoginUser=Null

    Set oSWbemLocator = CreateObject("WbemScripting.SWbemLocator")

    On Error Resume Next

    Set oSWbemServices = oSWbemLocator.ConnectServer _

(sComputer, "root\cimv2",sAdminName,sAdminPasswd)

    If Err.Number <> 0 Then

        Context.LogMessage("The 1st try to connect to " & sComputer & " failed. Err:" & Err.Description)

        Err.Clear

        'If the specified user name and password for WMI connection failed, then

        'try to connect without user name and password. Can't specify user name

        'and password when connecting to local machine.

        On Error Resume Next

        Set oSWbemServices = oSWbemLocator.ConnectServer(sComputer, "root\cimv2")

        If Err.Number <> 0 Then

            Err.Clear

            On Error Resume Next

            Context.SetResult 1,"Failed to access " & sComputer & " " & _

            "using username:" & sAdminName & " password." & " Err: " & Err.Description

            Exit Function

        End If

    End If

    Set colSWbemObjectSet = oSWbemServices.InstancesOf("Win32_ComputerSystem")
```

```
For Each oSWbemObject In colSWbemObjectSet

    On Error Resume Next

    'Context.SetResult 0,"User Name: " & oSWbemObject.UserName & " at " & sComputer

    sCurrentLoginUser = oSWbemObject.UserName

    Err.Clear

Next

If Cstr(sCurrentLoginUser) = "" Then

    GetCurrentLoginUser = " "

Else

    GetCurrentLoginUser = sCurrentLoginUser

End If

Set oSWbemServices = Nothing

Set oSWbemLocator = Nothing

End Function
```

Monitor bandwidth utilization on an interface



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This active monitor is used to monitor the total bandwidth utilization (both in and out octets) of an interface by polling values of the interface MIB.

```
// Settings for this monitor:
// the interface index ifIndex:
var nInterfaceIndex = 65540;

// this monitor will fail if the interface utilization goes above this current ratio:
// current bandwidth / maxBandwidth > nMaxInterfaceUtilizationRatio
var nMaxInterfaceUtilizationRatio = 0.7; // Set to 70%

// Create an SNMP object, that will poll the device.
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");

// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");

// This function polls the device returns the ifSpeed of the interface indexed by
nIfIndex.
// ifSpeed is in bits per second.
function getIfSpeed(nIfIndex) {
    var oResult = oSnmpRqst.Initialize(nDeviceID);
    if (oResult.Failed) {
        return null;
    }
    return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.5." + nIfIndex)); // ifSpeed
}

// Function to get SNMP ifInOctets for the interface indexed by nIfIndex (in bytes).
// Returns the value polled upon success, null in case of failure.
function getInOctets(nIfIndex) {
    var oResult = oSnmpRqst.Initialize(nDeviceID);
    if (oResult.Failed) {
        return null;
    }
    return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.10." + nIfIndex)); // inOctets
}

// Function to get SNMP ifOutOctets for the interface indexed by nIfIndex (in bytes).
// Returns the value polled upon success, null in case of failure.
function getOutOctets(nIfIndex) {
    var oResult = oSnmpRqst.Initialize(nDeviceID);
```

```
        if (oResult.Failed) {
            return null;
        }
        return parseInt(SnmpGet("1.3.6.1.2.1.2.2.1.16." + nIfIndex)); // outOctets
    }

    // Helper function to get a specific SNMP object (OID in sOid).
    // Returns the value polled upon success, null in case of failure.
    function SnmpGet(sOid) {
        var oResult = oSnmpRqst.Get(sOid);
        if (oResult.Failed) {
            return null;
        }
        else {
            return oResult.GetPayload;
        }
    }

    // Get the current date. It will be used as a reference date for the SNMP polls.
    var oDate = new Date();
    var nPollDate = parseInt(oDate.getTime()); // get the date in millisec in an integer.
    // Do the actual polling:
    var nInOctets = getInOctets(nInterfaceIndex);
    var nOutOctets = getOutOctets(nInterfaceIndex);
    var nIfSpeed = getIfSpeed(nInterfaceIndex);
    if (nInOctets == null || nOutOctets == null || nIfSpeed == null) {
        Context.SetResult(1, "Failure to poll this device.");
    }
    else {
        var nTotalOctets = nInOctets + nOutOctets;
        // Retrieve the octets value and date of the last poll saved in a context variable:
        var nInOutOctetsMonitorPreviousPolledValue =
        Context.GetProperty("nInOutOctetsMonitorPreviousPolledValue");
        var nInOutOctetsMonitorPreviousPollDate =
        Context.GetProperty("nInOutOctetsMonitorPreviousPollDate");
        if (nInOutOctetsMonitorPreviousPolledValue == null ||
        nInOutOctetsMonitorPreviousPollDate == null) {
            // the context variable has never been set, this is the first time we are
            polling.
            Context.LogMessage("This monitor requires two polls.");
            Context.SetResult(0, "success");
        }
        else {
            // compute the bandwidth that was used between this poll and the previous poll
            var nIntervalSec = (nPollDate - nInOutOctetsMonitorPreviousPollDate) / 1000; //
            time since last poll in seconds
            var nCurrentBps = (nTotalOctets - nInOutOctetsMonitorPreviousPolledValue) * 8 /
            nIntervalSec;
            Context.LogMessage("total octets for interface " + nInterfaceIndex + " = " +
            nTotalOctets);
            Context.LogMessage("previous value = " + nInOutOctetsMonitorPreviousPolledValue);
        }
    }
}
```

```
Context.LogMessage("difference: " + (nTotalOctets -
nInOutOctetsMonitorPreviousPolledValue) + " bytes");
Context.LogMessage("Interface Speed: " + nIfSpeed + "bps");
Context.LogMessage("time elapsed since last poll: " + nIntervalSec + "s");
Context.LogMessage("Current Bandwidth utilization: " + nCurrentBps + "bps");
if (nCurrentBps / nIfSpeed > nMaxInterfaceUtilizationRatio) {
    Context.SetResult(1, "Failure: bandwidth used on this interface " +
nCurrentBps + "bps / total available: " + nIfSpeed + "bps is above the specified ratio: "
+ nMaxInterfaceUtilizationRatio);
}
else {
    Context.SetResult(0, "Success");
}
}
// Save this poll information in the context variables:
Context.PutProperty("nInOutOctetsMonitorPreviousPolledValue", nTotalOctets);
Context.PutProperty("nInOutOctetsMonitorPreviousPollDate", nPollDate);
}
```

Monitor an SNMP agent running on a non standard port



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This active monitor watches an SNMP agent running on a non-standard port (the standard SNMP port is 161).

```
var nSNMPPort = 1234; // change this value to the port your agent is running on
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
// Get the device ID
var nDeviceID = Context.GetProperty("DeviceID");

// Initialize the SNMP request object
var oResult = oSnmpRqst.Initialize(nDeviceID);

if(oResult.Failed)
{
    Context.SetResult(1, oResult.GetPayload());
}
else
{
    // Set the request destination port.
    var oResult = oSnmpRqst.SetPort(nSNMPPort);

    // Get sysDescr.
    var oResult = oSnmpRqst.Get("1.3.6.1.2.1.1.1.0");
    if (oResult.Failed)
```



```
        {
            Context.SetResult(1, "Failed to poll device using port " + nSNMPPort + ".
Error=" + oResult.GetPayload);
        }
        else
        {
            Context.SetResult(0, "SUCCESS. Detected an SNMP agent running on port " +
nSNMPPort );
        }
    }
}
```

Monitor for unknown MAC addresses



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This active monitor watches MAC addresses present on a network by polling an SNMP-managed switch and the bridge MIB. In the example script, you define a list of MAC addresses you will allow to connect to the network. This monitor will fail if it finds devices that do not match the addresses specified in the list.

```
// Modify the list below. It defines a list of allowed mac addresses with mapping to
switch interface
// on the network.
// This script will poll a managed switch using SNMP and the bridge MIB to detect MAC
addresses present
// on your network that should not be and to detect misplaced machines (connected to the
wrong port).
//
// The MAC addresses should be typed lowercase with no padding using ':' between each
bytes
// for instance "0:1:32:4c:ef:9" and not "00:01:32:4C:EF:09"
//
var arrAllowedMacToPortMapping = new ActiveXObject("Scripting.Dictionary");
arrAllowedMacToPortMapping.add("0:3:ff:3b:df:1f", 17);
arrAllowedMacToPortMapping.add("0:3:ff:72:5c:bf", 77);
arrAllowedMacToPortMapping.add("0:3:ff:e2:e5:76", 73);
arrAllowedMacToPortMapping.add("0:11:24:8e:e0:a5", 63);
arrAllowedMacToPortMapping.add("0:1c:23:ae:b0:4c", 48);
arrAllowedMacToPortMapping.add("0:1d:60:96:e5:58", 73);
arrAllowedMacToPortMapping.add("0:e0:db:8:aa:a3", 73);

var ERR_NOERROR = 0;
var ERR_NOTALLOWED = 1;
var ERR_MISPLACED = 2;
function CheckMacAddress(sMacAddress, nPort)
{
```

```
sMacAddress = sMacAddress.ToLowerCase();

if (!arrAllowedMacToPortMapping.Exists(sMacAddress))
{
    return ERR_NOTALLOWED;
}

var nAllowedPort = arrAllowedMacToPortMapping.Item(sMacAddress);
if (nAllowedPort != nPort)
{
    return ERR_MISPLACED;
}
return ERR_NOERROR;
}

var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");

var oComResult = oSnmpRqst.Initialize(Context.GetProperty("DeviceID"));

if (oComResult.Failed)
{
    Context.SetResult(1, oComResult.GetErrorMsg);
}
else
{
    var DOT1DTONFDBPORT_OID = "1.3.6.1.2.1.17.4.3.1.2";
    var DOT1DTONFDBADDRESS_OID = "1.3.6.1.2.1.17.4.3.1.1";
    var sOid = DOT1DTONFDBPORT_OID
    var bStatus = true;
    var arrMisplacedAddresses = new Array();
    var arrNotAllowedAddresses = new Array();
    var i=0;
    while (i++<1000)
    {
        oComResult = oSnmpRqst.GetNext(sOid);
        if (oComResult.Failed)
        {
            break;
        }
        sOid = oComResult.GetOID;
        if (sOid.indexOf(DOT1DTONFDBPORT_OID) == -1)
        {
            // we are done walking
            break;
        }
        var nPort = oComResult.GetPayload;

        // the last 6 elements of the OID are the MAC address in Oid format
        var sInstance = sOid.substr(DOT1DTONFDBPORT_OID.length+1, sOid.length);

        // get it in hex format...
```

```
oComResult = oSnmpRqst.Get(DOT1DТОFDBADDRESS_OID + "." + sInstance);
if (oComResult.Failed)
{
    continue;
}
var sMAC = oComResult.GetValue;

var nError = CheckMacAddress(sMAC, nPort);

switch (nError)
{
case ERR_NOTALLOWED:
    arrNotAllowedAddresses.push(sMAC + "(" + nPort + ")");
    break;
case ERR_MISPLACED:
    arrMisplacedAddresses.push(sMAC + "(" + nPort + ")");
    break;
case ERR_NOERROR:
default:
    // no problem
}

}

//Write the status
Context.LogMessage("Found " + i + " MAC addresses on your network.");
if (arrMisplacedAddresses.length > 0)
{
    Context.LogMessage("Warning: Found " + arrMisplacedAddresses.length + "
misplaced addresses: " + arrMisplacedAddresses.toString());
}
if (arrNotAllowedAddresses.length > 0)
{
    Context.SetResult(1, "ERROR: Found " + arrNotAllowedAddresses.length + "
unknown MAC addresses on your network: " + arrNotAllowedAddresses.toString());
}
else
{
    Context.SetResult(0, "SUCCESS. No anomaly detected on the network");
}
}
```

Scripting Performance Monitors

Active Script Performance Monitors let you write VBScript and JScript to easily poll one or more SNMP or WMI values, perform math or other operations on those values, and graph a single output value. You should only use the Active Script Performance Monitor when you need to perform calculations on the polled values. Keep in mind that although you can poll

multiple values using the feature, only one value will be stored to the database: the outcome of your scripted calculation.

Reference Variables

Edit Active Script Performance Monitor

Name: Script type:

Description: Timeout (sec):

Reference variables:

| Variable | Type | Description | Object | Instance |
|--------------|------|------------------------|-------------------------|----------|
| nIfHighSpeed | SNMP | High capacity count... | 1.3.6.1.2.1.31.1.1.1.15 | 1 |
| nIfInOctets | SNMP | High capacity count... | 1.3.6.1.2.1.31.1.1.1.6 | 1 |
| nIfOutOctets | SNMP | High capacity count... | 1.3.6.1.2.1.31.1.1.1.10 | 1 |

Buttons: Add, Edit, Remove

Script text:

```
var ifHighSpeed = Context.GetReferenceVariable("ifHighSpeed");
var ifHCInOctets = Context.GetReferenceVariable("ifHCInOctets");
var ifHCOutOctets = Context.GetReferenceVariable("ifHCOutOctets");

if (ifHCInOctets == null || ifHCOutOctets == null || ifHighSpeed == null)
{
    // polling of reference variables failed.
    Context.SetResult(1, "Failed to poll this device.");
}
else
{
    // total bandwidth:
    var nTotalOctets = parseInt(ifHCInOctets) + parseInt(ifHCOutOctets);
    Context.LogMessage("Current polled value: " + nTotalOctets);

    // Get the current date. It will be used as a reference date for the SNMP polls.
    var oDate = new Date();
    var nPollDate = parseInt(oDate.getTime()); // get the date in millisec in an integer.
}
```

Buttons: OK, Cancel, Help

Reference variables simplify your scripting code and enable you to write scripts efficiently, without having to grab a list of device properties, as with the Script Action and Script Active Monitor. They take care of the underlying SNMP or WMI mechanisms that you would normally have to deal with to access SNMP or WMI counters on a remote device.

By using the `Context.GetReferenceVariable(variable name)`, you only need to specify the name of a pre-defined variable. WhatsUp Gold uses a device's credentials to connect to the target device using SNMP or WMI to retrieve the requested information. This information is stored in a variable that you can use later in your script.



Important: The use of reference variables in the Active Script Performance Monitor is optional. If you do use them, you must use `Context.GetReferenceVariable`, for reference variables to be polled and their data graphed.

Keep In Mind

- You need to include error handling in your monitor script. Your script either needs a value to graph by using `Context.SetValue`, or you must use `Context.SetResult` to tell WhatsUp Gold that the script failed.
- `Context.GetReferenceVariable` will return 'null' if the poll fails for any reason.
- If you do not have a call to `SetValue` or `SetResult`, the script does not report any errors and no data is graphed.
- If `SetValue` is used, it is not necessary to use `SetResult`, as `SetValue` implicitly sets `SetResult` to 0, or "good."
- Results from this performance monitor are displayed on *Custom Performance Monitors* (on page 639) full and dashboard reports.
- Errors from this performance monitor are displayed in the *Performance Monitor Error log* (on page 691) as well as EventViewer.exe.

Using the Context object with Performance Monitors

The context object provides an interface for your script to interact with WhatsUp Gold.

All methods and properties are retrieved using the `Context` namespace.



Note: You may have to remove the copyright information from the cut and paste if it appears when you copy from this help file.

Methods

`LogMessage (sText) ;`

Method description

This method allows for a message to be written to the WhatsUp Gold debug log.

Example

JScript

```
Context.LogMessage( "Checking Monitor name using  
Context.GetProperty( ) " );
```

VBScript

```
Context.LogMessage "Checking Address using Context.GetProperty()
```

`PutProperty(sPropertyName) ;`

This method allows you to store a value in the INMSerialize object. This value is retained across polls.

Example

JScript

```
var nCount = parseInt(nNum) +1;  
Context.PutProperty( "MyNumeric", nCount );
```

`SetResult(nCode, sText) ;`

This method allows for a result code and result message to

be set. This is how you can tell the WhatsUp Gold system if the monitor succeeds or fails.

Every script should call `SetResult`. If `SetResult` is not called, the script is always assumed to have succeeded.

Example

JScript

```
Context.SetResult(0, "Script completed  
successfully."); //Success  
Context.SetResult(1, "An error occurred.");  
//Failure
```

VBScript

```
Context.SetResult 1, "An error occurred."
```

```
GetReferenceVariable(sRefVarName  
);
```

This method allows the code to grab a reference variable to be used in the monitor.

Example

JScript

```
Context.GetReferenceVariable("A")
```

A reference variable "A" would have had to have been created.

```
SetValue(nValue);
```

This method allows you to graph a value.

Example

JScript

```
Context.SetValue(245)
```

`GetProperty(sPropertyName) ;`

This method offers access to any of the device properties listed below. These names are case sensitive.

| Property | Description |
|-------------------------------|--|
| "ActiveMonitorTypeName" | The active monitor display name |
| "Address" | The IP address of the device |
| "DeviceID" | The device ID |
| "Mode" | 1 = doing discovery 2 = polling 3 = test |
| "ActiveMonitorTypeID" | The active monitor's type ID |
| "CredSnmpV1:ReadCommunity" | SNMP V1 Read community |
| "CredSnmpV1:WriteCommunity" | SNMP V1 Write community |
| "CredSnmpV2:ReadCommunity" | SNMP V2 Read community |
| "CredSnmpV2:WriteCommunity" | SNMP V2 Write community |
| "CredSnmpV3:Username" | SNMP V3 Username |
| "CredSnmpV3:Context" | SNMP V3 Context |
| "CredSnmpV3:AuthPassword" | SNMP V3 Authentication password |
| "CredSnmpV3:AuthProtocol" | SNMP V3 Authentication protocol |
| "CredSnmpV3:EncryptPassword" | SNMP V3 Encrypt password |
| "CredSnmpV3:EncryptProtocol" | SNMP V3 Encrypt protocol |
| "CredWindows:DomainAndUserId" | Windows NT Domain and User ID |
| "CredWindows:Password" | Windows NT Password |

Example

JScript

```
var sAddress = Context.GetProperty("Address");
var sReadCommunity =
Context.GetProperty("CredSnmpV1:ReadCommunity");
var nDeviceID = Context.GetProperty("DeviceID");
```

Example Active Script Performance Monitors

These scripts demonstrate a few potential uses of Active Script Performance Monitors. To view other Active Script Performance Monitors created by other WhatsUp Gold users, visit *the WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

- *Graphing printer ink level percent utilization* (on page 931)
- *Poll a reference variable and perform a calculation* (on page 932)
- *Graph a temperature monitor* (on page 933)
- *Poll the storage table using SNMP GetNext* (on page 934)
- *Poll multiple reference variables* (on page 935)

Graphing printer ink level utilization



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This performance monitor uses two reference variables to poll and compute the ink level percent utilization of a printer for later graphing.



Note: This was tested on an HP MIB.

Run the SNMP MIB Walker net tool to check the OIDs of the two reference variables and eventually adjust their instance (1.1 in this example):

1.3.6.1.2.1.43.11.1.1.8.1.1 and 1.3.6.1.2.1.43.11.1.1.9.1.1.

// prtMarkerSuppliesLevel is an snmp reference variable defined with an OID of 1.3.6.1.2.1.43.11.1.9 and an instance of 1.1

// prtMarkerSuppliesMaxCapacity is an snmp reference variable defined with an OID of 1.3.6.1.2.1.43.11.1.8 and an instance of

1.1

```
Context.LogMessage("Print the current marker level");
```

```
var prtMarkerSuppliesLevel = Context.GetReferenceVariable("prtMarkerSuppliesLevel");
```

```
Context.LogMessage("Print the maximum marker level");
```

```
var prtMarkerSuppliesMaxCapacity = Context.GetReferenceVariable("prtMarkerSuppliesMaxCapacity");
```



```
if (prtMarkerSuppliesMaxCapacity == null || prtMarkerSuppliesLevel == null) {

    Context.SetResult(0, "Failed to poll printer ink levels.");

}

else {

    Context.LogMessage("marker lever successfully retrieved");

    var nPercentMarkerUtilization = 100 * prtMarkerSuppliesLevel / prtMarkerSuppliesMaxCapacity;

    Context.LogMessage("Percent utilization=" + nPercentMarkerUtilization + "%");

    Context.SetValue(nPercentMarkerUtilization);

}
```

Poll a reference variable and perform a calculation



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This performance monitor polls a reference variable, and then performs an arithmetic calculation with the returned value.

```
// This script is a JScript that demonstrates how to use a reference variable in a
script.
// The reference variable "RVsysUpTime" is an SNMP reference variable defined
// with an OID of 1.3.6.1.2.1.1.3 and instance of 0.

// Poll reference variable RVsysUpTime
var RVsysUpTime = Context.GetReferenceVariable("RVsysUpTime");

if (RVsysUpTime == null) {
    // Pass a non zero error code upon failure with an error message.
    // The error message will be logged in the Performance Monitor Error Log
    // and in the eventviewer.
    Context.SetResult(1, "Failed to poll the reference variable.");
}
else {
    // Success, use the polled value to convert sysUpTime in hours.
    // sysUpTime is an SNMP timestamp which is in hundredths of seconds:
    var sysUpTimeHours = RVsysUpTime / 3600 / 100;
    // Save the final value to graph:
    Context.SetValue(sysUpTimeHours);
}
```

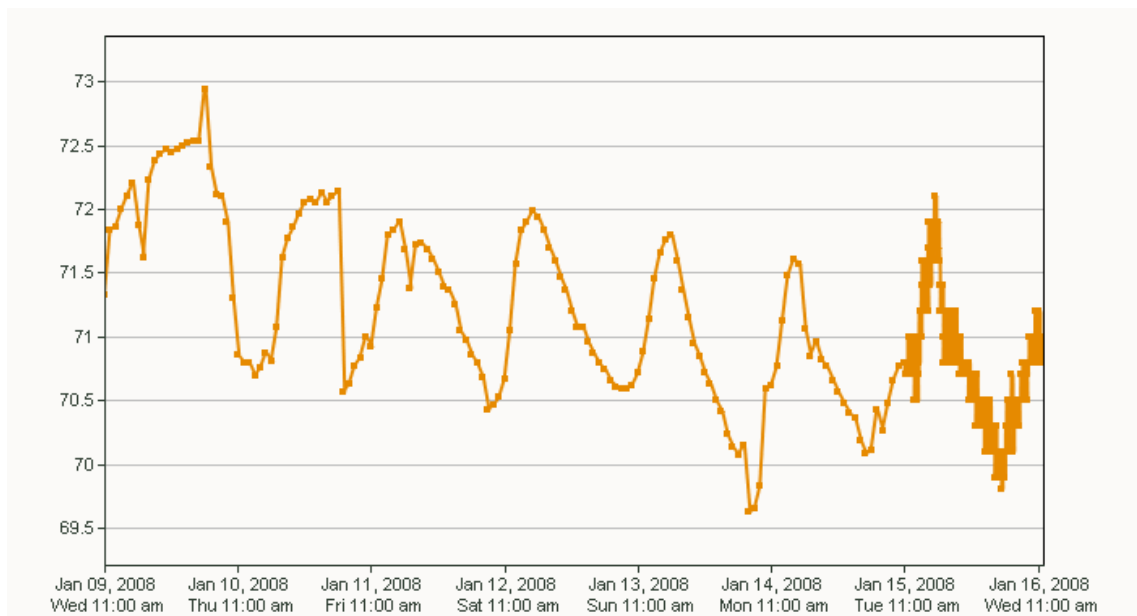
Graph a temperature monitor



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This performance monitor polls an SNMP-enabled temperature sensor using the CurTemp reference variable.

A typical graph for this script:



```
// This script is a JScript script that polls the temperature of an snmp-enabled sensor
from "uptime devices" (www.uptimedevices.com).
// It uses an SNMP reference variable named CurTemp defined with an OID of
1.3.6.1.4.1.3854.1.2.2.1.16.1.14
// and an instance of 1.
//
// That device indicates the temperature in degrees Fahrenheit.

var oCurTemp = Context.GetReferenceVariable("CurTemp");
if (oCurTemp == null) {
    Context.SetResult(1, "Unable to poll Temperature Sensor");
}
else {
    // convert temperature from tenth of degrees to degrees
    var nFinalTemp = oCurTemp / 10.0;

    // comment out the line below to convert the temperature in Celsius degrees:
```

```
//nFinalTemp = (nFinalTemp - 32) * 5 / 9;  
Context.SetValue(nFinalTemp);  
}
```

Use SNMP GetNext.



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This performance monitor walks the hrStorageType MIB to find hard disks in the storage table. After a hard disk is found, it obtains indexes of it and polls new objects (the storage size and units).

```
// This scripts walks hrStorageType to find hard disks in the storage table.  
// A hard disk as a hrStorageType of "1.3.6.1.2.1.25.2.1.4" (hrStorageFixedDisk).  
// Then it gets the indexes of the hard disk in that table and for each index, it polls  
two new  
// objects in that table, the storage size and the units of that entry.  
// It adds everything up and converts it in Gigabytes.  
var hrStorageType = "1.3.6.1.2.1.25.2.3.1.2";  
  
// Create and initialize the snmp object  
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");  
var nDeviceID = Context.GetProperty("DeviceID");  
var oResult = oSnmpRqst.Initialize(nDeviceID);  
  
var arrIndexes = new Array(); // array containing the indexes of the disks we found  
// walk the column in the table:  
var oSnmpResponse = oSnmpRqst.GetNext(hrStorageType);  
if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload());  
var sOid = String(oSnmpResponse.GetOid);  
var sPayload = String(oSnmpResponse.GetPayload());  
  
while (!oSnmpResponse.Failed && sOid < (hrStorageType + ".9999999999"))  
{  
    if (sPayload == "1.3.6.1.2.1.25.2.1.4") {  
        // This storage entry is a disk, add the index to the table.  
        // the index is the last element of the OID:  
        var arrOid = sOid.split(".");  
        arrIndexes.push(arrOid[arrOid.length - 1]);  
    }  
  
    oSnmpResponse = oSnmpRqst.GetNext(sOid);  
    if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload());  
    sOid = String(oSnmpResponse.GetOid);  
    sPayload = String(oSnmpResponse.GetPayload());  
}
```

```
Context.LogMessage("Found disk indexes: " + arrIndexes.toString());
if (arrIndexes.length == 0) Context.SetResult(1, "No disk found");

// now that we have the indexes of the disks. Poll their utilization and units
var nTotalDiskSize = 0;
for (var i = 0; i < arrIndexes.length; i++) {

    oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.25.2.3.1.5." + arrIndexes[i])
    if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload);
    nSize = oSnmpResponse.GetPayload;
    oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.25.2.3.1.4." + arrIndexes[i])
    if (oSnmpResponse.Failed) Context.SetResult(1, oSnmpResponse.GetPayload);
    nUnits = oSnmpResponse.GetPayload;

    nTotalDiskSize += (nSize * nUnits);
}
// return the total size in gigabytes.
Context.SetValue(nTotalDiskSize / 1024 / 1024 / 1024); // output in Gigabytes
```

Poll multiple reference variables



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This performance monitor graphs the percentage of retransmitted TCP segments over time using two reference variables: RVtcpOytSegs and RVtcpRetransSegs.

```
// This script is a JScript that will allow you to graph the percentage of retransmitted
TCP
//' segments over time on a device.
// For this script, we use two SNMP reference variables:
//' The first Reference variable RVtcpOutSegs is defined with OID 1.3.6.1.2.1.6.11 and
instance 0. It polls the
//' SNMP object tcpOutSegs.0, the total number of tcp segments sent out on the network.
var RVtcpOutSegs = parseInt(Context.GetReferenceVariable("RVtcpOutSegs"));

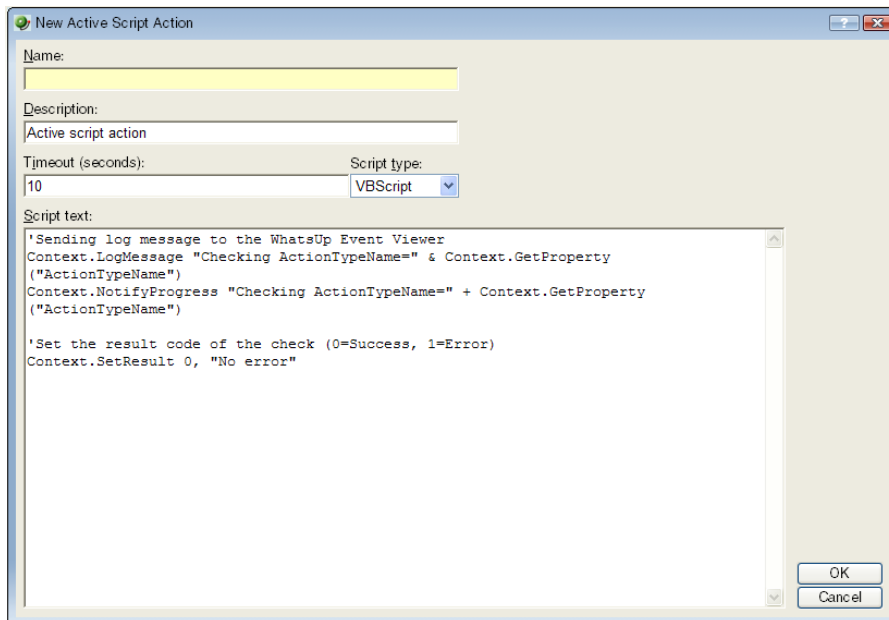
// The second reference variable RVtcpRetransSegs is defined with OID 1.3.6.1.2.1.6.12
and instance 0. It polls
// the SNMP object tcpRetransSegs.0, the total number of TCP segments that were
retransmitted on the system.
var RVtcpRetransSegs = parseInt(Context.GetReferenceVariable("RVtcpRetransSegs"));

if (isNaN(RVtcpRetransSegs) || isNaN(RVtcpOutSegs)) {
    Context.SetResult(1, "Failed to poll the reference variables.");
}
else {
    // Compute the percentage:
```

```
var TCPRetransmittedPercent = 100 * RVtcpRetransSegs / RVtcpOutSegs;  
// Set the performance monitor value to graph  
Context.SetValue(TCPRetransmittedPercent);  
}
```

Scripting Actions

Active Script Actions can be configured to trigger when an active monitor's state changes. They can be programmed to perform a variety of tasks, from running automated remediation scripts to posting data to external, third party services via API.



Keep In Mind

- You need to include error handling in your monitor script. Your script must use `Context.SetResult` to report the status of the action to WhatsUp Gold.
- Your script should check periodically to see if it has been canceled by the user. To do this, use the `IsCancelled()` method described in Using the Context object with Actions.
- Errors from this performance monitor appear in EventViewer.exe.

Using the Context object with Actions

The context object provides an interface for your script to interact with WhatsUp Gold.

All methods and properties are retrieved using the `Context` namespace.



Note: You may need to remove the copyright information from the cut and paste if it appears when you copy from this help file.

Method

`LogMessage(sText);`

Method description

This methods allows for a message to be written to the WhatsUp Gold debug log. Messages are displayed in the Event Viewer.

Example

JScript

```
Context.LogMessage( "Checking action name using  
Context.GetProperty()");
```

VBScript

```
Context.LogMessage "Checking Address using Context.GetProperty0"
```

`SetResult(LONG nCode,
sText);`

This method allows for a result code and result message to be set. This is how you can tell the WhatsUp Gold system if the action succeeded or failed.

Example

JScript

```
Context.SetResult(0, "Script completed successfully.");  
//Success  
Context.SetResult(1, "An error occurred."); //Failure
```

VBScript

```
Context.SetResult 1, "An error occurred."
```

`NotifyProgress(sText);`

This method allows for a message to be written to the actions progress dialog. Messages are displayed in the Test dialog and Running Actions dialog.

Example

JScript

```
Context.NotifyProgress( "Checking action name using  
Context.GetProperty()" );
```

VBScript

```
Context.NotifyProgress "Checking Address using Context.GetPropertyQ"
```

`IsCancelled();`

This method tests whether the action has been cancelled by the user. If the return is true, then the script should terminate.

A cancel can be issued by the user in the action progress dialog and by the WhatsUp Gold engine when shutting down.

`GetProperty(sPropertyName)`; This property offers access to many device specific aspects. You obtain access to these items using the names listed. These names are case sensitive.

| | |
|--------------------|----------------------------------|
| "ActionName" | The action display name |
| "Address" | The IP Address of the device |
| "Name" | Network name of the device |
| "DisplayName" | Display name of the device |
| "DeviceID" | The device ID |
| "ActionTypeID" | The action type ID |
| "TriggerCondition" | The reason the action was fired. |

Trigger values:

1 Monitor changed from DOWN to UP
2 Monitor changed from UP to DOWN
4 A Passive Monitor was received...
8 The "Test" Button was hit
16 This is a recurring action...
32 Device is UP
64 Device is DOWN

Example

JScript

```
var sAddress = Context.GetProperty("Address");  
var nDeviceID = Context.GetProperty("DeviceID");
```

Example Active Script Actions

These scripts demonstrate a few potential uses of Active Script Actions. To view other Active Script Actions created by other WhatsUp Gold users, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

- *Post device status to Twitter* (on page 940)
- *Acknowledge all devices* (on page 940)

Post device status to Twitter



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This action posts the status of the device to which it's applied to the microblogging service Twitter. This is useful for creating an externally viewable and off-site list of device status.

Dim xml

Set xml = createObject("Microsoft.XMLHTTP")

'Update to include your account's username and password.

sUser = "username"

sPass = "password"

sStatus = "WhatsUp Gold says, '%Device.DisplayName %Device.State at %System.Time on %System.Date'"

xml.Open "POST", "http://" & sUser & ":" & sPass & "@twitter.com/statuses/update.xml?status=" & sStatus, False

xml.setRequestHeader "Content-Type", "content=text/html; charset=iso-8859-1"

xml.Send

Context.SetResult 0, xml.responseText

Set xml = Nothing

Acknowledge all devices



Note: This example is provided as an illustration only and is not supported. Technical support is available for the Context object, SNMP API, and scripting environment, but Ipswitch does not provide support for JScript, VBScript, or developing and debugging Active Script monitors or actions. For assistance with this example or with writing your own scripts, visit the *WhatsUp Gold user community* (<http://www.whatsupgold.com/wugspace>).

This action resets the acknowledge flag on all devices. When a device is unacknowledged, the label on its icon renders as white text on black. If you don't use the acknowledge feature, this action can be used to make sure that icons always show as acknowledged.

```
// This JScript action sets the acknowledge flag to true for all devices.
// Written by Tim Schreyack of Dynamics Research Corporation

// Get the database info
var oDb = Context.GetDB;

if (null == oDb) {
    Context.SetResult( 1, "Problem creating the DB object");
}
else {
    var sSql = "UPDATE ActiveMonitorStateChangeLog SET bAcknowledged = 1 WHERE
bAcknowledged = 0";
    var oRs = oDb.Execute(sSql);
    var sSql = "UPDATE Device SET nUnAcknowledgedActiveMonitors = 0 WHERE
nUnAcknowledgedActiveMonitors = 1";
    var oRs = oDb.Execute(sSql);
    var sSql = "UPDATE Device SET nUnAcknowledgedPassiveMonitors = 0 WHERE
nUnAcknowledgedPassiveMonitors = 1";
    var oRs = oDb.Execute(sSql);
}
```

Using the SNMP API

The WhatsUp Gold SNMP COM API has been enhanced to improve the performance of your scripted monitors and actions. With the addition of `GetMultiple`, you have the ability to get multiple OIDs within a single SNMP request. `GetNext` issues the SNMP `GetNext` command to retrieve the value of the object that follows a specified object. Finally, the addition of the `SetFunction` allows you to send SNMP set commands to your SNMP manageable devices.

The SNMP API includes the following objects:

- `CoreAsp.Snmprqst`. The main SNMP object used to send SNMP requests (`Get`, `GetNext`, `Set`) to a remote device.
- `CoreAsp.ComResult`. An object returned by certain methods of the `Snmprqst` object to indicate success or failure.
- `CoreAsp.ComResponse`. A response object returned by certain methods of the `Snmprqst` object that contain the status (either error or success) of an SNMP request and the value of the polled object(s).



Note: There are several things to keep in mind when attempting to use the SNMP API. If you are experiencing errors, please see *Troubleshooting the SNMP API* (on page 949).

CoreAsp.Snmprqst


This object is used to send SNMP requests to a remote device.

`Initialize` or `Initialize2` must be called prior to any other members.

CoreAsp.Snmprqst uses a three step process:

- 1 Calls `Initialize` or `Initialize2` to initialize the object against a particular device.
- 2 Sets optional parameters such as timeout value, port, etc.
- 3 Performs any number of `Get`, `GetNext`, `GetMultiple` or `Set` operations against a device. Those operations return an `ComSnmprResponse` object that contains the status of the operation and the value either directly (use `Failed/GetValue/GetOid`) or as a list of SNMP variable binding returned as XML data (use `GetPayload`).

| Method | Description | Returns |
|---------------------------------------|---|-------------------------------|
| Initialize (nDeviceID) | Initializes the <code>Snmprqst</code> object for the device with the device ID specified in <code>nDeviceID</code> . If a device is not configured with a valid SNMP credential, the operation will fail. <ul style="list-style-type: none">▪ <code>nDeviceID</code>. A positive integer corresponding to the device ID of a device configured in WhatsUp Gold. | <code>ComResult</code> object |

| Method | Description | Returns |
|---|---|------------------|
| | <p>Tip: In Active Script Monitor and Script Performance Monitors, the device ID of the device to which the monitor is assigned can be obtained from the Context object:</p> <pre>Context.GetProperty("DeviceID")</pre> | |
| Initialize2 (sDeviceAddress, nCredentialID) | <p>Initializes the <code>SnmpRqst</code> object by creating a connection to a device using the IP address of a device and a credential stored in WhatsUp Gold. This method can be used to initialize <code>SnmpRqst</code> for a device that is not configured in WhatsUp Gold as long as the credentials for the device are configured in the credential library.</p> <ul style="list-style-type: none"> ▪ <code>sDeviceAddress</code>. The address or hostname of the device to be queried. ▪ <code>nCredentialID</code>. A positive integer corresponding to the credential ID of a credential configured in WhatsUp Gold. | ComResult object |
| SetTimeoutMs (nTimeoutInMilliSec) | <p>Sets the timeout value in milliseconds. If not specified, the timeout defaults to 2000 milliseconds.</p> <p><code>nTimeoutInMilliSec</code>. A positive integer representing the number of milliseconds after which unresolved requests should be terminated.</p> <div>  <p>Note: This method returns a value if the method fails and requires an object variable to capture this value. For example: <code>varComResult = SnmpRqst.SetTimeoutMs(5000);</code> where <code>varComResult</code> is a ComResult object.</p> </div> | ComResult object |
| SetNumRetries (nNumberRetries) | <p>Sets the number of times to retry a request that has timed out. If not specified, failed requests are retried one time.</p> <ul style="list-style-type: none"> ▪ <code>nNumberRetries</code>. A positive integer representing the number of times to retry timed out requests. <p>Tip: To send only one SNMP packet per request, set <code>nNumberRetries</code> to 0 (zero).</p> | ComResult object |
| SetPort (nPort) | <p>Sets the TCP/IP port to be used by <code>SnmpRqst</code>. If not specified, port 161 is used.</p> | ComResult object |

| Method | Description | Returns |
|---|--|-------------------------|
| | <ul style="list-style-type: none"> ▪ <code>nPort</code>. A positive integer between 1 and 65535 corresponding to the port to be used. | |
| Get (<code>sOid</code>) | <p>Issues an SNMP Get command to retrieve the value of the specified object.</p> <ul style="list-style-type: none"> ▪ <code>sOid</code>. A string containing a valid OID. | ComSnmppResponse object |
| GetNext (<code>sOid</code>) | <p>Issues an SNMP GetNext command to retrieve the value of the object that follows the specified object in lexicographic order.</p> <ul style="list-style-type: none"> ▪ <code>sOid</code>. A string containing a valid OID. | ComSnmppResponse object |
| GetMultiple (<code>sListOfOids</code>) | <p>Issues an SNMP Get command for each of the objects specified. <code>GetMultiple</code> sends all commands in a single SNMP protocol data unit, so it is more efficient than issuing multiple <code>Get</code> commands independently.</p> <ul style="list-style-type: none"> ▪ <code>sListOfOids</code>. A comma-separated list of valid OIDs. | ComSnmppResponse object |
| Set (<code>sOid</code> , <code>sType</code> , <code>sValue</code>) | <p>Issues an SNMP Set command to set an OID value on a device.</p> <ul style="list-style-type: none"> ▪ <code>sOid</code>. A string containing a valid OID for the object for which you want to set the value. ▪ <code>sType</code>. A single character corresponding to the type of value to set. <ul style="list-style-type: none"> <code>i</code> = integer <code>u</code> = unsigned integer <code>s</code> = string <code>x</code> = hexadecimal string <code>d</code> = decimal string <code>n</code> = NULL object <code>o</code> = object ID <code>t</code> = timeticks <code>a</code> = IPv4 address <code>b</code> = bits ▪ <code>sValue</code>. A string containing the value to set. | ComSnmppResponse object |



Note: The Set function will not work unless the MIB object and the community string for the device have the Read Write access right.

CoreAsp.ComResult

This object is returned by members of the `SnmpRqst` object or other objects to indicate the status of an operation.

| Member | Description |
|--------------------|--|
| Failed | Returns <code>true</code> if this object contains a failure and <code>false</code> if the object contains a success. |
| GetErrorMsg | If Failed is <code>true</code> , this member returns the associated error message. |



Note: All the members of the `ComResult` object are methods. They have no arguments and should be called without parenthesis.

CoreAsp.ComSnmpResponse

This object contains a response from an SNMP request. It is returned by `SnmpRqst` member functions: `Get`, `GetNext`, `GetMultiple` and `Set`.

| Member | Description |
|--------------------|---|
| GetOid | Returns the OID of the polled object. This member cannot be used with operations that poll multiple objects, such as <code>SnmpRqst.GetMultiple</code> . Note: This member is only useful when used with <code>SnmpRqst.GetNext</code> . It can be used with <code>SnmpRqst.Get</code> and <code>SnmpRqst.Set</code> , but it returns the same OID that you specified when calling those functions. |
| GetValue | Returns the value of the polled object. This member can only be used with functions that poll a single object (<code>SnmpRqst.Get</code> , <code>SnmpRqst.GetNext</code> and <code>SnmpRqst.Set</code>). |
| Failed | If the request succeeded, returns <code>false</code> . If the request failed, returns <code>true</code> . Note: When polling multiple objects, <code>Failed</code> returns <code>true</code> if even one error exists in the results returned by <code>GetPayload</code> . |
| GetErrorMsg | If <code>Failed</code> returns <code>true</code> , this member returns the associated error message. |
| GetPayload | Returns XML data describing SNMP variable bindings (each containing OID, Type and Value). This XML data consists of a single <code>VarBindList</code> node which contains one or many <code>SnmpVarBind</code> nodes. <pre><VarBindList> <SnmpVarBind bHasError="false" sError="" sOid="1.3.6.1.2.1.1.1.0" sValue="HELLO" /></pre> |

```
<SnmpVarBind bHasError="false" sError=""
sOid="1.3.6.1.2.1.1.1.1" sValue="WORLD" />
</VarBindList>
```

You can use the Microsoft XML DOM object to access this information. For more information, see the **Read multiple objects in one request** example.



Note: All the members of the `ComSnmpResponse` object are methods. They have no arguments and should be called without using parenthesis.

Example scripts using the SNMP API

These example scripts demonstrate the SNMP API in use. All of these examples are written in JScript.

Initialize an SNMP object with error check from a device ID

The `SnmpRqst.Initialize` method returns a `ComResult` object that tells if the initialization succeeded or failed.

This script uses the `Failed` method to detect an error and logs an error message using `GetErrorMsg` if the initialization failed:

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
```

Alternatively, initialization using a device address and an SNMP credential ID:

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var sAddress = "192.168.3.1";
var nCredentialID = 1;
var oComResult = oSnmpRqst.Initialize2(sAddress, nCredentialID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
```

Send a standard Get and log the polled value

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
var oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.2.1.0");
if (oSnmpResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
    Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ", got " +
oSnmpResponse.GetValue);
}
```

Send a Get using non-standard port and timeout

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
oComResult = oSnmpRqst.SetPort(1234);
oComResult = oSnmpRqst.SetTimeoutMs(5000); // 5 second timeout
var oSnmpResponse = oSnmpRqst.Get("1.3.6.1.2.1.2.1.0");
if (oSnmpResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
    Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ", got " +
oSnmpResponse.GetValue);
}
```


Walk the MIB using GetNext

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
var sOid = "1.3.6.1.2";
//get the next 10 objects
for (i=0; i<10; i++)
{
    var oSnmpResponse = oSnmpRqst.GetNext(sOid);
    if (oSnmpResponse.Failed)
    {
        Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
        break;
    }
    else
    {
        sOid = oSnmpResponse.GetOid;
        Context.LogMessage(sOid + "=" + oSnmpResponse.GetValue);
    }
}
```

Read multiple objects in one request

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = Context.GetProperty("DeviceID");
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}

// Get three objects in one packet:
var oSnmpResponse =
oSnmpRqst.GetMultiple("1.3.6.1.2.1.1.1.0,1.3.6.1.2.1.1.2.0,1.3.6.1.2.1.1.3.0");

if (oSnmpResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
    var sXML = oSnmpResponse.GetPayload;

    var objXMLDocument = new ActiveXObject("Microsoft.XMLDOM");
    objXMLDocument.async = false;
    objXMLDocument.loadXML(sXML);
}
```

```
var oVarBinds = objXMLDocument.getElementsByTagName("SnmpVarBind");

// For each variable binding, log OID=VALUE
for (var i=0; i<oVarBinds.length; i++)
{
    Context.LogMessage(oVarBinds(i).getAttribute("sOid") + "=" +
oVarBinds(i).getAttribute("sValue"));
}
}
```

Reboot a Cisco device using Set



Note: As of WhatsUp Gold v14, SNMP values can be set using the built-in SNMP Set Action. For more information, see Using an SNMP Set Action.

```
var oSnmpRqst = new ActiveXObject("CoreAsp.SnmpRqst");
var nDeviceID = 150;
var oComResult = oSnmpRqst.Initialize(nDeviceID);
if (oComResult.Failed)
{
    Context.LogMessage(oComResult.GetErrorMsg);
}
var oSnmpResponse = oSnmpRqst.Set("1.3.6.1.4.1.9.2.9.9.0", 'i', 2); /* reload */
if (oSnmpResponse.Failed)
{
    Context.LogMessage("Failure. Error=" + oSnmpResponse.GetErrorMsg);
}
else
{
    Context.LogMessage("Success. Polled " + oSnmpResponse.GetOid + ", got " +
oSnmpResponse.GetValue);
}
```

Troubleshooting the SNMP API

There are several things to keep in mind as you attempt to use the SNMP API.

Different results for different versions

Although the SNMP API works on all SNMP capable devices, the results returned depend on the SNMP version. For example, SNMPv1 and v2 return different results for the `GetMultiple` function. If one of the OIDs used in the function is incorrect, SNMPv1 returns only an error, while SNMPv2 returns results for the correct OIDs and an error for the incorrect OID.

The inability to work on certain versions of Windows with IPv6

The SNMP API does not work on the following versions of Windows when using IPv6:

- Windows 2003
- Windows XP
- Windows Vista

Maximum packet size on routers and switches

Routers and switches have a default packet size limitation of 1500 bytes. The `GetMultiple` will return an error if the parameter size exceeds the limit.

Troubleshooting and Maintenance

In This Chapter

| | |
|---|-----|
| Troubleshooting your network | 951 |
| Maintaining the Database | 952 |
| Recovering from a "Version Mismatch" error | 954 |
| Task Tray Application fails on Windows Vista | 955 |
| Co-located SQL Server and WhatsUp Gold server clocks must be synchronized | 956 |
| Connecting to a Remote Desktop | 956 |
| WhatsUp Gold engine message | 956 |
| Troubleshooting SNMP and WMI connections..... | 957 |
| Re-enabling the Telnet protocol handler | 958 |
| Passive Monitor payload limitation | 958 |
| Receiving entries in the SNMP Trap Log | 959 |
| Recommended SMS modems and troubleshooting tips..... | 959 |
| Uninstalling Ipswitch WhatsUp Gold..... | 961 |
| Troubleshooting the WhatsUp Health Threshold | 961 |

Troubleshooting your network

WhatsUp Gold is a tool used to monitor your network. It is up to you to fix the items that WhatsUp Gold brings to light.

The following are questions you should think about while troubleshooting problems detected through WhatsUp Gold.

- Is the entire subnet affected, or a single device?
- Is the entire device affected, or a service monitor on the device?
- What type of device is down?

Actions to take

After you have determined the scope of the network problems, one of the following may help you fix the problem.

- If it is the entire subnet that appears to be down, you should check your hub, router, or switch.

- Begin with checking the physical connections of the device to the network and to the power supply. Check the network cables and power cables.
- Check wireless network cards and signal strength.
- Check the Device Health log to see whether a single monitor or the entire device is down. If the device is down, all of the monitors will appear to be down.
- Using the Ping monitor, verify that the connection between the device and the network is up.
- If a monitor appears to be down, try restarting the service that the monitor is watching. To restart a service, you must access the device directly; this cannot be done through WhatsUp Gold.

Maintaining the Database

You can use the WhatsUp database utilities to back up and restore the database and to perform database maintenance and troubleshooting. If you have a WhatsUp Gold Flow Monitor license, you can also back up and restore the Flow Monitor databases via the WhatsUp database utilities.

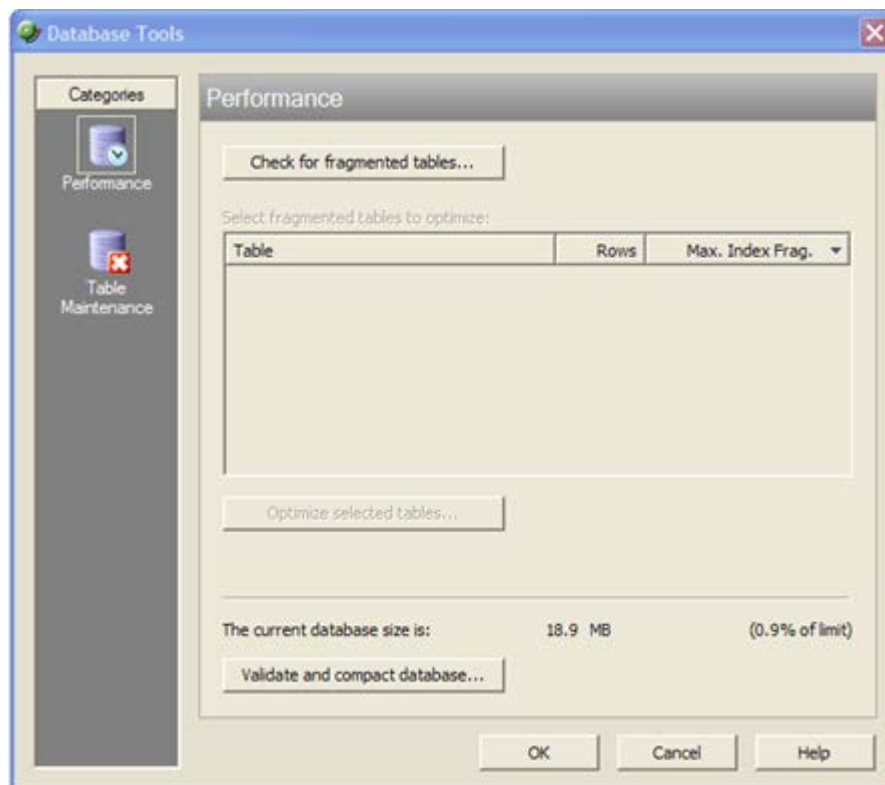
To access the database utilities, open the WhatsUp Gold console, then select **Tools > Database Utilities** from the main menu.

About the database tools

The database tools let you manage index fragmentation and purge expired data.

To access the tools:

- 1 From the main menu in the WhatsUp Gold console, select **Tools > Database Utilities > Tools**. The Database Tools dialog appears.



- 2 Select one of the tools:
 - Performance
 - Table Maintenance

Database Performance Tool

The Database Performance Tool is used to monitor the size of your database, and to manage the index fragmentation percentage of the individual tables. Fragmented indexes can cause database operations to slow down considerably, in much the same way that disk fragmentation causes your computer to run slower.

Click **Check for fragmented tables** to begin. This may take a considerable amount of time (up to a few minutes), depending on how many records are in your database.

- **Select fragmented tables to optimize.** This list shows all database tables with greater than 10% index fragmentation, along with the total number of data rows in that table.
- **Optimize selected tables.** Select the tables in the list above to defragment those database tables. WhatsUp Gold automatically stops and restarts the WhatsUp Service. The status of the operation appears on the dialog, next to this button.

- **The current database size is.** This section of the dialog shows the total amount of space used by the database. If you are using SQL Server 2005 Express as the WhatsUp Gold database, this section also displays the percentage of the 4 GB file size limit currently in use.
- **Validate and compact database.** Click this button to execute commands that validate the database, index, and database links, and to compact the database. WhatsUp Gold automatically stops the Ipswitch Service Control Manager (ISCM) and restarts it once the operation is complete.

The validation phase executes the SQL Server commands `DBCC CHECKCONSTRAINT`, `DBCC CHECKCATALOG`, and `DBCC CHECKDB`. These commands check the integrity of all constraints in the database, check for consistency in and between system tables in the database, and check the allocation and structural integrity of all the objects in the database.

The compacting phase executes the SQL Server command `DBCC SHRINKDATABASE`, which shrinks the size of the data files in the database. Note that no compression is used; the database is simply compacted by removing empty space.

For more information on validating or compacting the database, see *Getting Started with SQL Server* (http://www.msdn.microsoft.com/library/default.asp?url=/library/en-us/startsql/getstart_4fht.asp) on the Microsoft Web site..

Database Tools Table Maintenance

This feature lets you purge expired data from data tables in your database. Be very careful when using this dialog, as data that is purged through this process is lost and cannot be restored.

- **Select tables to purge.** The data tables are grouped by the purpose they serve (active monitors, report data collection, and other). Select the tables you want to purge from the three lists.
- **Total Rows.** The total number of data rows in this table that currently holds data. This includes live and expired rows.
- **Expired Rows.** The total number of expired data rows in this table. Expired data is data that has been rolled up, and has not yet been purged by the application or has not been reused. These are rows that are marked for deletion, or have been kept longer than needed, according to your data roll-up settings. See Program Options - Report Data for more information on setting your data roll-up settings.

Click **Purge Expired Rows** to remove those records from the database.

Recovering from a "Version Mismatch" error

When starting the WhatsUp Gold or Flow Monitor application, you may get a "Version Mismatch" error if the program version does not match the database version. The WhatsUp Gold and Flow Monitor applications can only use a database that is compatible with the version of the software currently installed.

If the install encounters an error during upgrade, and you abort the database upgrade portion of the install, or you choose the Ignore option and allow the upgrade process to continue the install, the database may not be upgraded properly. To attempt to resolve this issue, reboot your machine and run the same install again. During the install, select the Repair option.



Important: If running the repair does not correct the database issue, review your log file to help identify the issue (located in the `..\Program Files\Ipswitch\WhatsUp\RemoteDBConfig.txt`, search the *Ipswitch Knowledge Base* (<http://www.whatsupgold.com/wugtechsupport>) for technical support resources, or contact *Ipswitch Technical Support* (<http://www.whatsupgold.com/wugtechsupport>) for troubleshooting help.

You may also get a "Version Mismatch" error if you restore a WhatsUp Gold or Flow Monitor database from an earlier version of the application. To attempt to resolve this issue, reboot your machine and run the same install again. During the install, select the Repair option.



Important: The WhatsUp Gold polling engine will not run, nor can the WhatsUp Gold, Alert Center, or Flow Monitor applications be used until this database version mismatch error is corrected.

Task Tray Application fails on Windows Vista

After installing WhatsUp Gold on Microsoft Vista, the WhatsUp Gold Task Tray Application does not connect to the database if you log in to Windows using any account other than the account used to install the application. To correct this issue, execute this script from the command line in the `C:\Program Files\Ipswitch\WhatsUp\DB Scripts\` folder:

```
sqlcmd -E -S (local)\WHATSUP -d WHATSUP -i  
grant_all_users_read_access.sql
```



Important: If you run the above script, all database users (admin and others) are granted read access to the WhatsUp Gold database.

Co-located SQL Server and WhatsUp Gold server clocks must be synchronized

If a WhatsUp Gold and SQL Server is not located on the same physical machine (server) and the system clocks are not synchronized to the same time zone, inaccurate data may occur in reports. To correct this issue, set the system clock for the same time zone and ensure that the clocks are synchronized to the same time.

Connecting to a Remote Desktop

WhatsUp Gold provides a quick link to the Remote Desktop/Terminal Services client that allows you to connect to your devices remotely. If the client is installed on your WhatsUp Gold computer, and the Remote Desktop/Terminal Services is installed and activated on the device you want to connect to, you are prompted for the user name and password for that device.

This application allows you to troubleshoot problems with your devices and monitors identified by WhatsUp Gold.

To connect to a remote desktop:

- 1 Right-click the device you want to connect to.
- 2 From the right-click menu, select **Remote Desktop**. If the connection is successful, the log in dialog appears. If the connection fails, an error message appears.



Note: For more information about the Remote Desktop feature, see the online help for the Remote Desktop client itself.

WhatsUp Gold engine message

This message means that WhatsUp Gold is not operating properly, because the WhatsUp Gold Engine service has stopped.

To stop and restart the WhatsUp Gold engine from the console:

- 1 From the console, select **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
- 2 Select **WhatsUp Polling Engine**, click **Stop**, then click **Start**.

Troubleshooting SNMP and WMI connections

If you experience connection problems when connecting to a device via the Web Task Manager, Web Performance Monitor, or any other WhatsUp Gold feature that uses WMI or SNMP, please consult the lists below to troubleshoot the problem.

Troubleshooting a WMI connection



Important: You must have administrative credentials to establish WMI connections. For more information, see *Using Credentials* (on page 75). Also, see Microsoft article 875605 (<http://support.microsoft.com/default.aspx?scid=kb;en-us;875605>).

- Establishing a WMI connection can be very slow.

This slow connection time can worsen when attempting to connect with devices running Microsoft Vista.

We recommend that you open RPC port 135 on both the WhatsUp device's firewall and the firewall for device to which you are attempting to connect. Also be sure to open this port on any firewall between the connecting devices. Refer to the operating system Help for more information.

- Connected devices that are running different versions of Microsoft software (i.e. - Microsoft XP and Vista) may experience delayed or slow communication.
- WMI over VPN connections can take up to 120 seconds (possibly longer) to establish an initial connection. After the initial connection is made, subsequent connections take 8 to 10 seconds.
- Again, we recommend that you open RPC port 135 on each device's firewall, and any firewall between the connecting devices.
- A WMI memory leak exists in Windows 2003 and XP. Microsoft has developed hotfix 911262 (<http://support.microsoft.com/kb/911262/en-us>) that minimizes the leak in XP, and completely fixes the leak in Windows 2003.

For more information regarding WMI and connection problems, see Microsoft articles 389290 (<http://msdn2.microsoft.com/en-us/library/aa389290.aspx>), 389286 (<http://msdn2.microsoft.com/en-us/library/aa389286.aspx>), and the section entitled "I can't connect to a remote computer" in the Microsoft Script Center article, *WMI Isn't Working!* (<http://www.microsoft.com/technet/scriptcenter/topics/help/wmi.msp#E2C>).

Troubleshooting an SNMP connection



Important: The SNMP Trap Listener must be enabled to collect data for the SNMP Trap Log. To enable the WhatsUp Gold SNMP Trap Listener, the Microsoft SNMP Trap Listener must be disabled. Also, be sure to open SNMP port 162 for incoming SNMP traps.

- If you receive invalid values when attempting to monitor the IfOperStatus OID from a device running Vista, download Microsoft's hotfix 935876 (<http://support.microsoft.com/kb/935876>) to solve the problem.
- If you experience connection problems with a specific device, ensure that the device has SNMP enabled. Also ensure that SNMP port 161 is open on the device you are attempting to monitor.
- If you get what looks like a "stair-step" in your CPU and Process Utilization graphs, this is caused by Microsoft's 60-second polling interval. Increasing WhatsUp Gold's polling interval could help compensate for the lengthy Microsoft polling interval.
- Similarly, if you experience delays and/or unexpected, weird spikes in your graphs, try increasing the polling interval.

Re-enabling the Telnet protocol handler

The Telnet protocol handler is disabled by default in Microsoft Internet Explorer 7. In order to use the Telnet tool in WhatsUp Gold, you need to re-enable the Telnet protocol.

To re-enable the Telnet protocol:

- 1 Click **Start > Run**. The Run dialog box opens.
- 2 In the Open box, enter: `Regedit`, then click **OK**. The Registry Editor opens.
- 3 Go to the following key:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl`
- 4 Under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl`, create a new key named `FEATURE_DISABLE_TELNET_PROTOCOL`.
- 5 Add a `DWORD` value named `iexplore.exe` and set the value to 0 (decimal).
- 6 Close the Registry Editor and restart Microsoft Internet Explorer. The Telnet protocol is enabled.

Passive Monitor payload limitation

Passive monitors have a payload limitation of 3 KB for WMI, SNMP, and Syslog Passive Monitors.

Receiving entries in the SNMP Trap Log

In order for entries to be added to the SNMP Trap Log, the SNMP Trap Listener must be enabled. For more information, see [Enabling the SNMP Trap Listener](#).

Additionally, if the trap receiving port is not on the firewall's list of exceptions, traps may not be receivable, and as a result, will not be added to the SNMP Trap Log. Please ensure that the trap receiving port is on the firewall's list of exceptions.

Recommended SMS modems and troubleshooting tips

Ipswitch has tested the following SMS modems for use with the SMS Direct Action (not the SMS Action):

- *Motorola® RAZR V3* (<http://www.motorola.com>) (Recommended)

This cell phone was connected to the WhatsUp device acting as a GSM modem.

- *MultiModem® GPRS external wireless modem* (<http://www.multitech.com/PRODUCTS/Families/MultiModemGPRS/>), model: MTCBA-G-F2
- *Siemens TC65 Terminal* (<http://www.usa.siemens.com>)

Unlike the other modems that have their own drivers to install, this modem did not have specific drivers to install. The Windows Standard 56000 bps modem driver was used with the maximum port speed set to 115200.

- *Falcom Samba 75 (GSM/GPRS/EDGE)* (<http://www.falcomusa.com>)



Note: Falcom Samba 75 modem is not supported on Windows Server operating systems.

- *Vodafone USB modem for SMS Direct* (<http://www.vodafone.com/index.VF.html>) tested on Huawei, Model E220, HSDPA USB modem)
- *ConiuGo GPRS GSM Quadband Modem / USB-Busp (850, 900, 1800 & 1900 MHz)* http://www.coniugo.com/pdf/e_gprs_gsm_quadband_modem_rs232_usb.pdf
- *Zoom 56k serial modem* (http://www.zoomtel.com/graphics/datasheets/dial_up/30481101.pdf)

To consider

- GSM networks operate in the 850/900/1800/1900 Mhz bands.
- GSM modems are typically either dual or quad band.



Note: You must acquire a dual modem that operates at the correct frequency, or purchase a quad band modem.

- European markets typically use 900/1800 Mhz capable devices.
- The U.S. and Canada use 850/1900 Mhz capable devices.

Troubleshooting SMS Modems

If an SMS modem is not working as expected, verify that the communications port (COM port) to which the modem is attached is configured to use settings supported by the modem.

- 1 In the Windows Control Panel, double-click **Device Manager**. The Device Manager appears.
- 2 Expand **Ports**.
- 3 Double-click the communications port used by the SMS modem. The Communications Port Properties dialog appears.
- 4 Select the **Port Settings** tab.
- 5 Using the documentation provided by the modem manufacturer, verify that the port settings listed are supported by the modem. If the listed settings are not supported, make any necessary changes.



Note: If you are using the MultiModem® GPRS external wireless modem, model MTCBA-G-F2, set **Flow Control** to **Hardware**.

- 6 Click **OK** to save changes.

Using line feeds and carriage returns to correct SMS modem issues

Some SMS Direct enabled phones do not work correctly with SMS Direct Actions because new line characters are not always handled properly. This issue may be corrected by adding the following new registry key entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Network Monitor\Whatsup plug-ins\Actions\ActSmsDirect\NewLine
```

In the **Value data** box, enter a combination of a carriage return (\r) and/or line feed (\n) command. For example enter one of the following:

- newline \r\n (recommended)
- newline \r
- newline \n

Uninstalling Ipswitch WhatsUp Gold

To uninstall Ipswitch WhatsUp Gold:

- 1 Select **Start > Settings > Control Panel**, then select **Add or Remove Programs**.
- 2 Select Ipswitch WhatsUp Gold.
- 3 Select **Remove**.

You can also run the Ipswitch WhatsUp Gold installation program, then select **Remove**.

Select one of the following dialog options:

- **Remove the WhatsUp Gold application, but leave network data I have collected intact.** This uninstalls the WhatsUp Gold program but keeps all your WhatsUp configuration data as well as the monitoring data you have collected. SQL Server 2005 Express will not be uninstalled.
- **Remove both the WhatsUp Gold application, and all network data I have collected.** This uninstalls the WhatsUp program and removes all of your WhatsUp configuration and monitoring data.
- **Also, remove the "WhatsUp" copy of SQL Server Express Edition.** This also removes the "WhatsUp" SQL Server Express Edition instance that was created during the installation. Select this option to remove **ALL** WhatsUp components from the system.



Note: When this option is selected, WhatsUp Gold leaves SOME data behind, such as the \HTML directory and the \Data directory for situations where there may be user-modified or user-created files in those directories.

Troubleshooting the WhatsUp Health Threshold

If you are encountering errors in the Alert Center Log after configuring and running the WhatsUp Health Threshold's service checks, there are several steps you can take to troubleshoot the occurrence of these errors.

First, from a CMD window, run the following commands:

Windows XP and later

```
wmiadap/clearadap
```

```
wmiadap/resyncperf
```

Windows 2000

```
winmgmt/clearadap
```

```
winmgmt/resyncperf
```



Note: These commands may take some time to execute.

If after running these commands the errors persists, run the Microsoft WMI Diagnosis Utility, found on Microsoft's web site:

<http://www.microsoft.com/downloads/details.aspx?familyid=d7ba3cd6-18d1-4d05-b11e-4c64192ae97d&displaylang=en>

Terminal Services

Additionally, you may encounter problems with your service-level threshold checks if you are using Microsoft Terminal Services (Remote Desktop Services) to run the WhatsUp Gold web server. If more than one person is logged in to Terminal Services at a time, the following WhatsUp Health Threshold service checks/performance counters may fail:

- WhatsUp polling service SQL query check
- WhatsUp web service HTTP response check
- WhatsUp web service SQL query check

You may experience a high volume of errors logged to the Alert Center Log from these service checks until the number of Terminal Service users drops to one or none.

Using WhatsUp Gold Flow Monitor

In This Chapter

| | |
|--|------|
| Flow Monitor Overview | 964 |
| Preparing network devices | 972 |
| Managing Flow Sources | 992 |
| Managing Flow Monitor Settings | 1006 |
| Configuring Applications | 1018 |
| Configuring Flow Groups | 1022 |
| Configuring Type of Service | 1025 |
| Managing unclassified traffic | 1027 |
| Configuring Data Export Settings | 1030 |
| Maintaining Flow Databases | 1032 |
| Managing users and user rights | 1036 |
| Using Flow Monitor reports | 1038 |
| Using Flow Monitor dashboard reports | 1066 |

Flow Monitor Overview

In This Chapter

| | |
|---|-----|
| Welcome to WhatsUp Gold Flow Monitor..... | 964 |
| What is Flow Monitor? | 964 |
| How does Flow Monitor work? | 965 |
| System requirements | 967 |
| Flow Monitor Home..... | 968 |

Welcome to WhatsUp Gold Flow Monitor

Flow Monitor collects, analyzes, and reports on NetFlow, sFlow, J-Flow (sampled NetFlow), or IP Flow Information Export (IPFIX) data from routers, switches, and other network devices, creating visible trends and patterns in network bandwidth utilization. Flow Monitor offers versatile reporting on the hosts generating and receiving traffic and the applications over which traffic is transmitted.

This help system includes information about the features and benefits of WhatsUp Flow Monitor. For more information, use the Contents, Index, or Search to the left, or select one of the sections below.

- **WhatsUp Flow Monitor Overview**

Learn about the NetFlow protocol, discover how Flow Monitor works, and view system requirements for Flow Monitor.

- **Configuring Flow Monitor**

Discover how to configure NetFlow sources to send data to Flow Monitor, define traffic over non-standard ports, manage users, and maintain the Flow Monitor database.

- **Navigating Flow Monitor**

Find out about the features of the Flow Monitor home page and learn how to search for traffic to or from a specific host.

- **Using Reports**

Learn about the Flow Interface Details report, the Flow Interface Overview report, the Flow Bandwidth Usage report, and the Flow Log. Explore using dashboard reports in Flow Monitor and in WhatsUp Gold.

What is Flow Monitor?

WhatsUp Gold Flow Monitor is a network traffic monitor that lets you gather, analyze and report on network traffic patterns and bandwidth utilization in real-time.

WhatsUp Flow Monitor:

- Uses network protocols such as NetFlow, sFlow, Jflow and IPFIX to collect and analyze information about the traffic on a router, switch, or other network device.
- Highlights overall utilization for the LAN or WAN, individual devices, or specific interfaces, and provides information about the users, applications and protocols that consume network resources.
- Provides reports that allow you to:
- View network usage trends to determine when to upgrade hardware to increase network capacity.
- Recognize and correct network configuration issues that may needlessly consume network resources or expose your network to security vulnerabilities.
- Identify traffic which may indicate undesired network usage, such as unauthorized use of peer-to-peer file sharing applications or a denial-of-service attack against your organization.
- Troubleshoot and correct causes of spikes in network traffic before they become problems.

How does Flow Monitor work?

What is Netflow?

NetFlow is a protocol used to collect data about network IP traffic and is used to monitor and record network usage, give indications of traffic routes and provide data in support of traffic accounting, usage-based billing and other network related activities. This data is classified using the concept of a network flow.

A network *flow* is a unidirectional sequence of packets that has the following characteristics in common:

- Source IP address and port number
- Destination IP address and port number
- IP Protocol
- Ingress interface
- IP Type of Service (ToS)

How does NetFlow work?

To capture, transmit and analyze NetFlow data the following NetFlow enabled components must be in place:

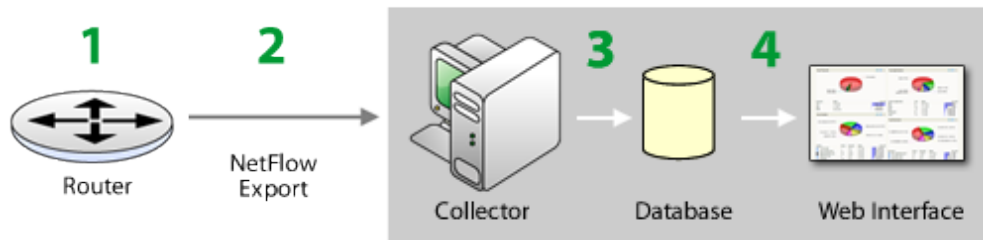
- **NetFlow exporter.** observes packet data and creates records from the monitored network traffic and transmits that data to the NetFlow collector.
- **NetFlow collector.** collects the records sent from the exporter, stores them in a local database and forwards the records to an analyzer.
- **NetFlow analyzer.** analyzes the NetFlow records for information of interest, which may include bandwidth usage, policy adherence, and forensic research.



Note: The exporter can be either an included function of the network device, such as the NetFlow export functionality on Cisco routers, or it can be an external probe configured to monitor one or more interfaces on the device, such as the Ipswitch NetFlow Probe.

How does Flow Monitor fit into the NetFlow architecture?

Flow Monitor acts as a flow collector and analyzer, providing a central location for the collection, summarization, storage and analysis of network traffic data. This network traffic data is captured as *flow* data, and is delivered by network monitoring protocols implemented on network devices throughout the network. When a router or other device sends flow data to Flow Monitor, it follows the process shown below.



- 1 The router gathers information about the traffic that is passing through it and summarizes that data into a NetFlow, sFlow, J-Flow (sampled NetFlow) or IP Flow Information Export (IPFIX) export datagram.
- 2 The router sends the flow export to Flow Monitor, which acts as a flow collector.



Note: sFlow data is sent every x number of packets (configurable on the sFlow device), whereas all NetFlow data is collected and monitored. This means that sFlow data provides a sampling of network traffic data, whereas NetFlow data provides all network traffic data.

- 3 The Flow Monitor collector stores the NetFlow, sFlow, J-Flow (sampled NetFlow) or IP Flow Information Export (IPFIX) export in the database.
- 4 When the report data is viewed on the web interface, Flow Monitor retrieves the data from the database and manipulates it to produce the report.



Tip: Flow Monitor can collect and generate reports for Flow data from multiple devices.

System requirements

WhatsUp Gold Flow Monitor has the same base *system requirements* (<http://www.whatsupgold.com/WUG15relnotes>) as WhatsUp Gold. In addition, WhatsUp Gold Flow Monitor requires:

- WhatsUp Gold Standard Edition, Premium Edition, MSP Edition, or Distributed Edition
- One or both of the following:
- At least one routing device that supports NetFlow version versions 1, 5, 7, and 9, sFlow versions 2 and 5, J-flow (sampled NetFlow) or IP Flow Information Export (IPFIX).
- A Flow Publisher monitoring a flow source.
- 32-bit MS SQL Server 2005 Standard Enterprise Edition, 32-bit or 64-bit Microsoft SQL Server 2008 or 2008 R2 Standard or Enterprise Edition, or 32-bit or 64-bit Microsoft SQL Server Cluster 2005, 2008, or 2008 R2 (all editions except Microsoft SQL Server Express edition)



Note: WhatsUp Gold Flow Monitor is more demanding on the database than WhatsUp Gold. While WhatsUp Gold Flow Monitor can successfully use SQL Server 2005 Express, we recommend either 32-bit MS SQL Server 2005 Standard or Enterprise Edition or 32-bit or 64-bit Microsoft SQL Server 2008 or 2008 R2 Standard or Enterprise Edition for best performance.

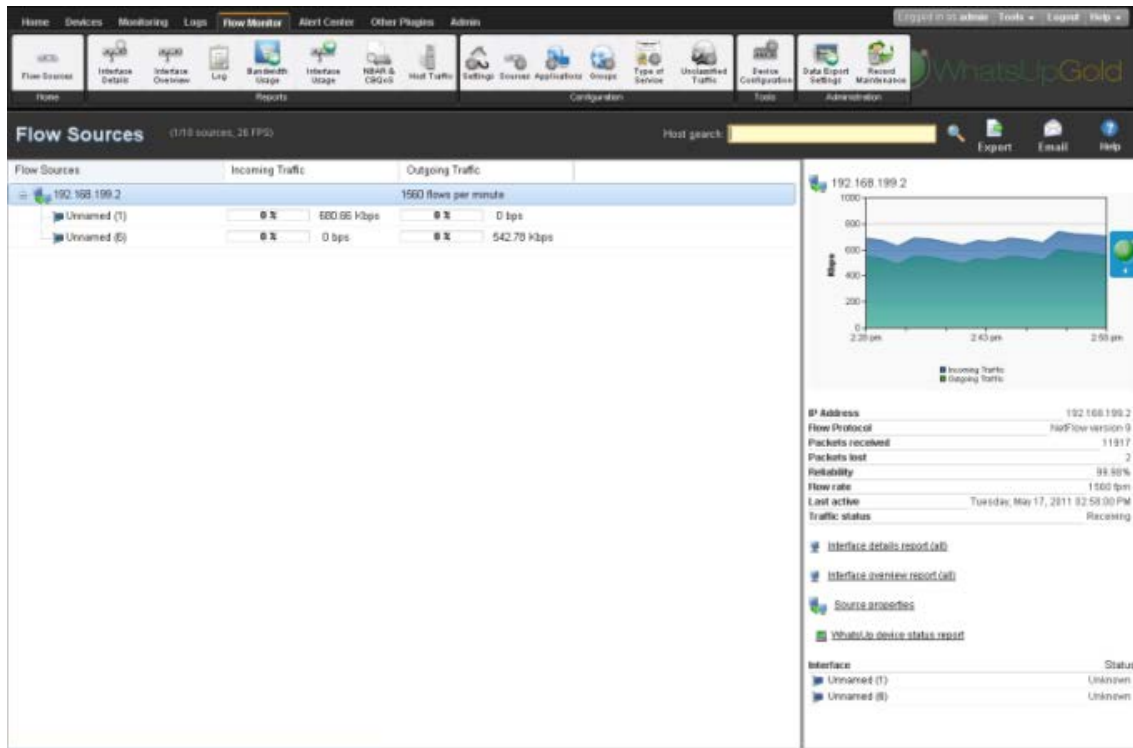
- 2 GHz dual-core processor (required) to quad-core processor (recommended)
- An additional 2 (required) to 4 GB RAM (recommended)
- 16 GB (required) to 22 GB (recommended) hard disk space for the databases



Note: If using Microsoft SQL Server 2005 or Microsoft SQL Server 2008 or 2008 R2, the database size is limited by available hard disk space.

Flow Monitor Home



The Flow Monitor Flow Sources page provides a summary of the current usage and status of Flow Monitor sources, and acts as the Home page for the Flow Monitor plug-in. The left and right panes of the content pane display different types of data; Flow Sources on the left and Source and Interface Details on the right. Click **Flow Monitor > Flow Sources** to open the Flow Monitor Flow Sources screen.



Flow Monitor sources

The left pane of the page lists each of the monitored sources and the interfaces associated with each source.

In the Flow Sources title bar, the number of licensed sources and total licenses available is displayed along with the total number of flows per second received by all of the licensed sources. For example, the following (2/10 sources, 65 FPS) indicates that there are 2 licensed sources of 10 available licenses, and that the total flows per second being received by all of the sources is 65 flows per second.

- **Flow Sources.** Routers and switches that have been configured to send flow data to Flow Monitor and are enabled in Flow Monitor are listed in this column. In the list, sources are organized at the top level. Associated interfaces for each source are below the source name. Use the  collapse and  expand buttons to show or hide source interfaces. For each source, the number of flows per minute (fpm) for Flow devices and samples per minute (spm) for sFlow devices generated by all interfaces on the selected source over the the last period is displayed. When you select a source from the Flow Sources list, its total traffic is displayed in the right pane, along with all of the other information about the source.



Note: Interfaces can be hidden; if you do not see an interface listed on this dashboard report, check to see if it has been hidden via the Flow Interface dialog.



Tip: If you do not see a source listed that you would like to monitor, first go to the Flow Sources dialog to configure source settings. If you still do not see the router listed, check to see that the router is configured to send flow data. For more information, see *Configuring Flow Monitor sources* or *Configuring sFlow sources* (on page 975).

- **SNMP Sources.** SNMP Sources are Flow Sources that have been created for the purpose of collecting NBAR and CBQoS statistics from a device using SNMP polling instead of flow data. SNMP Sources appear as normal Flow Sources. For information on creating an SNMP source, see *Create Flow Source*.
- **Aggregate Sources.** Aggregate Sources are individual interfaces existing on one or many Flow Sources that are aggregated into a single logical group that is treated as a separate source for reporting purposes. These sources appear as folders below the Flow Sources. For information on creating an Aggregate Source, see *Creating an Aggregate Source*.
- **Incoming Interface Traffic.** Incoming traffic is reported as a percentage of usage according to the interface's speed, and number of incoming bytes per second (bps) based on the last traffic to enter the interface.
- **Outgoing Interface Traffic.** Outgoing traffic is reported as a percentage of usage according to the interface's speed, and as the number of outgoing bytes per second (bps) based on the last traffic to leave the interface.

Source and interface details

The right side of the page gives detailed information about a selected source or interface.



Note: If you have not enabled Flow sources at this time, a Welcome dashboard report is displayed on the right side of the Flow Monitor Home page. Consult this dashboard report for information on configuring your routers to send Flow data, and for other general Flow Monitor configuration information.

Source details

Click a source, or device in the list to view the Source details on the right side of the Home page.

- **IP address.** The source router's IP address.
- **Flow protocol.** The version of Flow or sFlow the source uses when exporting flow data.
- **Sample rate.** The rate at which the source is polling interface data.



Note: The sample rate appears for only for sources sending sampled NetFlow data.

- **Packets received.** The number of packets the collector received from the source since the collector service was started.
- **Packets lost.** The number of packets sent from the source but not received by the collector since the collector service was started.
- **Reliability.** The percentage of packets received versus packets lost by the source since the collector service was started.
- **Flow rate.** The number of flows per minute (fpm) reported by the source during the last collection interval.
- **Last active.** The last time traffic was received from the source.
- **Traffic status.** Whether Flow Monitor is receiving traffic from the source; either receiving, or not receiving.



Note: If any traffic has been received within the last 30 minutes, the traffic status is displayed as receiving.

Use the Source Properties link at the bottom of the source details to view the Flow Source dialog and use the Interface links to view the WhatsUp Gold Interface Details report.



Note: A link for the WhatsUp Gold Interface Details report appears only if the source is monitored in WhatsUp Gold.

Interface details




Click a source device interface in the list to view the Interface details on the right side of the Home page. The Interface Traffic report for the last collection interval is displayed at the top of the interface's details.

- **Last incoming details.** The last time traffic transmitted over the incoming interface.
- **Last outgoing details.** The last time traffic transmitted over the outgoing interface.
- **Interface type.** The type of the interface; for example, Ethernet CSMA/CD.

- **In speed.** The speed at which data is flowing to the interface.
- **Out speed.** The speed at which data is flowing from the interface.
- **Status.** The status of the interface; either Up, Down, or Unknown.

Use the links at the bottom of the interface details to view the Interface Details and Interface Overview reports, as well as the Flow Interface Properties.


Exporting, emailing, scheduling and managing reports

 Use the **Export**  icon, at the top right of the page, to export reports. Use the **Email**  icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 1064).

Host Search

Use the Host Search tool in the upper-right side of the page to locate traffic to or from a host or group of hosts.

To perform a host search:

- 1 Enter search criteria, such as an IP address or host name, in the **Host search** field.
- 2 Click the search button 
 - When a host name is entered for search, the Host Search dialog appears with a list of interfaces where traffic to that host has been logged. You can use the search options in the Host Search dialog to further narrow your search. For more information, see the Flow Monitor Host Search dialog help.
 - When a complete IP address is entered for search, the Select Interface dialog appears with a list of interfaces where traffic to that IP has been logged.

Note: The Domain, Country, and Last Resolved fields may show as Not Available if the IP address is not available in the DNS.



Tip: Use the right-click menu on this page to view and configure parts of the application. For more information, see Using the Flow Home page right-click menu.

Preparing network devices

In This Chapter

| | |
|---|-----|
| Determining which network devices to monitor..... | 972 |
| Manually configuring devices to export flow data to Flow Monitor..... | 973 |
| Configuring sFlow enabled devices to export flow data to Flow Monitor | 975 |
| About Flexible NetFlow..... | 978 |
| About Network Based Application Recognition (NBAR) | 982 |
| About CBQoS | 984 |
| Viewing potential Flow Monitor sources | 988 |
| Using Flow Monitor to Configure Cisco NetFlow Devices..... | 988 |

Determining which network devices to monitor

When planning your Flow Monitor deployment, it is important to understand which network devices are likely to provide you the information you want. In identifying those devices, questions about the data flowing through an individual device, its location in respect to other network devices and the types of addresses (internal/external) available to that device are all of importance.

Are you interested in monitoring the internet gateway routers connecting to your ISP for application level traffic analysis, performing forensics and diagnostics on a core router of a public facing network, or monitoring your WAN core in order to plan for additional capacity? The answers to these and similar questions about the purpose of your monitoring will provide you with some indication as to which devices in your network are of most interest as potential sources for Flow Monitor.

Once a potential Flow Monitor source has been identified, you should consider the location of the device with respect to other networking devices, particularly those devices that perform network address translation (NAT). Depending on where the source is located relative to the device performing NAT, traffic to and from an internal (private) IP addresses are reported differently in the exported NetFlow data.

- If the device is inside the firewall, or if no firewall exists, the exported flow data includes the internal IP address for devices generating and receiving traffic. This allows you to pinpoint the exact device in the internal network to which the traffic belongs.

- If the device is outside the firewall, the exported flow data aggregates all traffic to and from internal devices and reports it as belonging to a single public address belonging to the device performing the address translation. In this case, you can only determine that an internal device originated or received traffic, but you cannot pinpoint the traffic as belonging to a specific internal device.
- If the device exporting flows is also performing NAT, you can configure the device to export the flow data using either the private or the public translated address, mimicking either of the above scenarios. To see internal IP addresses, configure the device to export data on `ingress` and `egress` for the **internal** interface. To see all traffic reported using the external translated IP address, configure the device to export data on `ingress` and `egress` for **external** interfaces. For more information, see *Manually configuring network devices to export flow data to Flow Monitor* (on page 973).

Other conditions that may also change the nature of the data reported by Flow Monitor include:

- When address translation occurs anywhere in the path between the source and the destination, IP addresses reported are altered to include the translated address. In most cases, this does not present a problem, but it may require monitoring multiple flow-enabled devices to track traffic in complex network environments.
- Virtual private networks and other tunneling technology (such as ESP or SSH) can appear to distort reports. In these cases, Flow Monitor reports large amounts of traffic sent over a small number of flows. This is expected behavior, as VPNs and other tunnels aggregate traffic from multiple connections and funnel it through a single connection.

Manually configuring devices to export flow data to Flow Monitor

Network devices must be configured to generate and send NetFlow data to Flow Monitor. This is accomplished manually using the device's command line interface (CLI), or automatically through the Source configuration dialog (**Flow Monitor > Configuration**) for devices that are NetFlow enabled and have the Cisco NetFlow MIB (OID: 1.3.6.1.4.1.9.9.387).

To manually configure NetFlow enabled devices to send Flow data to Flow Monitor:

Caution: This procedure is an example that applies to a Cisco 1812 router and should not be used for other devices. The process for configuring a device to export Flow data varies widely from device to device and dependent upon your network configuration. Please see your router's documentation to determine the correct process for your device.

- **Step 1.** Open the configuration interface for the router and enter the commands detailed in the following table to configure global options for all interfaces on the router.

| Command | Purpose |
|---|---|
| <code>enable</code> | Enters privileged EXEC mode. Enter your password if prompted. |
| <code>configure terminal</code> | Enters configuration mode. |
| <code>ip flow-export version <version_number></code> | Sets the version of the NetFlow protocol that should be used to export data. Flow Monitor supports versions 1, 5, 7, and 9 only. |
| <code>ip flow-export destination <IP> <port></code> | Enables the router to export Flow data. Substitute the Flow Monitor server's IP address for <IP> and the listener port specified in the Flow Monitor Flow Settings dialog for <port>. |

- **Step 2.** Enter the commands detailed in the following table to enable the router to export Flow data about the traffic on an interface. You must repeat these commands for each interface.

| Command | Purpose |
|--|--|
| <code>interface <interface></code> | Enters the configuration mode for the interface you specify. Substitute <interface> with the interface's name on the router. |

| | |
|--|---|
| <pre>ip flow ingress</pre> <p>- or -</p> <pre>ip flow egress</pre> | <p>Enables Flow data export. Select the command that best fits your needs.</p> <ul style="list-style-type: none"> ▪ <code>ip flow ingress</code> exports flows of all inbound traffic that uses the interface. ▪ <code>ip flow egress</code> exports flows of all outbound traffic that uses the interface. |
|--|---|



Tip: If the device exporting Flow data is also performing network address translation (NAT), we recommend exporting egress data from the internal interface so that private network addresses are communicated. Any other configuration results in all private addresses reporting as the public addresses of the device performing the network address translation.



Note: Other options exist for configuring NetFlow. For a complete list of available options, see *Configuring NetFlow* (http://www.whatsupgold.com/NF_CiscoCfg) on the Cisco Web site.

Configuring sFlow enabled devices to export flow data to Flow Monitor

Before you can view meaningful sFlow reports, you must configure sFlow-enabled devices, such as routers or switches, to communicate network activity back to the Flow Monitor listener application. There are two methods to configure sFlow to send data to Flow Monitor:

- Configure the sFlow device with the device OS commands using the command line interface (CLI).
- or -
- Configure the sFlow device using SNMP commands.

The following examples shows how to configure sFlow devices to send data to Flow Monitor.

Configuring sFlow using the CLI

To configure a sFlow enabled device to send sFlow data to Flow Monitor using the command line interface (CLI):



Caution: This procedure is an example that applies only to an HP ProCurve 3500 switch and should not be used for other devices. The process for configuring a device to export sFlow data varies widely from device to device and is dependent upon your network configuration.

The following example uses CLI configuration to enable sFlow on an HP ProCurve 3500 series switch. The configuration is for Flow Monitor running on a system with IP address 192.168.3.31 and receiving sFlow data on UDP port 9999.

- 1 Access the sFlow device via the command line interface (CLI).
- 2 Set the sFlow device IP (sFlow collector) using the following commands.

| Command | Purpose |
|--|--|
| (config)# sflow 1 destination <ipaddress> <port> | Sets the sFlow receiving device address (192.168.3.31) and UDP port (9999). For example: (config)# sflow 1 destination 192.168.3.31 9999 |
| (config)# sflow 1 sampling ethernet <interface ID> <sample every n packets> | Sets the sFlow sample rate for each interface (1-24). One out of every 128 packets will be collected in this example. For example: (config)# sflow 1 sampling ethernet A1-A24 128 |
| (config)# sflow 1 polling ethernet <interface ID> <polling frequency in seconds> | Sets the sFlow polling interval. Polls every 30 seconds in this example. For example: config)# sflow 1 polling ethernet A1-A24 30 |

Configuring sFlow using SNMP

The following example uses SNMP commands to enable sFlow on an HP ProCurve 2610 series switch. We recommend configuring the sFlow device via the device OS commands from the command line interface (CLI); however, some sFlow devices do not include this capability. In this case, you can use SNMP commands to configure sFlow. This configuration example is for Flow Monitor running on a system with IP address 192.168.3.31 and receiving sFlow data on UDP port 9999.

To configure an sFlow device, using SNMP commands, to send sFlow data to Flow Monitor:





Important: This procedure is an example that applies to an HP ProCurve 2610 switch and should not be used for other devices. The process for configuring a device to export sFlow data varies widely from device to device and is dependent upon your network configuration. Refer to the documentation to determine the correct process for your device.



Important: An sFlow device configured with the SNMP commands typically do not save the configuration to memory. If the device is rebooted, or power is lost, all sFlow configuration is lost and must be manually reset using the SNMP commands. Make sure that you save the SNMP configuration commands for future device configuration.



| Command | Purpose |
|--|--|
| <pre>setmib sFlowRcvrAddress.1 -o <collector IP address in hexadecimal format></pre> | <p>Sets the sFlow receiving device address. In this example, the IP address (192.168.3.31) must be provided as a hexadecimal value (C0A8031F). For example:</p> <pre>setmib sFlowRcvrAddress.1 -o C0A8031F</pre> <div>  <p>Important: The example IP address must be entered as a hexadecimal value. Use an IP to hexadecimal calculator to determine the hexadecimal value for your sFlow collector's IP address. This example IP address breaks down into a hex value as follows:</p> <ul style="list-style-type: none"> 192 = C0 168 = A8 3 = 03 31 = 1F </div> |
| <pre>setmib sFlowRcvrPort.1 -i <port></pre> | <p>Sets the sFlow receiving device port address. The default Flow Monitor port is 9999. For example: <code>setmib sFlowRcvrPort.1 -i 9999</code></p> |
| <pre>setmib sFlowRcvrOwner.1 -D <Display String value> sFlowRcvrTimeout.1 -i <Timeout integer value></pre> | <p>Sets the sFlow receiver owner. The -D is a TYPE-STR identifier that specifies a Display String value. This value can be any string, for example NFmonitor (referring to Flow Monitor application which will receive the sFlow data).</p> <p>The -i is a TYPE-STR identifier that specifies an Integer value. The 100,000,000 value is a timeout value that defines the timeout countdown starting point value (in milliseconds).</p> <p>For example: <code>setmib sFlowRcvrOwner.1 -D NFmonitor sFlowRcvrTimeout.1 -i 100000000</code></p> |

| | |
|--|--|
|  Note: Repeat the following settings for each interface on the sFlow device you want to monitor. The last number in the MIB OID represents the interface number. | <pre>setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6. 1.2.1.2.2.1.1.1.<interface integer value> For example: setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6. 1.2.1.2.2.1.1.1.1</pre> |
| <pre>setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1. 3.6.1.2.1.2.2.1.1.1.1 -i <sample every n packets></pre> | <p>Sets the sFlow sample rate. One out of every 128 packets will be collected in this example. For example:</p> <pre>setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6. 1.2.1.2.2.1.1.1.1 -i 128</pre> |
| <pre>setmib 1.3.6.1.4.1.14706.1.1.5.1.3.11.1. 3.6.1.2.1.2.2.1.1.1.1 -i <Enable/Disable sFlow integer value></pre> | <p>Enables sFlow on the device. 1 enables / 0 disables sFlow. For example:</p> <pre>setmib 1.3.6.1.4.1.14706.1.1.5.1.3.11.1.3.6. 1.2.1.2.2.1.1.1.1 -i 1</pre> |
| <pre>setmib 1.3.6.1.4.1.14706.1.1.6.1.4.11.1. 3.6.1.2.1.2.2.1.1.53.1 -i <polling frequency in seconds></pre> | <p>Sets the sFlow polling interval. Polls every 30 seconds in this example. For example:</p> <pre>setmib 1.3.6.1.4.1.14706.1.1.6.1.4.11.1.3.6. 1.2.1.2.2.1.1.53.1 -i 30</pre> |
| <pre>setmib 1.3.6.1.4.1.14706.1.1.6.1.3.11.1. 3.6.1.2.1.2.2.1.1.53.1 -i <Enable/Disable sFlow polling integer value></pre> | <p>Enables sFlow polling. 1 enables / 0 disables sFlow polling. For example:</p> <pre>setmib 1.3.6.1.4.1.14706.1.1.6.1.3.11.1.3.6. 1.2.1.2.2.1.1.53.1 -i 1</pre> |

For more configuration options for sFlow, see the *NetFlow Settings help* <http://www.whatsupgold.com/NetFlowSettings>.

About Flexible NetFlow

Cisco IOS Flexible Netflow provides the next level of flexibility and scalability in monitoring network traffic, bringing a new understanding to who is using the network, what applications they are employing, when they are using the applications, and where the traffic originated.

Flexible NetFlow Components

Flexible NetFlow is implemented using flow monitors, the following is a definition of a flow monitor and its components.



Note: A NetFlow flow monitor is a component used to implement Flexible NetFlow and should not be confused with WhatsUp Flow Monitor, which is a NetFlow collector.

Flow monitors. Flow monitors are applied to interfaces to perform network traffic monitoring. These flow monitors consist of the following components:

- **Flow records.** A record is a combination of key fields, used to uniquely define a flow, and nonkey fields, which are used to provide additional information about a flow, but are not used to define the flow. In Flexible NetFlow, both key and nonkey fields can be defined in the record definition, which allows for customized data collection.
- **Flow cache.** Collects IP data flow records in a router or switch, analyzes this data and prepares the data for export. Flexible Netflow tracks and monitors multiple NetFlow caches, each configured to monitor specific information.
- **NetFlow exporter.** Exports the data in the flow monitor cache to a remote system, such as Flow Monitor, for analysis and storage. You can create more than one flow exporter, each assigned to one or more NetFlow collectors.
- **NetFlow collector.** An application that utilizes exported data from one or more NetFlow enabled routers or switches, aggregates and filters the data, then performs real-time visualization and analysis of the recorded and aggregated flow data. The WhatsUp Flow Monitor is an example of a NetFlow collector.

Flexible NetFlow records

Flexible NetFlow can track packet information from Layer 3, as well as some Layer 2 information. The Flexible NetFlow record can be customized to monitor data based on your specific monitoring needs. The information available includes:

- Source and Destination MAC addresses
- Source and Destination IP addresses
- Type of Service
- Differentiated Services Code Point (DSCP)
- Packet and byte counts
- Flow timestamps
- Input and output interface numbers

- TCP flags
- Routing information

Where traditional NetFlow provided a strict definition of which fields in a record are key field, used to define a flow, Flexible NetFlow allows you to define a flow based on the fields and data you want to monitor, which allows for the ability to export only the data needed by the collector to conduct its analysis and reporting. Additionally, there is more data available in Flexible NetFlow than in traditional NetFlow which allows for extensive customization and flexibility in defining flow records.

Flexible NetFlow and Network Based Application Recognition (NBAR)

Through this definition of flows, it is possible to gather information that can be used by Cisco Network Based Application Recognition (NBAR) to identify application data within a flow and provide flow statistics on the application traffic.

Configuring Flexible NetFlow on a Cisco device

Flexible NetFlow can be used to support the implementation of Cisco Network Based Application Recognition (NBAR) technology.

To configure a network device to utilize Flexible NetFlow, perform the following tasks:

- Create a flow monitor.
- Define the flow record.
- Create a flow exporter.

These tasks are described in the following sections, using an example configuration to illustrate how to complete the tasks from the Cisco IOS command line interface (CLI).



Important: The network device you want to configure must be running a Cisco IOS release that supports Cisco IOS Flexible NetFlow.

Creating a flow monitor

The following example illustrates how to configure a Flexible NetFlow enabled device to utilize Flexible NetFlow in support of NBAR and Flow Monitor application monitoring. For more information see the *Cisco IOS Flexible NetFlow configuration guide* (http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html#wp1056535).

To create a flow monitor:

- 1 Enter the privileged EXEC mode, and then enter the global configuration mode.

```
Router> enable
```

```
Router# configure terminal
```

- 2 Create a flow monitor, and enter the flow monitor configuration mode.

```
Router(config)# flow monitor application-mon
Router(config-flow-monitor)# description app traffic analysis
Router(config-flow-monitor)# cache timeout active 60
```

Defining a flow record

To define a flow record:

- 1 Enter the privileged EXEC mode, and then enter the global configuration mode.

```
Router > enable
Router# configure terminal
```

- 2 Enter the flow monitor configuration mode.

```
Router(config)# flow monitor application-mon
```

- 3 Name the record and enter a description.

```
Router(config-flow-monitor)# flow record nbar-appmon
Router(config-flow-record)# description NBAR Flow Monitor
```

- 4 Define key fields, using the `match` keyword.

```
Router(config-flow-record)# match ipv4 tos
Router(config-flow-record)# match ipv4 protocol
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match transport source-port
Router(config-flow-record)# match transport destination-port
Router(config-flow-record)# match interface input
Router(config-flow-record)# match application name
```



Note: By using the application name as a match parameter, you can utilize Network Based Application Recognition (NBAR) to collect statistics and report on network usage by individual applications.

- 5 Define nonkey fields, using the `collect` keyword.

```
Router(config-flow-record)# collect interface output
Router(config-flow-record)# collect counter bytes
Router(config-flow-record)# collect counter packets
Router(config-flow-record)# collect transport tcp flags
```

- 6 Enter the flow monitor configuration mode and configure the flow monitor to use the newly configured record.

```
Router(config)# flow monitor application-mon
```

```
Router(config-flow-monitor)# record nbar-appmon
```

Creating a flow exporter

When the record is complete, you can create the flow exporter. This component exports records from the flow monitor on the network device to the flow collector, in this case Flow Monitor.

To create a flow exporter:

- 1 Enter the privileged EXEC mode, then enter the global configuration mode.

```
Router > enable
```

```
Router# configure terminal
```

- 2 Create and describe the flow exporter.

```
Router(config)# flow exporter export-to-ipswitch-flow-monitor
```

```
Router(config-flow-exporter)# description Flexible NF v9
```

- 3 Set the destination flow collector IP address.

```
Router(config-flow-exporter)# destination 192.168.3.47
```

- 4 Define the source interface.

```
Router(config-flow-exporter)# source GigabitEthernet0/0
```

- 5 Define the PDU type and destination port.

```
Router(config-flow-exporter)# transport udp 9996
```

- 6 Set options for exporter operation.

```
Router(config-flow-exporter)# template data timeout 120
```

```
Router(config-flow-exporter)# option interface-table
```

```
Router(config-flow-exporter)# option exporter-stats timeout 120
```

```
Router(config-flow-exporter)# option application-table timeout 120
```

- 7 Enter the global configuration mode and configure the flow monitor to use the new flow exporter.

```
Router# configure terminal
```

```
Router(config)# exporter export-to-ipswitch_flow_monitor
```

About Network Based Application Recognition (NBAR)

Network Based Application Recognition (NBAR) is an application classification engine used to recognize a wide variety of applications. It can detect both Web-based and client-server applications.

NBAR identifies applications and protocols in Layer 4 to layer 7 using the following information:

- Static TCP and UDP port numbers
- Non UDP or TCP IP protocols
- Dynamically assigned TCP and UDP port numbers
- Sub-port classification
- Deep packet inspection

Protocol Discovery is a NBAR feature that collects application and protocol statistics for each interface based on the results of the application identification. Flow Monitor collects these statistics from the interface using Simple Network Management Protocol (SNMP) to poll the NBAR PD Management Information Base (MIB) where these statistics are stored.

The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

Configuring NBAR on a Cisco device

You must enable NBAR on each interface from which you want to collect application statistics. The following example describes how to enable NBAR on an interface.

To enable NBAR on an interface:

- 1** Enter the privileged EXEC mode, then the global configuration mode.

```
Router> enable  
Router# configure terminal
```
- 2** Enable Cisco Express Forwarding (cef).

```
Router(config)# ip cef
```
- 3** Enter the interface configuration mode for the interface on which you want to enable NBAR.

```
Router(config)# interface FastEthernet 0/1
```
- 4** Initiate NBAR protocol discovery on the interface.

```
Router(config-if)# ip nbar protocol-discovery
```
- 5** Exit the interface configuration mode.

```
Router(config-if)# exit
```

About CBQoS

Class-based quality of service (CBQoS) is the ability of a network to provide improved services to identified classes of network traffic. These services include supporting dedicated bandwidth, improving loss characteristics, managing network congestion, traffic shaping and setting traffic priorities. CBQoS involves two major components, traffic classes, and traffic policies.

Traffic classes

In the classification of network traffic, a traffic descriptor categorizes a packet as belonging to a group or class. By classifying network traffic, you can divide it into multiple priority levels or classes of service. Traffic classes are created using the `class-map` command which maps protocols and applications to a particular class.

Traffic policies

A traffic policy provides the mapping between the classes and the network controls used to provide the traffic priority, bandwidth guarantee, traffic shaping and other services available to traffic classes. Traffic policies are created using the `policy-map` command and are assigned to a particular interface using the `service-policy` command.

Configuring CBQoS on a Cisco device

To configure class-based QoS (CBQoS) on a Cisco device, perform the following tasks:

- Create the traffic classes using the `class-map` command
- Create the traffic policy using the `policy-map` command
- Attach the traffic policy to an interface using the `service-policy` command.



Note: The following procedures illustrate how to create a traffic class, how to create a traffic policy and how to attach the policy to an interface. The specific commands used to illustrate how these steps may be accomplished on a Cisco router are only for the purposes of this example. For more detailed information on how to implement QoS for your network, see Creating a Traffic Policy in the *Cisco IOS Quality of Service Solutions Configuration Guide* (http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html).

To create a traffic class:

- 1 Enable the privileged EXEC mode and enter the global configuration mode.

```
Router> enable
```

```
Router# configure terminal
```

- 2 Create the class name and enter the configure class map mode.

```
Router(config)# class-map match-any NMclass
```



Note: The `match-any` keyword is used when all of the match criteria in the traffic class must be met in order for a packet to be placed in the specified traffic class.

- 3 Use one or more match commands to specify the match criteria. Packets that match the specified match criteria will be placed in the traffic class.

```
Router(config-cmap)# match protocol snmp
```

```
Router(config-cmap)# match protocol icmp
```



Note: You can repeat the steps that create a class name and specify the match criteria to create as many classes as are needed to define the policy you want to apply to the interface.

- 4 Exit the class map configuration mode.

```
Router(config-cmap)# exit
```

Example: Class Map configuration

The following is an example of a class map configuration.

```
class-map match-any nm
    match protocol snmp
    match protocol icmp
class-map match-any p2p
    match protocol kazaa2
    match protocol gnutella
    match protocol edonkey
    match protocol bittorrent
    match protocol fasttrack
    match protocol directconnect
    match protocol winmx
class-map match-all FTP
    match protocol ftp
class-map match-any web
    match protocol http
class-map match-any utube
    match protocol http s-header-field "*http://www.youtube.com/*"
```

To create a traffic policy:

- 1 Enable the privileged EXEC mode and enter the global configuration mode (`config`).

```
Router> enable
```

```
Router# configure terminal
```
- 2 Create the traffic policy and enter the policy-map configuration mode (`config-pmap`).

```
Router(config)# policy-map newPolicy
```
- 3 Specify the name of the class to associate with the policy and enter the policy-map class configuration mode (`config-pmap-c`).



Note: In the policy-map class configuration mode you can define one or more QoS features which supply services supporting dedicated bandwidth, improving loss characteristics, managing network congestion, traffic shaping and setting traffic priorities. For more information see *Creating a Traffic Policy in the Cisco IOS Quality of Service Solutions Configuration Guide* (http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html).

```
Router(config-pmap)# class NMclass
```

- 4 In the policy-map class configuration mode define the QoS features you want to apply to the class.

```
Router(config-pmap-c)# drop
```



Note: You can repeat the steps associating a class with the policy and defining the QoS features to apply to the class as many times as is necessary to create a policy that establishes services for all of the defined classes.

- 5 Exit the policy-map class configuration mode.

```
Router(config-pmap-c)# exit
```

Example: Traffic policy

The following is an example of a traffic policy:

```
policy-map crTest2
  class p2p
  drop
  class FTP
  drop
  class nm
    set dscp af43
  class web
    set dscp af12
  class utube
    set dscp af43
```

To associate a policy with an interface:

- 1 Enable the privileged EXEC mode and enter the global configuration mode (`config`).

```
Router> enable
```

```
Router# configure terminal
```

- 2 Select the interface to configure and enter the interface configuration mode.

```
Router(config)# interface GigabitEthernet0/0
```

- 3 Attach the policy map to the interface.

```
Router(config-if)# service-policy output input newPolicy
```

- 4 Exit the interface configuration mode.

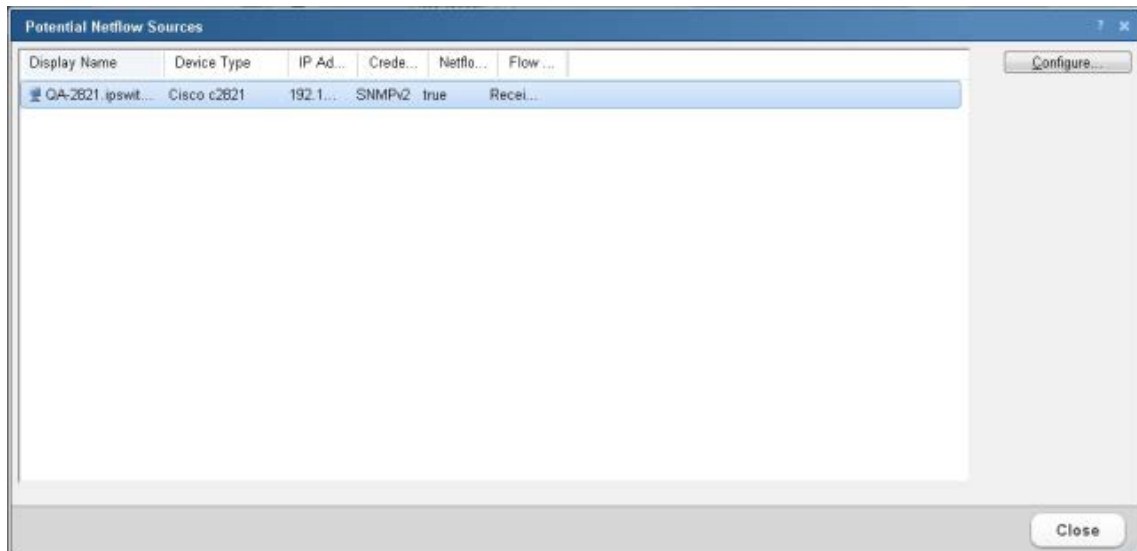
```
Router(config-if)# exit
```



Note: For more information on associating a policy with an interface, see Attaching a Traffic policy to an Interface in the *Cisco IOS Quality of Service Solutions Configuration Guide* (http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html).

Viewing potential Flow Monitor sources

The Potential Flow Monitor sources dialog is a list of the devices discovered by WhatsUp Gold that have the potential of being a NetFlow source. When a network device such as a router is discovered and WhatsUp Gold has the necessary credentials to access the device using SNMP, the discovery process determines if the device is NetFlow enabled, and if the NetFlow MIB used to perform remote configuration of the device is available on the device.

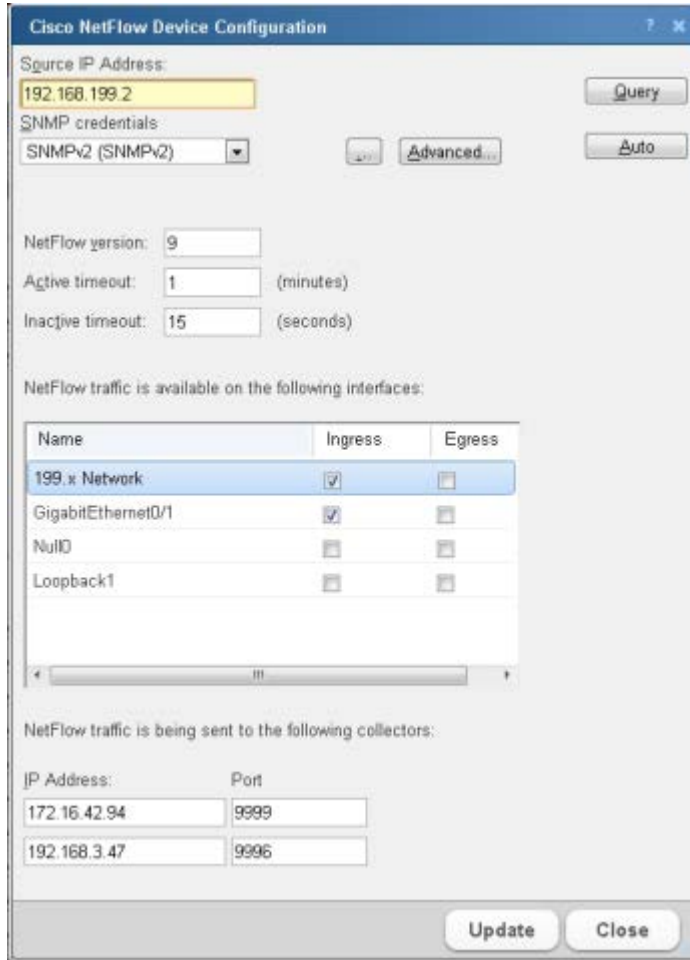


Information about devices that are potential Flow Monitor sources are displayed on this dialog along with the options for selecting a device for configuration using the Cisco NetFlow Device Configuration dialog.

- **Display Name.** The name of the device as provided by the WhatsUp Gold discovery engine.
- **Device Type.** The type of the device. Only Cisco devices can be remotely configured using the Cisco NetFlow Device Configuration dialog.
- **IP Address.** The IP address of the device.
- **Credentials.** The name of the credential that will be used when authenticating with the device.
- **Netflow MIB.** Displays a true if the device has the MIB object with the OID matching the NetFlow MIB.
- **Flow Monitor Status.** Displays the status of the device with respect to Flow Monitor (Receiving, Never Received, or Disabled).

Using Flow Monitor to Configure Cisco NetFlow Devices

The Cisco NetFlow Device Configuration dialog provides Flow Monitor with the ability to configure a Cisco device to send flow records to Flow Monitor.



The dialog box is titled "Cisco NetFlow Device Configuration". It contains the following fields and controls:

- Source IP Address:** A text field containing "192.168.199.2" and a "Query" button.
- SNMP credentials:** A dropdown menu showing "SNMPv2 (SNMPv2)" and "Advanced..." and "Auto" buttons.
- NetFlow version:** A text field containing "9".
- Active timeout:** A text field containing "1" with "(minutes)" next to it.
- Inactive timeout:** A text field containing "15" with "(seconds)" next to it.
- NetFlow traffic is available on the following interfaces:** A table with columns "Name", "Ingress", and "Egress".

| Name | Ingress | Egress |
|--------------------|-------------------------------------|--------------------------|
| 199.x Network | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| GigabitEthernet0/1 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Null0 | <input type="checkbox"/> | <input type="checkbox"/> |
| Loopback1 | <input type="checkbox"/> | <input type="checkbox"/> |
- NetFlow traffic is being sent to the following collectors:** A table with columns "IP Address" and "Port".

| IP Address | Port |
|--------------|------|
| 172.16.42.94 | 9999 |
| 192.168.3.47 | 9996 |
- Buttons:** "Update" and "Close" at the bottom right.

Use this dialog to:

- Enter connection information and credentials used to connect to the Cisco device.
- Set the NetFlow version to be used by the flow exporter.
- Set the active and inactive timeouts used for cache management.
- Select the interfaces from which you want the device to collect and send flow data.
- Configure the NetFlow collectors, which in most cases includes Flow Monitor.

Enter the connection information and credentials to connect and authenticate with the Cisco network device.

- **Source IP address.** Enter the IP address of the Cisco NetFlow enabled device from which you want to collect NetFlow statistics.
- **SNMP credentials.** Select or create the SNMP credentials to use to connect to the Cisco NetFlow enabled device. Click the browse (...) button to add, edit or delete SNMP credentials. Click the **Advanced** button to set SNMP timeout and retry parameters.



Tip: When you have selected valid SNMP credentials, the dialog queries the device and populates the NetFlow configuration parameters as well as the interface list. Use the **Query** button to update this information from the Cisco device. A message will appear if you do not have a valid credential.

- Click **Auto** to automatically configure the device to collect and send flow data to Flow Monitor. When automatically configured, the device will enable collection of flow data on the device and will add itself as a netflow collector.

Enter the NetFlow configuration parameters to set the NetFlow version and configure the NetFlow cache on the Cisco device.

- **NetFlow version.** Enter the NetFlow version you want the exporter to deliver the flow records.
- **Active timeout.** Enter the Active timeout for flow records in the NetFlow cache. This value determines how long active, long-lived flows are kept in the NetFlow cache before sending to the collector. (Range: 1-60 minutes) (Default: 2 minutes)
- **Inactive timeout.** Enter the Inactive timeout value for flow records in the NetFlow cache. This value is used to ensure that completed or inactive flows are not kept in the NetFlow cache indefinitely. (Range 10 - 600 seconds) (Default: 30 seconds)

The Interface list displays the interfaces that can provide NetFlow data.

- **Name.** Displays the interface name as configured on the Cisco network device.
- **Ingress.** Select this option if you want to collect flow statistics on incoming traffic on this interface.
- **Egress.** Select this option if you want to collect flow statistics on outgoing traffic on this interface.



Note: If you have selected to collect flow statistics from both Ingress and Egress traffic on a single interface, we recommend that you do not select to collect flow statistics from any other interface, otherwise traffic may be duplicated as traffic that is internally routed will appear on two interfaces within the device.

Enter the IP address and port number for the devices collecting Flow Monitor traffic.

- **IP address.** Enter the IP address of the collector.

- **Port.** Enter the Port number on which the collector is listening for flow data. (Default port for Flow Monitor: 9999)

Click **Update** to save the settings.

Managing Flow Sources

In This Chapter

| | |
|---|------|
| About Flow Sources..... | 992 |
| Configuring Flow Monitor to listen for NetFlow data | 993 |
| Viewing Flow Sources..... | 994 |
| Configuring a Flow Source..... | 996 |
| Creating flow sources | 1004 |

About Flow Sources

Flow *sources* are network devices that use one of the following supported network monitoring protocols to send flow data to Flow Monitor.

- **NetFlow.** A network protocol developed by Cisco Systems and later adopted as an IETF informational standard for collecting IP traffic information. Flow Monitor supports NetFlow versions 1, 5, 7, and 9 as well as Flexible NetFlow, which is based on NetFlow v9. Flexible NetFlow is often used to support Cisco's Network Based Application Recognition (NBAR) technology.
- **sFlow.** A network monitoring technology that provides IP traffic information using packet sampling. Flow Monitor supports sFlow versions 2 and 5.
- **JFlow.** A network protocol developed by Juniper to run on the JUNOS for collecting IP traffic flow statistics.
- **IPFIX.** An IETF informational standard developed to create a non-proprietary network protocol that is compatible with NetFlow.

Flow sources that utilize these network protocols provide detailed data about individual flows to Flow Monitor gathered from flow records. An example of the types of information that can be contained in a flow record are:

- Version numbers
- Sequence numbers
- Input and output interface indices
- Timestamps for the flow start and finish time, in milliseconds since the last boot.
- Number of bytes and packets observed in the flow
- Layer 3 headers including:
 - Source & destination IP addresses
 - Source and destination port numbers
 - IP protocol

- Type of Service (ToS) value
- The union of all TCP flags observed over the life of the flow (TCP flows).
- Layer 3 Routing information, including:
- IP address of the immediate next-hop along the route to the destination
- Source and destination IP masks (prefix lengths in CIDR notation)

Configuring Flow sources is a three-part process:

- 1 Configuring Flow devices to send Flow data to Flow Monitor. For more information, see *Manually configuring devices to export flow data to Flow Monitor* (on page 973).
- 2 Configure Flow Monitor to listen for flow data on the appropriate port. For more information, see *Configuring Flow Monitor to listen for NetFlow data* (on page 993).
- 3 Setting options for the Flow source in Flow Monitor.

SNMP Polling

While Flow Monitor normally receives flow data from a flow source, it can also poll a source using SNMP to gather data from a network device. Flow Monitor can actively poll a source for the following data:

- **Total interface traffic.** Provides summary data for incoming and outgoing interface traffic.
- **NBAR information.** Provides summary data for each application identified using Cisco Systems Network Based Application Recognition (NBAR) technology.
- **CBQoS information.** Provides summary data for each class in the Quality of Service class map for the interface. Before you can view meaningful reports, you must configure Flow Monitor and Flow-enabled devices, such as routers or switches, to communicate network activity back to the Flow Monitor listener application.

Configuring Flow Monitor to listen for NetFlow data

Use the Listener port settings on the Flow Settings to configure Flow Monitor to listen for NetFlow data. You can enter the TCP/IP port numbers which the Flow Monitor collector service should use to listen for flow information in the **Listener port** box. Flow Monitor can listen on one or more ports, with port 9999 being the default. The sources sending flow information to Flow Monitor must send data using one of these ports.



Note: If you configure Flow Monitor to listen on more than one port or on a port other than the default port, you should verify that the port is not being used by another service and ensure that an exception is added to the firewall if you are using Windows Firewall.

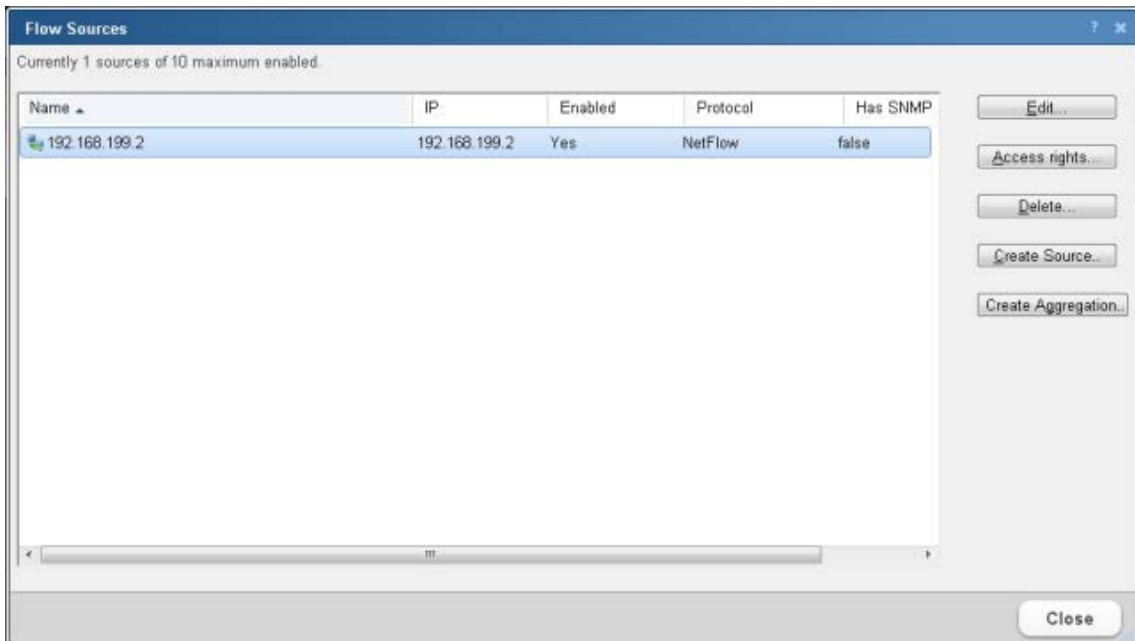
To configure Flow Monitor to listen for NetFlow data:

Note: By default, Flow Monitor listens for Flow data on port 9999. If you want to use that port, you do not need to perform this procedure.

- 1 Navigate to the Flow Settings dialog (**Flow Monitor > Settings**). The Flow Settings dialog appears.
- 2 In **Listener port**, enter the port numbers, separated by commas, over which Flow Monitor should listen for Flow data.
- 3 Click **OK** to save the changes.

Viewing Flow Sources

Use the Flow Sources dialog to view the list of all of the flow sources that are available in Flow Monitor. This list of flow sources is automatically updated when the system receives data from sources that have been configured to send flow data to Flow Monitor.



Use the Flow Sources dialog to:

- Access the Flow Source dialog for each change a source's configuration.
- Stop and start data collection from a source.
- Set access rights to the flow data generated by a source.
- Create an SNMP source.
- Create an Aggregate source.

To change a source's configuration, or to stop and start data collection from a source, select a source, then click **Edit**.

To set access rights to flow data from a source, select a source, then click **Access rights**.



Note: If you do not have permissions to manage users, the **Access rights** button is not be visible.

For more information, see Configuring Flow sources.

To Delete a Flow Source, see Deleting Flow Sources below.

Click **Create Source** to create an SNMP Source to poll for NBAR or CBQoS data.

Click **Create Aggregation** to create an Aggregate source.

Deleting Flow Sources

When you no longer want to gather flow data from a source, it can be deleted. When you delete a flow source, both the configuration information and all flow data associated with the source is deleted.

To delete a flow source:

- 1 Navigate to the Flow Sources dialog (**Flow Monitor > Flow Sources**).
- 2 Disable the source.
 - a) On the Flow Sources list, select the source you want to delete.
 - b) Click **Edit**. The Flow Source edit dialog appears.
 - c) Clear the **Enable flow data collection from this source** option.
 - d) Click **OK**. The Flow Sources list appears with the source listed as disabled.
- 3 Delete the source.
 - a) Verify that the source you wish to delete is not enabled. The word *No* appears in the Enabled column when the source is not enabled.
 - b) Click **Delete**. A delete verification dialog appears.
 - c) Click **Yes** to verify that you want to delete the source. The Flow Sources list dialog appears with the source deleted.

Configuring a Flow Source

Use the Flow Source dialog to configure the selected source and the interfaces associated with the source.

The Flow Source dialog box is titled "Flow Source" and contains the following configuration options:

- Source:** 192.168.199.2
- Flow Protocol:** NetFlow v9
- Display Name:** 192.168.199.2
- ☒ **Enable data collection from this source**
- SNMP Polling:**
 - Credentials:** (No Credentials) [Advanced...] [Query]
 - ☐ Poll source for total interface traffic. *Needed only for sampled flow protocol where total interface traffic is not available
 - ☐ Poll source for NBAR information
 - ☐ Poll source for CBQoS information
- Access rights...**
- Interfaces:**

| Name | Type | Speed | Status | Hidden |
|-------------|---------|-----------|---------|--------|
| Unnamed (1) | Unknown | Undefined | Unknown | No |
| Unnamed (5) | Unknown | Undefined | Unknown | No |
| Null() | Unknown | Undefined | Unknown | Yes |

Buttons at the bottom: OK, Cancel. An Edit... button is next to the interfaces table.

The Flow Source dialog provides the options to:

- Enable and disable data collection.
- Configure Flow Monitor to use SNMP to poll the source for total interface traffic, NBAR and CBQoS statistics. You can then select the types of statistics you would like to collect.
- Set access rights to data generated by the source.
- Configure interface properties for interfaces attached to the source.

To navigate to the Flow Source dialog:

- 1 Navigate to the Flow Sources dialog (**Flow Monitor > Sources**).
- 2 Select the source you want to configure, then click **Edit**. The Flow Source dialog opens.

The source identifying information is displayed and in some cases can be edited:

- **Source.** The device (source) IP address.
- **Flow Protocol.** Indicates the flow protocol used by the source device.
- **Display Name.** The device (source) display name.

To enable or disable data collection from a source:

- 1 Select **Enable data collection from this source** to start receiving data from a newly configured, or previously disabled source. (Default).
- 2 Deselect **Enable data collection from this source**, to stop receiving data from this source.



Note: You must deselect Enable data collection from this source to delete a source. When you delete a source, you will no longer receive data from the source. All data you have collected prior to deleting the source will be maintained in the Flow Monitor database until it is aged out.

To use SNMP polling to collect data from the source:

- 1 In the SNMP Polling group, select the credential that is valid for the interface from the list, or click the browse (...) button to go to the Credentials Library to configure a new set of credentials.



Note: If you select a different set of credentials, the dialog automatically uses the new credentials to update information about the source interfaces. If you receive an error, click **Advanced** to update timeout and retry values, then click **Query** to try the credentials again.

- **Advanced.** Click to configure the device (source) SNMP timeout and retry settings.
 - **Query.** Click to use the updated retry and timeout values for the selected SNMP credential.
- 2 If you want to poll the source for total interface traffic, select **Poll source for total interface traffic**.



Important: When you poll a source for interface traffic, the aggregate of the individual flows is not used to represent total interface traffic. Instead the polled value is used to represent total interface value.



Important: When a sampled flow protocol is being used that does not supply total interface traffic statistics, you can select **Poll source for total interface traffic** to provide these statistics.



Note: When a source uses packet sampling to collect flow data and the protocol does not provide total interface traffic statistics, the aggregate of individual flow data used to calculate total interface traffic will be inaccurate because the data used in the calculation is sampled, this commonly results in errors in total interface traffic statistics.



Note: To poll a source for interface traffic, the proper SNMP credentials for the interface must be selected, and the NetFlow collector must be configured to collect data from this source.

- 3 If you want to poll the source for Network-Based Application Recognition (NBAR) statistics, select **Poll Source for NBAR Information**.



Note: The source device from which you want to gather NBAR statistics must be configured to generate NBAR statistics using the `<ip> nbar protocol-discovery` command. For more information, see *Configuring NBAR on a Cisco device* (on page 983).

- 4 If you want to poll the source for class-based Quality of Service (CBQoS) information, select **Poll Source for CBQoS information**.



Note: The source device from which you want to gather CBQoS statistics must be configured to generate these statistics. For more information, see *Configuring CBQoS on a Cisco device* (on page 984).

To set access rights for the source:

Click **Access Rights** to configure user access to the source and its associated data. The **Flow Source Access Rights** dialog appears. For more information, see *Configuring Flow Source Access Rights* (on page 1000).



Note: If you do not have permissions to manage users, the **Access rights** button will not be visible.

Interfaces

Each of the Flow Monitor source's interfaces are listed in the Interfaces list. The following columns provide information about the source interface:

- **Name.** List the unique device interface name.



Note: In the case where the interface name is listed as *Null(0)*, this indicates one of two possibilities:
1) A router has dropped traffic, so traffic does not exit the router and the output interface is named Null(0). **OR** 2) When a router generated (originated) traffic, so traffic has not entered the router and the input interface is named Null(0). In both cases the `ifIndex = 0` and as a default convention we name an interface = Null because the interface is none existent.

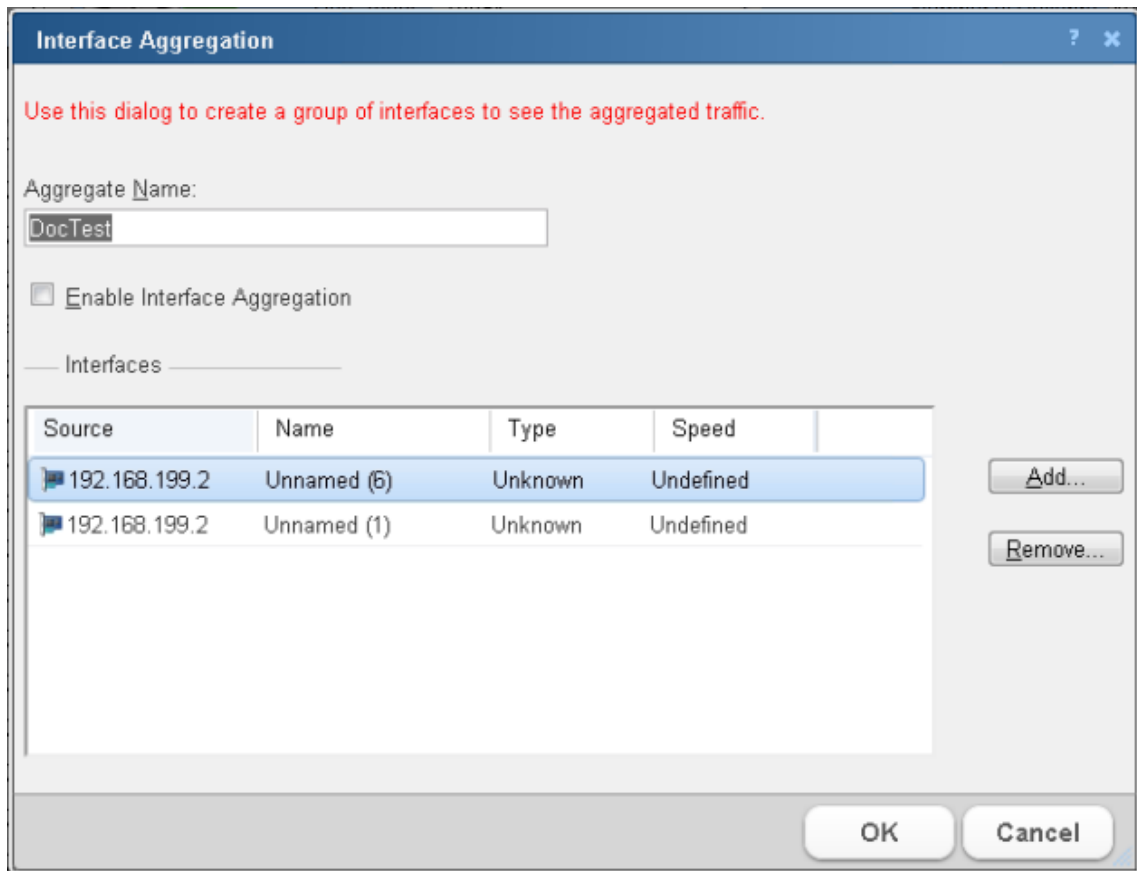
- **Type.** List the interface type. For example, Ethernet.
- **Speed.** List the interface speed in bits per second (bps).
- **Status.** List the current interface status (Up or Down).
- **Hidden.** List whether the interface is hidden from view on the Flow Monitor Home page (Yes or No) and Interface Details combo-box.

To configure flow interface properties:

Select an interface from the Interfaces list, then click **Edit**. The Flow Interface dialog appears. For more information, see *Configuring Flow Interface Properties* (on page 1002).

Creating an Aggregate source

Use the Create Aggregation dialog to add one or more interfaces from any of the licensed Flow Monitor sources to an aggregate source. An aggregate source combines the data from all of the assigned interfaces, and reports on that data as if it originated from a single Flow Monitor source. This aggregation allows for reporting on data from many, or all, of the interfaces on your licensed Flow Monitor sources without having to manually add the data between reports from individual interfaces.



The dialog box is titled "Interface Aggregation" and contains the following elements:

- A red instruction: "Use this dialog to create a group of interfaces to see the aggregated traffic."
- An "Aggregate Name:" label followed by a text box containing "DocTest".
- An unchecked checkbox labeled "Enable Interface Aggregation".
- A label "Interfaces" above a table.
- A table with the following data:

| Source | Name | Type | Speed |
|---------------|-------------|---------|-----------|
| 192.168.199.2 | Unnamed (6) | Unknown | Undefined |
| 192.168.199.2 | Unnamed (1) | Unknown | Undefined |
- Buttons "Add..." and "Remove..." to the right of the table.
- "OK" and "Cancel" buttons at the bottom right.

To create an aggregate source:

- 1 Navigate to the Flow Sources dialog (**Flow Monitor > Sources**).
- 2 Click **Create Aggregation**. The Interface Aggregation dialog appears.



Tip: If you want to edit an existing aggregate source, select the aggregate source from the source list and click **Edit**. The Interface Aggregation dialog appears.

- 3 In the Aggregate Name box, type a name for the aggregate source. This name will appear as the name of the source in the Flow Sources dialog.

4 Select **Enable Interface Aggregation**.



Note: When you enable an interface aggregation, it will use a Flow Monitor source license.

5 Click **Access rights** to set access rights to flow data from the Aggregate source.



Note: If you do not have permissions to manage users, the **Access rights** button is not visible.

6 Click **Add** to add an interface to the aggregate source. The Add Interface dialog appears.

7 Select an interface to add, then click **OK**. The interface will be added to the Interfaces list on the Interface Aggregation dialog.

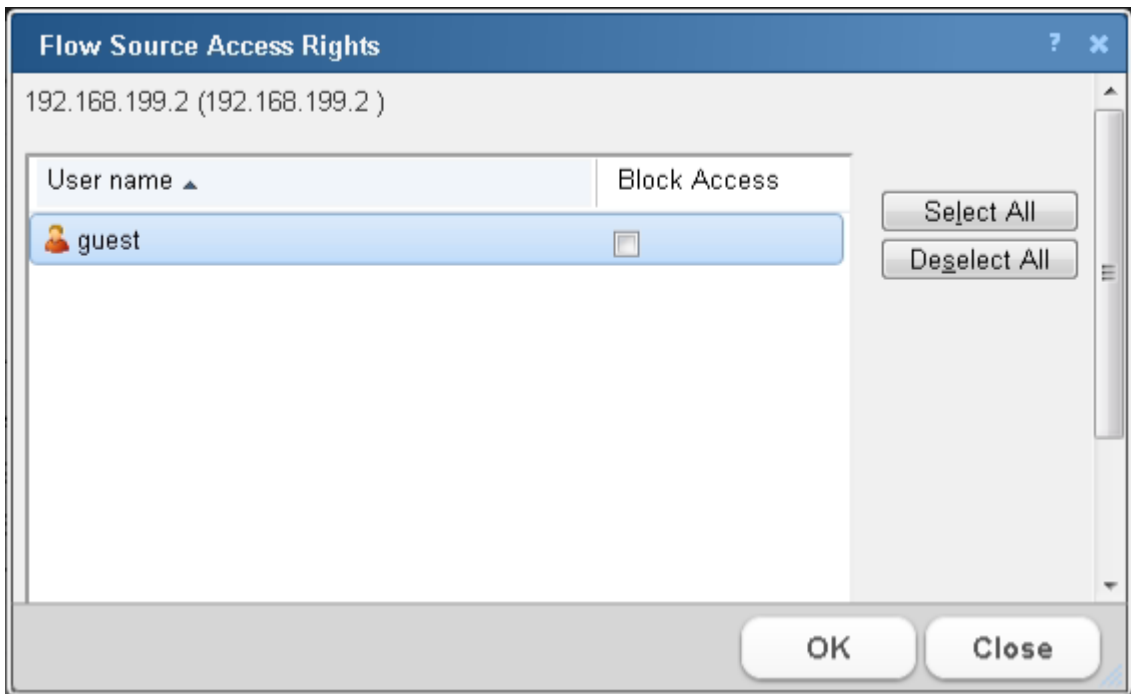


Tip: If you want to remove an interface from an aggregation, select the interface from the Interfaces list, then click **Remove**.

8 When you have added all of the interfaces you wish to combine using the aggregate source, click **OK**. The aggregate source appears on the Flow Sources list.

Configuring Flow Source Access Rights

Use the Flow Source Access Rights dialog to block access by one or more users to the flow data generated by a particular Flow Monitor source.





Note: In order for a user to be able to block access for other WhatsUp Gold users, the user must have the Manage Users access right (**Admin > Manage Users**). Additionally, the user for which you are trying to block access should not have this right, as this will allow them to block access for other users.

To configure Flow Source access rights:

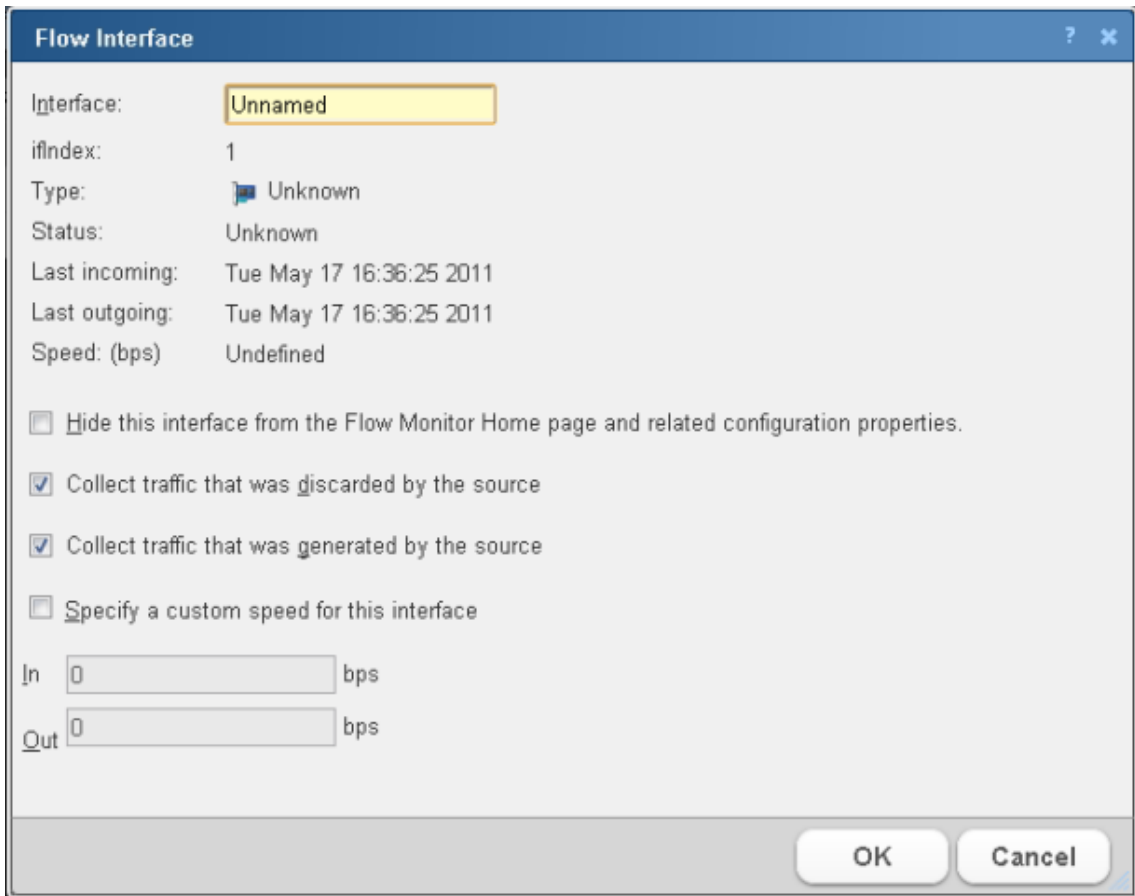
- 1 Navigate to the Flow Sources dialog (**Flow Monitor > Sources**).
- 2 Select the flow source for which you want to configure access rights, then click **Edit**. The Flow Source dialog for that source appears.
- 3 Click **Access rights**. The Flow Source Access Rights dialog appears.
- 4 Select a user or multiple users from the list of usernames by clicking the Block Access box for that user or user(s).
- 5 Click **OK** to save changes.



Tip: You can also **Select All** users, or **Deselect All** users.

Configuring Flow Interface Properties

Use the Flow Interface dialog to view and configure the Flow Monitor properties attributed to the selected interface.



The Flow Interface dialog box is shown with the following fields and options:

- Interface: Unnamed
- ifindex: 1
- Type: Unknown
- Status: Unknown
- Last incoming: Tue May 17 16:36:25 2011
- Last outgoing: Tue May 17 16:36:25 2011
- Speed: (bps) Undefined
- ☐ Hide this interface from the Flow Monitor Home page and related configuration properties.
- ☒ Collect traffic that was discarded by the source
- ☒ Collect traffic that was generated by the source
- ☐ Specify a custom speed for this interface
- In: 0 bps
- Out: 0 bps
- OK button
- Cancel button

The Flow Interface dialog provides the options to:

- Hide the interface from Flow Monitor Home.
- Configure traffic collection options.
- Allow interface speed specification.
- Configure options for collecting translated addresses on Cisco Adaptive Security Appliance (ASA) devices.

To navigate to the Flow Interface Properties dialog:

- 1 Navigate to the Flow Sources dialog (**Flow Monitor > Flow Sources**).
- 2 In the Interfaces group, select the source to which the interface is connected, then click **Edit**. The Flow Source dialog appears.
- 3 Select the interface you want to edit, then click **Edit**. The Flow Interface dialog appears.

To hide this interface from the Flow Sources dialog:

- 1 Select **Hide this interface from the Flow Home page and related configuration properties** to hide the selected interface from the Flow Monitor Home page and other menu options in Flow Monitor. This lets you display only those interfaces that are relevant to your bandwidth monitoring requirements.



Note: Although, after selecting this option the interface is not listed on the source list, Flow Monitor still collects data from the interface.

- 2 Click **OK** to save changes.

To configure traffic retention properties for the interface:

- 1 Select **Collect traffic that was discarded by the source** to collect data about the traffic that came to the device but was not forwarded by the device. Examples of this type of traffic are ping traffic, telnet connections, routing table updates, and other network management traffic.
- 2 Select **Collect traffic that was generated by the source** to collect data about the network traffic that is generated by the device. Examples of this type of traffic are any traffic generated by routing protocols.
- 3 Click **OK** to save changes.

To configure the speed of an interface:

- 1 Select **Specify a custom speed for this interface**. The In and Out fields are enabled.
In In and Out, enter the upper limit of the interface in bps (bits per second). Common interface speeds expressed in bps are:
 - 1 Gbps = 1,000,000,000 bps
 - 100 Mbps = 100,000,000 bps
 - 10 Mbps = 10,000,000 bps
- 2 Click **OK** to save changes.

Creating flow sources

Use the Flow Source dialog to manually create SNMP sources when detailed flow data is not needed or is unavailable for a particular source.

The Flow Source dialog box contains the following fields and sections:

- Source IP Address:** 192.168.199.2
- Display Name:** DocTest
- ☐ Enable data collection from this source
- SNMP credentials:**
 - SNMPv2 (SNMPv2) [Advanced...] [Query]
 - ☒ Poll source for total interface traffic. *Needed only for sampled flow protocol where total interface traffic is not available
 - ☒ Poll source for NBAR information
 - ☒ Poll source for CBQoS information
- Interfaces:**

| Name | Type | Speed | Status | Hidden |
|--------------------|------------------|------------|--------|--------|
| 199.x Network | Ethernet CSM... | 1000000000 | Up | No |
| GigabitEthernet0/1 | Ethernet CSM... | 1000000000 | Up | No |
| Null0 | Other | 1000000000 | Up | No |
| Loopback1 | Software Loop... | 8000000000 | Down | No |
| 58.x Network | L2 VLAN | 1000000000 | Up | No |
| 10.0.2.x Network | L2 VLAN | 1000000000 | Up | No |

Buttons: OK, Cancel, Edit...

You can manually create a flow source and configure it to use SNMP to collect the following types of data:

- Total counts for incoming and outgoing interface data.
- CBQoS information.
- Total counts for NBAR data.

To create an SNMP source:

- 1 Navigate to the Flow Source creation dialog (**Flow Monitor > Sources**).
- 2 Click **Create Source**. The Flow Source dialog appears.
- 3 Identify and enable the flow source.
 - a) In the **Source IP Address** box, type the IP address of the device you want to make a Flow Monitor source.
 - b) In the **Display Name** box, type the name you want to use to identify the flow source.

- c) Select **Enable data collection from this source**.

4 Set SNMP options.



Note: Flow Monitor uses SNMP to query information about the interfaces on the source.

- a) Select the appropriate **SNMP credentials**. If the credentials you want to use are not included in the list, click the browse button (...) to open the Credentials Library. For more information on configuring credentials, see *Using Credentials*.
 - b) To set advanced options, such as timeout and number of retries, click **Advanced**. The Advanced dialog appears. Set the appropriate values, then click **OK** to return to the Flow Sources dialog.
 - c) Select **Query** to query the router using SNMP to get updated names and speeds for available interfaces.
- 5 Select the data you want to gather using SNMP polling.
- To collect total interface data, select **Poll source for total interface traffic**.
 - To collect NBAR information, select **Poll source for NBAR information**.
 - To collect CBQoS information, select **Poll source for CBQoS information**.
- 6 Configure the speed of each interface, which is used to calculate capacity as a percentage of the total interface speed.
- a) Select an interface, then click **Edit**. The Flow Interface dialog appears.
 - b) Select **Hide this interface from the Flow Monitor Home page and related configuration properties** to hide the selected interface from the Flow Monitor Home page and other menu options in Flow Monitor. This lets you display only the interfaces that are relevant to your bandwidth monitoring requirements.



Note: Null(0) interface names are hidden by default because they are not a true source interface. Null(0) interfaces show traffic that a router has dropped or traffic that a router has generated. In both cases the ifIndex = 0 and as a default convention we name an interface = Null because the interface is none existent. If you want Null(0) interface information to display as a source interface, make sure that you uncheck the **Hide this interface from the Flow Monitor Home page and related configuration properties** option.

- c) Select **Specify a custom speed for this interface**. The **In** and **Out** fields are enabled.
 - d) In **In** and **Out**, enter the upper limit of the interface in bps (bits per second). Common interface speeds expressed in bps are:
 - 1 Gbps = 1,000,000,000 bps
 - 100 Mbps = 100,000,000 bps
 - 10 Mbps = 10,000,000 bps
- 7 Click **OK** when you have completed configuring the SNMP flow source. The Flow Source dialog closes and the source is added to the Flow Sources list.

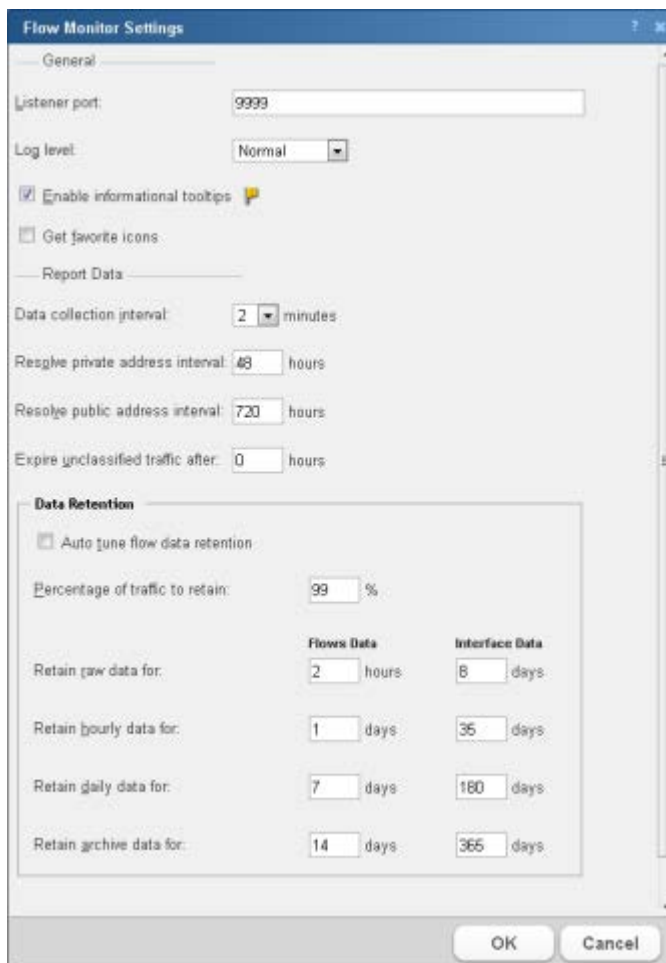
Managing Flow Monitor Settings

In This Chapter

| | |
|---|------|
| Flow Monitor Settings | 1006 |
| Configure Flow Monitor to listen for NetFlow data | 1010 |
| Setting the logging level | 1011 |
| Data retention strategy and tuning..... | 1012 |
| Configuring data retention settings..... | 1014 |

Flow Monitor Settings

The Flow Monitor Settings dialog provides general settings, data retention, and data management settings used to configure and manage Flow Monitor.



The image shows the 'Flow Monitor Settings' dialog box. It has a title bar with a question mark and a close button. The dialog is divided into two main sections: 'General' and 'Data Retention'. The 'General' section includes fields for 'Listener port' (9999), 'Log level' (Normal), and checkboxes for 'Enable informational tooltips' (checked) and 'Get favorite icons' (unchecked). The 'Report Data' section includes fields for 'Data collection interval' (2 minutes), 'Resolve private address interval' (48 hours), 'Resolve public address interval' (720 hours), and 'Expire unclassified traffic after' (0 hours). The 'Data Retention' section includes a checkbox for 'Auto tune flow data retention' (unchecked), a field for 'Percentage of traffic to retain' (99 %), and a table for retention periods.

| | Flows Data | Interface Data |
|--------------------------|------------|----------------|
| Retain raw data for: | 2 hours | 8 days |
| Retain hourly data for: | 1 days | 35 days |
| Retain daily data for: | 7 days | 180 days |
| Retain archive data for: | 14 days | 365 days |

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

General

- **Listener port.** Enter the TCP/IP port numbers which the Flow Monitor collector service should use to listen for flow information. Flow Monitor can listen on one or more ports, with port 9999 being the default. The sources sending flow information to Flow Monitor must send data using one of these port numbers.



Note: If you configure Flow Monitor to listen on more than one port or on a port other than the default port, you should verify that the port is not being used by another service and ensure that an exception is added to the firewall if you are using Windows Firewall.

- **Log level.** Select the level of details you want to write to the log.
 - **Normal.** Select this option to record errors and some general event information.
 - **Verbose Logging.** Select this option to record more detailed information than normal logging. This option can create a very large file and may be resource intensive, however, it is especially helpful for troubleshooting issues.
 - **Errors Only.** Select this option to record only errors.
- **Enable informational tooltips.** Select this option to enable Flow Monitor to display tooltips with information about possible problems and other information about report details.
- **Get favorite icons.** Select this option to allow Flow Monitor to retrieve and display favicons (favorite icons) from hosts and domains when they are provided.



Note: If you select the **Get favorite icons** option, Flow Monitor will make connections to a host in the domain to retrieve the favicon. This will impact the connections statistics for both the host and the domain.

Report Data

- **Data collection interval.** Select how often Flow Monitor writes raw data from its sources to the database. You may select 1, 2, 3, 4, 5, or 10 minutes. By default, raw data is written to the database every 2 minutes.



Note: Modifying collection interval settings affects the granularity you see in Flow Monitor reports. If the interval is set to 5 minutes, you cannot distinguish traffic collected during the first minute from traffic collected during the fourth minute.

- **Resolve private address interval.** When the Flow Monitor collector service encounters an IP address, it tries to determine information about the host attached to the IP address. After this information is resolved, it is stored in the Flow Monitor database. Enter the interval (in hours) that you want Flow Monitor to wait, before it checks the private IP address again, to resolve information that may have changed for the address. By default, private addresses are resolved every 48 hours.

- **Resolve public address interval.** When the Flow Monitor collector service encounters an IP address, it tries to determine information about the host attached to the IP address. After this information is resolved, it is stored in the Flow Monitor database. Enter the interval (in hours) that you want Flow Monitor to wait, before it checks the public IP address again, to resolve information that may have changed on the address. By default, public addresses are resolved every 720 hours (30 days).



Tip: Because public IP addresses are less likely to be changed, you may want to use longer intervals than used for the **Resolve private address interval** option.

- **Expire unclassified traffic after.** Enter the number of hours after which Flow Monitor should purge unclassified traffic. Unclassified traffic is traffic transmitted over ports that are currently not monitored by Flow Monitor. By default, this option is set to 0 (zero), which causes Flow Monitor to aggregate and retain data for all unclassified ports as a single value; detailed information about the individual unclassified ports over which traffic was transmitted is immediately discarded.



Note: The collector will purge any unclassified data that has no activity after the **Expire unclassified traffic after** value is satisfied.

You can use the data retention section of the Flow Monitor Settings dialog to set data retention parameters for flow and interface data. Periodic roll-up and archival of flow data minimizes system resources needed for data storage and improves system responsive during data intensive operations.

Data retention settings

Flow data includes many parameters (input and output interfaces, source and destination IP addresses, port numbers, byte rates, flow end times, etc.) which while useful in providing information may quickly fill available storage. Rolling up the data makes for efficient storage, but there may be losses of time related information within individual flows. Flow Monitor provides a data retention scheme that allows the user to choose to either manually tune data retention or to allow Flow Monitor to automatically tune the retention of flow data, which in turn actively manages the growth rate of the Flow Monitor databases. The following parameters are used to control the cleanup of flow data.

- **Auto tune flow data retention.** Select this option if you want Flow Monitor to automatically tune the flow data cleanup settings to manage database size and system performance. This option is selected by default.
- **Percentage of traffic to retain.** Use this option to determine the percentage of raw traffic the collector will write to the database. This option is enabled when you clear the **Auto tune flow data retention** check box.



Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.



Note: When you place the cursor in a box to change a value, a message appears at the bottom of the dialog. This message will provide information about the number and percentage of the recommended maximum flow records being stored in the Flow Monitor data and archive databases. As you make changes, the message will predict how the change will affect the number of records stored in the Flow Monitor data and archive databases.

- **Retain raw data for.** Enter the number of hours of raw flow data you would like to maintain. This setting establishes a sliding time window of raw data that spans the specified period. Raw data that reaches the end of the period is rolled up. The roll up of raw data happens every hour on the hour. After data has been rolled up, Flow Monitor can only report using the hourly summations. By default, raw data is rolled up after 4 hours.
- **Retain hourly data for.** Enter the number of days you would like to maintain hourly data. This setting establishes a sliding time window of hourly data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly data takes place daily. After hourly data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly data is maintained for 1 day.
- **Retain daily data for.** Enter the number of days of daily data you would like to maintain before archiving. This setting establishes a sliding time window of daily data that spans the specified number of days. As daily data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived data with some restrictions. By default, daily data is archived after 3 days.
- **Retain archive data for.** Enter the number of days of daily data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily data that spans the specified number of days. As the archived daily data ages beyond this period it is purged from the database. After archived data is purged, Flow Monitor can no longer report on the data. By default, archive data is purged from the database after 7 days.

Interface Data Retention Settings

Raw interface data is provided by the flow collector, or the collector can be configured to collect raw interface data directly from the network device when the collector is receiving sampled flow data. This raw interface data is used to represent total interface traffic for the period and to calculate 95th percentile values for the Interface Overview and Interface Usage reports. Because of the data compaction, interface data has a smaller impact on data storage, so it can be maintained for longer periods of time.

The following parameters are used to control the clean up of interface data.

- **Retain raw data for.** Enter the number of days of raw interface data you would like to maintain. This setting establishes a sliding time window of raw interface data that spans the specified number of days. As raw interface data ages beyond this point it is rolled up. After data has been rolled up, Flow Monitor can only report using the summations produced in the roll-up process. By default, raw interface data is rolled up after 8 days.



Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.



Important: If 95th percentile values are going to be used for billing purposes, you should maintain a set of raw interface data that matches the billing period to ensure accurate results. To gather the data needed to calculate the 95th percentile values for the interface, set the **Roll up raw data after** setting for Interface Data to match or exceed the billing period.

- **Retain hourly data for.** Enter the number of days you would like to maintain hourly interface data. This setting establishes a sliding time window of hourly interface data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly interface data takes place daily. After hourly interface data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly interface data is maintained for 35 days.
- **Retain daily data for.** Enter the number of days of daily interface data you would like to maintain before archiving. This setting establishes a sliding time window of daily interface data that spans the specified number of days. As daily interface data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived interface data. By default, daily interface data is archived after 180 days.
- **Retain archive data for.** Enter the number of days of daily interface data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily interface data that spans the specified number of days. As the archived daily interface data ages beyond this period it is purged from the database. After archived interface data is purged, Flow Monitor can no longer report on the data. By default, archive interface data is purged from the database after 365 days.

Click **OK** to save changes.

Configure Flow Monitor to listen for NetFlow data

Use the Listener port settings on the Flow Settings to configure Flow Monitor to listen for NetFlow data. You can enter the TCP/IP port numbers which the Flow Monitor collector service should use to listen for flow information in the **Listener port** box. Flow Monitor can listen on one or more ports, with port 9999 being the default. The sources sending flow information to Flow Monitor must send data using one of these ports.



Note: If you configure Flow Monitor to listen on more than one port or on a port other than the default port, you should verify that the port is not being used by another service and ensure that an exception is added to the firewall if you are using Windows Firewall.

To configure Flow Monitor to listen for NetFlow data:



Note: By default, Flow Monitor listens for Flow data on port 9999. If you want to use that port, you do not need to perform this procedure.

- 1 Navigate to the Flow Settings dialog (**Flow Monitor > Settings**). The Flow Settings dialog appears.
- 2 In **Listener port**, enter the port numbers, separated by commas, over which Flow Monitor should listen for Flow data.

Click **OK** to save the changes.

Setting the logging level

Use the Flow Settings dialog to specify the level of information that is recorded for the Flow Log.



Note: The logging level that you specify on the Flow Settings dialog determines the level of data that Flow Monitor records, whereas the logging level that you specify on the Flow Log report page determines the level of data displayed within the report.



Important: Keep in mind that if you choose the Normal or Errors Only levels, you will not be able to view the Verbose level from the Flow Log report page.

To set the Flow Monitor logging level:

- 1 Navigate to the Flow Settings dialog (**Flow Monitor > Settings**). The Flow Settings dialog appears.

- 2 Under General, select the **Log level**.
 - **Normal**. Select this option to record errors and some general event information.
 - **Verbose Logging**. Select this option to record more detailed information than normal logging. This option can create a large number of records and may be resource intensive; it is only recommended for use while troubleshooting issues.
 - **Errors Only**. Select this option to record only events that register as errors.
- 3 Click **OK** to accept changes.

Data retention strategy and tuning

Flow Monitor can process millions of NetFlow records per minute from NetFlow enabled devices and the Flow Publisher, while also gathering interface data through direct SNMP polling of individual devices. The number of flow records retained in raw form directly impacts the size of the Flow Monitor databases and performance of data intensive operations such as report generation and display. Flow Monitor uses data compression, culling, and archival strategies to minimize the impact data retention has on system storage and operations. The following diagram illustrates the different stages of the data retention strategy and the relative impact of each stage on the number of flow records stored in the Flow Monitor databases.

Initial data compression

The first step of the data retention strategy is accomplished during the interval between collections of the raw data. Flow records with the same key data that occur during the interval between consecutive data collections are consolidated into a single flow record. This results in a small reduction in records, with a longer data collection interval creating a larger reduction. Use the **Data collection interval** option to adjust this interval.

Raw data compression

Raw data compression happens during the hourly roll-up. Each hour an hour's worth of raw NetFlow records are aged out of the hourly retention period and are compressed into a single record. While the start and stop times for individual flows may be lost, this compression provides an initial savings in data storage. Use the **Retain raw data for x hours** option to determine how long you want to maintain raw data before rolling it up into an hourly data records.

Culling flow data

The next step in the retention strategy is to cull the flow data so that the smallest flow records are removed from the data to be stored. This is done by ordering the flow records by size, and retaining a percentage of the total number of flow records, based on the size in bytes of the traffic represented by the flow.

The system is configured to maintain between 97 and 99 percent of the flow records by size (number of bytes), discarding the bottom 1-3 percent of the flow traffic. While the discarded records represent only a small percentage with respect to the total number of bytes represented by the flow data, they can represent thousands of individual flow records in environments where there are many dropped connections, port scans, or other activity resulting in flows with small byte counts.

By culling these records, we can see a large reduction in storage requirements, and a corresponding increase in performance of data intensive operations, all with a minimal reduction in data retention. This culling of flow data takes place during the hourly roll-up, as raw flow data is converted to hourly data. Use the **Percentage of traffic to retain** option to set the percentage of the flow data you want to retain.

Daily flow data compression

Following this culling of data, a data compression takes place during the daily roll-up. Each day, a days worth of hourly roll-ups are aged out of the daily retention period, and are compressed into a single record for the day. Use the **Retain hourly data for x days** option to determine how long you want the hourly roll-up records to be maintained in the Active Flow Monitor database, before they are rolled-up into a daily record.

Flow data archival

Finally, each day, daily data is archived. The archival removes daily data that has aged out of the daily retention period. Each day during the daily roll-up, a daily record is written to the NetFlow Archive and is removed from the NetFlow Active database. Use the **Retain daily data for x days** option to determine how long you want the daily roll-up records maintained in the Active Flow Monitor database before they are archived in the Flow Monitor Archive database.

Data retention tuning

Data retention can be tuned manually, by adjusting the **Data collection interval**, **Percentage of traffic to retain**, and the retention periods for the various stages of the data retention strategy (Raw flow data, hourly flow data and daily flow data), or it can be tuned automatically by selecting the **Auto tune flow data retention** option.

When you have enabled auto tuning of the system (**Auto tune flow data retention** option is selected), the system will adjust the data retention periods to maintain the number of records within a normal range that will optimize data storage and system performance.

Using information gathered from the database, Flow Monitor will approximate the growth rate of the database, and adjust the retention settings to ensure that the total size of the database is maintained in the recommended band of a minimum of 1 million to a maximum of 10 million flow records. The recommended band is based on storage requirements for each stage in the data retention strategy.

When you manually adjust the Data Retention settings (**Auto tune flow data retention** option is cleared), you will be presented with guidance in the message area at the bottom of the dialog as you adjust each setting. This feedback provides you with information about how the current or proposed setting will affect the database size with respect to the maximum recommended database size (10 million records).

For the raw data, hourly data, and daily data, the maximum recommended database size is compared against all of the data in these categories and is based on the size of the Flow Monitor Active database. For the Archive daily data after setting, the guidance is based on the size of the Flow Monitor Archive database.

Configuring data retention settings

Flow Monitor is designed to serve two primary purposes:

- To give a minute-by-minute view of recent network traffic.
- To give an overview of historical network traffic.

To accomplish these goals while keeping the size of its database reasonable, Flow Monitor uses a process of summarizing data at certain time intervals.

By default, Flow Monitor rolls up data on this schedule:

- Complete raw data (which is collected every other minute and provides the detailed view of recent traffic) is kept for 4 hours.
- After 4 hours, raw data is summarized into hourly averages.
- After 1 days, hourly averages are summarized into daily averages.
- After 3 days, daily data is archived.
- After 7 days, archive data is purged from the archive database.

To configure the data collection interval:

- 1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
- 2 In the **Data collection interval** box, select how often you want Flow Monitor to write raw data from its sources to the Flow Monitor Active database. You may select 1, 2, 3, 4, 5, or 10 minutes. By default, raw data is written to the database every 2 minutes.
- 3 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure address resolution intervals:

- 1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
- 2 In the **Resolve private address interval** box, type the interval (in hours) that you want Flow Monitor to wait before it checks a private IP address to resolve information that may have changed for the address since the last private address lookup. By default, private addresses are resolved every 48 hours.
- 3 In the **Resolve public address interval** box, type the interval (in hours) that you want Flow Monitor to wait before it checks a public IP address to resolve information that may have changed for the address since the last public address lookup. By default, public addresses are resolved every 720 hours.
- 4 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure unclassified traffic collection:

- 1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
- 2 In the **Expire unclassified traffic after** box, type the number of hours after which Flow Monitor should purge unclassified traffic. Unclassified traffic is traffic transmitted over ports that are currently not monitored by Flow Monitor. By default, this option is set to 0 (zero), which causes Flow Monitor to aggregate and retain data for all unclassified ports as a single value; detailed information about the individual unclassified ports over which traffic was transmitted is immediately discarded.
- 3 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure flow data retention:

- 1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
- 2 If you want to allow Flow Monitor to automatically manage your data retention settings, select **Auto tune flow data retention** to automatically tune the flow data cleanup settings to manage database size and system performance. This option is selected by default. For more information on tuning flow data retention, see *Data retention strategy and tuning*.
- 3 If you want to manually manage your data retention settings, clear **Auto tune flow data retention** and set the following settings:



Note: When you manually adjust the Data Retention settings (**Auto tune flow data retention** option is cleared), you will be presented with guidance in the message area at the bottom of the dialog as you adjust each setting. This feedback provides you with information about how the current, or proposed setting will affect the database size with respect to the maximum recommended database size (10 million records). For the raw data, hourly data, and daily data, the maximum recommended database size is compared against all of the data in these categories and is based on the size of the Flow Monitor Active database. For the Archive daily data after setting, the guidance is based on the size of the Flow Monitor Archive database.

- **Percentage of traffic to retain.** Use this option to determine the amount of the total hourly data you want to maintain during the hourly roll-up. This option is enabled when you clear the Auto tune flow data retention check box.



Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.

- **Retain raw data for.** Enter the number of hours of raw flow data you would like to maintain. This setting establishes a sliding time window of raw data that spans the specified period. Raw data that reaches the end of the period is rolled up. The roll up of raw data happens every hour on the hour. After data has been rolled up, Flow Monitor can only report using the hourly summations. By default, raw data is rolled up after 4 hours.
 - **Retain hourly data for.** Enter the number of days you would like to maintain hourly data. This setting establishes a sliding time window of hourly data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly data takes place daily. After hourly data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly data is maintained for 1 day.
 - **Retain daily data for.** Enter the number of days of daily data you would like to maintain before archiving. This setting establishes a sliding time window of daily data that spans the specified number of days. As daily data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived data with some restrictions. By default, daily data is archived after 3 days.
 - **Retain archive data for.** Enter the number of days of daily data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily data that spans the specified number of days. As the archived daily data ages beyond this period it is purged from the database. After archived data is purged, Flow Monitor can no longer report on the data. By default, archive data is purged from the database after 7 days.
- 4 Click **OK**. The setting is saved and the Flow Monitor Settings dialog closes.

To configure interface data retention:

- 1 Navigate to the Flow Monitor Settings dialog (**Flow Monitor > Settings**).
- 2 Set the following settings to tune your interface data retention:



Note: Raw interface data is used to represent total interface traffic for the period and to calculate 95th percentile values for the Interface Overview and Interface Usage reports. Because of data compaction, interface data has a smaller impact on data storage, so it can be maintained for longer periods of time.

- **Retain raw data for.** Enter the number of days of raw interface data you would like to maintain. This setting establishes a sliding time window of raw interface data that spans the specified number of days. As raw interface data ages beyond this point it is rolled up. After data has been rolled up, Flow Monitor can only report using the summations produced in the roll-up process. By default, raw interface data is rolled up after 8 days.



Caution: While the default settings for data cleanup are conservative, when you modify the roll-up settings it can directly affect the size of the Flow Monitor databases and the performance of the application. We recommend that you modify these settings cautiously, and monitor the effects of changes to these settings on database size and application performance.



Important: If 95th percentile values are going to be used for billing purposes, you should maintain a set of raw interface data that matches the billing period to ensure accurate results. To gather the data needed to calculate the 95th percentile values for the interface, set the Roll up raw data after setting for Interface Data to match or exceed the billing period.

- **Retain hourly data for.** Enter the number of days you would like to maintain hourly interface data. This setting establishes a sliding time window of hourly interface data that spans the specified number of days. As hourly data ages beyond this period it is rolled up. The roll up of hourly interface data takes place daily. After hourly interface data is rolled up, Flow Monitor can only report aggregated totals for the entire 24-hour block of time. By default, hourly interface data is maintained for 35 days.
- **Retain daily data for.** Enter the number of days of daily interface data you would like to maintain before archiving. This setting establishes a sliding time window of daily interface data that spans the specified number of days. As daily interface data ages beyond this period, it is archived. Flow Monitor continues to have visibility into archived interface data. By default, daily interface data is archived after 180 days.
- **Retain archive data for.** Enter the number of days of daily interface data you would like to maintain in the archive database. This setting establishes a sliding time window of archived daily interface data that spans the specified number of days. As the archived daily interface data ages beyond this period it is purged from the database. After archived interface data is purged, Flow Monitor can no longer report on the data. By default, archive interface data is purged from the database after 365 days.



Important: Any changes made to data roll up intervals are not enforced until the Flow Monitor collector service is restarted. For more information, see *Stopping or restarting the collector* (on page 1034).

Configuring Applications

In This Chapter

| | |
|--|------|
| Monitoring traffic on non-standard ports | 1018 |
| Configure Applications..... | 1019 |
| Map Ports to Application | 1021 |

Monitoring traffic on non-standard ports

Flow Monitor automatically classifies traffic for most common applications. However, in some cases, you may need to create a custom definition to ensure that Flow Monitor properly classifies some traffic. This need is most common when:

- Your device routes traffic for applications that use a proprietary protocol. This may be a custom program that uses a protocol developed in-house to send data across the network or a third-party application that uses its own custom protocol to transmit data.
- Your device routes traffic for standard applications over non-standard ports. Examples include a standard Web server running on a port other than 80 or an FTP client connecting to an FTP server that runs on a port other than 21.



Note: In Flow Monitor, for traffic to be considered "unclassified," both the port from which the data is sent, and the receiving port must not be classified in the Flow Ports dialog. If either the sending or receiving port is classified, the traffic is associated with the application of the classified port.

To accommodate these cases, you can classify traffic that meets specific rules so that Flow Monitor reports that traffic as belonging to a certain application.



Important: You can configure the amount of time unclassified traffic data is kept. For more information, see *Configuring data roll-up intervals* (on page 1014).



Tip: If Flow Monitor detects a large amount of traffic to an unmonitored port, the Top Applications dashboard report displays a yellow warning flag that explains the situation and guides you in defining the unmonitored port. This can help you to proactively detect emerging non-standard traffic on your network. You can also use the Unclassified Traffic dialog (available from any page in Flow Monitor by selecting **Configure > Flow Unclassified Traffic**) to view all unclassified traffic since the last hourly rollup.

To define rules for classifying traffic that uses non-standard ports:

- 1** From any dashboard view or report in the web interface, select **GO**. The GO menu appears.
- 2** If the Flow Monitor section is not visible, click **Flow Monitor**. The Flow section of the GO menu appears.
- 3** Select **Configure > Applications**. The Applications dialog appears.
- 4** Click **New** to configure a new port definition. The Flow Port dialog appears.
- 5** In **Port**, enter the port number over which the traffic is sent.
- 6** In **Application**, enter a name for the traffic that you are classifying. This should be the name of the protocol (for instance, the definition for port 80 includes `HTTP` as the application).
- 7** Select **Monitor the following protocols on this port**, and then select the protocols that the application uses (**TCP**, **UDP**, or **SCTP**).
- 8** Click **OK** to save changes.

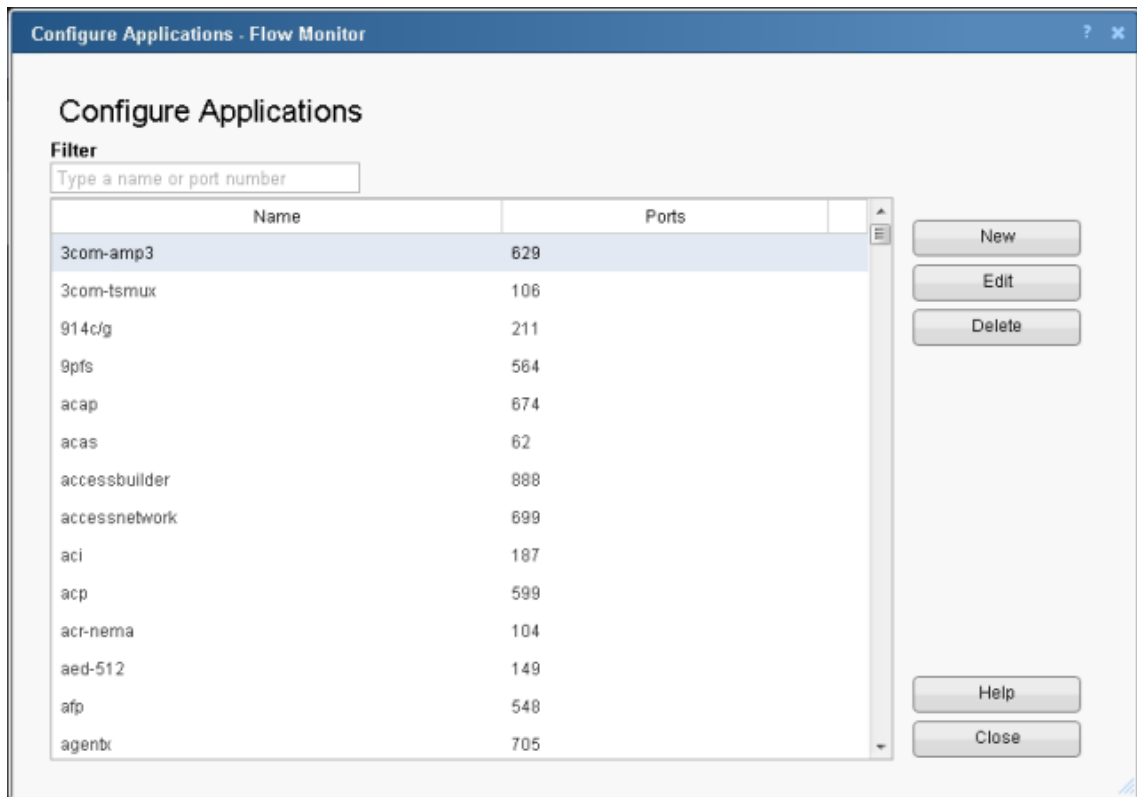
Configure Applications

Use this dialog to create application definitions. Application definitions create a mapping between one or more ports and an application. These port mappings are applied either globally, for all IP addresses, or for a defined subnet. This *network scoping* allows application definitions to have global scope, where the definition is valid for all hosts in a network, or limited scope, where the definition is valid only for a defined subnet.

Flow data is compared with the application definition and is associated with the application based on the following criteria:

- If the network scope is global, a flow is classified as belonging to an application when a port number in either the source or destination IP-port pair matches a port mapped to the application.
- If the network scope is limited to a defined subnet, a flow is classified as belonging to an application when a port number in either the source or destination IP-port pair matches a port mapped to the application, and the IP address falls within the defined subnet.

The application classified flow data is then used to create the Top Applications report. This report is a Top "n" report that provides the bandwidth and percentage of the interface throughput used by each identified application.



The Configure Applications list provides the following information:

- **Name.** Displays the name assigned to the application. This name can simply identify the application, or it can provide additional information to identify a specific instance of the application.
- **Ports.** Displays the first port associated with the application. If the application definition has more than one port associated with an application, the port will be displayed in parenthesis.

The following controls are provided for filtering, adding, editing and deleting application definitions.

- **Filter.** Enter an application name or port number to filter the application definitions.
- Click **New** to create a new application definition. The Map Ports to Application dialog appears.
- Select an application definition, then click **Edit** to modify an existing application definition. The Map Port to Application dialog appears.
- Select an application definition, then click **Delete** to remove an existing application definition. A delete confirmation message appears. Click **Yes**. The application definition is deleted.
- Click **Close** to close this dialog.

Map Ports to Application

Use this dialog to define applications using port mapping. You can name the application, assign ports and protocols, and define the scope of the application definition within the network. You can map a port or port range to a network, subnet, or individual host. This allows you to configure a port for an application globally (port 80 for http) and on a single host (port 80 for http on 192.168.3.33).

| Port or Range | Protocols | Global | Subnet [?] | Actions |
|---------------|-----------|--------------------------|----------------|---------|
| 78 | TCP, UDP | <input type="checkbox"/> | 192.168.3.0/32 | Save |

- **Name.** Enter the name of the application. This name can also be used to define an instance of the application that is applied to a specific subnet which is defined in the subnet field.
- **Port.** Enter a port number, or range of port numbers to be mapped to the application. For each port, you can select the protocol and the network scope to be applied.
- **Protocols.** Select the transport protocols used to provide services to the application.
- **Global.** Select this option if port to application mapping is to be applied to the entire network. When this option is selected, the Subnet field is not active. When this option is not selected, the Subnet field is active and a subnet can be defined.
- **Subnet.** When the Global option is not selected this option is available. Use this box to define the subnet to which the application definition is to be applied. The format for defining the subnetwork is the standard Classless Inter-Domain Routing (CIDR) format (10.0.0.0/8). You can map the port(s) to a single host by using a /32 subnet mask.
- **Actions.** The icons displayed in this column provide you with controls to edit or delete a port entry in the application definition.

Configuring Flow Groups

In This Chapter

| | |
|---------------------------------|------|
| Using Flow Groups..... | 1022 |
| WUG15.0 - NF - Flow Groups..... | 1023 |
| NF - Flow Group | 1023 |

Using Flow Groups

In some cases, you may prefer to track a range of IP addresses as belonging to a different domain, top level domain, or country than the IP addresses resolve to. For example, internal IP addresses do not usually have host names registered on a domain name server, so Flow Monitor cannot automatically determine their domains, top level domains, or countries.

To overcome this limitation, Flow Monitor lets you use Groups to override the domain, top level domain, and country of ranges of IP addresses so that each group can be tracked as a whole. This allows you to easily track sections of your internal network so that you can view reports by divisions, departments, or other groupings.



Tip: After you configure a group, you can use that group's name to filter reports to show only the traffic sent to or received by devices that belong to the group.

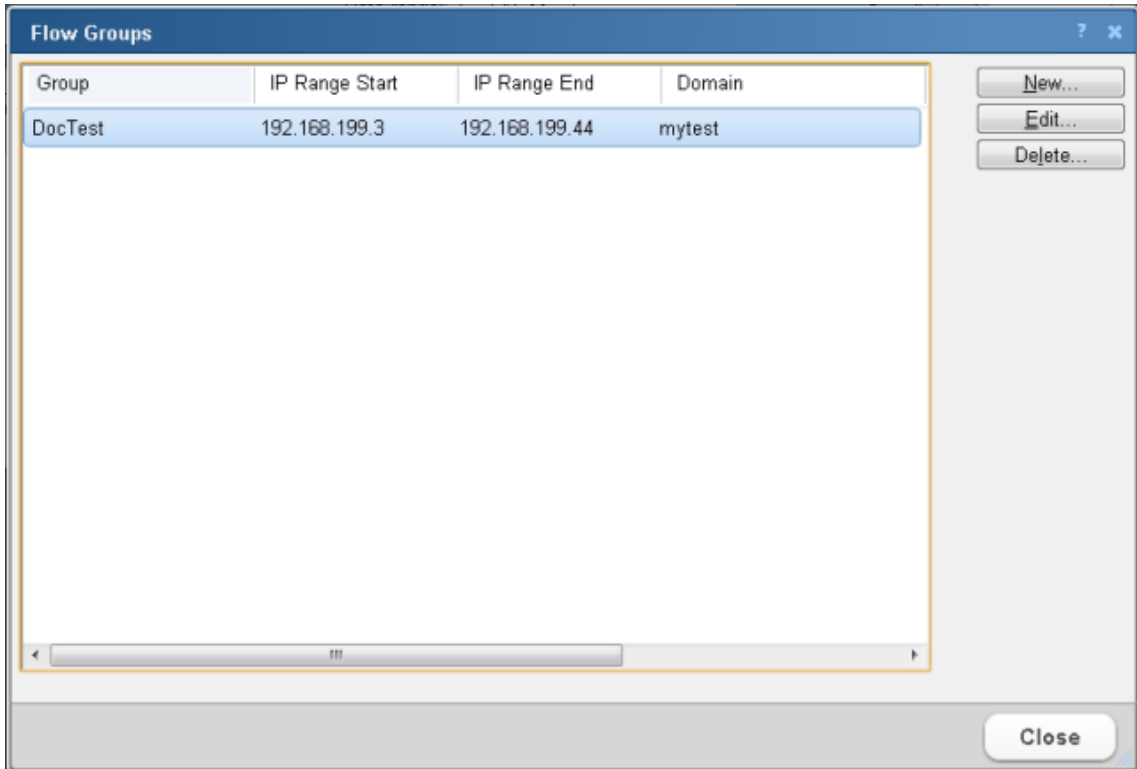
To create or edit a group:

- 1 Navigate to the Flow Groups dialog (**Flow Monitor > Groups**). The Flow Groups dialog appears.
- 2 Click **New**. The Flow Group dialog appears.
- or -
Select a group, then click **Edit**. The Flow Group dialog appears.
- 3 Enter or select the appropriate information in the following fields.
 - **Group.** Enter a name for the Flow group.
 - **IP Range Start.** Enter the first IP address for the Flow source group range.
 - **IP Range End.** Enter the last IP address for the Flow source group range.
 - **Domain.** Enter the domain that you want Flow Monitor to report for the specified IP addresses. For example, *yourcompany.com*.
 - **Top Level Domain.** Select the domain that you want Flow Monitor to report for the specified IP addresses. For example, *com*.

- **Country.** Select the country that you want Flow Monitor to report for the specified IP addresses.
- 4 Click **OK** to save changes.

Flow Groups

This dialog lists all of your Flow Groups by **Name**, **IP Range**, **Domain**, **Top Level Domain**, and **Country**.



Groups allow you to reclassify groups of devices as belonging to a specific domain, top level domain, and country.

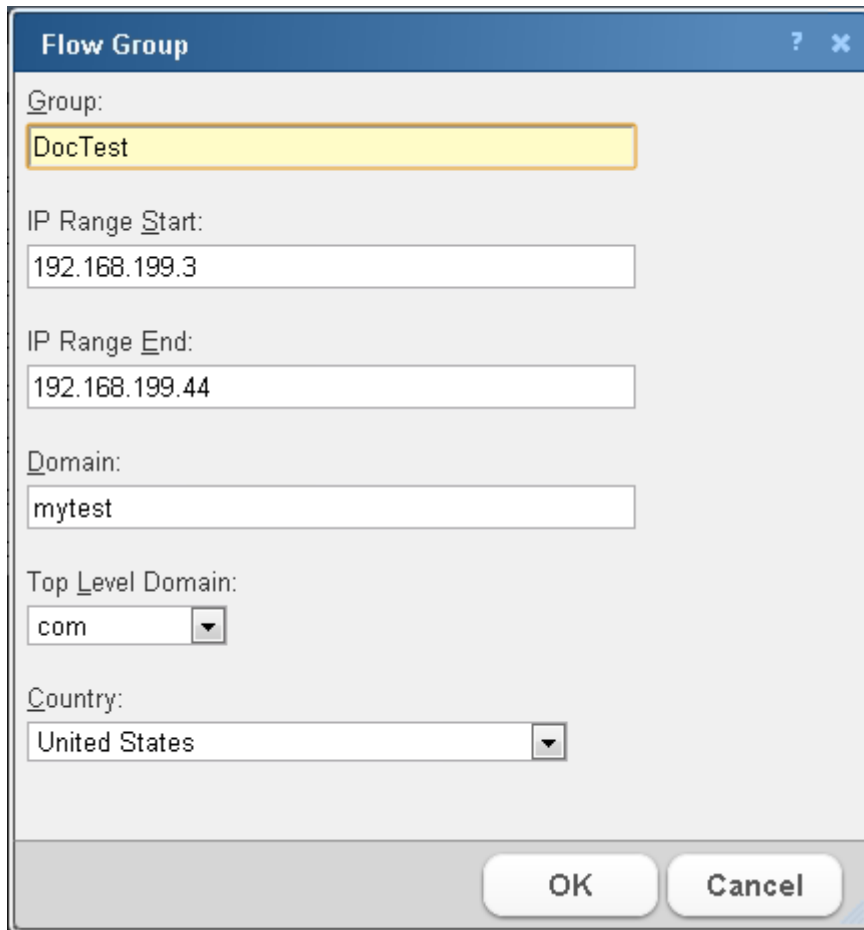
Use this dialog to create, change, and delete Flow groups. After you define a Flow group, the devices associated with the group can be filtered by keywords or viewed as groups in dashboard reports.

To use this dialog:

- To create a new Flow Group, click **New**.
- To change an existing group, select a group, then click **Edit**.
- To remove a group, select a group, then click **Delete**.

Flow Group

Use this dialog to configure a group. Groups allow you to reclassify groups of devices as belonging to a specific domain, top level domain, and country.

A screenshot of a 'Flow Group' dialog box. The dialog has a title bar with a question mark and a close button. It contains several input fields: 'Group' with the text 'DocTest', 'IP Range Start' with '192.168.199.3', 'IP Range End' with '192.168.199.44', 'Domain' with 'mytest', 'Top Level Domain' with a dropdown menu showing 'com', and 'Country' with a dropdown menu showing 'United States'. At the bottom are 'OK' and 'Cancel' buttons.

Flow Group

Group:
DocTest

IP Range Start:
192.168.199.3

IP Range End:
192.168.199.44

Domain:
mytest

Top Level Domain:
com

Country:
United States

OK Cancel



Tip: You can group devices that are not automatically associated with a domain, top level domain, or country. For example, you may have a range of local network devices that you want to associate with yourcompany.com.

Enter or select the appropriate information in the following fields.

- **Group.** Enter a name for the Flow group.
- **IP Range Start.** Enter the first IP address for the Flow source group range.
- **IP Range End.** Enter the last IP address for the Flow source group range.
- **Domain.** Enter the domain that you want Flow Monitor to report for the specified IP addresses. For example, *yourcompany.com*.
- **Top Level Domain.** Select the domain that you want Flow Monitor to report for the specified IP addresses. For example, *com*.
- **Country.** Select the country that you want Flow Monitor to report for the specified IP addresses.

Click **OK** to save changes.

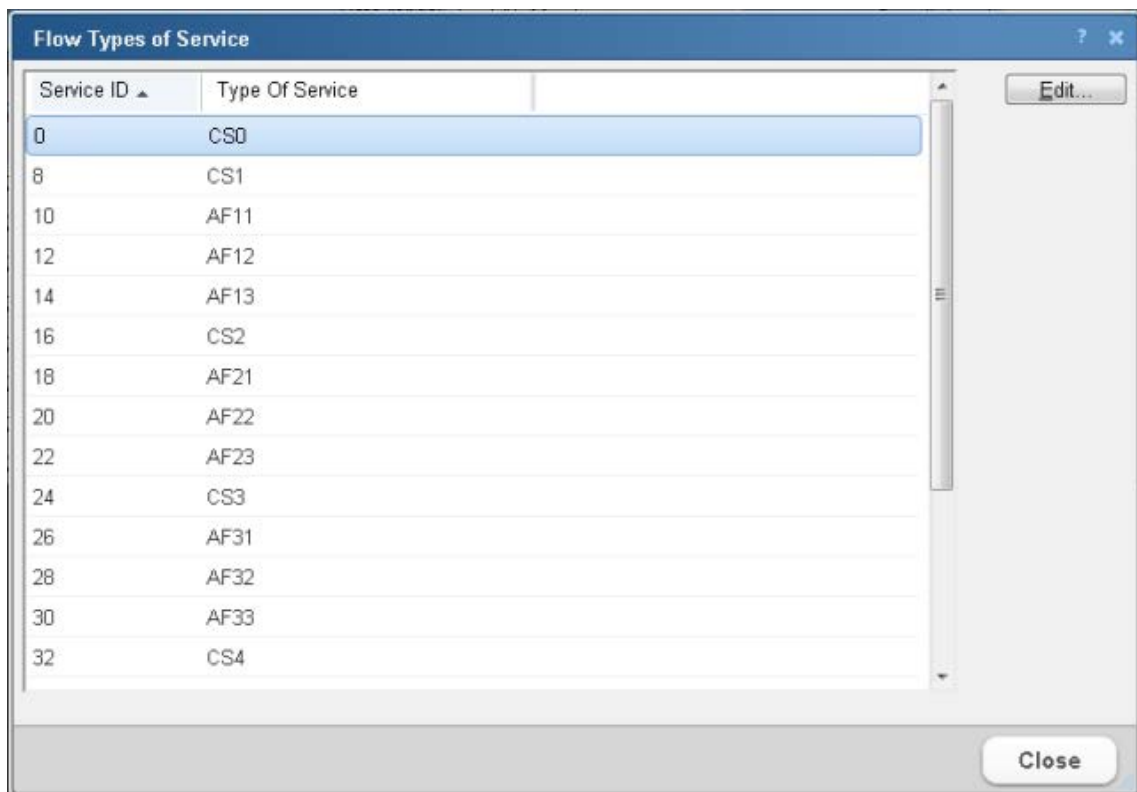
Configuring Type of Service

In This Chapter

| | |
|---------------------------------|------|
| Flow Types of Service | 1025 |
| Edit Flow Type of Service | 1026 |

Flow Types of Service

The Flow Types of Service dialog lists the Flow Types of Service and their associated service IDs. Types of Service (ToS) is a part of an IP specification that allows routers to use routing protocols that help optimize how data is routed (according to the type of service requested). The ToS is assigned by the routers on your network.



You can assign service type display names to make the Top Types of Service dashboard report more meaningful to you.

Renaming a Type of Service

To rename a Type of Service, select it from the list, then click **Edit**.

Edit Flow Type of Service

Use The Edit Type of Service dialog to assign a display name to a Type of Service.

A screenshot of a Windows-style dialog box titled "Flow Type of Service". The dialog has a blue header bar with a question mark icon and a close button. Inside, there are two input fields: "Type of service ID:" with the value "8" and "Type of service name:" with the value "CS1". At the bottom right, there are two buttons: "OK" and "Cancel".

Flow Type of Service

Type of service ID: 8

Type of service name: CS1

OK Cancel

- **Type of service ID.** This is a numeric value that is automatically assigned by the router.
- **Type of service name.** Enter the desired ToS display name. The name assigned here will be displayed in the Flow Types of Service dialog, and the Top Types of Service dashboard report.

Click **OK** to save changes.

Managing unclassified traffic

In This Chapter

| | |
|---|------|
| Classifying traffic that is considered unclassified | 1027 |
| Flow Unclassified Traffic..... | 1028 |

Classifying traffic that is considered unclassified

In Flow Monitor, for traffic to be considered "unclassified," both the port from which the data is sent, or the source port, and the receiving, or destination port, are not classified in the Flow Ports dialog. If either the source or destination port is classified, the traffic is associated with the application of the classified port.

You can classify traffic that is considered unclassified by classifying the source and/or destination ports over which the traffic is transmitted via the Flow Unclassified Traffic dialog.

To classify a source port:

- 1 Navigate to the Unclassified Traffic dialog (**Flow Monitor > Unclassified Traffic**). The Unclassified Traffic dialog appears.
- 2 Use the list fields at the top of the dialog to manipulate the port data displayed in this dialog.
 - Select an **Interface** over which unclassified traffic is transmitting.
 - Select a **Traffic direction** (Inbound, Outbound, Inbound and Outbound, Bounce) in which the unclassified traffic is traveling.
 - Select a filter (Conversations; Source IP, Port; Source Port; Destination IP, Port; Destination Port) by which to group the unclassified traffic from the **Group by** field.
- 3 To begin monitoring a source port, select the port from the list, then click **Classify Src Port**.

To classify a destination port:

- 1 Navigate to the Unclassified Traffic dialog (**Flow Monitor > Unclassified Traffic**). The Unclassified Traffic dialog appears.
- 2 Use the list fields at the top of the dialog to manipulate the port data displayed in this dialog.
 - Select an **Interface** over which unclassified traffic is transmitting.
 - Select a **Traffic direction** (Inbound, Outbound, Inbound and Outbound, Bounce) in which the unclassified traffic is traveling.
 - Select a filter (Conversations; Source IP, Port; Source Port; Destination IP, Port; Destination Port) by which to group the unclassified traffic from the **Group by** field.

- 3 To begin monitoring a destination port, select the port from the list, then click **Classify Dst Port**.

Flow Unclassified Traffic

Use this dialog to view unclassified traffic by the interface over which the traffic is transmitted.

The screenshot shows the 'Unclassified Traffic' dialog in Ipswitch WhatsUp Gold. The dialog is titled 'Unclassified Traffic - Interface: 192.168.199.2'. It has a 'Traffic Direction' dropdown set to 'Inbound and Outbound' and a 'Date range' dropdown set to 'Today'. The 'Number of Records' is set to 100, and 'Group By' is set to 'None'. The main area displays a table of traffic data. The table has the following columns: Time, Source IP, Source Port, Destination IP, Destination Port, Protocol, Traffic, Flows, and Packets. The data is sorted by time, showing traffic from 5/17/11 5:28PM to 5/17/11 5:32PM. The traffic is unclassified, meaning the source and destination ports are not mapped to any application.

| Time | Source IP | Source Port | Destination IP | Destination Port | Protocol | Traffic | Flows | Packets |
|----------------|---------------|-------------|----------------|------------------|----------|------------|-------|---------|
| 5/17/11 5:28PM | 192.168.203.2 | 50551 | 172.16.59.110 | 9997 | UDP | 49.95 KB | 1 | 50 |
| 5/17/11 5:28PM | 192.168.203.2 | 55294 | 192.168.199.2 | 1967 | UDP | 80 Bytes | 1 | 1 |
| 5/17/11 5:28PM | 192.168.203.2 | 64774 | 192.168.199.2 | 1967 | UDP | 80 Bytes | 1 | 1 |
| 5/17/11 5:30PM | 156.21.3.1 | 63302 | 172.16.59.110 | 9997 | UDP | 1.21 MB | 2 | 851 |
| 5/17/11 5:30PM | 192.168.3.1 | 57878 | 172.16.59.110 | 9997 | UDP | 3.67 MB | 2 | 2577 |
| 5/17/11 5:30PM | 192.168.3.4 | 50468 | 172.16.59.110 | 9997 | UDP | 42.25 KB | 2 | 29 |
| 5/17/11 5:30PM | 192.168.3.9 | 57478 | 172.16.59.110 | 9997 | UDP | 689.18 ... | 2 | 473 |
| 5/17/11 5:30PM | 192.168.3.56 | 64448 | 172.16.59.110 | 9997 | UDP | 29.69 KB | 2 | 28 |
| 5/17/11 5:30PM | 192.168.3.137 | 56367 | 172.16.59.110 | 9997 | UDP | 1.98 KB | 2 | 2 |
| 5/17/11 5:30PM | 192.168.30.2 | 57953 | 172.16.59.110 | 9997 | UDP | 545.44 ... | 2 | 467 |
| 5/17/11 5:30PM | 192.168.199.2 | 52044 | 172.16.59.110 | 9997 | UDP | 176.25 ... | 2 | 125 |
| 5/17/11 5:30PM | 192.168.203.2 | 50551 | 172.16.59.110 | 9997 | UDP | 88.33 KB | 2 | 86 |
| 5/17/11 5:30PM | 192.168.203.2 | 51202 | 192.168.199.2 | 1967 | UDP | 80 Bytes | 1 | 1 |
| 5/17/11 5:30PM | 192.168.203.2 | 54036 | 192.168.199.2 | 1967 | UDP | 80 Bytes | 1 | 1 |
| 5/17/11 5:30PM | 192.168.203.2 | 54445 | 192.168.199.2 | 100 | UDP | 58.59 KB | 1 | 1000 |
| 5/17/11 5:30PM | 192.168.203.2 | 54445 | 192.168.199.2 | 1967 | UDP | 80 Bytes | 1 | 1 |
| 5/17/11 5:30PM | 192.168.203.2 | 55294 | 192.168.199.2 | 100 | UDP | 58.59 KB | 1 | 1000 |
| 5/17/11 5:30PM | 192.168.203.2 | 61722 | 192.168.199.2 | 100 | UDP | 195.31 ... | 1 | 1000 |
| 5/17/11 5:30PM | 192.168.203.2 | 61722 | 192.168.199.2 | 1967 | UDP | 80 Bytes | 1 | 1 |
| 5/17/11 5:30PM | 192.168.203.2 | 64774 | 192.168.199.2 | 100 | UDP | 195.31 ... | 1 | 1000 |
| 5/17/11 5:32PM | 156.21.3.1 | 63302 | 172.16.59.110 | 9997 | UDP | 1.34 MB | 2 | 940 |
| 5/17/11 5:32PM | 192.168.3.1 | 57878 | 172.16.59.110 | 9997 | UDP | 3.99 MB | 2 | 2802 |



Note: The ports listed in this dialog have not been mapped to any application. The traffic displayed is the total in bytes for the period since the last hourly roll up time.



Note: In Flow Monitor, for traffic to be considered "unclassified," both the port from which the data is sent, or the source port, and the receiving, or destination port, must not be classified in the Flow Ports dialog. If either the source or destination port is classified, the traffic is associated with the application of the classified port.

The dialog displays unclassified traffic data in the following fields.

- **Time.** The time which the traffic data was received.
- **Source IP.** The IP from which traffic originates.
- **Source Port.** The port from which traffic originates.

- **Destination IP.** The IP to which traffic is sent.
- **Dst. Port.** The destination port, or port to which traffic is sent.
- **Protocol.** The protocol used to send the traffic.
- **Traffic.** The amount of traffic (in bytes) sent during the conversation between the source IP and the destination IP.

Manipulating dialog data

Use the list fields at the top of the dialog to manipulate the port data displayed in this dialog.

- Select an **Interface** over which unclassified traffic is transmitting.
- Select a **Traffic direction** (Inbound, Outbound, Inbound and Outbound, Bounce) in which the unclassified traffic is traveling.
- Select the **Date range** for which you want the report to display data.
- Type the **Number of Records** you want the report to display.
- Select a filter (Conversations; Source IP, Port; Source Port; Destination IP, Port; Destination Port) by which to group the unclassified traffic from the **Group by** field. Select **None** to display unclassified traffic as it is received.

Classifying ports

If you want to classify a port so that Flow Monitor will monitor the port for inbound or outbound traffic, select one of the following options:

- To begin monitoring a source port, select a port from the list, then click **Classify Src Port**.
- To begin monitoring a destination port, select a port from the list, then click **Classify Dst Port**.



Note: After you classify a new source or destination port, only the new traffic will display under the newly classified port(s). Any previously unclassified traffic will not be displayed under the newly classified port(s).

Exporting the Unclassified Traffic report

Click **Export** to create a PDF file containing the contents of the Unclassified Traffic report. You can save the file, or view the file in a PDF viewer.

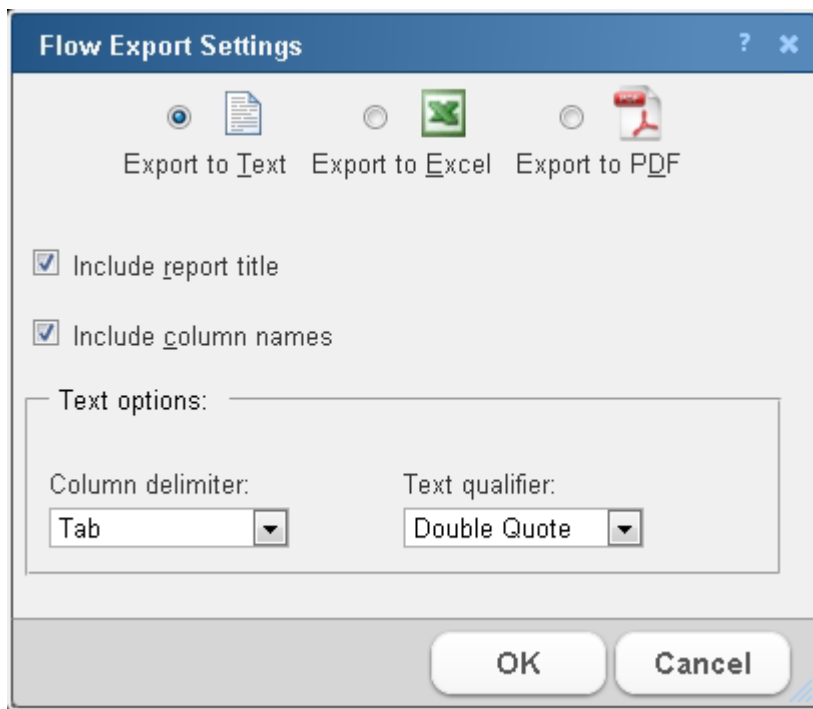
Configuring Data Export Settings

In This Chapter

Flow Export Settings 1030

Flow Export Settings

Use the Flow Export Settings dialog to set the parameters for exporting data from Flow Monitor. You can export data to a text file, Microsoft Excel, or a PDF.



- Select **Export to Text** to export Flow data to text.
- Select **Export to Excel** to export Flow data to Microsoft Excel.
- Select **Export to PDF** to export data to PDF.
- Select **Include report title** to include the report name in the exported data.
- Select **Include column names** to include the column titles in the exported data.
- Select **Include graphs** to include graph(s) with the exported data (available on select reports).

When exporting data to text, set the **Text options**.

- Select the **Column delimiter** that separates the table columns; choose either comma, semicolon, tab, or vertical bar.
- Select the **Text qualifier** in which table text is wrapped; choose either double quote, single quote, or none.

Click **OK** to save changes.

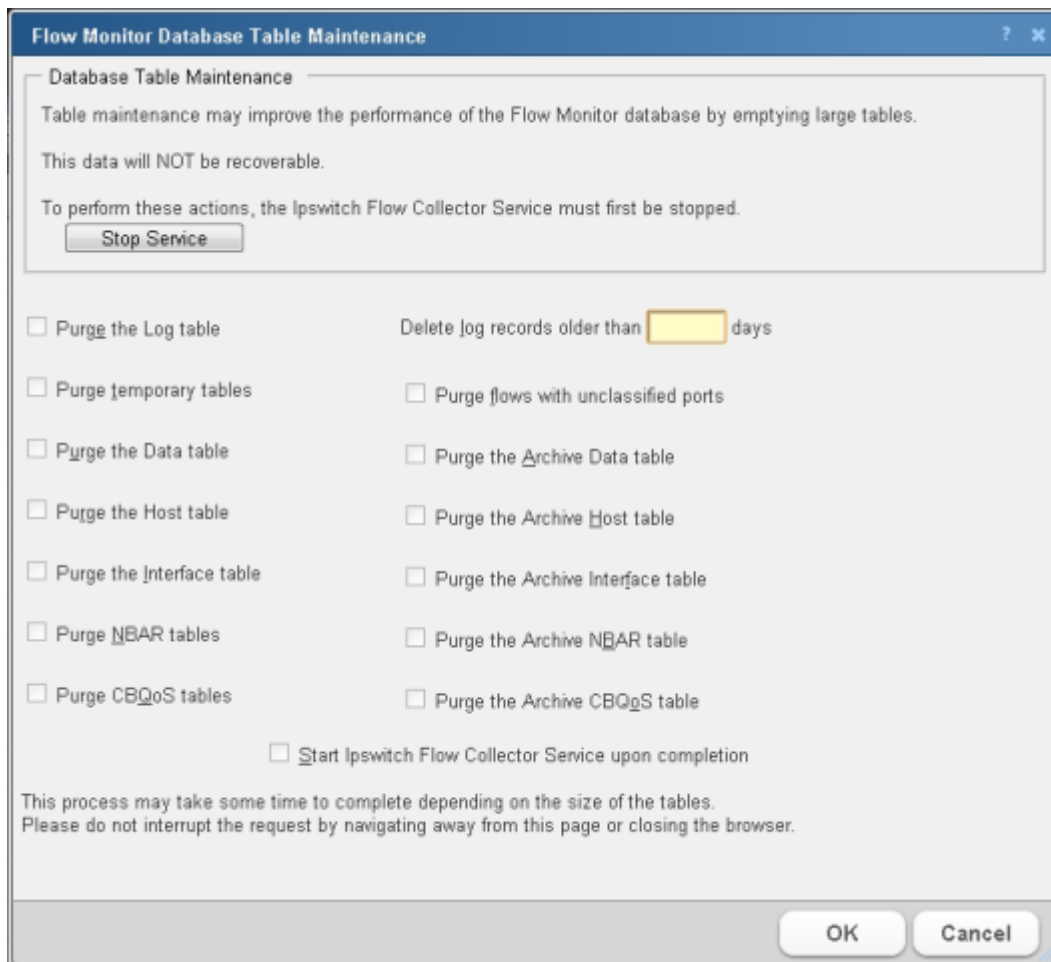
Maintaining Flow Databases

In This Chapter

- Flow Database Table Maintenance 1032
- Stopping or restarting the collector 1034
- Backing up and restoring the Flow Monitor databases..... 1035
- Using the database backup and restore backup utility for Flow Monitor 1035

Flow Database Table Maintenance

Use the Flow Database Table Maintenance dialog to perform table maintenance on the Flow Monitor database and archive database.



Regularly purging database tables can improve performance of Flow Monitor.



Important: Purged data cannot be recovered. Make sure that you export and save any Flow data you need for your records.

Stopping the Ipswitch Flow Collector service

To perform any of the purge actions listed in this dialog, you must first stop the Flow Collector service.

Click **Stop service** to stop the collector while you perform database maintenance.

Selecting items to purge

When the Ipswitch Flow Collector service has been stopped, you can select the Flow Monitor database tables you want to purge.

- **Purge the log table.** Select this option to purge the log table. The log table holds messages generated by Flow Monitor about the status of Flow Monitor, as well as errors and warnings that have occurred during operations.
- **Purge temporary tables.** Select this option to purge host update and flush tables. These tables temporarily hold data during the configuration and flushing of configuration data.
- **Purge the Data table.** Select this option to purge flow data. This table holds flow data gathered from the NetFlow exporter on the Flow Monitor source, this information includes source and destination IP addresses, with traffic values in number of flows, packets and bytes.
- **Purge the Host table.** Select this option to purge host data. This table holds information on hosts discovered during the processing of flow information, and successfully resolved using DNS.
- **Purge the Interface table.** Select this option to purge interface traffic data. This table holds information about interface traffic, including traffic values in number of flows, packets and bytes.
- **Purge NBAR tables.** Select this option to purge NBAR information gathered by Flow Monitor. These tables hold information gathered using NBAR, including application identification as well as traffic values in number of packets and bytes.
- **Purge CBoS tables.** Select this option to purge CBoS information. These tables hold information defining class maps as well as information about the effectiveness of policies based on the defined classes. The effectiveness of the policy is measured by comparing the traffic values in packets, bytes and bit-rate prior to the application of the policy with the traffic values after the application of the policy.
- **Purge flows with unclassified ports.** Select this option to purge flows with unclassified ports from the Data table. Ports are classified by mapping the port to an application.

- **Purge the Archive Data table.** Select this option to purge archived flow data. This table holds archived flow information, includes source and destination host identification as well as traffic values in number of flows, packets and bytes.
- **Purge the Archive Host table.** This table holds archived host information discovered during the processing of flow information.
- **Purge the Archive Interface table.** Select this option to purge interface traffic data. This table holds archived information about interface traffic, including traffic values in number of flows, packets and bytes.
- **Purge the Archive NBAR table.** Select this option to purge NBAR information gathered by Flow Monitor. This table holds archived information gathered using NBAR, including application identification as well as traffic values in number of packets and bytes.
- **Purge the Archive CBQoS table.** Select this option to purge archived CBoS information. These tables hold archived CBQoS information about the effectiveness of policies based on the defined classes.

Maintaining log data during a purge

You can configure Flow Monitor to keep a given number of days of log data during a purge of the Log table.

Enter the number of days of logs you want Flow Monitor to maintain in **Delete log records older than xx days**. Log data that is older than the configured number of days will be purged from the Log table.

Restarting the Ipswitch Flow Collector service

After you have selected or configured all of the appropriate database table maintenance tasks, select **Start Ipswitch Flow Collector service upon completion**. This restarts the service so that Flow data collection can resume.

Review your selections, then click **OK** to begin database maintenance. The database maintenance process could be lengthy depending on the size of the tables in your Flow Monitor database and archive database.



Important: Do not navigate away from this page or close the Web browser until the process finishes completely. Failure to wait on the process to complete may result in database corruption or data loss.

Stopping or restarting the collector

You can restart the Flow Collector Service through WhatsUp Gold, and Windows.

To restart the Flow Collector Service through WhatsUp Gold:

From the WhatsUp Gold web interface, (**Admin > Admin Panel**) select the Flow Collector service, then click **Stop** or **Restart**.

To stop or restart the Flow Collector through the WhatsUp Services Controller:

- 1 Go to the WhatsUp Services Controller dialog.
 - From the console, select **Tools > Services Manager**. The WhatsUp Services Controller dialog appears.
- or -
 - From the the Programs menu, click **Ipswitch WhatsUp Gold > Utilities > Service Manager**. The WhatsUp Services Controller dialog appears.
- 2 In the WhatsUp Services Controller, select **Flow Collector**.
- 3 Click **Stop** or **Restart**.

Backing up and restoring the Flow Monitor databases

You can use the WhatsUp Gold database utilities to back up and restore the WhatsUp Flow Monitor database and archive database.



Caution: Make sure that the Discovery Console in the WhatsUp Gold console application is closed and make sure all users are logged out of the WhatsUp Gold web interface before running a database restore. Running the Discovery Console or having users logged in to the WhatsUp Gold web interface while running a database restore could cause the database restore to fail.

To access the database utilities:

From the WhatsUp Gold console main menu, select **Tools > Database Utilities**.

Using the database backup and restore backup utility for Flow Monitor

You can back up your complete Flow Monitor SQL Server database and archive database to any mapped directory you have on your network. Database backups are saved as `.bak` files and can be restored at any time. Restoring a `.bak` file overwrites your current database with the data in a `.bak` file.



Caution: Make sure that the Discovery Console in the WhatsUp Gold console application is closed and make sure all users are logged out of the WhatsUp Gold web interface before running a database restore. Running the Discovery Console or having users logged in to the WhatsUp Gold web interface while running a database restore could cause the database restore to fail.



Important: You can use this feature with any local instance of SQL Server (default databases are named `Netflow` and `NFArchive`). This feature does not work with remote databases.



Important: You can use this feature with any local instance of SQL Server. This feature does not work with remote databases.



Important: We strongly suggest that you backup and restore the Netflow database and archive database as a set. When you backup the Netflow database, you should also backup the archive database. Similarly, when you restore the Netflow database, you should restore the archive database to the version that was most recently generated by the Netflow database.

If you want to back up the SQL database to a mapped drive, the Logon settings for the SQL Server must have write access to the mapped drive (default database name for Flow Monitor is `NETFLOW` and the default database name for Flow Monitor archive is `NFArchive`).

To change the SQL database logon settings:

- 1 Click **Start > Control Panel > Administrative Tools > Services**, then double-click the SQL Server (`NETFLOW` or `NFArchive`) service. The SQL Service Properties dialog appears.
- 2 Click the **Log On** tab on the Properties dialog.
- 3 Change the account logon settings as required.



Note: This is a complete backup and restore, so any change that you make after the backup will be overwritten and lost after restoring a backup.

To access the Database Utilities Backup and Restore features:

From the main menu in the WhatsUp Gold console, select **Tools > Database Utilities > Back Up Flow Monitor Current or Archive Database**.

- or -

select **Tools > Database Utilities > Restore Flow Monitor Current or Archive Database**.

Managing users and user rights

User accounts and user rights serve two purposes in Flow Monitor:

- User rights govern who can access Flow Monitor reports from, or add Flow Monitor dashboard reports to, the main WhatsUp Gold web interface.
- User rights govern who can modify the Flow Monitor configuration.

To grant a user the right to view Flow Monitor reports and data:



Note: To complete this procedure, you must be logged in as a user who has been granted the Manage Users right in WhatsUp Gold.

- 1 Select **Admin > Manage Users**. The Manage Users dialog appears.
- 2 Select the user to which you want to grant rights to view Flow Monitor reports, then click **Edit**. The Edit User dialog appears.

- 3 Under User rights, in the Flow Monitor section, select **Access Flow Reports**.
- 4 Click **OK** to save changes.

To grant a user the right to configure Flow Monitor:

- 1 Select **Admin > Manage Users**. The Manage Users dialog appears.
- 2 Select the user you want to allow to configure Flow Monitor, then click **Edit**. The Edit User dialog appears.
- 3 Under User rights, in the Flow section, select **Configure Flow Monitor**.
- 4 Click **OK** to save changes.

To block a user from viewing Flow Monitor data for a specific Flow Monitor source:

- 1 Click **Admin > Flow Sources**. The Flow Sources dialog appears.
- 2 Select a source, then click **Access Rights**. The Flow Source Access Rights dialog appears.
- 3 To block a user or multiple users, select the specific user(s) from the list of usernames by clicking inside a check box in the Block Access column.



Tip: You can **Select All** users, or **Deselect All** users.

- 4 Click **OK** to save changes.



Note: In order for a user to be able to block access for other WhatsUp Gold users, the user must have the Manage Users access right. Additionally, the user for which you are trying to block access for should not have this right, as this will allow them to block access for other users.

For more information on managing user accounts, see *Managing Users (on page 852)*.

Using Flow Monitor reports

In This Chapter

| | |
|--|------|
| About the Flow Monitor Reports group..... | 1038 |
| About the Interface Details report | 1039 |
| Flow Monitor Interface Overview report | 1048 |
| Flow Log | 1052 |
| Flow Bandwidth Usage report..... | 1056 |
| Flow Interface Usage Report | 1059 |
| About the NBAR and CBQoS Reports | 1061 |
| Using Scheduled Reports: printing, exporting, and emailing reports | 1064 |

About the Flow Monitor Reports group

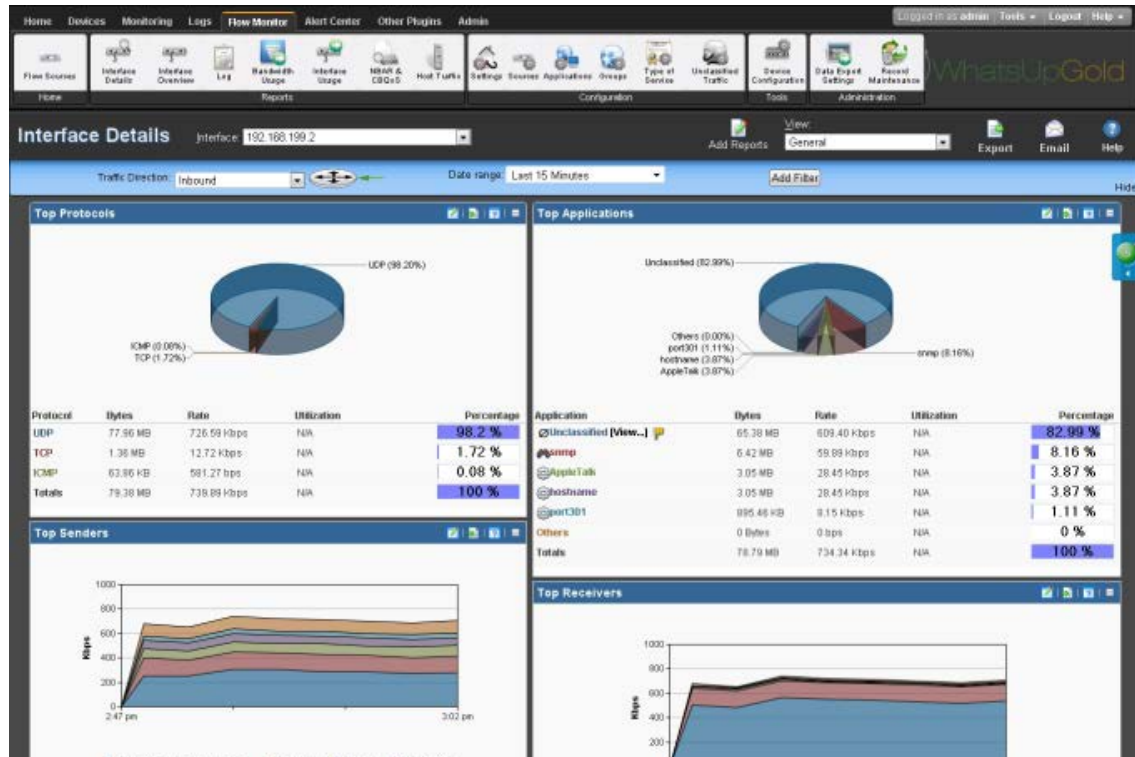
The Flow Monitor Reports group lists the available Flow Monitor reports.

- Interface Details
- Interface Overview
- Flow Monitor Log
- Bandwidth Usage
- Interface Usage
- *NBAR & CBQoS* (on page 1061)

To view a report, double-click its title in the list.

About the Interface Details report

The Interface Details report is a collection of dashboard reports that provide quick insight into the traffic flowing through a specific interface.



When you first access the Interface Details report, it shows the General view for all traffic on the selected interface. You can refine the report in several ways.

- **Select a different interface.** Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Changing the traffic direction.** Use the **Traffic direction** list at the top of the page to select a direction for which the report data is displayed.
- **Selecting a different date range.** Use the **Date range** list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 1044).
- **Filter report results.** You can filter the current dashboard reports to show only data matching search criteria. For more information, see *Filtering by keywords* (on page 1045). You can also drill-down into certain report entries. For more information, see *Filtering by drilling-down* (on page 1047).
- **Managing report views.** Use the **Dashboard View** list at the top of the page to switch between the pre-configured report view and report views you've configured, or to create new report views.



Note: sFlow data is sent every x number of packets (configurable on the sFlow device), whereas typically *all* NetFlow data is collected and monitored. This means that sFlow data provides a sampling of network traffic data, whereas Flow data provides all network traffic data.

sFlow data sampling methods may result in Interface Overview and Interface Detail reports that appear to have more or less traffic than is shown in the Flow Monitor Home page source information. This is because the sampled data shown in the Interface Overview and Interface Detail reports are derived the sampled data and the Flow Monitor Home page source information is derived from the total interface traffic data.

For more information on how to refine the low Interface Details report, see *Filtering data in a view* (on page 1044).



Tip: You can view the **Interface Overview** report for the selected interface by clicking Interface Overview at the top of the page.

General view

The Flow Monitor Interface Details' main view is the General view. The General view displays an overview of traffic for the selected interface.

By default, the report contains the following Interface Details dashboard reports:

- Top Protocols
- Top Applications
- Top Senders
- Top Receivers
- Top Conversations

You can add additional Interface Details dashboard reports to the General view, or delete an existing dashboard report from both the **Edit Layout** button and the **Dashboard View** list. For more information, see *Managing report views* (on page 1043).



Tip: Click **Edit Layout** to add a dashboard report to the currently selected dashboard view.



Note: Sender dashboard reports are displayed on the left side of the report, while receiver dashboard reports are displayed on the right side. A page with no sender or receiver reports displays dashboard reports in one column.

NetFlow Interface Details

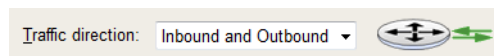
The Interface Details report is a collection of dashboard reports that provide quick insight into the traffic flowing through a specific interface.

General is the main view for the Flow Interface Details report.



When you first access the Flow Interface Details report, it shows the *General* (on page 1040) view for all traffic on the selected interface. You can refine the report in several ways.

- **Select a different interface.** Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Changing the traffic direction.** By default, the Flow Interface Details report displays information about traffic inbound to the selected interface. Use the **Traffic direction** list at the top of the page to select a direction for which the report data is displayed. The router icon to the right of the **Traffic direction** list illustrates what direction traffic is traveling in relation to the source. For more information about traffic direction, see *Filtering by traffic direction*.



- **Selecting a different date range.** Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 1044). You can also change the report date and time by using the Report Zoom Tool. For more information, see *Report Zoom Tool*.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- **Filtering the results by a keyword.** Use the **Add Filter** button to apply a filter by which the report data will sort. For more information, see *Filtering by keywords* (on page 1045).



Note: When you are using a type of filter that matches a device using an IP address, you can use CIDR notation to identify a subnet of hosts from which the reports will display data. For example, When you select a Sender filter type, you can specify a subnet using 192.168.11.0/24 to display information from all of the hosts in the subnet.

- **Managing report views.** Use the **Dashboard View** list at the top of the page to switch between the pre-configured report view and report views you've configured, or to create new report views.

Selecting and configuring the dashboard reports in this report

In addition to customizing the report data, there are several ways you can configure the individual dashboard reports within the Interface Details report.


- **Editing the dashboard reports displayed within a report view.** Use the **Edit layout** button at the top of the screen to select which reports to display within the report's views.
- **Configure the report.** Use the configure button on a dashboard report menu to change the report configuration. For more information, see *Configure Flow* dialog.
- **Expand and collapse dashboard reports.** Use the collapse and expand buttons on the report toolbar to open and close the dashboard reports within the report.



Note: Collapsing a dashboard report does not remove it from the report. Instead, it collapses the dashboard report data and displays only the dashboard report title bar.

Exporting, emailing, scheduling and managing reports



Use the **Export**  icon, at the top right of the page, to export reports. Use the **Email**



Email icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 1064).

Exporting individual dashboard report data

Use the Export button on a dashboard report's menu to export data to either a text file, Microsoft Excel, or a PDF. For more information, see *Exporting report data* (on page 1075).



Tip: You can view the **Interface Overview** report for the selected interface by clicking Interface Overview at the top of the page.

Managing report views

You can customize the default view, General, of the Flow Monitor Interface Details report, or create new views tailored to your needs.

To customize an existing view:

- 1 Navigate to the Interface Details report (**Flow Monitor > Interface Details**).
- 2 From the **View** list in the toolbar, select the view you want to customize. The view you select appears.
- 3 In the toolbar, click **Edit View**. The Configure Flow Interface Report dialog appears.
- 4 Customize the view.
 - a) In **View**, enter a descriptive name for the view. This name appears in the **View** select list in the toolbar.
 - b) From the list of available reports, select the checkboxes next to the names of the reports you want to include in this view.
- 5 Click **OK** to save changes. The customized Flow Interface Details report appears.

To create a new Interface Details report view:

- 1 Navigate to the Interface Details report (**Flow Monitor > Interface Details**).
- 2 From the **View** select list in the toolbar, select **Add View**. The Configure Flow Interface Report dialog appears.
- 3 Configure the new view.
 - a) In **View**, enter a descriptive name for the view. This name appears in the **View** select list in the toolbar.
 - b) From the list of available reports, select the checkboxes next to the names of the reports you want to include in this view.
- 4 Click **OK** to save changes. The Flow Monitor Interface Details report appears and displays the new view.

To delete a Flow Interface Details report view:

- 1 Navigate to the Interface Details report (**Flow Monitor > Interface Details**).
- 2 From the **Dashboard View** select list in the toolbar, select the view you want to delete. The view you select appears.
- 3 From the **Dashboard** select list in the toolbar, select **Delete Current View**. You will be prompted to confirm you want to delete the current view.
- 4 Verify that you want to delete the view, then click **Yes**. The report view is deleted and the Flow Monitor Interface Details report appears.

Selecting an interface

The Flow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports display data in context of a single interface on the source router or switch.

To change the interface for which data is reported:

- 1 From the toolbar at the top of the screen, click the **Interface** list. A list of all of the available interfaces appears.
- 2 Select the interface for which you want to view the current report. The report refreshes with data from the selected interface.

Filtering data in a view

You can filter the data in the Interface Details report in several ways.

- Date and time
- Traffic direction
- Keywords

After you apply a filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Interface Details report views shows data for the previous fifteen minutes. You can modify this time range by selecting the time frame from the Date range field.

To change the time frame for which the Interface Details report displays data:

- 1 At the top of the report, select **Date range**. A list of common time periods appears.
- 2 Select one of the available time periods.
- 3 If you select **Custom**, the **Start time** and **End time** fields appear.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- a) In **Start time**, select the date and time that corresponds with the beginning of the time period.
- b) In **End time**, select the date and time that corresponds with the end of the time period.



Note: When you set a start and end time for report data, you will most likely see a larger data total than expected. This is because the data displayed is a summation of the start time, or data greater than or equal to the selected start time, and the end time, or data less than or equal to the selected end time.

- 4 Click **Go** to apply the filter to the report. The report refreshes showing only data from the selected time period.

Filtering by traffic direction

By default, the Interface Detail report displays information about inbound traffic to the selected interface.

The router graphic to the right of the Traffic direction list illustrates the direction traffic is moving in relation to the router.



In the graphic above, the arrow is pointing to the router, illustrating that traffic is moving toward the router, and is therefore *inbound*.

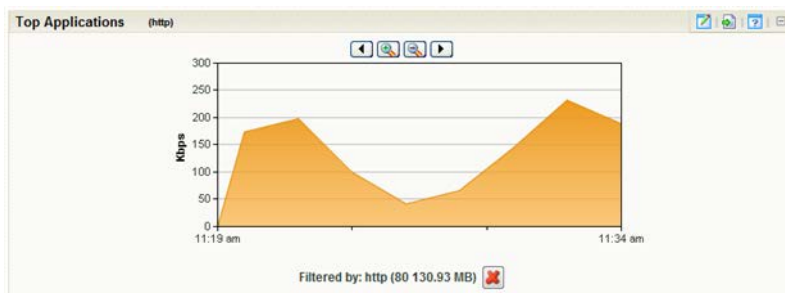
To filter report data by traffic direction:

- 1 At the top of the report, select **Traffic direction**. A list of available traffic directions appears.
- 2 Select a traffic direction.
 - **Inbound**. Select this option to show only data that is being sent to the interface.
 - **Outbound**. Select this option to show only data that is being sent from the interface.
 - **Inbound and Outbound**. Select this option to show both inbound and outbound traffic for the interface.
 - **Bounce**. Select this option to see traffic that routed into and out of the same interface. In some cases, this may represent a router misconfiguration.
- 3 After you select a traffic direction, the report refreshes showing only data from traffic that matches your selection.

Filtering by keywords

You can use keyword filters to create complex Flow Monitor interface report views. This is useful when you need to view data about the traffic generated by a specific computer, to a specific domain, etc.

After you apply a filter to the Interface Details report, the dashboard report that coincides with the filter reloads with a time graph for the filtered traffic component. For example, if you apply a filter for the http application, the Top Applications dashboard report displays a time graph of http application use for the time period selected at the top of the Interface Details report.



You can easily determine which dashboard report contains the time graph by looking for the filter enclosed in parenthesis to the right of the dashboard report title name.



Tip: You can remove the applied filter by clicking the red X under the time graph.

To filter by keywords:

- 1 At the top of the report, select **Add Filter**. Filter fields appear below the button.
- 2 Select the type of filter you want to apply.



Note: When you are using a type of filter that matches a device using an IP address, you can use CIDR notation to identify a subnet of hosts from which the reports will display data. For example, When you select a Sender filter type, you can specify a subnet using 192.168.11.0/24 to display information from all of the hosts in the subnet.

- **Sender.** Show traffic sent by the specified device. You can match a device using its host name or its IP address.
- **Receiver.** Show traffic received by the specified device. You can match a device using its host name or its IP address.
- **Protocol.** Show traffic that used the specified protocol (such as UDP, TCP, or ICMP).
- **Service.** Show traffic that used the specified type of service.
- **Application.** Show traffic that used the specified application. The keyword must match the application name as configured in the Flow ports dialog.



Tip: You can enter a port number instead of an application name to show all traffic transmitting over a certain port.

- **Sender Domain.** Show traffic sent by hosts on the specified domain.
- **Receiver Domain.** Show traffic received by hosts on the specified domain.
- **Sender Country.** Show traffic sent by devices whose IP addresses are registered to the specified country.
- **Receiver Country.** Show traffic received by devices whose IP addresses are registered to the specified country.
- **Sender Group.** Show traffic sent by the specified group.
- **Receiver Group.** Show traffic received by the specified group.
- **Sender TLD.** Show traffic sent by domains that have the specified top level domain (such as .com, .net, .us, or .uk).
- **Receiver TLD.** Show traffic received by domains that have the specified top level domain (such as .com, .net, .us, or .uk).
- **ICMP Type.** Show traffic by ICMP type.

- **Packet Size.** Show traffic by packet size.
- 3 Optionally, click **Add Filter** to add additional filters.
 - 4 Click **Apply Filters**. The report refreshes showing only data that matches the filters you have configured.



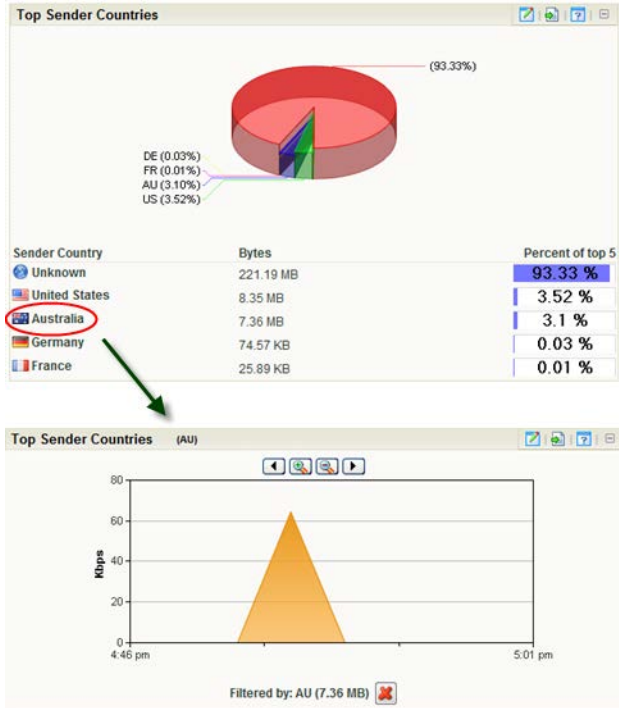
Tip: If you configure a filter incorrectly, you can remove it from the current view by clicking the red X located to the right of the keyword field.

Filtering by drilling-down

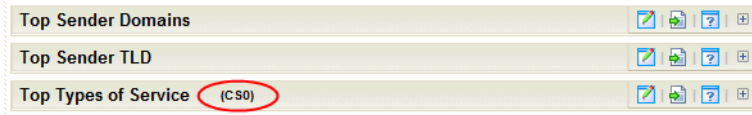
Another way to filter report data is by clicking on report entries, or *drilling-down*. This method of report-filtering allows you to dig deeper into data that peaks your interest or raises red flags—with just one click.

When you click an entry in the farthest-left column of an Interface Details dashboard report, the report reloads using the entry as a filter. Also, you can click inside a dashboard graph area to apply a filter.

Similarly to filtering by keywords, after you apply a filter to the report, the dashboard report that coincides with the filter will display a time graph for the filtered traffic component. For example, if you click an entry in the Sender Country column of the Top Sender Countries dashboard report, the dashboard report reloads with a time graph for the country that you clicked.



Several keyword filters coincide with more than one dashboard report and more than one time graph is displayed after the filter is applied. You can easily distinguish which dashboard reports in the Interface Details report are displaying time graphs by looking for the applied filter's name in parenthesis next to a report name.



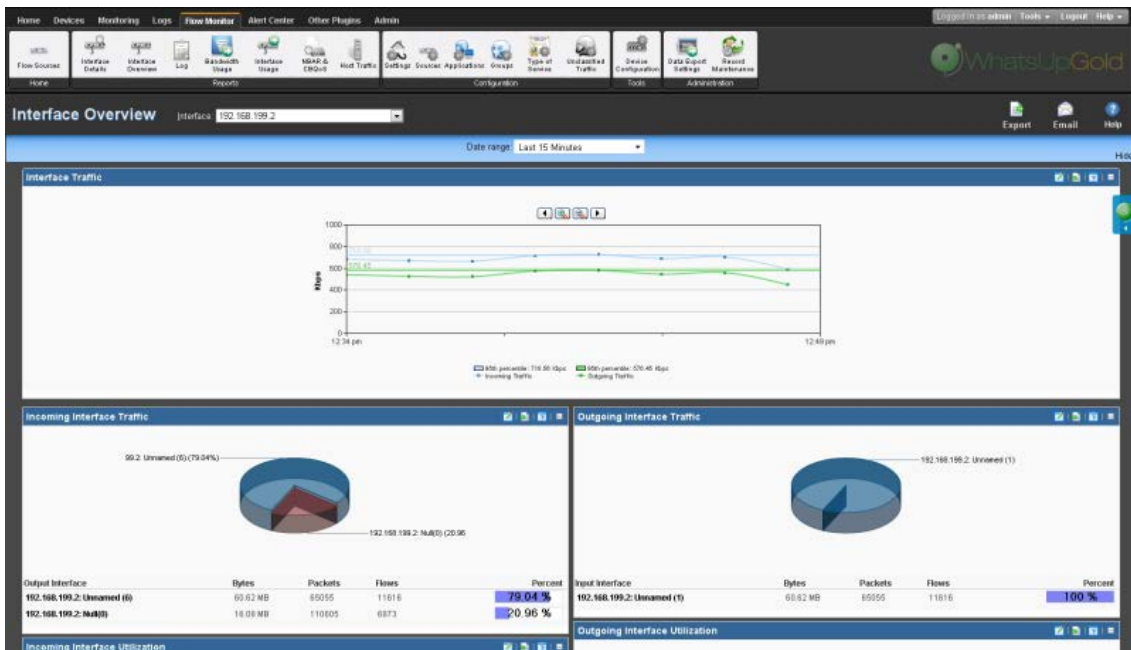
Interface Details - Options

The Interface Details report has the following options available on the Options menu.

- **Export to PDF.** Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.
- **Email / Schedule Report.** Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports.** Select this option to configure Flow Monitor to run this report on a recurring basis.

Flow Monitor Interface Overview report

The Interface Overview report is a collection of Flow dashboard reports that provide a summary of the traffic and utilization of a specific interface.



The Interface Overview consists of individual Flow dashboard reports that highlight both inbound and outbound traffic and utilization for the selected interface.

- Interface Traffic
- Incoming Interface Traffic
- Outgoing Interface Traffic
- Incoming Interface Utilization
- Outgoing Interface Utilization

By default, the report displays data for the last interface you selected from the Source list.



Note: sFlow data is sent every x number of packets (configurable on the sFlow device), whereas typically *all* NetFlow data is collected and monitored. This means that sFlow data provides a sampling of network traffic data, whereas Flow data provides all network traffic data.

sFlow data sampling methods may result in Interface Overview and Interface Detail reports that appear to have more or less traffic than is shown in the Flow Monitor Home page source information. This is because the sampled data shown in the Interface Overview and Interface Detail reports are derived the sampled data and the Flow Monitor Home page source information is derived from the total interface traffic data.

- **Select a different interface.** Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Selecting a different date range.** Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 1044). You can also change the report date and time by using the Report Zoom Tool. For more information, see Report Zoom Tool.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- **Configure the report.** Use the configure button on a dashboard report menu to change the report configuration. For more information, see Configure Flow dialog.

Configuring the dashboard reports in this report

In addition to customizing the report data, you can configure the individual dashboard reports within the Interface Overview report.


- **Expand and collapse dashboard reports.** Use the collapse and expand buttons on the report toolbar to open and close the dashboard reports within the report.



Note: Collapsing a dashboard report does not remove it from the report. Instead, it collapses the dashboard report data and displays only the dashboard report title bar.

Exporting, emailing, scheduling and managing reports



Use the **Export**  icon, at the top right of the page, to export reports. Use the **Email**



Email icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 1064).

Exporting individual dashboard report data

Use the Export button on a dashboard report's menu to export data to either a text file, Microsoft Excel, or a PDF. For more information, see *Exporting report data* (on page 1075).



Tip: You can view the Interface Details report for the selected interface by clicking **Interface Details** at the top of the page.

Filtering report data

You can filter the data displayed in the Interface Overview by *time and date* (on page 1050). After you apply a date and time filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Interface Overview report shows data for the previous fifteen minutes.

To change the time frame for which the Interface Overview report displays data:

- 1 At the top of the report, select **Date range**. A list of common time periods appears.
- 2 Select one of the available time periods.
- 3 If you select **Custom**, the **Start time** and **End time** fields appear.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- a) In **Start time**, select the date and time that corresponds with the beginning of the time period for which you want to see data.
 - b) In **End time**, select the date and time that corresponds with the end of the time period for which you want to see data.
- 4 Click **Go** to apply the filter to the report. The report refreshes showing only data from the time period selected.

About the Report Zoom Tool

Use the zoom tool to navigate through a report. The zoom tool is tied-in to the report date/time picker and will change the date and time of a report as you page up and down, or zoom in and out.



Page up

Moves the report date forward. For example, clicking the Page up button will move the date from today to tomorrow.



Zoom in

Decreases the amount of time displayed in the report. For example, click the Zoom in button will decrease the display time from 24 hours to 12 hours.



Zoom out

Increases the amount of time displayed in the report. For example, clicking the Zoom out button will increase the display time from 12 hours to 24 hours.



Page down

Moves the report date backward. For example, clicking the Page down button will moved the date from today to yesterday.

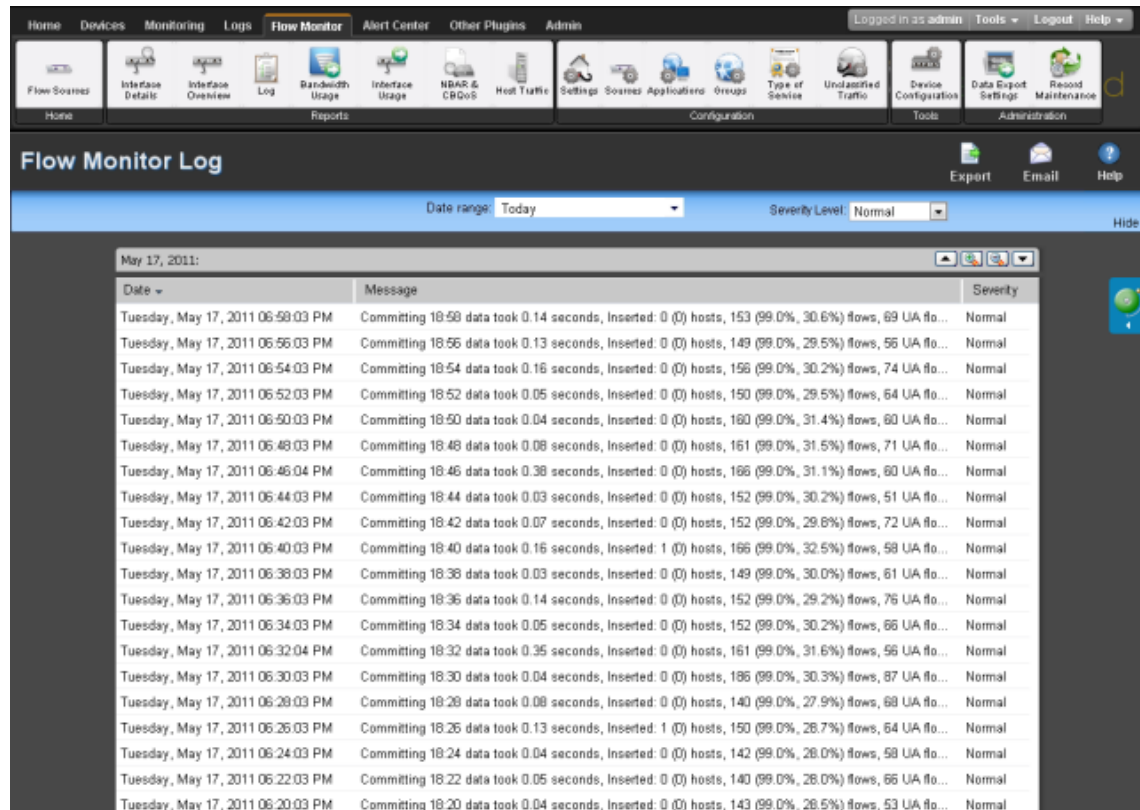
Interface Overview - Options

The Interface Overview report has the following options available on the Options menu.

- **Export to PDF.** Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.
- **Email / Schedule Report.** Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports.** Select this option to configure Flow Monitor to run this report on a recurring basis.

Flow Log

The Flow Monitor Log is a history of system-wide messages generated by Flow Monitor. When you access the Flow Monitor Log, it shows messages generated during the time period selected at the top of the report.



| Date | Message | Severity |
|-----------------------------------|--|----------|
| Tuesday, May 17, 2011 06:58:03 PM | Committing 18:58 data took 0.14 seconds, Inserted: 0 (0) hosts, 153 (99.0%, 30.6%) flows, 69 UA flo... | Normal |
| Tuesday, May 17, 2011 06:56:03 PM | Committing 18:56 data took 0.13 seconds, Inserted: 0 (0) hosts, 149 (99.0%, 29.5%) flows, 56 UA flo... | Normal |
| Tuesday, May 17, 2011 06:54:03 PM | Committing 18:54 data took 0.16 seconds, Inserted: 0 (0) hosts, 156 (99.0%, 30.2%) flows, 74 UA flo... | Normal |
| Tuesday, May 17, 2011 06:52:03 PM | Committing 18:52 data took 0.05 seconds, Inserted: 0 (0) hosts, 150 (99.0%, 29.5%) flows, 64 UA flo... | Normal |
| Tuesday, May 17, 2011 06:50:03 PM | Committing 18:50 data took 0.04 seconds, Inserted: 0 (0) hosts, 160 (99.0%, 31.4%) flows, 60 UA flo... | Normal |
| Tuesday, May 17, 2011 06:48:03 PM | Committing 18:48 data took 0.08 seconds, Inserted: 0 (0) hosts, 161 (99.0%, 31.5%) flows, 71 UA flo... | Normal |
| Tuesday, May 17, 2011 06:46:04 PM | Committing 18:46 data took 0.38 seconds, Inserted: 0 (0) hosts, 166 (99.0%, 31.1%) flows, 60 UA flo... | Normal |
| Tuesday, May 17, 2011 06:44:03 PM | Committing 18:44 data took 0.03 seconds, Inserted: 0 (0) hosts, 152 (99.0%, 30.2%) flows, 51 UA flo... | Normal |
| Tuesday, May 17, 2011 06:42:03 PM | Committing 18:42 data took 0.07 seconds, Inserted: 0 (0) hosts, 152 (99.0%, 29.8%) flows, 72 UA flo... | Normal |
| Tuesday, May 17, 2011 06:40:03 PM | Committing 18:40 data took 0.16 seconds, Inserted: 1 (0) hosts, 166 (99.0%, 32.5%) flows, 58 UA flo... | Normal |
| Tuesday, May 17, 2011 06:38:03 PM | Committing 18:38 data took 0.03 seconds, Inserted: 0 (0) hosts, 149 (99.0%, 30.0%) flows, 61 UA flo... | Normal |
| Tuesday, May 17, 2011 06:36:03 PM | Committing 18:36 data took 0.14 seconds, Inserted: 0 (0) hosts, 152 (99.0%, 29.2%) flows, 76 UA flo... | Normal |
| Tuesday, May 17, 2011 06:34:03 PM | Committing 18:34 data took 0.05 seconds, Inserted: 0 (0) hosts, 152 (99.0%, 30.2%) flows, 66 UA flo... | Normal |
| Tuesday, May 17, 2011 06:32:04 PM | Committing 18:32 data took 0.35 seconds, Inserted: 0 (0) hosts, 161 (99.0%, 31.6%) flows, 56 UA flo... | Normal |
| Tuesday, May 17, 2011 06:30:03 PM | Committing 18:30 data took 0.04 seconds, Inserted: 0 (0) hosts, 186 (99.0%, 30.3%) flows, 87 UA flo... | Normal |
| Tuesday, May 17, 2011 06:28:03 PM | Committing 18:28 data took 0.08 seconds, Inserted: 0 (0) hosts, 140 (99.0%, 27.9%) flows, 68 UA flo... | Normal |
| Tuesday, May 17, 2011 06:26:03 PM | Committing 18:26 data took 0.13 seconds, Inserted: 1 (0) hosts, 150 (99.0%, 28.7%) flows, 64 UA flo... | Normal |
| Tuesday, May 17, 2011 06:24:03 PM | Committing 18:24 data took 0.04 seconds, Inserted: 0 (0) hosts, 142 (99.0%, 28.0%) flows, 58 UA flo... | Normal |
| Tuesday, May 17, 2011 06:22:03 PM | Committing 18:22 data took 0.05 seconds, Inserted: 0 (0) hosts, 140 (99.0%, 28.0%) flows, 66 UA flo... | Normal |
| Tuesday, May 17, 2011 06:20:03 PM | Committing 18:20 data took 0.04 seconds, Inserted: 0 (0) hosts, 143 (99.0%, 28.5%) flows, 53 UA flo... | Normal |

Each entry shows the date logged, the message about the activity, and the severity of the entry.

- **Date** displays the date the message was logged.
- **Message** displays the activity message. This message contains the reason for the log entry, other information, such as error number, which may be useful in troubleshooting.
- **Severity** displays the logging level of the entries, either Normal, Verbose, or Errors Only.



Tip: You can sort the data in the report by clicking on a column title.

Changing the report date and time

Use the **Date range** list at the top of the report to select a time frame for the report. By default, the report displays log entries for the previous hour.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Monitor Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

Changing the report severity/logging level

Use the **Severity level** list to select a logging level for the report.

- **Verbose** displays all entries (including all three severity levels).
- **Normal** displays entries for Normal and Errors Only.
- **Errors only** displays only error entries.



Note: The logging level that you specify on the Flow Settings dialog determines the level of data that Flow Monitor records, whereas the logging level that you specify on the Flow Log report page determines the level of data displayed within the report.




Important: If you have specified the Normal or Errors Only levels on the Flow Settings dialog, you will not be able to view the Verbose level from the Flow Log report page.




Important: If your log includes an error that reads "It seems the collector is unable to keep up with the amount of traffic received," the amount of traffic you are currently collecting is too great for the Flow Monitor to handle. It is possible that you have a number of Flow sources and/or interfaces too great for the collector to handle. In an effort to reduce traffic, it may help to reduce the number of enabled sources and/or interfaces.

Exporting, emailing, scheduling and managing reports



- Use the **Export**  icon, at the top right of the page, to export reports. Use the



Email  icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 1064).

Filtering report data

You can filter the Flow Monitor Log by two criteria.

- *Date and time* (on page 1054)
- *Severity level* (on page 1054)

After you apply a filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Flow Monitor Log shows data for the previous fifteen minutes.

To change the time frame for which the Flow Monitor Log report displays data:

- 1 At the top of the report, select **Date range**. A list of common time periods appears.
- 2 Select one of the available time periods.
- 3 If you select **Custom**, the **Start time** and **End time** fields appear.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- a) In **Start time**, select the date and time that corresponds with the beginning of the time period for which you want to see data.
- b) In **End time**, select the date and time that corresponds with the end of the time period for which you want to see data.



Tip: Use the Standard Business Hours feature to set up group reports designed for business hours only. For more information, see [Changing the report date range](#).

- 4 Click **Go** to apply the filter to the report. The report refreshes showing only data from the time period selected.

Filtering by severity level

By default, the Flow Monitor Log displays data for the Normal severity level.

To change the severity level for which the Flow Monitor Log displays data:

- 1 At the top of the report, click the **Severity level** list. A list of the three available severity levels appears.
- 2 Select the severity level for which you want to view report data. The report refreshes with data for the selected severity level.

About the Report Zoom Tool

Use the zoom tool to navigate through a report. The zoom tool is tied-in to the report date/time picker and will change the date and time of a report as you page up and down, or zoom in and out.



Page up

Moves the report date forward. For example, clicking the Page up button will move the date from today to tomorrow.



Zoom in

Decreases the amount of time displayed in the report. For example, click the Zoom in button will decrease the display time from 24 hours to 12 hours.



Zoom out

Increases the amount of time displayed in the report. For example, clicking the Zoom out button will increase the display time from 12 hours to 24 hours.



Page down

Moves the report date backward. For example, clicking the Page down button will moved the date from today to yesterday.

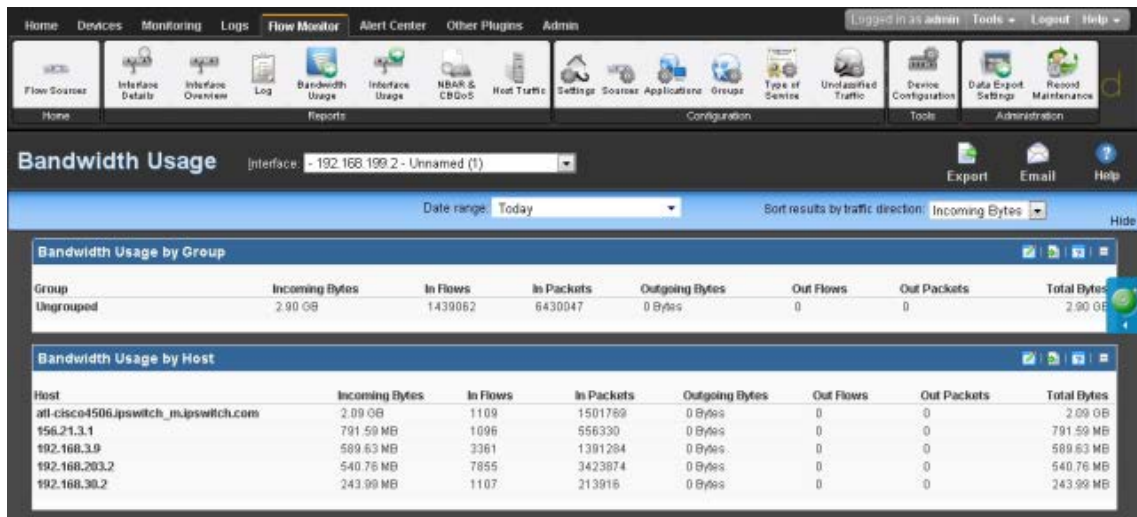
Flow Monitor Log - Options

The Flow Monitor Log report has the following options available on the Options menu.

- **Export to Text.** Select this option to export the contents of the current view to a text file. The Export to Text dialog opens.
- **Export to PDF.** Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.
- **Export to Excel.** Select this option to export the contents of the current view to an Excel file. The Export to Excel dialog opens.
- **Email / Schedule Report.** Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports.** Select this option to configure Flow Monitor to run this report on a recurring basis.

Flow Bandwidth Usage report

The Bandwidth Usage report displays network bandwidth usage information.



The report consists of Flow Monitor dashboard reports that summarize the incoming and outgoing traffic for Flow Monitor groups and hosts.

- Bandwidth Usage by Group displays bandwidth usage summaries for each of your Flow Monitor groups for the selected time period.
- Bandwidth Usage by Host displays bandwidth usage summaries for Flow hosts that are using the most bandwidth during the selected time period.

There are several ways you can refine this report.

- **Select a different interface.** Use the **Interface** list at the top of the page to select the interface for which the report data displays.
- **Sort results by traffic direction.** Use the **Sort by traffic direction** list at the top of the page to select a direction for which the report data is displayed. Select Incoming, Outgoing, or Total.
- **Selecting a different date range.** Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 1044).



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Monitor Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

Configuring the dashboard reports in this report

In addition to customizing the report data, there are several ways you can configure the individual dashboard reports within the Bandwidth Usage report.

- **Configure the report.** Use the configure button on a dashboard report menu to change the report configuration. For more information, see *Configure Flow* dialog.
- **Expand and collapse dashboard reports.** Use the collapse and expand buttons on the report toolbar to open and close the dashboard reports within the report.



Note: Collapsing a dashboard report does not remove it from the report. Instead, it collapses the dashboard report data and displays only the dashboard report title bar.

Exporting, emailing, scheduling and managing reports



Use the **Export** icon, at the top right of the page, to export reports. Use the **Email**



Email icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 1064).

Exporting individual dashboard report data



Use the Export button on a dashboard report's menu to export data to either a text file, Microsoft Excel, or a PDF. For more information, see *Exporting report data* (on page 1075).

Selecting an interface

The Flow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports display data in context of a single interface on the source router or switch.

To change the interface for which data is reported:

- 1 From the toolbar at the top of the screen, click the **Interface** list. A list of all of the available interfaces appears.
- 2 Select the interface for which you want to view the current report. The report refreshes with data from the selected interface.

Filtering report data

You can filter the data in the Bandwidth Usage report two ways.

- *Date and time* (on page 1058)
- *Traffic direction* (on page 1058)

After you apply a filter, the report data refreshes to display data relevant to the applied filter.

Filtering by date and time

By default, the Bandwidth Usage report shows data for the previous fifteen minutes.

To change the time frame for which the Flow Monitor Interface Details report displays data:

- 1 At the top of the report, select **Date range**. A list of common time periods appears.
- 2 Select one of the available time periods.
- 3 If you select **Custom**, the **Start time** and **End time** fields appear.



Note: Flow Monitor only displays data from one database at a time, and by default, displays the most current data. If you select a time period that includes data stored in both the Flow Monitor database and the Flow Monitor Archive database, a note displays below the date range informing you that not all data is shown for the specified date range. For example, if you select a date that includes 39 days of archived data, and one hour of current data, one hour of current data is displayed in the report. You must modify the report's date to view the archived data.

- a) In **Start time**, select the date and time that corresponds with the beginning of the time period for which you want to see data.
- b) In **End time**, select the date and time that corresponds with the end of the time period for which you want to see data.



Tip: You can also change the report date and time by using the Report Zoom Tool. For more information, see *About the Report Zoom Tool* (on page 1051).



Tip: Use the Standard Business Hours feature to set up group reports designed for business hours only. For more information, see *Changing the report date range*.

- 4 Click **Go** to apply the filter to the report. The report refreshes showing only data from the time period selected.

Filtering by traffic direction

By default, the Bandwidth Usage report displays information about incoming traffic for the selected interface.

To filter report data by traffic direction:

- 1 At the top of the report, select **Traffic direction**. A list of available traffic directions appears.
- 2 Select a traffic direction.
 - **Inbound.** Select this option to show only data that is being sent into the interface.
 - **Outbound.** Select this option to show only data that is being sent from the interface.
- 3 After you select a traffic direction, the report refreshes. After it refreshes, the report shows only data from traffic that matches your selection.

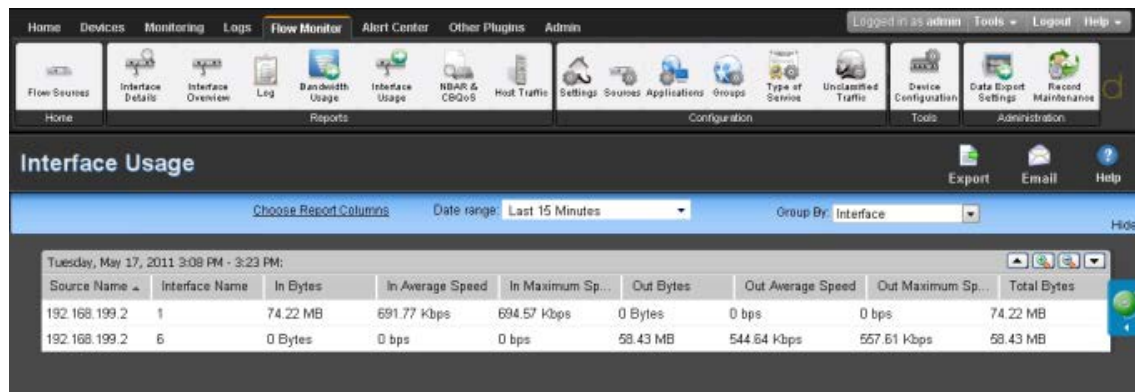
Bandwidth Usage - Options

The Bandwidth Usage report has the following options available on the Options menu.

- **Export to PDF.** Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.
- **Email / Schedule Report.** Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports.** Select this option to configure Flow Monitor to run this report on a recurring basis.

Flow Interface Usage Report

The Flow Interface Usage report gives a view of the total amount of incoming and outgoing traffic for source interfaces over the selected time period. Interfaces can be displayed separately, or grouped together by interface name. When you group together by interface name, all interfaces under a single display name are added together, and all data displayed is a total for those interfaces.



The screenshot shows the 'Interface Usage' report in the Ipswitch WhatsUp Gold interface. The report is titled 'Interface Usage' and includes a 'Choose Report Columns' button, a 'Date range' dropdown set to 'Last 15 Minutes', and a 'Group By' dropdown set to 'Interface'. The report data is as follows:

| Source Name | Interface Name | In Bytes | In Average Speed | In Maximum Sp... | Out Bytes | Out Average Speed | Out Maximum Sp... | Total Bytes |
|---------------|----------------|----------|------------------|------------------|-----------|-------------------|-------------------|-------------|
| 192.168.199.2 | 1 | 74.22 MB | 691.77 Kbps | 694.57 Kbps | 0 Bytes | 0 bps | 0 bps | 74.22 MB |
| 192.168.199.2 | 6 | 0 Bytes | 0 bps | 0 bps | 58.43 MB | 544.64 Kbps | 557.61 Kbps | 58.43 MB |

The report displays the following usage data for each interface.

- **Interface Name** the display name as configured by the user on the Flow Sources dialog in combination with the interface identifier.
- **Incoming Bytes.** Displays the number of incoming bytes for that interface or interface name over the selected time period.
- **Incoming Average Speed.** Displays the incoming rate in a multiple of bytes per second for the interface over the selected time period.
- **Incoming 95th Percentile.** Displays the results of the 95th percentile calculation for incoming traffic during the selected time period.
- **Incoming Maximum Speed.** Displays the maximum incoming rate in a multiple of bytes per second achieved during the selected time period.
- **Outgoing Bytes.** Displays the number of outgoing bytes for that interface or interface name over the selected time period.

- **Outgoing Average Speed.** Displays the outgoing rate in a multiple of bytes per second for the interface over the selected time period.
- **Outgoing 95th Percentile.** Displays the results of the 95th percentile calculation for outgoing traffic during the selected time period.
- **Outgoing Maximum Speed.** Displays the maximum outgoing rate in a multiple of bytes per second achieved during the selected time period.
- **Total Bytes.** Displays the total number of bytes for that interface or interface name over the selected time period.

By default, the report displays data grouped by interfaces. You can refine the report in several ways.

- **Grouping report data.** Choose to **Group by** *Interface* or *Interface Name*.
- **Selecting a different date range.** Use the Date range list at the top of the report to change the timeframe for which report data is displayed. If you select **Custom**, you will be prompted to enter a start and end time for the date range. For more information, see *Filtering by date and time* (on page 1044).

Exporting, emailing, scheduling and managing reports



Use the **Export** icon, at the top right of the page, to export reports. Use the **Email**



Email icon to E-mail a report or to manage Scheduled Reports. For more information see, *Using Scheduled Reports in Flow Monitor: printing, exporting, and emailing reports* (on page 1064).

Configure Interface Usage Report Columns

Use this dialog to configure which data you want to appear in each column of the Interface Usage report.



Note: **Column 1** always appears and by default contains the interface name.

For each column, select the data you want to appear. If you do not want data to appear in a column, select **none** for that column.

Interface Usage - Options

The Interface Usage report has the following options available on the Options menu.

- **Export to Text.** Select this option to export the contents of the current view to a text file. The Export to Text dialog opens.
- **Export to PDF.** Select this option to export the contents of the current view to a PDF file. The Export to PDF dialog opens.

- **Export to Excel.** Select this option to export the contents of the current view to an Excel file. The Export to Excel dialog opens.
- **Email / Schedule Report.** Select this option to configure an e-mail to capture the contents of the current view, and schedule to send the e-mail with updated information on a recurring basis.
- **Scheduled Reports.** Select this option to configure Flow Monitor to run this report on a recurring basis.

About the NBAR and CBQoS Reports

NBAR Report

Cisco Systems Network Based Application Recognition (NBAR) classification engine provides a network device with the ability to recognize applications, including those that dynamically assign TCP or UDP ports. The Top NBAR Applications report displays the top applications as identified using Cisco's NBAR classification engine.



You can choose to display and sort sender traffic by bytes, packets, or flows using the **Display and sort by** option on the report configuration dialog. Providing alternate sorting methods allows you to monitor and identify hosts that are the largest consumers of interface resources other than bandwidth.

- **Application.** Displays the application as identified by Cisco's NBAR classification engine.
- You can select one of the following units to display and sort the specific items in the report using the **Display and sort by** option on the report configuration dialog. The selected option will appear as the first column header in the report and will be used to sort the top "n" items.
- **Bytes.** Displays the total number of bytes transmitted for the specific item in the report category for the selected date range.
- **Packets.** Displays the total number of packets for the specific item in the report category for the selected date range.

- **Flows.** Displays the total number of flows for the specific item in the report category for the selected date range.
- **Rate.** Displays the average bit rate, packet rate or flow rate, in multiples of the selected unit (e.g. Kbps, Mbps, or Gbps) for the specific item in the report category for the selected date range.
- **Utilization.** Displays the percentage of the total available bandwidth used by the specific item in the report category for the selected date range.



Note: Utilization is displayed as N/A if a speed is not specified for the interface, or if you have selected to display packets or flows in the report. If you are displaying bytes, you can set the interface speed on the Flow Interface dialog. To navigate to the Flow Interface dialog, click the **Configure** link in the message appearing above the dashboard reports.

- **Percentage.** Displays the percentage of the total traffic for the specific item in the report category for the selected date range.
- **Others (row title).** The optional **Others** row title displays a summation of all of the unspecified items of the report category. The unspecified items are those items not specifically displayed in the top "n" items. The **Others** row provides a comparison between the specified items, or top "n" items selected for display, and the rest of the traffic on the interface. When displayed, the Others row will provide perspective as to the relative size of the specified items in comparison to the total traffic on the interface.
- **Totals (row title).** Displays the total of all of the items in the report category, specified and unspecified (**Others**). This row shows the interface totals for each column in the report.



Note: The source device must be configured to generate NBAR information in order for this report to generate data for the source device.



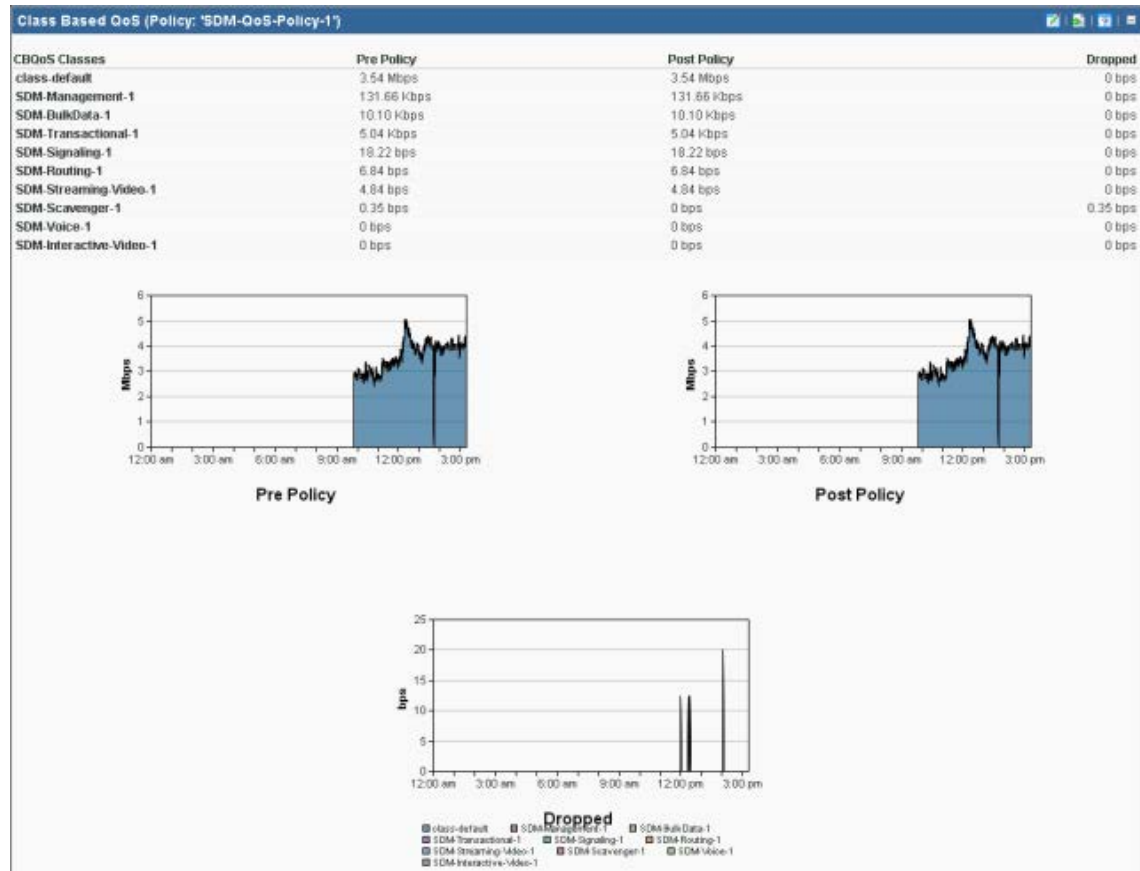
Note: For the **Top NBAR Applications - Flow Details** report, NBAR information generated by the source device is gathered by Flow Monitor from flow data using Flexible NetFlow.



Note: For the **Top NBAR Applications - Interface Totals** report, the NBAR information is gathered from the source device using SNMP polling. The **Poll source for NBAR information** option is available on the Flow Source dialog.

Class Based Quality of Service Report

The Class Based Quality of Service (CBQoS) report provides information about the effectiveness of class-based policies applied to an interface for all of the defined classes.



- **QoS Class Map.** Displays the QoS class name as defined by the policy assigned to the interface.
- **Pre-Policy.** Displays the amount of traffic for the class before the policy is applied.
- **Post-Policy.** Displays the amount of traffic for the class after the policy is applied.
- **Dropped.** Displays the number of bytes dropped as a result of applying the policy to the class.



Note: You must have defined QoS classes and policies on the source device before this report is able to display results.



Note: The CBQoS information generated by the source device must be gathered using SNMP polling for CBQoS information.

Using Scheduled Reports: printing, exporting, and emailing reports

The Flow Monitor Log and Interface Usage reports can be printed and exported to a formatted text file, Microsoft Excel, or a PDF. You can also email reports as a PDF, or send on scheduled intervals. The Flow Monitor Interface Details, Interface Overview, and Bandwidth Usage reports can be exported as PDF reports and emailed as scheduled reports. Click the



Export icon, available at the top of each report, to export reports, or the Email icon to email a report or manage Scheduled Reports. This option is available to users with user rights for **Manage Scheduled Report** enabled. For more information, see About user rights.



Important: To use the print and export features, make sure client side JavaScript is enabled in your browser's options.



Tip: In some cases, exported reports show more detailed data than the data displayed in the report in the web interface. For example, an exported Excel report may contain more data columns, or a floating data point with higher precision.

To print a report:

While viewing the report you want to print:

- Right-click anywhere inside the report window, then select **Print**.
- OR -
- From the WhatsUp Gold web interface, click **File > Print**.

To export a report to a text file (full reports only):

While viewing the full report you want to export:



- 1 On the Report Toolbar, click the **Export** icon. The Report Options list appears.
- 2 Select **Export to Text**.
- 3 Clear or select the following options: **Include report title**, **Include column names** to either include or remove the report title or column names from the exported file.
- 4 Select a **Column delimiter** from the list.
- 5 Select a **Text qualifier** from the list.
- 6 Click **OK** to export the report to text.

To export a report to Microsoft Excel (full reports only):

While viewing the full report you want to export:




- 1 On the Report Toolbar, click the **Export** icon. The Report Options list appears.
- 2 Select **Export to Excel**.

- 3 Clear or select the following options: **Include report title**, **Include column names** to either include or remove the report title or column names from the exported file.
- 4 Select a **Column delimiter** from the list.
- 5 Select a **Text qualifier** from the list.
- 6 Click **OK** to export the report to Excel.

To export a report to a PDF:

While viewing the full report you want to export:




- 1 On the Report Toolbar, click the **Export**  icon. The Report Options list appears.
- 2 Select **Export to PDF**. The Export to PDF dialog appears.
- 3 Select the following options:
 - **Page size**. Select from the list of page size options.
 - **Auto size**. Enable this option to, generally, make the best automatic adjustment to fit all page content on the PDF.
 - **Page orientation**. Select Portrait or Landscape PDF.
- 4 Select the **Live links** option if you want to include clickable url links in the PDF report.
- 5 Click **Export** to export the report to a PDF.

To email a report as a PDF:

While viewing the full report you want to export:



- 1 From the WhatsUp Gold web interface, on the Report Toolbar, click the **Email**  icon. The Email list appears.
- 2 Select **Email/Schedule Report**. The Email Report dialog appears.
- 3 Enter the following information for the email: **To**, **Subject**, **URL**, select the **PDF Options**. Refer to the dialog help for more information.
- 4 Click **Send Email** to send a PDF email immediately.
- OR -
Click **Schedule** to complete the scheduled email settings.
- 5 Click **Close**. The Email Report dialog closes.

Using Flow Monitor dashboard reports

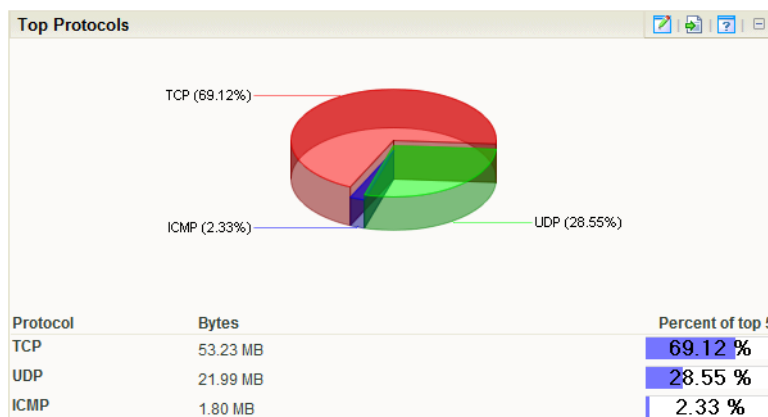
In This Chapter

| | |
|---|------|
| Understanding Flow Monitor dashboard reports | 1066 |
| Navigating dashboard reports..... | 1068 |
| Configuring dashboard reports..... | 1072 |
| Exporting dashboard report data..... | 1075 |
| Linking to Flow Monitor reports from WhatsUp Gold workspace reports | 1076 |

Understanding Flow Monitor dashboard reports

Dashboard reports are the individual small reports displayed in several of the Flow Monitor reports and their views. Flow Monitor report views are user-customizable; they let you organize various dashboard reports by the type of information they display.

Flow Monitor dashboard reports typically consist of a graph and a table of data related to the graph.



Dashboard reports that display data from Flow Monitor can be used within Flow Monitor report views and WhatsUp Gold dashboard views.



Note: While you can determine which dashboard reports appear in dashboard views in Flow Monitor and WhatsUp Gold, Flow Monitor report views are more structured than WhatsUp Gold dashboard views. In WhatsUp Gold, you can position dashboard reports anywhere within a view; in Flow Monitor, report positions cannot be modified. As a rule, sender dashboard reports display on the left side of the report, while receiver dashboard reports display on the right side. Further, a page with no sender or receiver reports displays dashboard reports in one column.

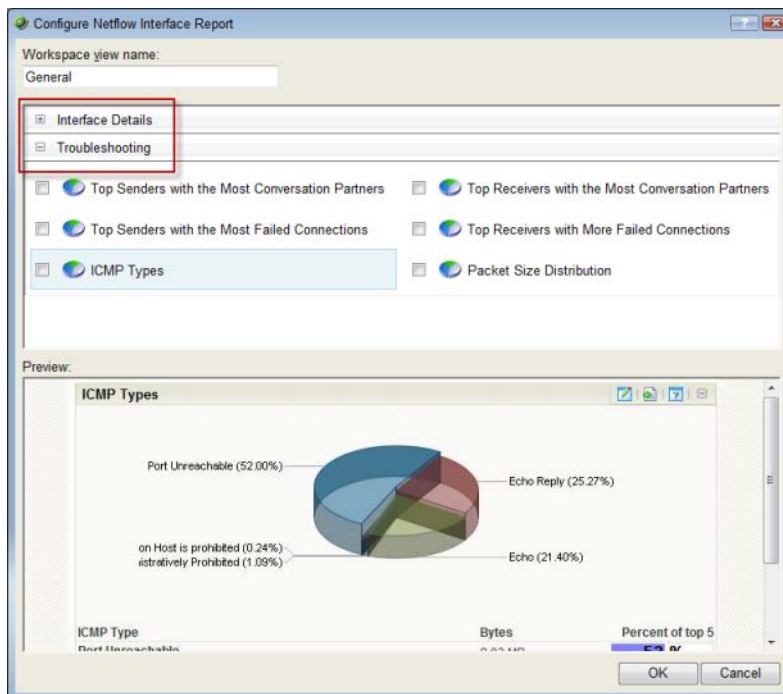
Flow Monitor dashboard report types

There are three types of Flow Monitor dashboard reports.

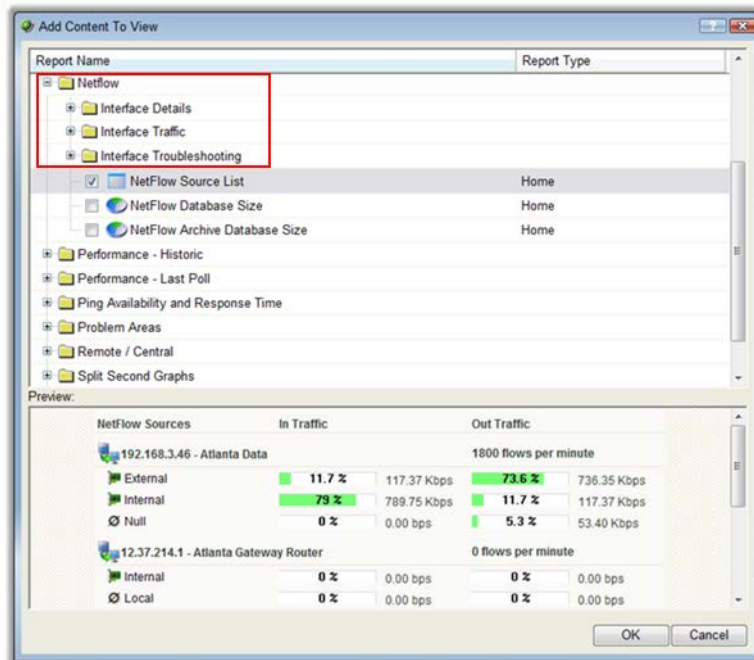
- **Interface Details** dashboard reports display summary information about specific details of an interface; for example, applications, protocols, and types of service.
- **Interface Troubleshooting** dashboard reports display data that would be useful in troubleshooting bandwidth problems; for example, failed connections.
- **Interface Traffic** dashboard reports display summary information about an interface's incoming and outgoing traffic.

These types vary depending from where in the application you modify your report and dashboard views.

If you add dashboard reports to the Interface Details report in Flow Monitor, you see Interface Details and Troubleshooting categories on the Configure Flow Interface Report dialog.



If you add dashboard reports to a dashboard view in WhatsUp Gold, you see Interface Details, Interface Troubleshooting, and Interface Traffic on the Add Content To View dialog.



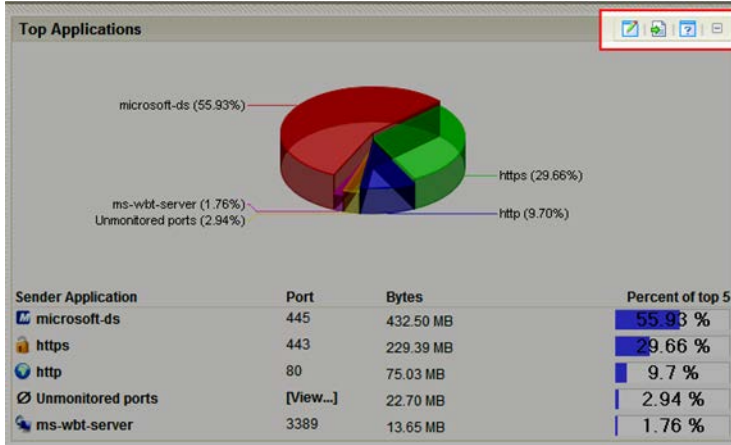
Navigating dashboard reports

There are several ways to navigate Flow Monitor dashboard reports.






- *Dashboard report menu* (on page 1069) gives you options to configure and access help for each dashboard report.
- *Links* (on page 1069) allow you to apply any criteria shown in a report as a filter.
- *Zoom control* (on page 1070) lets you change the amount of data shown in line graphs.
- *Informational tooltips* (on page 1072) alert you to conditions which may warrant further investigation.

Using the dashboard report menu

Each dashboard report has a menu on the right side of its title bar. Using the dashboard report menu, you can view help for the report, configure the report, export the report data, or expand and collapse the report.



Dashboard report menu buttons

-  Click the **Configure** button to open the Configure dialog for the report.
-  Click the **Export** button to export report data.
-  Click the **Help** button to view the help for the report.
-  Click the **Expand** button to expand the report within the dashboard view.
-  Click the **Collapse** button to collapse the report within the dashboard view. Collapsing a report does not remove it from the dashboard view.

Using links in Flow Monitor dashboard reports

Each Flow Monitor dashboard report contains links that allow you to refine the data displayed in the report. When you click on the data in the first column of one of the dashboard report's rows (or on a pie graph's wedges, or a bar graph's bars), the Flow Interface Details report appears with the selected data applied as a filter.

For example, as illustrated in the graphic below, if you click on `ipswitch.com` in the Top Sender Domains dashboard report, the Flow Interface Details report appears with a Sender Domain filter set to `ipswitch.com`.

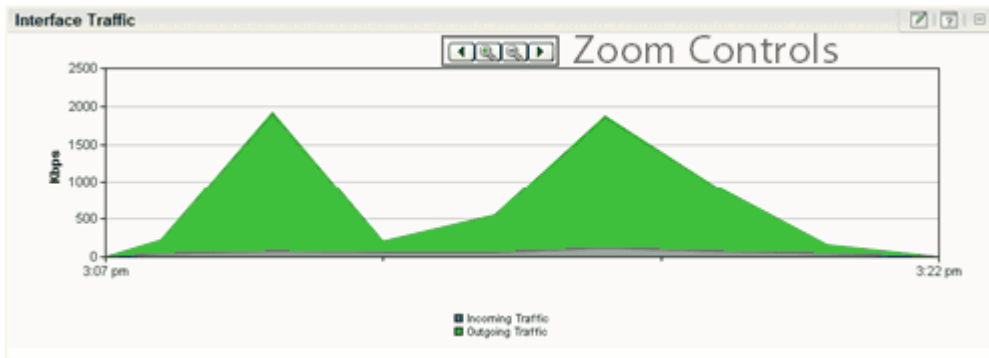
The screenshot shows the 'Top Sender Domains' dashboard report. The 'Interface' is set to '192.168.3.1 - Internal 3'. The 'Workspace View' is set to 'General'. The 'Sender Domain' filter is set to 'ipswitch.com'. The 'Top Applications' report is also visible.

| Sender Domain | Bytes | Percent of top 10 |
|---------------------|-----------|-------------------|
| Unknown | 99.78 MB | 77.82 % |
| ipswitch.com | 19.13 MB | 14.92 % |
| newsgator.com | 3.09 MB | 2.41 % |
| llnw.net | 1.72 MB | 1.34 % |
| fast.net | 1.11 MB | 0.86 % |
| google.com | 1.06 MB | 0.83 % |
| boingboing.net | 772.28 KB | 0.59 % |
| cache fly.net | 594.46 KB | 0.45 % |
| perfora.net | 577.28 KB | 0.44 % |
| wikimedia.org | 447.13 KB | 0.34 % |

If you are viewing the Flow Interface Details report with a filter applied, clicking a link in a dashboard report refreshes the report with the selected data applied as an additional filter (the previously applied filters remain).

Using zoom controls on line graphs

Dashboard reports that include line graphs, such as the Interface Traffic report, allow you to adjust the window of time for which data is reported using the zoom controls. These controls are located at the top center of the dashboard report.



Zoom controls



Page left

Moves the graph time frame backward by 50% of the total time of the graph. For example, if the graph shows data from 3:00 PM to 4:00 PM, clicking Page left shifts the time frame of the graph to 2:30 PM to 3:30 PM.



Zoom in

Decreases the amount of time displayed in the report by 50%. For example, if the report is displaying data for one hour, clicking the Zoom in button decrease the display time to 30 minutes. The report must display at least 30 minutes. If you attempt to zoom in on a report that shows 30 minutes, the report refreshes but the time frame is not changed.



Zoom out

Increases the amount of time displayed in the report. For example, if the report is displaying data for 30 minutes, clicking the Zoom out button increases the display time to 1 hour.

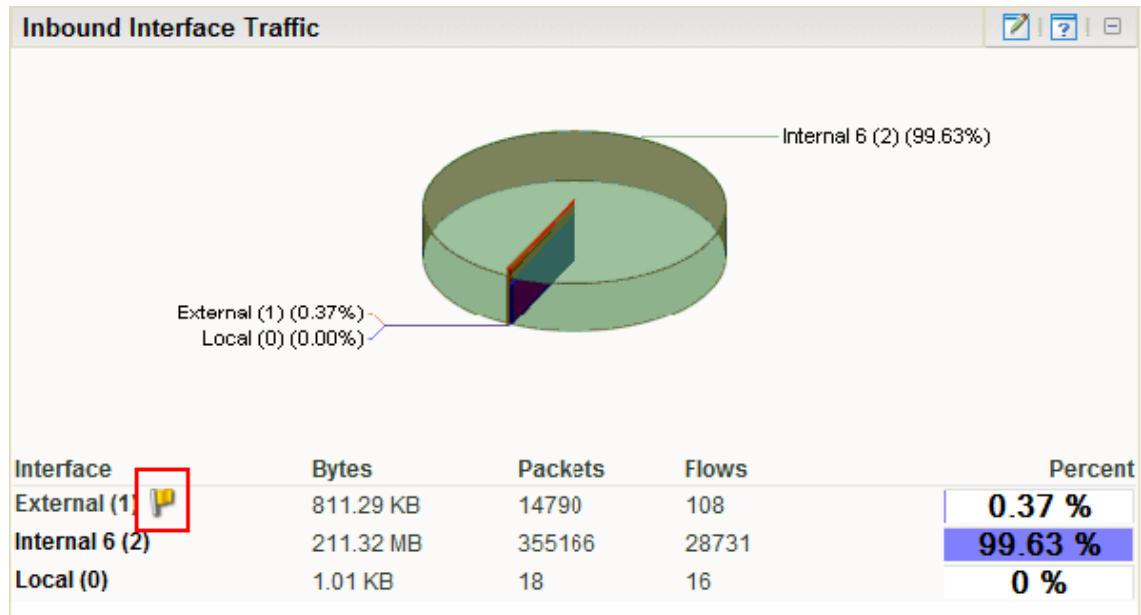


Page right

Moves the graph time frame forward by 50% of the total time of the graph. For example, if the graph shows data from 3:00 PM to 4:00 PM, clicking Page right shifts the time frame of the graph to 3:30 PM to 4:30 PM.

Using informational tooltips

In some reports, when Flow Monitor detects traffic patterns that may indicate a problem that requires intervention, a yellow warning flag icon is displayed.



Position the mouse cursor over the yellow flag icon to view an information tooltip about the specific issue, including links to related reports and specific help topics that may help resolve the issue.

If you do not want to see information tooltips, you can disable them throughout Flow Monitor. It is not possible to disable individual tooltips.


To disable informational tooltips throughout Flow Monitor:

- 1 From any dashboard view or report in the web interface, select **GO**. The GO menu appears.
- 2 If the Flow Monitor section is not visible, click **Flow Monitor**. The Flow section of the GO menu appears.
- 3 Select **Configure > Flow Settings**. The Flow Settings dialog appears.
- 4 Clear **Enable information tooltips**.
- 5 Click **OK** to save changes.

Configuring dashboard reports

The process for configuring dashboard reports varies depending on where in the application the dashboard report is viewed.

To configure a Flow Monitor dashboard report in Flow Monitor:

- 1 In the title bar of the dashboard report pane, click the Configure button . The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - **Maximum number of items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
 - **Display.** Select the display type you want to use in the dashboard report. Choose Chart and data, Data only, or Chart only.
 - **Chart type.** Select the type of chart you would like the report to display. Choose Pie chart, Pie chart (3D), Pie chart (transparent 3D), Bar chart, Bar chart (horizontal), Bar chart (transparent 3D), or Stacked Time graph.
 - **Width.** Specify how wide, in pixels, the graph or chart should appear.
 - **Height.** Specify how tall, in pixels, the graph or chart should appear.
 - **Time graph scale.** Select the transfer speed format for which you want to view data. Choose Auto scale, bps, Kbps, Mbps, or Gbps.
 - **Minimum value.** Enter a minimum value for the graph.
 - **Maximum value.** Enter a maximum value for the graph.
- 3 Click **OK** to save changes.

To configure a Flow Monitor dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, click **Menu > Configure**. The Configure Report dialog appears.
- 2 Enter or select the appropriate information in the following fields.
 - **Report name.** Enter a title for the dashboard report. This name appears in the title bar of the dashboard report's pane.
 - **Date range.** Select the timeframe for the traffic about which you want to see a report. You can select either the last 5, 15, or 30 minutes, or the last hour.
 - **Interface.** Select the router interface that is used by the traffic you want to see in this report.
 - **Interface traffic direction.** Select a direction for which the report will display data for the selected interface (In, Out, or Both).

- **Maximum number of Items to display.** Enter the number of individual items within the category you want to display in the dashboard report. The report will display the top values based on the sort option selected in **Display and Sort by**. All other items in the category are included in the 'Others' category, and will be displayed when **Include 'Others'** is selected.
- **Display.** Select the display type you want to use in the dashboard report. Choose Chart and data, Data only, or Chart only.
- **Chart type.** Select the type of chart you would like the report to display. Choose Pie chart, Pie chart (3D), Pie chart (transparent 3D), Bar chart, Bar chart (horizontal), Bar chart (transparent 3D), or Stacked Time graph.
- **Width.** Specify how wide, in pixels, the graph or chart should appear.
- **Height.** Specify how tall, in pixels, the graph or chart should appear.
- **Filter.** Click this button to apply a filter to the dashboard report. If a filter is applied, only data that meets the filter criteria is displayed in the dashboard report. After clicking, filter fields appear below the button.

Select the type of filter you want to apply. If appropriate, select a secondary filter type from the second filter field. For more information on filters, see *Filtering Flow Monitor dashboard reports in WhatsUp Gold* (on page 1074).



Note: Filters applied here are listed at the top of the dashboard report in **Current filters**.

3 Click **OK** to save changes.

Filtering Flow Monitor workspace reports in WhatsUp Gold

You can apply filters to many Flow Monitor dashboard reports in WhatsUp Gold using the dashboard report configuration dialog.

Filtering is essentially drilling down to find more detailed information in a dashboard report.

Dashboard reports available for filtering in WhatsUp Gold:


- Top Senders
- Top Receivers
- Top Protocols
- Top Types of Service
- Top Applications
- Top Sender Domains
- Top Receiver Domains
- Top Sender Countries
- Top Receiver Countries
- Top Sender Groups
- Top Receiver Groups

- Top Sender TLD
- Top Receiver TLD
- ICMP Types
- Packet Size Distribution

Applied filters are listed in **Current Filter**.

Exporting dashboard report data


Exporting report data

You can export data displayed in dashboard reports by clicking the Export  button on the dashboard report menu.



Note: Flow Monitor data is exported according to the parameters set in the *Flow Data Export Settings* (on page 1075) dialog.

To export report data:

- 1 Click the Export  button. The File Download dialog appears.
- 2 Click **Save**. The Save As dialog appears.
- 3 Enter, or browse to select, the location where you want to save report data. Click **Save**.

Configuring export settings

Use the Flow Export Settings dialog to configure the parameters for exporting report data. Each time you export Flow Monitor data, it will use the parameters set in this dialog. You can export data to a text file, Microsoft Excel, or a .PDF.

To configure the Flow Monitor export settings:

- 1 Select **Flow Monitor > Data Export Settings**. The Flow Export Settings dialog appears.
- 2 Select the desired options.
 - Select **Export to Text** to export Flow Monitor data to text.
 - Select **Export to Excel** to export Flow Monitor data to Microsoft Excel.
 - Select **Export to PDF** to export data to .PDF.
 - Select **Include report title** to include the report name in the exported data.
 - Select **Include column names** to include the column titles in the exported data.
 - Select **Include graphs** to include graph(s) with the exported data (available on select reports).
 - Select the Text options:
 - **Column delimiter**. Select the character type you want to use to separate fields for each set of data when reports are exported. The delimiter options are: Comma, Semicolon, Tab, or Vertical Bar.

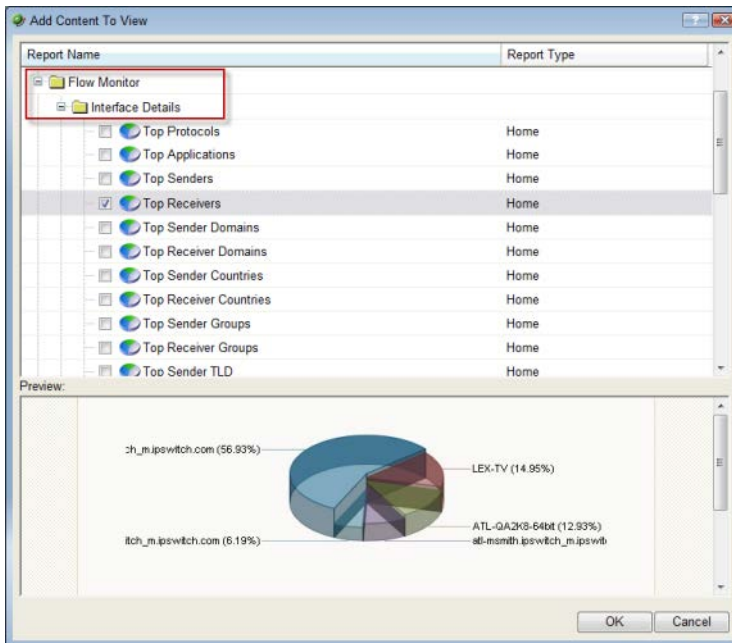
- **Text qualifier.** Select the quote type you want to use to separate field data from column delimiters. The text qualifier options are: Double Quote, Single Quote, or None.
- 3 Click **OK** to save changes.

Linking to Flow Monitor reports from WhatsUp Gold workspace reports

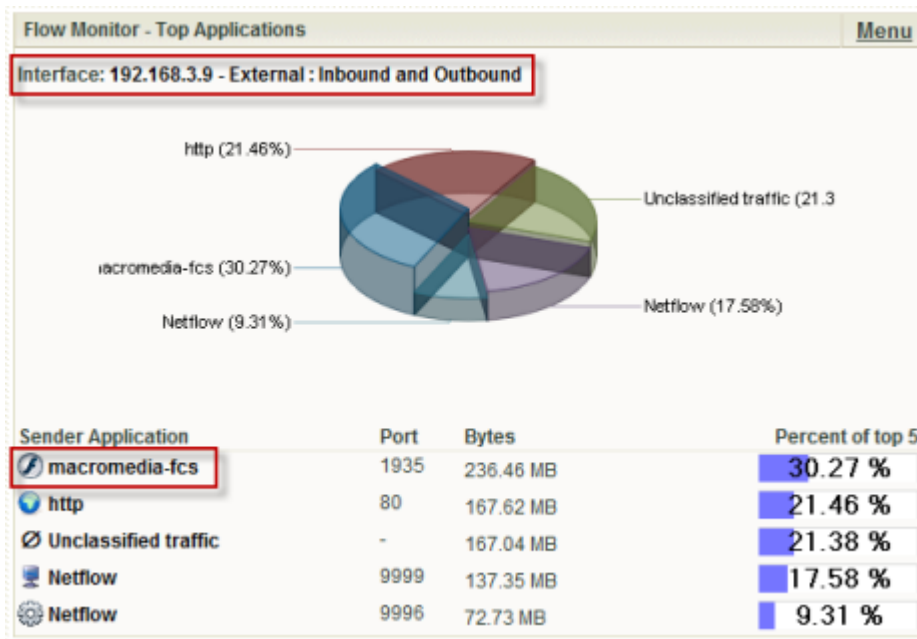
There are several ways to connect to Flow Monitor reports from WhatsUp Gold.

Linking to the Interface Details report from dashboard reports in WhatsUp Gold

The Interface Details dashboard reports in WhatsUp Gold link to the Interface Details report in Flow Monitor. The Interface Details dashboard reports can be found on the WhatsUp Gold dashboard report picker under **Flow Monitor**.



To link to the Interface Details report from an Interface Details dashboard report:



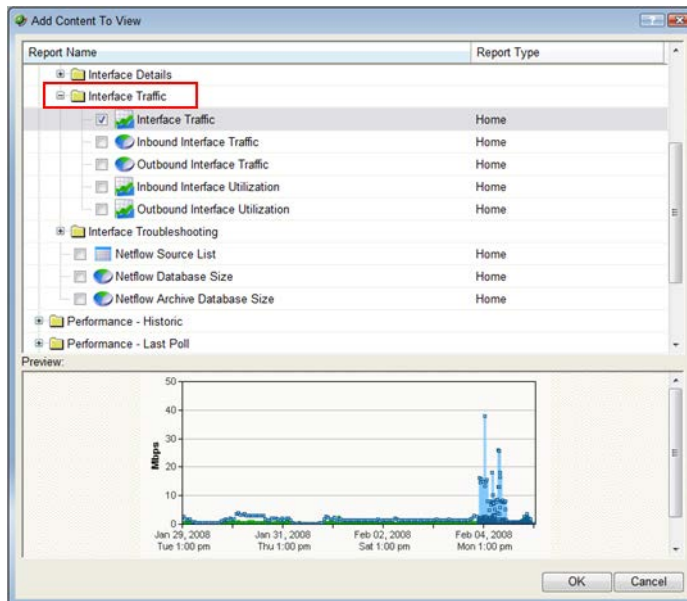
- Click the interface name at the top of the dashboard report. The Interface Details report for the selected interface appears.
- or -
- Click an entry in the far left column of the dashboard report. The Interface Details report for the selected interface appears. The entry that you click is applied to the report as a keyword filter.
- or -
- Click in the dashboard report's graph area. The Interface Details report for the selected interface appears.



Note: Any applied filters carry over to the Interface Details report.

Linking to the Interface Overview report from dashboard reports in WhatsUp Gold

Interface Traffic dashboard reports in WhatsUp Gold link to the Interface Overview report in Flow Monitor. Interface Traffic dashboard reports can be found on the WhatsUp Gold dashboard report picker under **Flow Monitor**.



To link to the Interface Overview report from an Interface Traffic dashboard report, click the interface name at the top the dashboard report. The Interface Overview report for that interface appears.

Using WhatsVirtual

In This Chapter

| | |
|--|------|
| Welcome to Ipswitch WhatsVirtual | 1080 |
| Using WhatsVirtual..... | 1081 |

Welcome to Ipswitch WhatsVirtual

In This Chapter

Welcome to Ipswitch WhatsVirtual 1080

Welcome to Ipswitch WhatsVirtual

As an integrated plug-in for WhatsUp Gold, Ipswitch WhatsVirtual provides the capability to discover, map, monitor, alert and report on both small virtual environments, hosted by a single VMware host, or entire data centers, managed by one or more VMware vCenter servers.

When you use a vCenter server to manage your virtual environment, it becomes the point of communication between WhatsVirtual and the virtual machines within that environment. WhatsVirtual communicates with the vCenter server to discover the virtual environment, poll the virtual machines, collect events associated with actions taken on virtual machines, and issue actions to individual virtual machines.

Using WhatsVirtual

In This Chapter

| | |
|--|------|
| STEP 1: Purchase and enable the WhatsVirtual license | 1081 |
| STEP 2: Create Credentials and Perform Discovery | 1081 |
| STEP 3: Manage and monitor virtual devices | 1087 |
| STEP 4: View the WhatsVirtual maps | 1097 |
| STEP 5: View the WhatsVirtual reports..... | 1099 |

STEP 1: Purchase and enable the WhatsVirtual license

The files for WhatsVirtual plug-in are installed automatically with Ipswitch WhatsUp Gold. Your license file determines whether or not you can access the WhatsVirtual plug-in.

To update your license with a purchased WhatsVirtual plug-in, visit the *MyIpswitch portal* (<http://www.myipswitch.com>).

STEP 2: Create Credentials and Perform Discovery

Perform these tasks to configure WhatsUp Gold and WhatsVirtual to discover your virtual environment:

- Edit the Device Role settings as necessary to meet your operational requirements.
- Set the scan type to **VMware Scan**, and enter the vCenter server or VMware hosts you want to discover.



Note: Ensure that VMware Tools are installed on each virtual machine you want to discover. If VMware tools are not installed on a virtual machine, the device will not be discovered during the VMware Scan.

- Create VMware credentials for each vCenter server or VMware host you want to discover.



Note: If you are managing your virtual environment using a vCenter server and want to collect detailed hardware information about the VMware hosts within that environment, you must add and select the credentials for those VMware hosts as well as for the vCenter server.

- Configure the Discovery Console to use the VMware credentials.
- Set the Scan Advanced Settings so that WhatsUp Gold automatically scans the virtual machines associated with each discovered host.

- Run the VMware discovery scan and view your output.

Editing Device Role settings

The Device Role Settings dialog can be found in the console version of the Discovery Console in the Advanced menu. (**Tools > Discover Devices > Advanced > Device Role Settings**)

This dialog is used to specify the default configuration behavior of WhatsUp Gold discovery. Use this dialog to manage vCenter Server and VMware Host device roles.

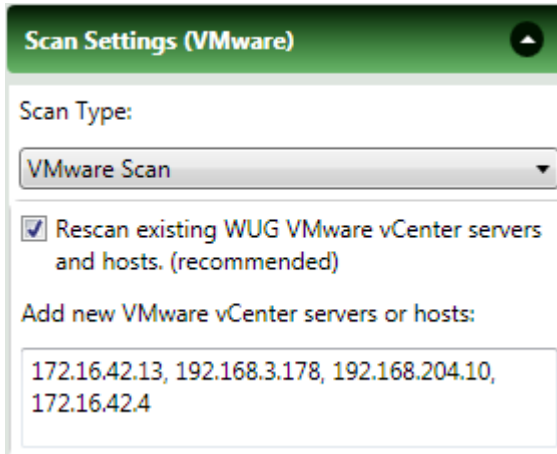


The Device Role Settings menu determines which monitors, context menu items, and custom web links are assigned to the device, as well as defining which device attributes are collected during polling. For more information, see [Configuring device role settings](#).

Setting the scan type

The scan type determines which tools WhatsUp Gold uses to scan and discover devices. The VMware scan type enables the discovery of vCenter servers, hosts and virtual machines.

Use the Scan Settings on the Discovery Console, to set the scan type, add VMware vCenter servers or VMware hosts as targets for the VMware scan, and select the option to rescan vCenter servers that have already been added to WhatsUp Gold using WhatsVirtual.



Scan Settings (VMware)

Scan Type:

VMware Scan

☒ Rescan existing WUG VMware vCenter servers and hosts. (recommended)

Add new VMware vCenter servers or hosts:

172.16.42.13, 192.168.3.178, 192.168.204.10, 172.16.42.4

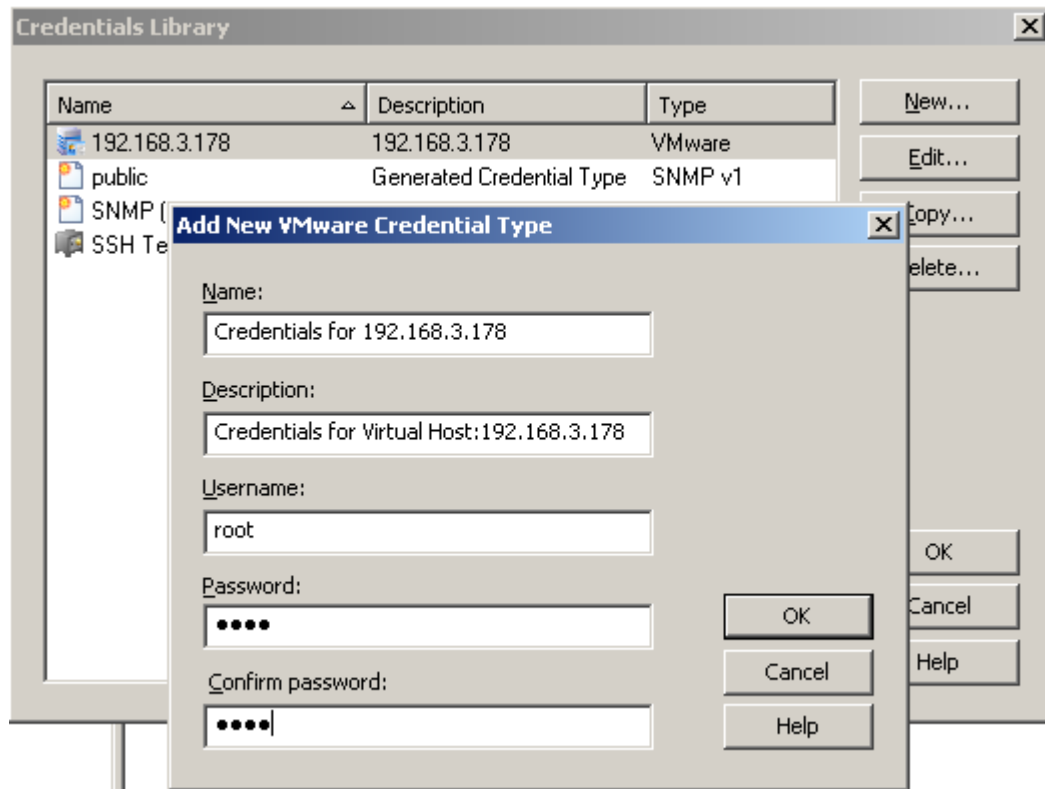


Note: If you are managing your virtual environment using a vCenter server and want to collect detailed hardware information about the VMware hosts within that environment, you must add and select the credentials for those VMware hosts as well as for the vCenter server.

While you can add as many targets to the VMware scan as is needed, you can also discover your virtual environment by selecting the vCenter server that is managing your environment as the target of the scan. This will result in the discovery of all of the virtual machines and hosts managed by the vCenter server. For more information, see Scan settings in the Discovery Settings help.

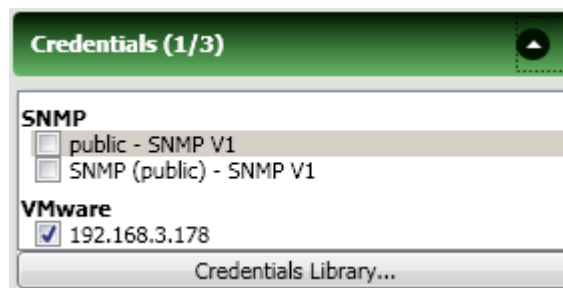
Creating credentials

The credentials in the Credentials Library allow WhatsUp Gold to connect to the vCenter server or VMware host using the VMware vSphere Web Services API. WhatsUp Gold uses this connection to establish the device's role as either a VMware vCenter Server, or VMware host. VMware credentials are also used to connect to the managing server during polling, and while performing actions on the virtual machines. To access the credentials library, click **Credentials Library** in the Credentials section of the Discovery Settings dialog.



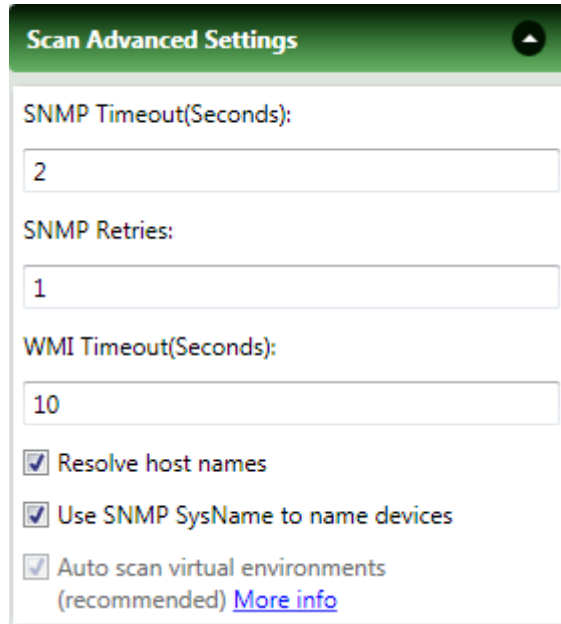
Enabling credentials

After you have created the VMware credentials in the Credentials Library, configure the Discovery Console Settings - Credentials section to use the VMware credentials.



Setting the Scan Advanced Settings

In the Discovery Console Settings - Scan Advanced Settings section, configure the scan to automatically scan the virtual machines associated with each host as it is discovered.



Scan Advanced Settings

SNMP Timeout(Seconds):
2

SNMP Retries:
1

WMI Timeout(Seconds):
10

☒ Resolve host names

☒ Use SNMP SysName to name devices

☒ Auto scan virtual environments
(recommended) [More info](#)



Note: If you do not select the **Auto scan virtual environments** option, virtual machines associated with the host that are outside of the scan range are not discovered, and virtual machines discovered because they are included in the scan range are not automatically associated with the virtual host.

Running the discovery scan

Virtual device discovery occurs during a discovery scan along with the discovery of physical devices. As each device is discovered, WhatsUp Gold attempts to connect using the VMware vSphere API.

If a connection is made using the VMware Credentials through the VMware vSphere API, the device is assigned to either the VMware vCenter server, or VMware Host role, and a query is made through the API to determine which virtual machines are associated with the managing server.

When the virtual machines are identified, WhatsVirtual scans the device and associates it with the vCenter server or VMware host that is managing the device.

Viewing discovery output

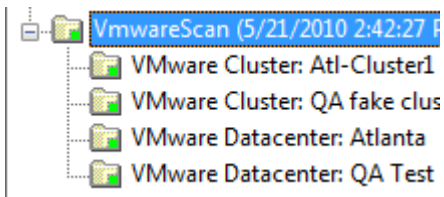
The Device View provides a hierarchical scheme for display and monitoring of the virtual environment. The following logical groupings are automatically created based on information gathered during a VMware scan:

- **VmwareScan.** A logical container that contains all of the Datacenters, virtual hosts, and virtual machines discovered during a VMware scan.
- **Datacenter.** A logical container that contains all of the virtual machines managed by a vCenter server, the virtual hosts providing managed resources, and the managing vCenter server as reported to WhatsVirtual during a VMware scan.

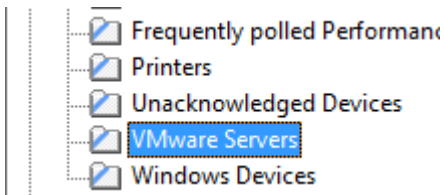


Note: While a vCenter server may manage one or more datacenters, virtual machines cannot be moved using VMotion to a host outside of the datacenter of its original host.

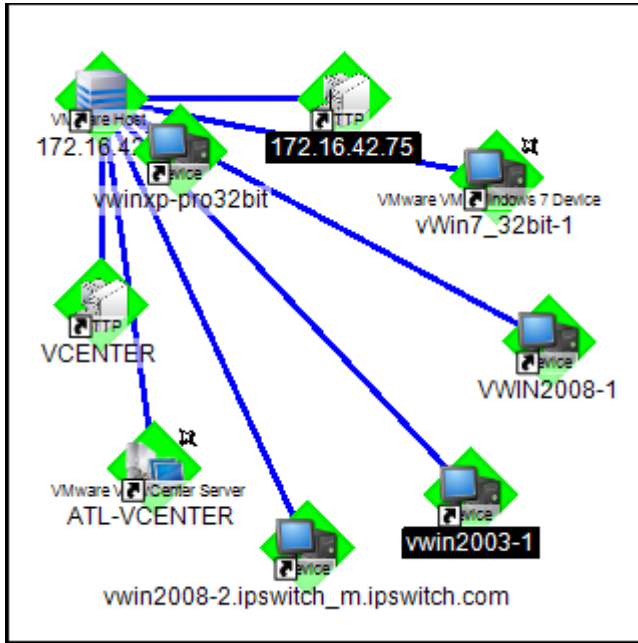
- **Cluster.** A logical container that contains a group of hosts that share resources and enable the VMware Distributed Resource Scheduler (DRS) and VMware High Availability (HA) solutions. A cluster lists the VMware hosts, virtual machines, and the managing vCenter server as reported to WhatsVirtual during a VMware scan.



A VMware Servers dynamic group identifies all VMware servers discovered during the discovery scan.



Discovered vCenter servers, virtual hosts and virtual machines can be viewed on the Map View. Select the Cluster or Datacenter you want to view from the **Device Groups** pane, then select the **Map View**. The selected vCenter, virtual hosts and all of the managed virtual machines appear on the Map View.



STEP 3: Manage and monitor virtual devices

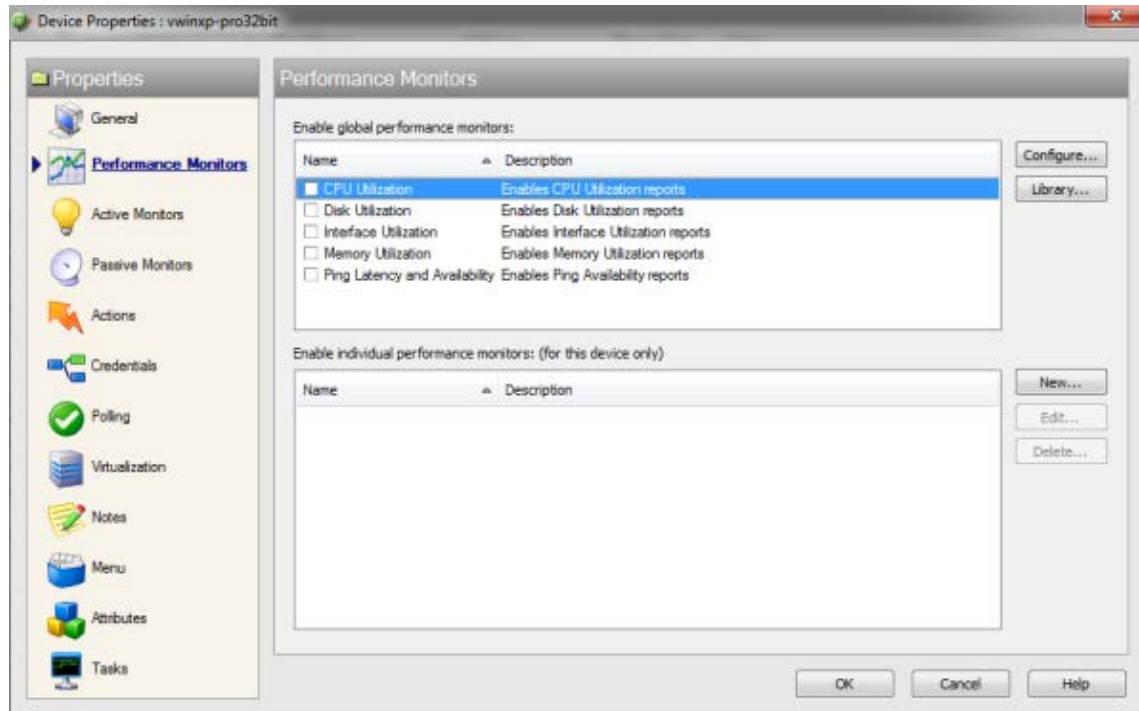
Using WhatsVirtual, WhatsUp Gold manages virtual devices similarly to physical devices; you can add performance monitors, active monitors, and passive monitors; set thresholds in the Alert Center and create alerts associated with these thresholds; create customized actions and create action policies that invoke these actions; and collect and view events created by the vCenter server in response to actions taken in support of vMotion, High Availability (HA) and virtual machine security.

While much of the management and monitoring of virtual devices is the same as physical devices, areas where there are differences include:

- Performance monitor data gathering methods for virtual hosts
- Extended right-click menu options for virtual machines
- vCenter server event collection in support of vMotion, High Availability (HA) and virtual machine security.
- Manual addition and classification of virtual hosts and virtual machines

Performance monitors

You can assign performance monitors to a virtual device using a device role, or manually from the Performance Monitors tab of the Device Properties menu.



vCenter servers and their managed virtual machines may use the VMware vSphere API to gather statistics for the CPU Utilization and Memory Utilization performance monitors. However, if the device supports SNMP and the credentials are available in WhatsUp Gold, these monitors can be configured to collect these statistics using SNMP.

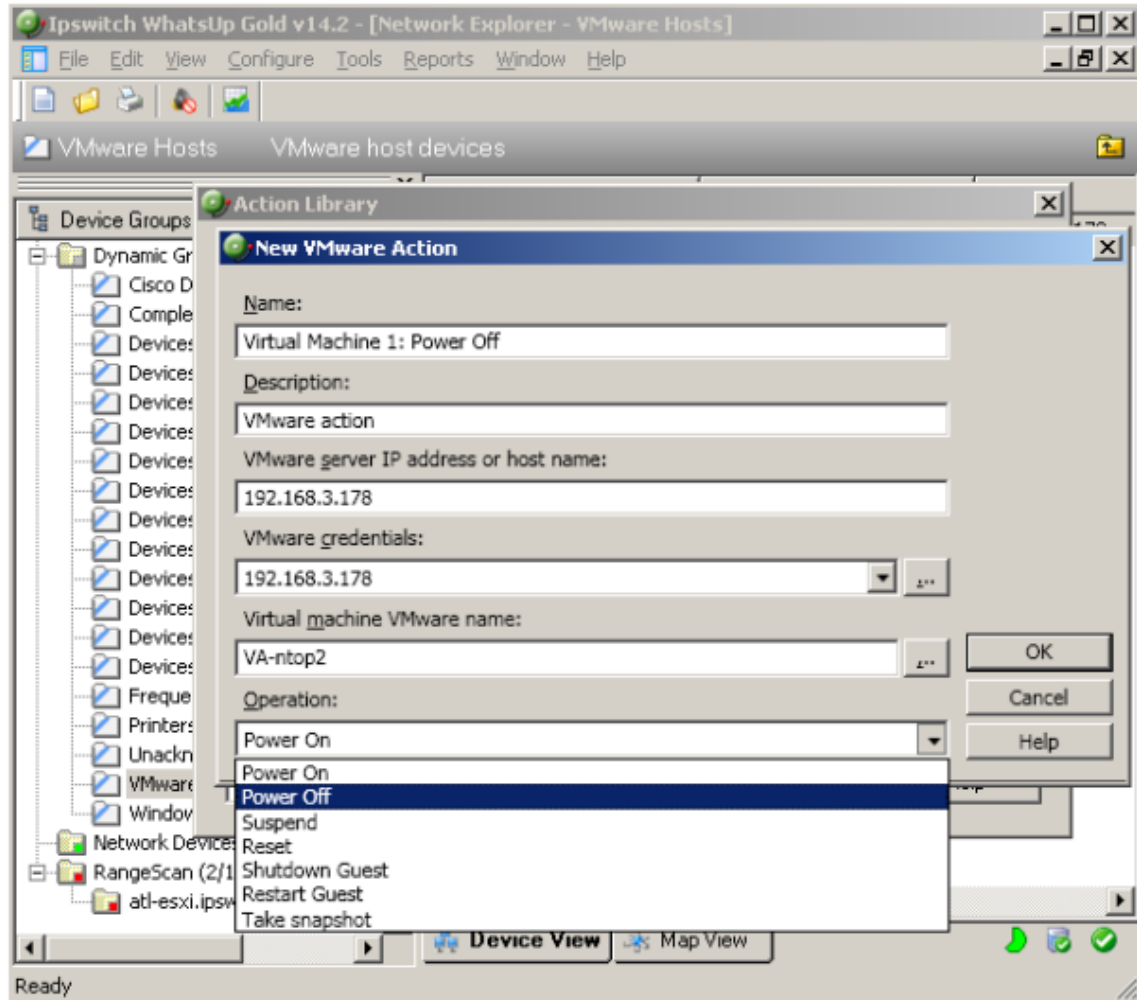


Note: If the VMware vSphere API is used to collect performance data, the real time and split second graphs, for reports generated by the CPU and Memory Utilization performance monitors, will not contain any data.

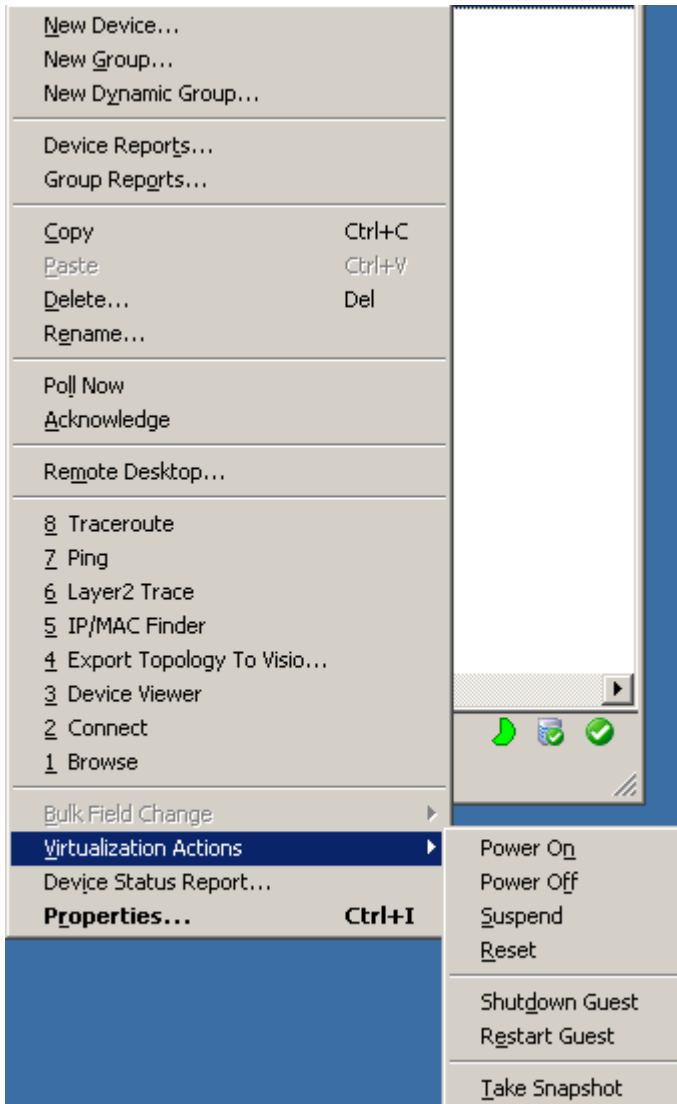
The Disk Utilization and Interface Utilization Performance Monitors for virtual machines use SNMP to gather data for using these monitors, therefore you must enable SNMP on these devices and add the SNMP credentials to WhatsUp Gold prior to enabling these performance monitors. You can add the SNMP credentials from the Credentials tab of the Device Properties dialog. For more information, see *Enabling SNMP on Windows devices* (on page 899) in the help.

Actions on virtual machines

You can create actions to be applied to virtual machines from the New VMware Action dialog (**Configure > Action Library > New > VMware**). You can power on, power off, suspend, reset, shutdown a guest, restart a guest, or take a snapshot of the virtual machine.



You can immediately run an action on a virtual machine from the Device or Map View by right-clicking on the virtual machine, then selecting the action you want to perform from the **Virtualization Actions** menu item.



vCenter server event collection

WhatsVirtual uses the VMware vSphere API to collect events from the vCenter server about your virtual environment. These events are generated by the vCenter server in support of VMware technologies such as VMotion, Distributed Resource Scheduler (DRS), High Availability (HA) and Fault Tolerance.

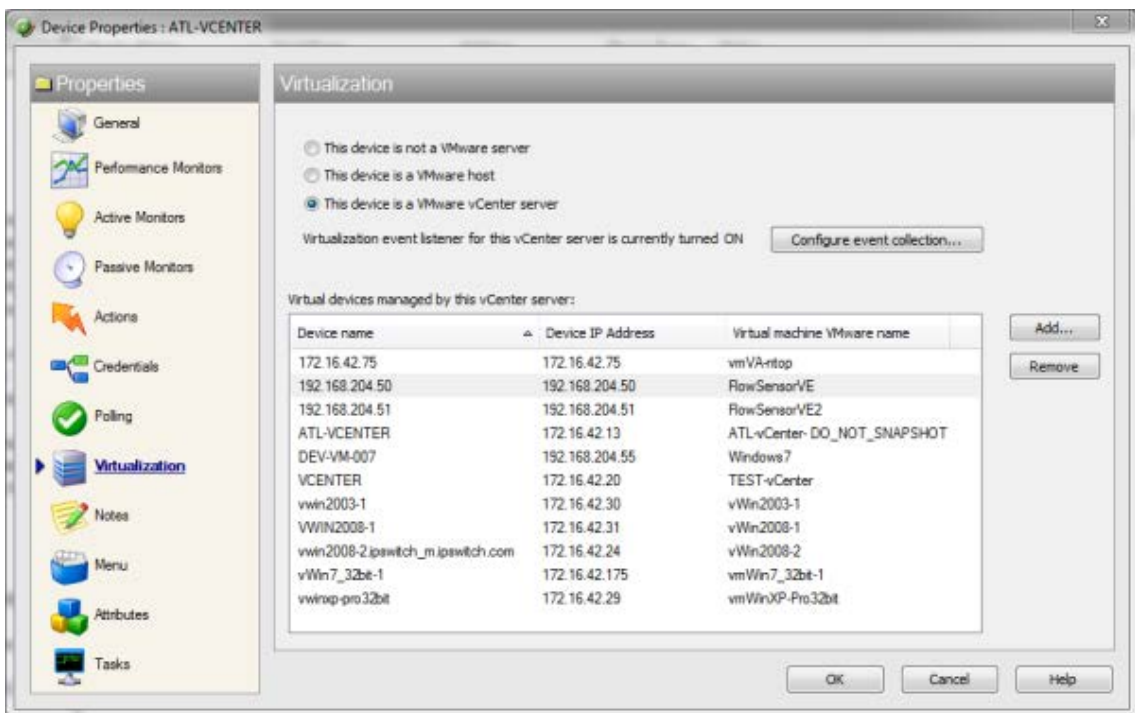
You can configure WhatsVirtual and WhatsUp Gold to collect events of interest from the vCenter. There are several groups of events that can be selected. By using thresholds in the Alert Center or actions defined in the Action Library, these event groups can then be used to trigger actions and alerts, as well as provide information to reports about your virtual environment.

The process for configuring WhatsUp Gold to collect, alert, and perform actions on events includes the following tasks:

- Enable event collection (Global setting to enable event collection)
- Configure event groups and start event collection for individual vCenters.

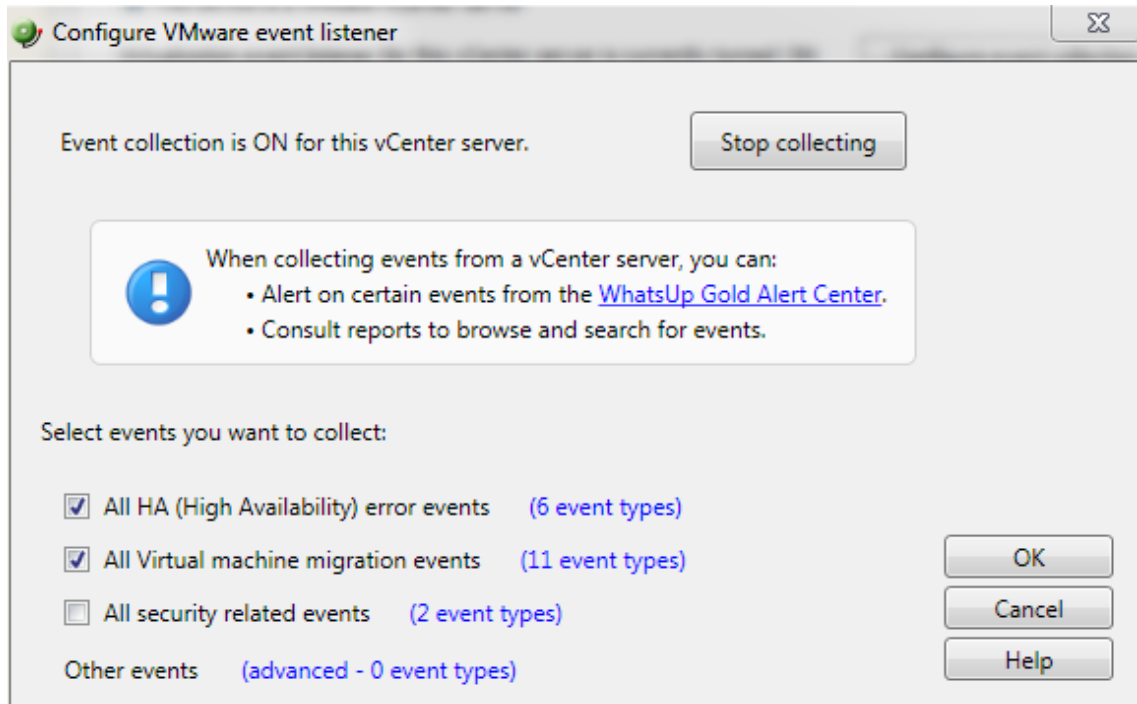
You enable the collection of events from the WhatsUp Gold console (**Configure > Program Options > General**). The **Enable WhatsVirtual event collection** option is selected by default. This is a global option that allows the collection of events from all of the vCenter servers WhatsUp Gold discovers.

After WhatsUp Gold has been enabled to collect events, each vCenter server must be configured to collect the events you wish to collect. The event collection configuration of a vCenter server is accomplished from the Configure VMware event listener dialog. To reach the Configure VMware event listener dialog, click **Configure event collection** on the Device Properties - Virtualization dialog.



Use the Configure VMware event listener dialog to:


- Control the collection of events from the vCenter server.
- Select the predefined event groups that contain the events you want to collect.
- Select a custom list of events from the Other events dialog.



Select the predefined groups of events you want to collect. To see the events included in each group, click the **<#> event types** link beside the group. For more information about the event types, see Configure VMware event listener in the dialog help.

Event collection is ON for this vCenter server.

Stop collecting

 When collecting events from a vCenter server, you can:

- Alert on certain events from the [WhatsUp Gold Alert Center](#).
- Consult reports to browse and search for events.

Select events you want to collect:

☒ All HA (High Availability) error events (6 event types)

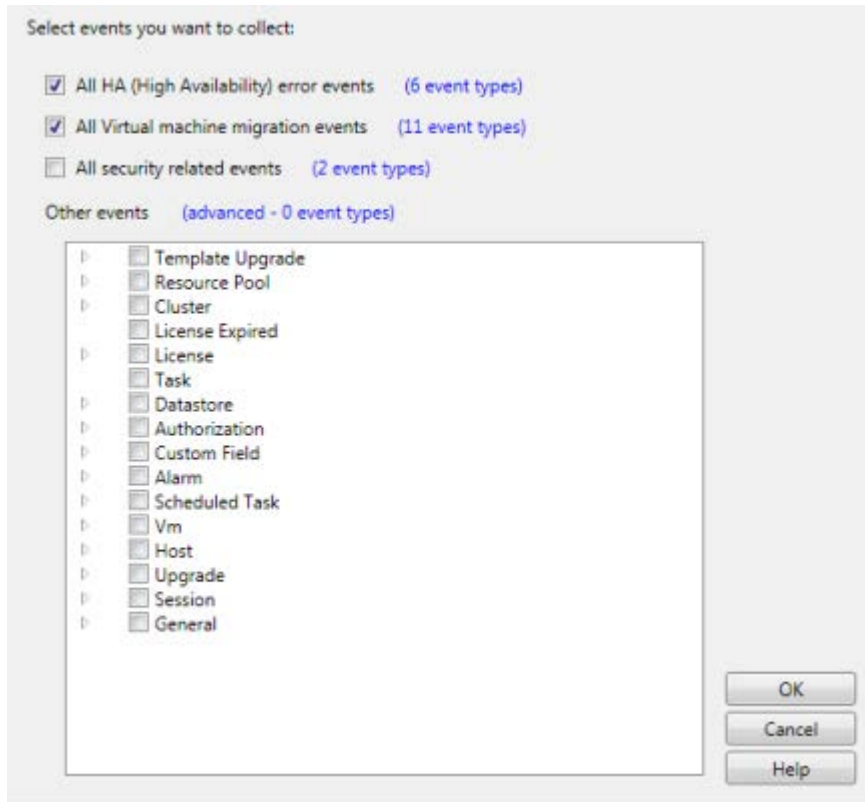
- Das Agent Unavailable
- Das Host Failed
- Insufficient Failover Resources
- Host Das Error
- Not Enough Resources To Start Vm
- Vm Das Update Error

☒ All Virtual machine migration events (11 event types)

☐ All security related events (2 event types)

Other events (advanced - 0 event types)

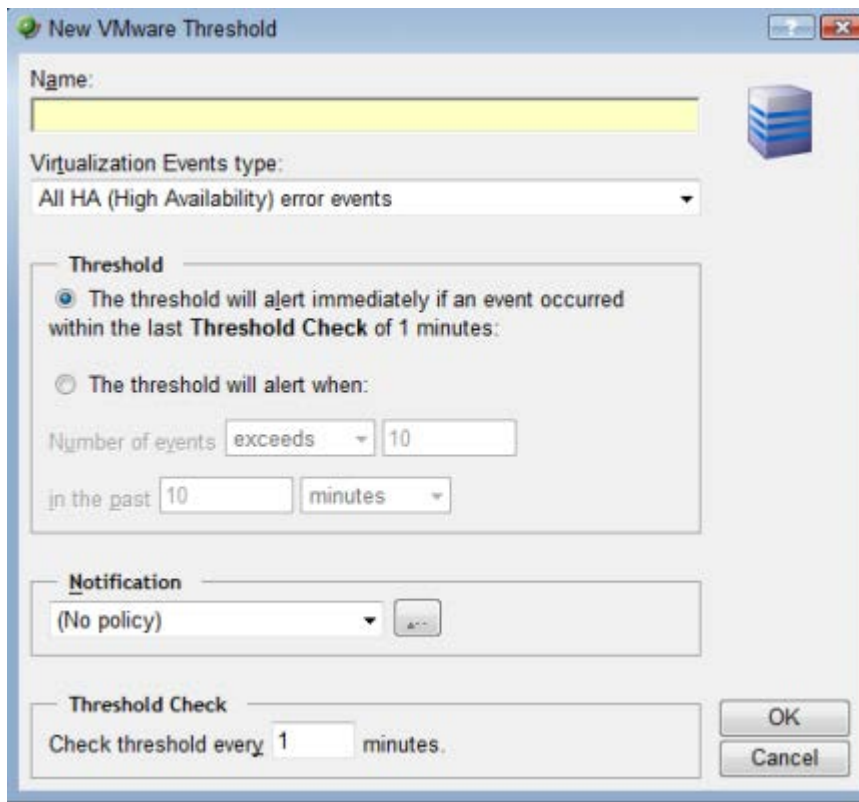
To select from the other events list, click on the **advanced - <#> event types** link. The Other events dialog will open. This window is a hierarchical tree of the available events. Selecting the root of any tree, selects all of the events associated with that event group. To open an event group, click the ▸ icon.



You can select any of the event types from the Virtualization Events type box. The threshold will alert when any event within that event type occurs during the threshold period.

Configuring a VMware threshold from the Alert Center

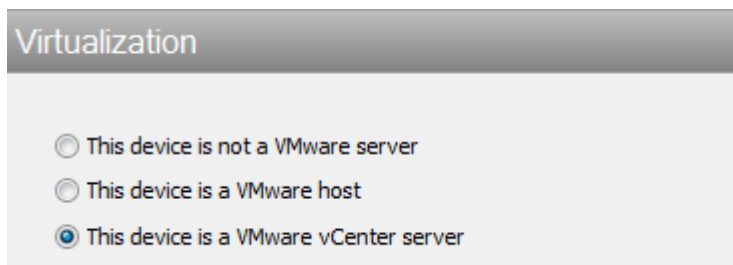
You can create a VMware event threshold in the WhatsUp Gold Alert Center on any event group WhatsVirtual is configured to collect from the managing vCenter server. Use the New VMware Threshold dialog to configure the alert threshold. (**Alert Center Tab > Manage Thresholds > New > VMware Threshold**)



The "New VMware Threshold" dialog box is shown. It has a title bar with a green icon and standard window controls. The "Name:" field is empty. The "Virtualization Events type:" dropdown is set to "All HA (High Availability) error events". The "Threshold" section has two radio buttons: the first is selected and says "The threshold will alert immediately if an event occurred within the last **Threshold Check** of 1 minutes:"; the second is unselected and says "The threshold will alert when:". Below the second radio button are fields for "Number of events" (set to "exceeds" and "10") and "in the past" (set to "10" and "minutes"). The "Notification" section has a dropdown set to "(No policy)" and a button with a plus sign. The "Threshold Check" section has a field "Check threshold every" set to "1" and "minutes". At the bottom right are "OK" and "Cancel" buttons.

Manually assigning a VMware server role to a device

You can manually designate discovered devices as vCenter servers or virtual hosts on the Device Properties - Virtualization dialog.

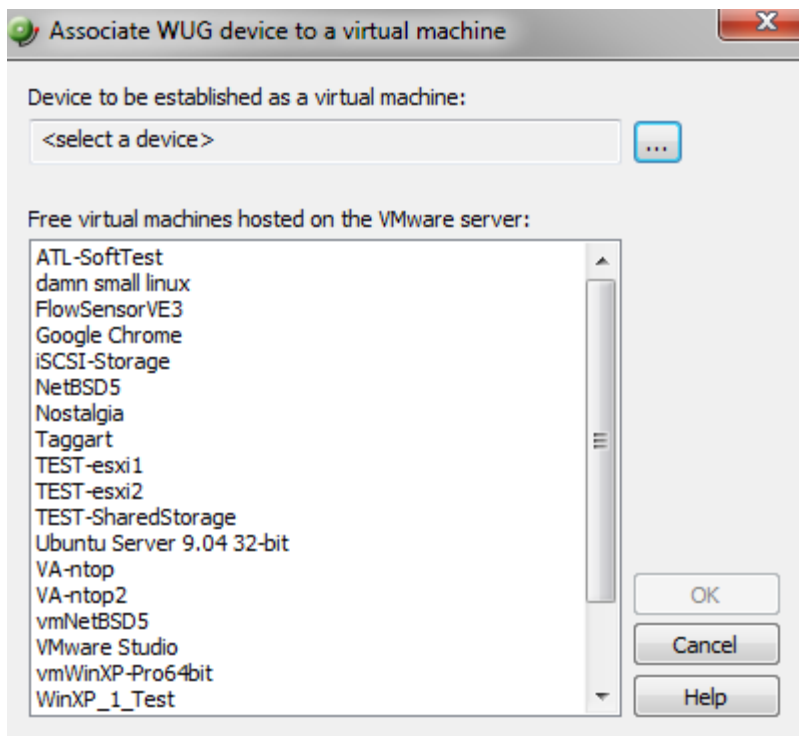


The "Virtualization" dialog box is shown. It has a title bar with a gray background. Below the title bar are three radio buttons: "This device is not a VMware server", "This device is a VMware host", and "This device is a VMware vCenter server". The third radio button is selected.

To manually designate a device as a vCenter server or virtual host, you must select or create VMware credentials for the device, and then select the VMware server role you want to assign to the device.

- Select **This device is a VMware host**, if you want to designate the device as a VMware host.
- Select **This device is a VMware vCenter server**, if you want to designate the device as a vCenter server.

After a device is designated as a vCenter server or VMware host, you can manually associate virtual machines by clicking the **Add** button on the **Virtualization** tab of the Device Properties dialog. WhatsUp Gold polls the vCenter server or VMware host to discover all of the virtual machines it is managing, and displays a list of these machines on the Associate WUG device to a virtual machine dialog.



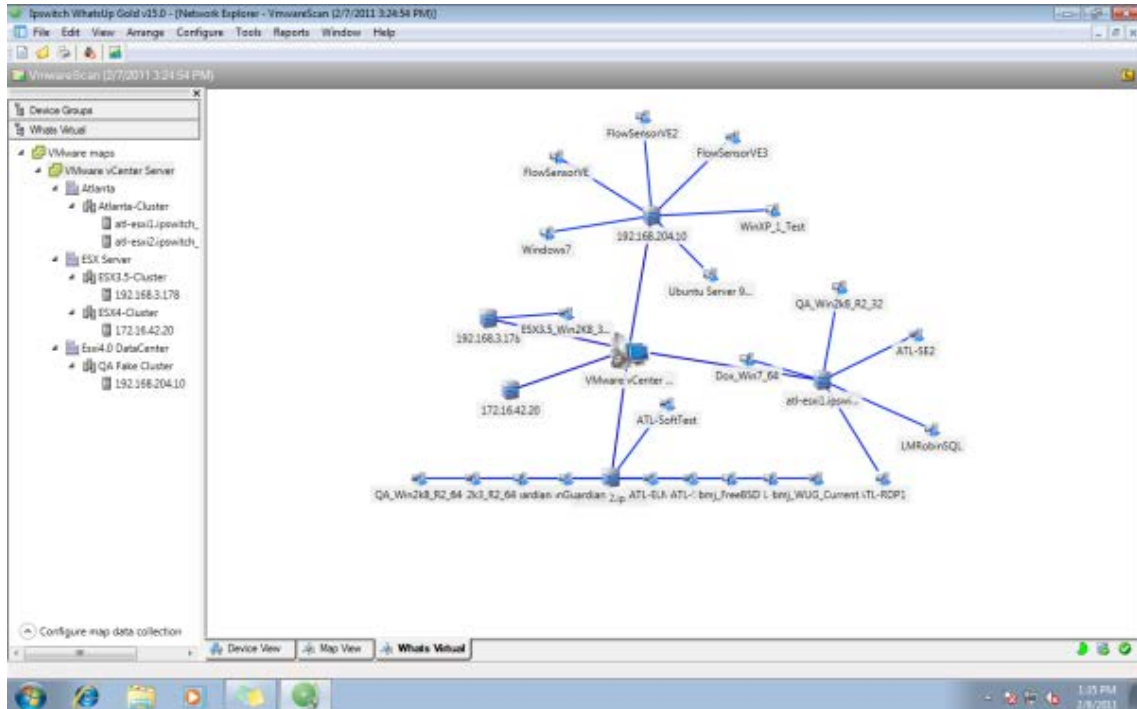
You can also use the Browse (...) button to locate the device you want to add as a virtual machine.



Note: Devices that are manually designated as a vCenter server, VMware host, or virtual device respond to actions created for virtual environments, and appear as virtual devices in dashboard reports, however they do not appear on the **Map View** as virtual devices until they are discovered using a VMware scan.

STEP 4: View the WhatsVirtual maps

When you have completed your VMware discovery scan, you can see a graphical representation of your virtual environment from the WhatsVirtual tab in the WhatsUp Gold views dialog.



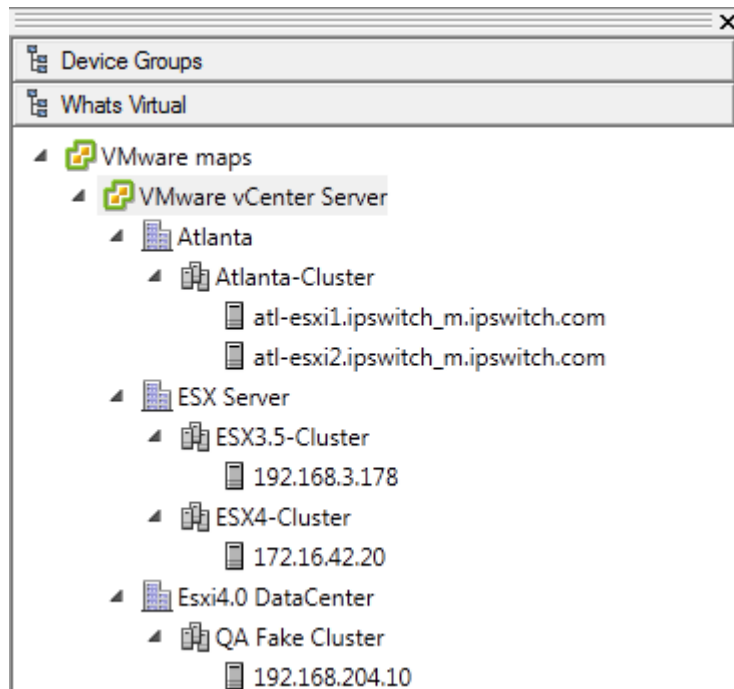
The WhatsVirtual maps are rendered from the information gathered from the vCenter server and show all reported connections between virtual machines, VMware hosts, DataCenters, and the vCenter server. Maps are generated specifically for each Cluster, DataCenter, VMware host, and vCenter server discovered during the VMware scan. Click **View > Refresh** to update the WhatsVirtual maps, so that changes to the virtual environment are reflected in the maps, such as when virtual machines are powered off, migrated or deleted. You can configure the WhatsVirtual maps to only show virtual machines that are powered on, and you can set the interval which WhatsVirtual will collect mapping data.

To open a WhatsVirtual map:

- 1 Click on the **WhatsVirtual** tab in the WhatsUp Gold views dialog.
- 2 In the navigation pane of the WhatsUp Gold views dialog, click **WhatsVirtual**. The WhatsVirtual navigation pane appears.

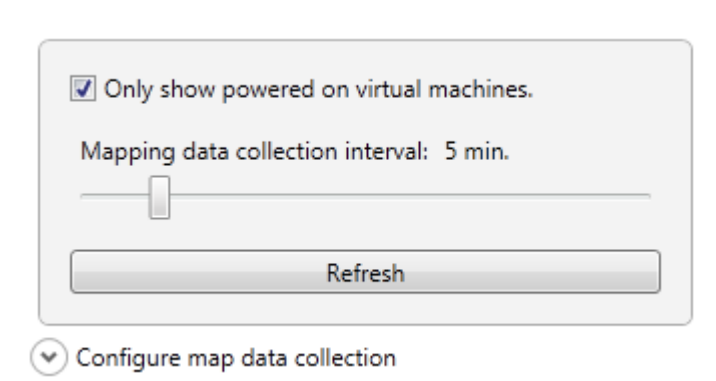


- 3 Expand the VMware maps tree and select the map you want to view.



Configuring WhatsVirtual maps

From the map data collection configuration dialog which is located in the WhatsVirtual navigation pane, you can set the data collection interval (vCenter polling interval for each device), configure the maps to show only those virtual machines that are currently powered on, and manually refresh WhatsVirtual maps.



To set the data collection interval for WhatsVirtual maps:

- 1 In the WhatsVirtual navigation pane, click **Configure map data collection**. The WhatsVirtual map configuration dialog appears.
- 2 Move the slider to the right to increase the collection interval, or move the slider to the left to decrease the collection interval.



Important: The default data collection interval is 5 minutes. Settings lower than the default may create a higher than normal CPU usage (up to an additional 20% of available CPU) on the WhatsUp Gold server and may increase overhead on the vCenter server.

To show only virtual machines that are powered on:

- 1 In the WhatsVirtual navigation pane, click **Configure map data collection**. The WhatsVirtual map configuration dialog appears.
- 2 Select **Only show powered on virtual machines**.

To refresh the WhatsVirtual maps:

Click **Refresh** to refresh the WhatsVirtual maps. The maps will refresh with information gathered during the latest poll of the vCenter server.

STEP 5: View the WhatsVirtual reports

Dashboard reports

The following reports have been added to WhatsUp Gold to provide information about your virtual environment.

- **Virtual Server.** This home and device level dashboard report provides a list of all the virtual machines managed by a virtual server. The virtual server may be a vCenter server or VMware host.
- **Virtual Server List.** This device level dashboard report provides system attributes for the virtual server, hardware information for VMware hosts, and a list of the virtual devices managed by the virtual server. The virtual server may be a vCenter server or a VMware host.



Note: Hardware information will be displayed only if the selected device is a VMware host for which credentials were supplied and selected during a VMware scan.

- **WhatsVirtual Events.** This home level dashboard report displays events that WhatsVirtual is configured to collect from the vCenter server. The events appear in reverse chronological order, so that the last event received appears at the top of the list.
- **Virtual Machine Instant CPU Utilization.** This home and device level dashboard report provides the current CPU utilization for the selected virtual machine.
- **Virtual Machine Instant Disk Utilization.** This home and device level dashboard report provides the current Disk utilization for the selected virtual machine.
- **Virtual Machine Instant Memory Utilization.** This home and device level dashboard report provides the current Memory utilization for the selected virtual machine.
- **Virtual Machine Instant Interface Utilization.** This home and device level dashboard report provides the current Interface utilization for the selected virtual machine.

Configuring VMware dashboard reports

Before you can configure a dashboard report, it must be added to your dashboard view. For information on adding dashboard reports to a dashboard view, see Adding dashboard reports to a dashboard view in the dialog help.

Configure VMware dashboard reports on the Configure Report dialog (**Menu > Configure Report**).

Click the Browse (...) button to select the device you want to use as a data source for the report.

Full reports

WhatsVirtual Events. This report displays events that WhatsVirtual is configured to collect from the vCenter server. The events appear in reverse chronological order, so that the last event received appears at the top of the list.

You can access the WhatsVirtual Events report from the WhatsUp Gold web interface from the Reports Tab. (**System > WhatsVirtual Events**)

Other Plugins

In This Chapter

| | |
|-----------------------------|------|
| Using WhatsConfigured | 1102 |
| Using WhatsConnected..... | 1157 |
| Using ELM Reports | 1165 |

Using WhatsConfigured

In This Chapter

| | |
|--|------|
| Welcome to WhatsConfigured | 1103 |
| Accessing WhatsConfigured Features in WhatsUp Gold | 1104 |
| Using WhatsConfigured reports | 1105 |
| Using Task Scripts..... | 1108 |
| Using Tasks | 1111 |
| Using Policies | 1123 |
| Using Archive Search | 1127 |
| About Device Properties - Tasks..... | 1129 |
| Using Alert Center with WhatsConfigured..... | 1132 |
| Managing the WhatsConfigured and TFTP services | 1134 |
| The WhatsConfigured Custom Script Language..... | 1135 |
| Using WhatsConfigured Comments..... | 1137 |
| Using WhatsConfigured Variables..... | 1138 |
| Using WhatsConfigured Commands..... | 1141 |
| Script Examples | 1153 |
| About the WhatsConfigured Custom Script Language..... | 1154 |
| Task Status | 1154 |
| About the WhatsConfigured Diff Viewer | 1154 |

Welcome to WhatsConfigured

In This Chapter

| | |
|---|-------------------------------------|
| What is WhatsConfigured? | 1103 |
| Finding more information and updates..... | 1103 |
| Sending feedback..... | Error! Bookmark not defined. |

What is WhatsConfigured?

WhatsConfigured enables effective management of one of the most critical assets on your network—device configurations. As a fully integrated plug-in for WhatsUp Gold, WhatsConfigured automates the key configuration and change management tasks required to maintain and control configuration files for networking devices, reducing the risk of network outages caused by misconfigured devices. Network managers can leverage this automated configuration to reduce the amount of time spent ensuring their network devices are configured correctly, freeing valuable time.

WhatsConfigured is built around an automated task execution engine that allows network managers to dynamically gather configuration data about their network devices through configuration tasks. These configuration tasks can be scheduled to run on a regular basis or can be manually ran as needed to upload, download, and backup configuration files, manage device credentials, and much more. WhatsConfigured comes with several pre-defined configuration tasks with the option to create custom tasks. Additionally, WhatsConfigured works with the WhatsUp Gold Alert Center and can alert you on the success or failure of a task, or when changes are detected on a device.

With support for heterogeneous networks, WhatsConfigured provides secure SNMP, SSH, Telnet or TFTP access, to download and store device configuration files in a secure repository, keeping them readily available for file compares and restoration on a device.

WhatsConfigured not only reduces the time and effort required to maintain device configurations and changes while providing increased security, compliance, and visibility, it also reduces the risk of costly network downtime.

Accessing WhatsConfigured Features in WhatsUp Gold

In This Chapter

| | |
|---|------|
| Finding WhatsConfigured on Device Properties | 1104 |
| Finding WhatsConfigured thresholds in Alert Center..... | 1104 |

Finding WhatsConfigured on Device Properties

WhatsConfigured can be found on the Tasks section of the WhatsUp Gold Device Properties dialog.

To access WhatsConfigured through Device Properties:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.

Finding WhatsConfigured thresholds in Alert Center

If you assign an Alert Center threshold to a WhatsConfigured task, a custom threshold dashboard report for the WhatsConfigured task threshold is displayed on the Alert Center tab.

For more information, see Using Alert Center with WhatsConfigured.

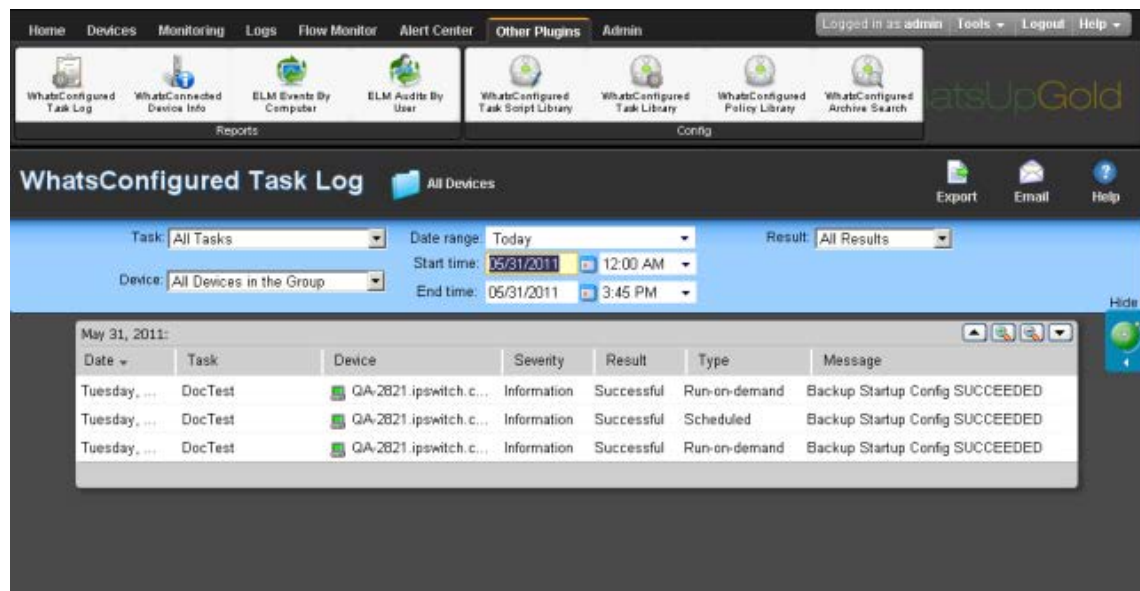
Using WhatsConfigured reports

In This Chapter

About the WhatsConfigured Task Log..... 1105

About the WhatsConfigured Task Log

The WhatsConfigured Task Log displays log messages generated by WhatsConfigured tasks.



Report body

- **Date.** Displays the date the task ran.
- **Task.** Displays the name of the specific task.
- **Device.** Displays the network device for which the task ran.
- **Severity.** Displays the severity of the task.
- **Result.** Displays the outcome of the task.
- **Type.** Displays the task type.
- **Message.** Displays the log message that generated according to the task's result.

Filtering the report

Date range

Use the date/time picker at the top of the report to select a date range and time frame.

In the Date range list, group reports also allow you to specify and customize the business hour report times for reports to display. This allows you to view the network activity only for specified business hours. The date and time format for the date on this report matches the format specified in Program Options > Regional set in the WhatsUp Gold console.



Note: The Business Hours setting is available for group reports only.

Task

Use the Task list to select a specific task for which to view report data. This list is populated with scheduled tasks currently configured in the Scheduled Task Library.

Device

Use the Device list to select a specific network device for which to view report data. You can view data for all devices in the group.



Tip: You can change the device group you are viewing by clicking the group name in the application bar at the top of the page.

Result

Use the Result list to select a specific result for which to view report data. You can choose to view data for all results.

Navigation

You can change the group you are viewing by clicking the group name in the application bar at the top of the page.

You can change to another group report by selecting one from the More Group Reports list.

Printing

You can print a fully formatted report through your browser by clicking the print icon in the browser's toolbar, or selecting **File > Print** from the browser's menu.

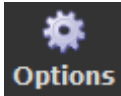
Toolbar buttons

Use the following toolbar buttons to manage report exports, schedule report emails, and get application help.



Click this icon to configure the following device group properties:

- Device Group Name
- Description
- Device Group Access Rights



Click this icon to add the current report to:

- your Favorites list (available in full reports).
Tip: After selected, Favorite reports can be accessed from the **Reports > Favorites** folder of the **WhatsUp** section of the GO Menu.
- export the report to a file (Text, Microsoft Excel, or PDF available in full reports and PDF available in dashboard reports).
- email a report as a PDF attachment.
- schedule reports to be emailed.
Note: JavaScript must be enabled on your browser for this feature to work.



Click this icon to view help for the current report.

Using Task Scripts

In This Chapter

| | |
|--|------|
| About Task Scripts..... | 1108 |
| Using the WhatsConfigured Task Script Library..... | 1108 |
| New/Edit WhatsConfigured Task Script | 1110 |
| Import WhatsConfigured Task Script | 1110 |
| Configuring custom task scripts..... | 1110 |

About Task Scripts

Task scripts login to devices through SSH or Telnet and run command-line interface (CLI) commands on devices. These tasks can perform a number of operations, such as restoring or backing up a running or startup configuration, or changing an application password.

WhatsConfigured comes with several pre-configured task scripts; you can also configure your own custom task scripts using the WhatsConfigured Custom Script Language.

Task scripts are configured from and stored in the Task Script Library and associated to WhatsConfigured tasks in the WhatsConfigured Task dialog.

Using the WhatsConfigured Task Script Library

The WhatsConfigured Task Script Library displays all task scripts currently configured for use in WhatsConfigured tasks.

Two pre-configured task scripts are available for use in WhatsConfigured.

- Backup Running Config
- Backup Startup Config

Backup Running Config

The backup running config task script makes a backup copy of a device's running config and stores it in the WhatsUp Gold database. After you have made a backup copy of a running config, you can restore it on the device at any time for as long as the copy is stored in the database.



Tip: You can set the number of maximum configuration files to store in WhatsUp Gold database on the New WhatsConfigured Task dialog's Schedule tab.

You can view a device's current and archived config files on the Device Properties - Tasks dialog.

Backup Startup Config

The backup running config task script makes a backup copy of a device's startup config and stores it in the WhatsUp Gold database. After you have made a backup copy of a startup config, you can restore it on the device at any time for as long as the copy is stored in the database.



Tip: You can set the number of maximum configuration files to store in WhatsUp Gold database on the New WhatsConfigured Task dialog's Schedule tab.

You can view a device's current and archived config files on the Device Properties - Tasks dialog.

Task Script Library

Use the WhatsConfigured Task Script Library to configure new or existing task scripts:



Note: The **Edit**, **Copy**, **Delete**, and **Export** buttons are disabled for the default, pre-configured task scripts, as you cannot modify or remove default scripts.

- Click **New** to configure a new task script.
- Select a custom task script, then click **Edit** to change its configuration.
- Select a custom task script, then click **Copy** to make a duplicate of the selected task script.
- Select a custom task script, then click **Delete** to remove it from the library.



Caution: When you delete a non-default task script from the WhatsConfigured Task Script Library, it is removed from all tasks that are using that task script.

- On the WhatsUp Gold console, select a task script, then click **Run Now** to run the task script immediately.



Note: The option to run a script on demand via the Task Script Library is not available on the WhatsUp Gold web interface.

- Select a custom task script, then click **Export** to export it as an XML file.
- Click **Import** to import an XML file into the library.



Note: Modifying XML files or attempting to create an XML file from scratch can invalidate a script file.



Note: You can only Export custom task scripts.

New/Edit WhatsConfigured Task Script

Use the dialog to configure a task script. Task scripts are used in WhatsConfigured scheduled tasks.

Enter the appropriate information into the following fields.

- Enter a **Name** for the script.
- Enter a brief **Description** for the script.
- Enter or paste the **Script** for the task that you want WhatsConfigured to complete.

Import WhatsConfigured Task Script

Use this dialog to import a custom task script into the WhatsConfigured Task Script Library.

Browse to the script file that you want to import.

Click **OK** to import that script file.

Configuring custom task scripts

In addition to the pre-configured task scripts included in WhatsConfigured, you can configure custom task scripts that either configure devices or gather device data and store it in the WhatsUp Gold database. These tasks are configured using the WhatsConfigured Custom Script Language, a combination of WhatsConfigured and device commands.

Using Tasks

In This Chapter

| | |
|--|------|
| About Tasks | 1111 |
| About the WhatsConfigured Task Library | 1111 |
| Assigning a task to a device..... | 1119 |
| Viewing Task results | 1119 |

About Tasks

Task scripts are powered by user-configured *tasks*. When you configure a WhatsConfigured task, you select the specific task script that you want the task to execute at the time it is run.

Tasks are configured from and stored in the WhatsConfigured Task Library and are associated with devices in the WhatsConfigured Task dialog. Additionally, if you use WhatsConfigured in WhatsUp Gold, you can view tasks associated with a specific device from the Device Properties - Tasks dialog in WhatsUp Gold.

About the WhatsConfigured Task Library

The WhatsConfigured Task Library displays all tasks configured for use in WhatsConfigured.

To access the WhatsConfigured Task Library click **Other Plugins > WhatsConfigured Task Library**.

Use the WhatsConfigured Task Library to configure new or existing tasks.

- Click **New** to configure a new task.
- Select an existing task, then click **Edit** to modify its configuration.
- Select an existing task, then click **Copy** to create a new task based on the selected task.
- Select an existing task, then click **Delete** to remove it from the list.
- Select a task, then click **Run Now** to perform the task immediately. The task will be run for all devices to which it is assigned. Additionally, to run a task only for a single device, use the **Run Now** option on the WhatsUp Gold Device Properties - Tasks dialog for a specific device.

Select Task Type

Use this dialog to select the type of WhatsConfigured task that you want to create.

You can select either *Schedulable* or *Password*.

Make the appropriate selection, then click **OK**.

New/Edit WhatsConfigured Scheduled Task

Use this dialog to configure a WhatsConfigured Scheduled Task.

Enter or select the appropriate information in the dialog fields.

- Enter a Name for the scheduled task. This name is listed in the WhatsConfigured Scheduled Task Library.
- Enter a brief Description for the scheduled task. This description is listed in the WhatsConfigured Scheduled Task Library to help you differentiate it from other scheduled tasks.
- Select the Task script that you want performed on the schedule you specify. Click **Add Script** to create a new task script.



Note: A new file is created each time the task runs regardless of whether the configuration changed since the last time the task was run.



Tip: Select a dialog tab to view information for its specific dialog fields.

Devices Tab

Use the Devices tab to select the device(s) to which you want to apply the task.

To apply the task to a device:

Click **Add**. The Select a Device dialog appears.

To remove a device from the task:

Select a device from the list, then click **Remove**.

Threshold Tab

Use the Threshold tab to configure an Alert Center threshold to notify you on the scheduled task.

- 1 Select **Enable this threshold** to enable and configure the threshold options.
- 2 Enter a **Name** for the threshold. This name is displayed in the WhatsUp Gold Alert Center Threshold Library.
- 3 Select to have the **Threshold** alert when the task **Detects configuration changes on a device**, if the task matches any of the selected conditions:
 - **Detects a successful execution of a task on a device**
 - **Fails to run for a device**
 - **Successfully runs for a device**
 - **Fails this policy**



Note: If you do not see the appropriate policy, or if the list is empty, browse (...) to the Policy Library to configure a new policy.

- 4 Select the **Notification** policy you would like Alert Center to use to notify you when the threshold is met. If the list is empty or you want to configure a new notification policy, browse (...) to the Alert Center Notification Policy Library.

Schedule Tab

Use the Schedule tab to configure the schedule on which you would like the task performed. You can configure the task to run daily, weekly, monthly, yearly, or on a custom schedule. You can also specify if this task can be run on demand, outside of the schedule you configure.

Select **Enable this schedule** to begin configuring the task's schedule.

Run this task

Select the type of schedule you are configuring, then configure its schedule. For more information on configuring a scheduled task, see *Configuring scheduled tasks* (on page 1113).



Tip: Select the type of schedule you are configuring to view information for its specific dialog fields.

At the bottom of the dialog, select either:

- **Keep up to ___ configuration backups**

- or -

- **Do not limit the number of configuration backups**

If you select the first option, specify the appropriate number of backup configuration files that WhatsConfigured should store for each device the to which task is assigned. The default number of backup configuration files saved per device is 5.

Configuring scheduled tasks

Schedulable tasks are configured to run on the regularly scheduled basis that you choose. You can configure a task to run on a daily, weekly, monthly, yearly, or custom schedule.

To configure a daily task schedule:

- 1 Open the Task Library from the WhatsUp Gold console at **Configure > WhatsConfigured Task Library**. The Task Library appears.
- 2 Click **New**. The WhatsConfigured Task dialog appears.
- 3 Select the **Schedule** tab.
- 4 Select **Enable this schedule**.
- 5 Under the **Interval** list, select **Daily**.
- 6 Specify the **Start Time**.

- 7 Specify how often the task should be performed. For example, if you want the task to run every other day, specify that the task should repeat every 2 days. You can select to have the task **run every ____ day**, or **every weekday** at the specified time.

To configure a weekly task schedule:

- 1 Open the Task Library from the WhatsUp Gold console at **Configure > WhatsConfigured Task Library**. The Task Library appears.
- 2 Click **New**. The WhatsConfigured Task dialog appears.
- 3 Select the **Schedule** tab.
- 4 Select **Enable this schedule**.
- 5 Under the **Interval** list, select **Weekly**.
- 6 Specify the **Start Time**.
- 7 Specify how often the task should be performed. For example, if you want the task to run every other week during the work week, specify that the task run every 2 weeks and select Monday through Friday.

To configure a monthly task schedule:

- 1 Open the Task Library from the WhatsUp Gold console at **Configure > WhatsConfigured Task Library**. The Task Library appears.
- 2 Click **New**. The WhatsConfigured Task dialog appears.
- 3 Select the **Schedule** tab.
- 4 Select **Enable this schedule**.
- 5 Under the **Interval** list, select **Monthly**.
- 6 Specify the **Start Time**.
- 7 Specify the day of the month the task should run. You can select a numerical date, such as the 15th, or a generic date, such as the third Wednesday.
- 8 Specify how often the task should be performed. For example, if you want the task to run every other month, specify that the task repeat every 2 months.

To configure a yearly task schedule:

- 1 Open the Task Library from the WhatsUp Gold console at **Configure > WhatsConfigured Task Library**. The Task Library appears.
- 2 Click **New**. The WhatsConfigured Task dialog appears.
- 3 Select the **Schedule** tab.
- 4 Select **Enable this schedule**.
- 5 Under the **Interval** list, select **Yearly**.
- 6 Specify the **Start Time**.
- 7 Specify the day and month the task should run. You can select a month with a numerical date, such as the June 1st, or a generic date with a month, such as the first Friday of June.

To configure a custom task schedule:

- 1 Open the Task Library from the WhatsUp Gold console at **Configure > WhatsConfigured Task Library**. The Task Library appears.
- 2 Click **New**. The WhatsConfigured Task dialog appears.

- 3 Select the **Schedule** tab.
- 4 Select **Enable this schedule**.
- 5 Under the **Interval** list, select **Custom**.
- 6 Specify the **Start Time**.
- 7 Specify how often the task should be performed. You can select minutes, hours, or days. For example, you can specify that the task run at 2:00:00 AM every 2 days.

New/Edit Password Task

Use this dialog to configure a WhatsConfigured Password Task. You can add, remove, or change a credential through the Password Task.

Enter or select the appropriate information in the dialog fields.

- Enter a **Name** for the task. This name is listed in the WhatsConfigured Task Library.
- Enter a brief **Description** for the task. This description is listed in the WhatsConfigured Task Library to help you differentiate it from other tasks.



Note: The following fields appear on the Details tab on the WhatsUp Gold web interface.

Under **What you would like to do using the Password Task**, select either *Add Credential*, *Remove Credential*, or *Change Credential*.

Select the Credential Type that you want to add, remove, or change. Select either *SNMP*, *SSH*, or *Telnet*.

If you are adding a credential:

- Select the specific **Credential to add**.
- Choose whether to **Associate this credential with devices in WUG**. Selecting this option will add the set of credentials to the selected device in WhatsUp Gold.
- Choose whether to **Add this credential with read only privileges**. Selecting this option adds read only privileges (limited access for running commands and the inability to change device configurations).



Note: If you are using HP ProCurve series devices, you must select to Add Credential or Change Credential first, then select the Add this credential with read only privileges box to remove the Operator credential password or you must clear the Add this credential with read only privileges box to remove the Manager credential password. The SNMP credential type only allows Manager credentials and the SSH and Telnet credential types allow both Manager and Operator credential types.

If you are removing a credential:

Select the specific **Credential to remove**. This list is populated from the credentials currently configured for the selected device.



Note: If you are using HP ProCurve series devices, you must select to Add Credential or Change Credential first, then select the Add this credential with read only privileges box to remove the Operator credential password or you must clear the Add this credential with read only privileges box to remove the Manager credential password. The SNMP credential type only allows Manager credentials and the SSH and Telnet credential types allow both Manager and Operator credential types.

If you are changing a credential:

Select the specific **Credential to change**. This list is populated from the credentials currently configured for the selected device.

- 1 Select the **Credential type** you want to change.
- 2 Select the **Credential to add**, then select the **Credential to remove**.



Note: If you are using HP ProCurve series devices, you must select to Add Credential or Change Credential first, then select the Add this credential with read only privileges box to remove the Operator credential password or you must clear the Add this credential with read only privileges box to remove the Manager credential password. The SNMP credential type only allows Manager credentials and the SSH and Telnet credential types allow both Manager and Operator credential types.



Note: The following fields appear on the Devices tab on the WhatsUp Gold web interface. Select the **Devices** tab to choose the device(s) for the Password Task.

Devices to update

To select a device for the task to update:

Click **Add**. The Select a Device dialog appears.

To remove a device from the list of devices the task is to update:

Select a device from the list, then click **Remove**.

Configuring password tasks

Password tasks allow you to add, change, or remove device SNMP, SSH, or Telnet credentials as needed.



Note: Password tasks only modify credentials by device. Changes made using a WhatsConfigured password task do not effect the WhatsUp Gold Credential Library.

Adding credentials to a device

To add SNMP, SSH, or Telnet credentials to a device:

- 1 Select **Other Plugins > WhatsConfigured Task Library**. The WhatsConfigured Task Library appears.
- 2 Do one of the following:
 - Click **New** to configure a new task. The Select Task type dialog appears.
 - Select **Password Task**, then click **OK**. The New WhatsConfigured Task dialog appears.
 - - or -
 - Select an existing task, then click **Edit**. The Edit WhatsConfigured Task dialog appears.
- 3 Enter or select the appropriate information in the dialog fields.
 - Enter a Name for the task. This name is listed in the WhatsConfigured Task Library.
 - Enter a brief Description for the task. This description is listed in the WhatsConfigured Task Library to help you differentiate it from other tasks.
- 4 Under **What you would like to do** using the Password Task, select *Add Credential*.
- 5 Select the **Credential Type** that you want to add, either *SNMP*, *SSH*, or *Telnet*.
- 6 Select the specific **Credential to add**.



Tip: On the WhatsUp Gold console, you can browse (...) to the Credentials Library.

- 7 Choose whether to **Associate this credential with devices in WUG**. Selecting this option will add the set of credentials to the selected device in WhatsUp Gold.
- 8 Choose whether to **Add this credential with read only privileges**. Selecting this option will disable the ability for other users to edit the credential.



Note: If you are using HP ProCurve series devices, you must select to Add Credential or Change Credential first, then select the Add this credential with read only privileges box to remove the Operator credential password or you must clear the Add this credential with read only privileges box to remove the Manager credential password. The SNMP credential type only allows Manager credentials and the SSH and Telnet credential types allow both Manager and Operator credential types.

- 9 Under **Devices to update**, click **Add** to select the device or device group to which you want to add the credentials.
- 10 Click **OK** to save changes.

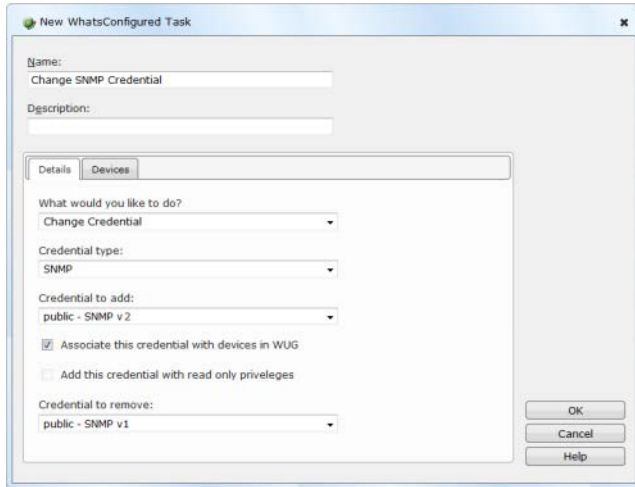
Changing a device's credentials

To change a device's SNMP, SSH, or Telnet credentials:

- 1 Select **Other Plugins > WhatsConfigured Task Library**. The WhatsConfigured Task Library appears.

- 2 Do one of the following:
 - Click **New** to configure a new task. The Select Task type dialog appears.
 - Select **Password Task**, then click OK. The New WhatsConfigured Task dialog appears.

- or -
- 3 Select an existing task, then click **Edit**. The Edit WhatsConfigured Task dialog appears.
- 4 Enter or select the appropriate information in the dialog fields.
 - Enter a Name for the task. This name is listed in the WhatsConfigured Task Library.
 - Enter a brief Description for the task. This description is listed in the WhatsConfigured Task Library to help you differentiate it from other tasks.
- 5 Under **What you would like to do** using the Password Task, select *Change Credential*.



- 6 Select the **Credential Type** that you want to modify, either *SNMP*, *SSH*, or *Telnet*.
- 7 Select the specific **Credential to add**.
- 8 Additionally,
 - Choose whether to **Associate this credential with devices in WUG**. Selecting this option will add the set of credentials to the selected device in WhatsUp Gold.
 - Choose whether to **Add this credential with read only privileges**.



Note: If you are using HP ProCurve series devices, you must select to Add Credential or Change Credential first, then select the Add this credential with read only privileges box to remove the Operator credential password or you must clear the Add this credential with read only privileges box to remove the Manager credential password. The SNMP credential type only allows Manager credentials and the SSH and Telnet credential types allow both Manager and Operator credential types.

- 9 Select the specific **Credential to remove**.
- 10 Under **Devices to update**, click **Add** to select the device or device group to which you want to modify credentials.
- 11 Click **OK** to save changes.

Removing credentials from a device

To remove a device's SNMP, SSH, or Telnet credentials:

- 1 Select **Other Plugins > WhatsConfigured Task Library**. The WhatsConfigured Task Library appears.
- 2 Do one of the following:
 - Click **New** to configure a new task. The Select Task type dialog appears.
 - Select **Password Task**, then click **OK**. The New WhatsConfigured Task dialog appears.

- or -
- 3 Select an existing task, then click **Edit**. The Edit WhatsConfigured Task dialog appears.
- 4 Enter or select the appropriate information in the dialog fields.
 - Enter a Name for the task. This name is listed in the WhatsConfigured Task Library.
 - Enter a brief Description for the task. This description is listed in the WhatsConfigured Task Library to help you differentiate it from other tasks.
- 5 Under **What you would like to do** using the Password Task, select *Remove Credential*.
- 6 Select the **Credential Type** that you want to remove, either *SNMP*, *SSH*, or *Telnet*.
- 7 Select the specific **Credential to remove**. This list is populated with credentials currently assigned to the device.
- 8 Under **Devices to update**, click **Add** to select the device or device group from which you want to remove credentials.
- 9 Click **OK** to save changes.

Assigning a task to a device

Tasks are assigned to individual devices from either the Device Properties - Tasks dialog or when configuring the task in the Task Library.

To assign a WhatsConfigured task to a device from Device Properties:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **WhatsConfigured tasks attached to this device**, click **Add**. The Add Task to Device dialog appears.
- 4 Select the task that you want to assign to the device, then click **OK**. If the list is empty, or you do not see the task you want to assign, browse (...) to the WhatsConfigured Task Library to configure a new task.

For information on assigning a device during task configuration, see Configuring Tasks.

Viewing Task results

The Task Results dialog displays results for tasks that have been run using the Scheduled Task Library's **Run Now** option.

To view Task Results for a task:

- 1 Select **Other Plugins > WhatsConfigured Task Library**. The WhatsConfigured Task Library appears.
- 2 Select a task, then click **Run Now**. A dialog displaying the task's progress appears.
- 3 When the task completes, click **View Results**. The Task Results dialog appears.

The dialog displays the following result for a task that was ran using the **Run Now** option:

- **Task status.** The result of the entire task. A task is considered to be successful only if the task completes successfully for all devices for which it runs. In the event that the task fails, the task message displays information regarding the failure.
- **Task Message.** A message that explains why the task failed. If the task runs successfully for all devices, this field is empty.
- **Task Devices.** The devices for which the task was run.



Tip: Select a device to view its result information in the following section of the dialog.

Below, the dialog displays device-specific results in six tabs.



Tip: Select a dialog tab to view information for its specific dialog fields.

The **Output** tab displays the task's result, relevant messages, and a trace of all communication between the device and the WhatsConfigured service.

For each task it displays:

- **Result.** The result of the task for the selected device.
- **Message.** Any message pertaining to the task for the selected device. In some instances, this field may be empty.
- **Trace.** A history of all communication that takes place between the device and the WhatsConfigured service during the task's attempted completion. If the task collects a configuration file as part of the task, it is included in the trace. If the task was successful for this device, the trace displays what the command prompt would have looked like if the user consoled into the device and run the commands manually using a command prompt.
- If the task failed and no communication took place between the device and the WhatsConfigured service due to communication or configuration errors, the box displays "No communication with the device was recorded." Finding the cause of this failure may be accomplished by reviewing the credentials listed on the Settings tab, reviewing device configurations, attempting to communicate with the device manually, or by checking the log.

The **Script** tab displays the task script assigned to this task as it is saved in the Task Script Library, and how the task looks after it is processed through the WhatsConfigured task runner.

For each task it displays:

- **Script Text.** The script assigned to be run by the task. If this script is a custom script, it appears exactly as it did when it was configured in the New/Edit WhatsConfigured Task Script dialog. If this is a predefined password or backup task, the script displayed is the script chosen for this device based on the WhatsConfigured script registry.



Note: Scripts for predefined WhatsConfigured tasks are looked up based on the OID associated with the device. If there is no OID assigned to the device, the lookup fails and no script is listed. OID's can be assigned to a device from the Device Properties - Tasks dialog, or collected by discovering the device. Due to the large number of devices and their varying commands this script to device mapping may fail.

- **Processed Text.** The WhatsConfigured scripting language allows for variable replacement within scripts. WhatsConfigured pre-defined scripts utilize this ability when running password tasks. Before the script is run the script is processed and all variable references are replaced with the variables corresponding value. The processed text displays the resulting script after processing. This field allows the user to ensure variable declarations are being assigned and interpreted properly.



Tip: If you are experiencing a problem with a script, Save the results listed in the script tab to a text (.txt) file. If you contact Technical Support, this file will aid in troubleshooting your script problem.

The **Variables** tab displays the name and value of all variables associated with the task script.

For each task it displays:

The **Commands** tab displays a list of the commands as they were interpreted by the WhatsConfigured script runner. It also displays the results of those commands if they were run against the device when the task was run.

For each task it displays:

- **Command.** The specific command; for example, login or show configuration.
- **Result.** The success or failure of the command when it was ran by the task.
- **Output.** The results of the responses declared by the WhatsConfigured script language.

The **Log** tab displays any error messages that were logged as the task ran.

The **Settings** tab displays the protocol credentials used to complete the task.

For each task it displays:

- **Type.** The type of protocol credentials; for example, SSH or Telnet.



Note: WhatsConfigured defaults to SSH credentials when available. If SSH credentials are not assigned to a device, WhatsConfigured will look for/use Telnet credentials.

- **Name.** The name of the credentials as assigned in the Credentials Library.
- **Description.** The description of the credentials as assigned in the Credentials Library.

Using Policies

In This Chapter

| | |
|--|------|
| About Policies | 1123 |
| About the Policy Library | 1123 |
| Configuring a WhatsConfigured Policy | 1123 |
| Auditing a Policy | 1125 |
| Archive Policy Audit | 1126 |

About Policies

WhatsConfigured policies search through archived configuration files for strings that are either expected or not expected within the file(s).

Policies can be added to Alert Center Task Threshold's. When a scheduled task fails a policy, any associated notification policies alert you that the policy has failed due to unexpected content that has been flagged in an archived config file.

About the Policy Library

The WhatsConfigured Policy Library displays all policies currently configured for use with WhatsConfigured archive configuration files.

Use the WhatsConfigured Policy Library to configure new or existing policies.

- Click **New** to configure a new policy.
- Select a policy, then click **Edit** to modify its configuration.
- Select a policy, then click **Copy** to make a duplicate of the selected policy.
- Select a policy, then click **Delete** to remote it from the library.
- Select a policy then click **Audit Now** to audit (test) a policy.

Configuring a WhatsConfigured Policy

Use this dialog to configure a WhatsConfigured Policy.

Enter or select the appropriate information in the following fields.

- Enter a **Name** for the policy. This name is displayed in the WhatsConfigured Policy Library.
- Enter a short **Description** for the policy. This description is displayed next to the policy's name in the WhatsConfigured Policy Library.

Include Patterns

Click **Add** to enter a string for which you expect to see in the archived configuration files.

- Select **RegEx** if you want the string to be interpreted as a Regular Expression.
- Select **Ignore Case** the case of the string is irrelevant to the string.



Tip: Select an include pattern, then click **Remove** to delete it from the list.

Exclude Patterns

Click **Add** to enter a string for which you do not expect to see in the archived configuration files.

- Select **RegEx** if you want the string to be interpreted as a Regular Expression.
- Select **Ignore Case** the case of the string is irrelevant to the string.



Tip: Select an exclude pattern, then click **Remove** to delete it from the list.

To configure a WhatsConfigured Policy:

- 1 On the WhatsUp Gold console, select **Configure > WhatsConfigured Policy Library**. The WhatsConfigured Policy Library appears.

Click **New**. The WhatsConfigured Policy dialog appears.

- or -

Select an existing policy, then click **Edit**. The WhatsConfigured Policy dialog appears.

- 2 Enter a **Name** for the policy. This name is displayed in the WhatsConfigured Policy Library.
- 3 Enter a short **Description** for the policy. This description is displayed next to the policy's name in the WhatsConfigured Policy Library.
- 4 In the following sections of the dialog, you have the opportunity to specify strings that you either expect or do not expect to see within the configuration files the policy audits. You can choose to enter only include patterns, only exclude patterns, or both.



Note: The more restrictive the audit criteria, the less audit results you may obtain as a result.

- 5 Under the **Include Patterns** section of the dialog, click **Add** to enter a string that you expect to see in the archived configuration files. Additionally,
 - Select **RegEx** if you want the string to be interpreted as a Regular Expression.
 - Select **Ignore Case** the case of the string is irrelevant to the string.



Tip: Select an include pattern, then click **Remove** to delete it from the list.

- 6 Under the **Exclude Patterns** section of the dialog, click **Add** to enter a string that you do not expect to see in the archived configuration files. Additionally,
 - Select **RegEx** if you want the string to be interpreted as a Regular Expression.
 - Select **Ignore Case** the case of the string is irrelevant to the string.



Tip: Select an include pattern, then click **Remove** to delete it from the list.

- 7 Click **OK** to save changes.

Auditing a Policy

To audit a WhatsConfigured policy:

- 1 On the WhatsUp Gold console, select Configure > WhatsConfigured Policy Library. The WhatsConfigured Policy Library appears.
Click **New**. The WhatsConfigured Policy dialog appears.
- or -
Select an existing policy, then click **Edit**.
- 2 Select a policy, then click **Audit Now**. The WhatsConfigured Policy Audit dialog appears.
- 3 Under the **Audit Criteria** section of the dialog, click **Add** to select the device(s) against which to audit the policy.



Tip: To delete a device from the list, select it, then click **Remove**.

- 4 Select the **Archive Key** of the configuration files for which the policy will be audited. For example, to view audit results for running config archives, select the *running-config* key from the list. This list is populated with all of the keys from the configuration files archived for the selected device(s). To view all possible archives, select *All*.



Tip: To limit audit results to a device's most recently archived configuration file for a particular key, select **Latest Archive Only**.

- 5 After you have specified the appropriate audit criteria, click **Audit** to verify the policy. Results from the audit are displayed in the Audit Results section of the dialog:
 - The either successful or failed Audit Result.
 - The Device Name of the device by which the policy was audited.
 - Any relevant Message regarding the policy audit. For example, the number of archives that failed against the policy.



Tip: Select an audit result, then click **View** to see the details for that result.

- 6 Click **Close** to exit the dialog.

Archive Policy Audit

This dialog displays the results of a WhatsConfigured policy audit.

Archives

The following information is displayed for each archive found as a result of the policy audit:

- The successful or failed **Audit Result**.
- The specific **Archive** config file and the time it was created.
- Any relevant **Message** regarding the policy audit.

Audit Results

The following information is displayed for any **Include Patterns** or **Exclude Patterns**.





- The audit **Result** of the pattern.
- The specific **Pattern** selected in the policy configuration.
- If the pattern was interpreted as a regular expression (**RegEx**).
- Whether the pattern's case was relevant to the audit results (**Ignore Case**).

Pattern Matches

Any matches found during the audit are displayed in the bottom section of the dialog.



Tip: Use the forward and backward buttons to navigate through the matches.

| Button | Description |
|---|--------------------------|
|  | Moves one match forward |
|  | Moves one match backward |
|  | Moves to the first match |
|  | Moves to the last match |

Using Archive Search

In This Chapter

| | |
|--|------|
| About Archive Search | 1127 |
| Performing an archive search | 1127 |
| View Configuration Archive..... | 1128 |
| Configuration Archive Search Result..... | 1128 |

About Archive Search

The Archive Search feature allows you to search the content of device configuration archives. A configuration archive is any device output captured when running a configuration task/script. When a configuration script is run, the output from one or more commands may be captured and stored in a user or system specified key. The output is saved to the device using the key name and the time-stamp as a look-up key. The archive is persisted with the device in the discovery *.dis* file.

Performing an archive search

To perform an archive search:

- 1 Go to the Archive Search dialog:
From WhatsConnected, click **Tools > Archive Search**. The Archive Search dialog appears.
From the WhatsUp Gold console main menu, select **Configure > WhatsConfigured Archive Search**. The Archive Search dialog appears.
- 2 Click **Add**. The Select Device dialog appears.
- 3 Select the device(s) for which you want to perform an archive search, then click **OK**.
- 4 Specify the Search Criteria:
 - Select an **Archive Key** for which to refine search results. For example, to view running config archives, select the running-config key from the list. This list is populated with all of the keys from the archived configuration files for the selected device(s). To view all possible archives, select **All**.
 - To view only the latest archives for the selected device(s), select **Latest Archive Only**.
 - Enter a **Search Pattern** for which the search should attempt to find in the archived config files. This can be a phrase or regular expression.
 - Select **Regular Expression** for the contents of search pattern to be interpreted as a regular expression.
 - If the contents of the search pattern are case insensitive, select **Ignore Case**.



Tip: Select a device, then click **Remove** to delete it from the list.

- 5 Click **Search**. The dialog displays the following Search Results in the bottom half of the dialog:
 - The **Archive Key** under which the file was saved in the database.
 - The **Device** for which the config file was saved.
 - The time at which the configuration file was created (**Time Created**).
 - The name of the configuration task for which the file was collected (**Created by**).



Tip: Select an archive file, then click **View** to see the specific archived file.

View Configuration Archive

Use this dialog to view an archived configuration for the selected device.

- **Archive** lists the config file name.
- **Time created** lists the date and time on which the config was created.
- **Archive results** displays the archived config file's details.

Click **Close** to return to the Device Properties - Tasks dialog.





Configuration Archive Search Result

This dialog displays the following results from a WhatsConfigured Archive Search.

- The specific **Archive** file and the time on which it was created.
- The **Search Pattern** used by WhatsConfigured to refine search results.
- The relevant archived file contents for each match are displayed under **Search Results**.



Tip: Use the forward and backward buttons to navigate through the matches.

| Button | Description |
|---|--------------------------|
|  | Moves one match forward |
|  | Moves one match backward |
|  | Moves to the first match |
|  | Moves to the last match |

About Device Properties - Tasks

In This Chapter

| | |
|--------------------------------------|------|
| Using Device Properties - Tasks..... | 1129 |
| Add Task to Device..... | 1130 |
| Restore Confirmation | 1130 |

Using Device Properties - Tasks

The Device Properties - Tasks dialog displays task and archived device data. For more information, see *Using WhatsConfigured Device Properties - Tasks* (on page 130)

From this dialog you can add or remove device tasks, run a task immediately, restore a device to a previously archived configuration file, or delete an archived configuration. In addition to these management capabilities, the Device Properties - Tasks dialog allows you to view and compare archived configuration files by accessing the WhatsConfigured Diff Viewer.

To view an archived configuration file for a device:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **Archives saved for this device**, select an archived config file, then click **View**. The View Configuration Archive dialog appears.

To compare two device config files:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **Archives saved for this device**, select two configuration files, then click **Compare**. The WhatsConfigured Diff Viewer appears.

To restore a device to an archived configuration:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **Configuration archives saved for this device**, select a configuration, then click **Restore** to restore the device to the selected configuration.

To delete an archived configuration file from a device:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **Archives saved for this device**, select an archived config file, then click **Delete**.

You can run a task on demand from either the Device Properties - Tasks dialog, or from the WhatsConfigured Task Library.



Note: If you run the task from Device Properties the task only runs for that specific device. If you run the task from the Task Library, the task runs for any device to which it is assigned.

To run a task immediately from Device Properties:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **Tasks attached to this device**, select a task, then click **Run Now** to perform the selected task immediately.

To run a task immediately from the Task Library:

- 1 On the WhatsUp Gold console, select **Configure > WhatsConfigured Task Library**. The WhatsConfigured Task Library appears.
- 2 Select the scheduled task that you would like to run at this time, then click **Run Now**.



Tip: To view the task's results, see the WhatsConfigured Task Log.

You can remove a task attached to a device from the Device Properties - Tasks dialog.

To remove a task from a device:

- 1 In the Device List or Map View, right-click a device, then click **Properties**. The Device Properties dialog appears.
- 2 Click **Tasks**. The Tasks section of Device Properties appears.
- 3 Under **Tasks attached to this device**, select a task, then click **Remove** to delete the task from this device.

Add Task to Device

Use this dialog to select a task to add to the device. This list is populated with tasks currently configured in the WhatsConfigured Scheduled Task Library.

Select a task from the list, then click **OK**.

If you do not see the task that you would like to add, browse (...) to the Scheduled Task Library to configure the appropriate scheduled task.

Restore Confirmation

Use this dialog to confirm that you want to replace the current Running Configuration or Startup Configuration with the selected archive configuration. The **Configuration contents** displays the configuration to be restored.

To restore the selected configuration to the Running Configuration:

- 1 Select **Running Configuration** from the **Restore this configuration to the** box.
- 2 Click **Yes**. The Restore Confirmation dialog appears.
- 3 Click **OK**. The Restore Confirmation dialog closes.

To restore the selected configuration to the Startup Configuration:

- 1 Select **Startup Configuration** from the **Restore this configuration to the** box.
- 2 Click **Yes**. The Restore Confirmation dialog appears.
- 3 Click **OK**. The Restore Confirmation dialog closes.

Using Alert Center with WhatsConfigured

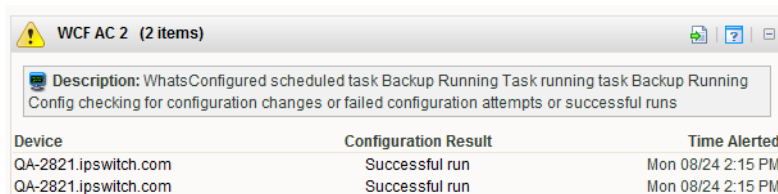
In This Chapter

Assigning an Alert Center threshold to a task..... 1132

Assigning an Alert Center threshold to a task

You can assign an Alert Center threshold to a task to notify you on task activities. You do this from the Threshold tab of the WhatsConfigured Task dialog.

After you have assigned a threshold to a task, a custom threshold dashboard report for the task threshold is displayed on the Alert Center tab.



The screenshot shows a window titled 'WCF AC 2 (2 items)'. It contains a description: 'WhatsConfigured scheduled task Backup Running Task running task Backup Running Config checking for configuration changes or failed configuration attempts or successful runs'. Below this is a table with three columns: 'Device', 'Configuration Result', and 'Time Alerted'. The table has two rows of data.

| Device | Configuration Result | Time Alerted |
|----------------------|----------------------|-------------------|
| QA-2821.ipswitch.com | Successful run | Mon 08/24 2:15 PM |
| QA-2821.ipswitch.com | Successful run | Mon 08/24 2:15 PM |

To assign a threshold to a WhatsConfigured task:

- 1 Navigate to the WhatsConfigured Task Library (**Other Plugins > WhatsConfigured Task Library**). The WhatsConfigured Task Library appears.
- 2 Do one of the following:
 - Click **New** to configure a new task. The Select Task type dialog appears.
 - Select **Schedulable Task**, then click **OK**. The New WhatsConfigured Task dialog appears.
 - - or -
 - Select an existing task, then click **Edit**. The Edit WhatsConfigured Task dialog appears.
- 3 Select the **Threshold** tab. The threshold tab appears.
- 4 Select **Enable this threshold** to enable and configure the threshold options.
- 5 Enter a **Name** for the threshold. This name is displayed in the WhatsUp Gold Alert Center Threshold Library.
- 6 Select to have the **Threshold** alert when the task **Detects configuration changes on a device**, if the task matches any of the selected conditions:
 - Detects a successful execution of a task on a device
 - Fails to run for a device
 - Successfully runs for a device
 - Fails this policy



Note: If you do not see the appropriate policy, or if the list is empty, browse (...) to the Policy Library to configure a new policy.

- 7 Select the Notification policy you would like Alert Center to use to notify you when the threshold is met. If the list is empty or you want to configure a new notification policy, browse (...) to the Alert Center Notification Policy Library.

Managing WhatsConfigured and TFTP services

In This Chapter

Starting, stopping and restarting WhatsConfigured services 1134

Starting, stopping and restarting WhatsConfigured services

To start, stop or restart the WhatsConfigured or TFTP service:

- 1** Navigate to the Admin Panel (**Admin > Admin Panel**).
- 2** Select the service you want to start, stop or restart, and perform one of the following actions:
 - If the status of the service is Stopped and you want to start the service, click **Start**. The service starts and the status changes to Running when the service start completes.
 - If the status of the service is Running and you want to restart the service, click **Restart**. The service stops, then starts. The status changes to Running when the service restart completes.
 - If the status of the service is Running and you want to stop the service, click **Stop**. The service stops. The status changes to Stopped when the service stop completes.

The WhatsConfigured Custom Script Language

In This Chapter

About the WhatsConfigured Custom Script Language..... 1135

About the WhatsConfigured Custom Script Language

WhatsConfigured users can write custom scripts that log in to devices through Telnet or SSH and run CLI commands on their devices. Scripts can be used to configure devices or to capture information about them in the WhatsConfigured database. For example, the following script uses Cisco IOS commands to capture a Cisco device's running configuration in the WhatsUp Gold database under the "running-config" key.

```
#  
  
# Cisco IOS Backup Running Configuration  
  
#  
  
# login to the device  
  
@login  
  
#enter privileged mode  
  
@enable  
  
# display the running configuration of the device and capture it in the  
WUG database [running-config] show run  
  
# logout from the device  
  
[-] exit
```

The WhatsConfigured custom script language is relatively simple and consists primarily of command-line interface (CLI) commands. The language is not meant to be a full-featured scripting language, such as JavaScript or VBScript, but rather is kept simple so that is accessible to all levels of WhatsConfigured users, including those with minimal programming skills. In order to meet the standards of this target audience, the language contains no constructs for looping, branching, or creating subroutines; it only supports simple sequences of commands.

The custom script language has three possible elements:

- Comments
- Variables
- Commands

Each of these elements will be explained in detail in the following sections.

Using WhatsConfigured Comments

In This Chapter

About WhatsConfigured comments 1137

About WhatsConfigured comments

In a script, you have the option to insert details or notes about the script. These notes and details are entered as comments, or lines having # as their first non-whitespace character. Comments are ignored by the script interpreter.



Note: A # character is interpreted as the beginning of a comment only if it is the first non-whitespace character on a line. If the # appears later in the line, it has no special significance.

Examples

```
# This is a comment
```

```
#      This is also a comment
```

```
123 # This is not a comment because '#' is not the first non-whitespace  
character in the line
```

Using WhatsConfigured Variables

In This Chapter

| | |
|---|------|
| About variables | 1138 |
| Accessing protocol settings..... | 1139 |
| Using reserved WhatsConfigured variable names | 1139 |

About variables

Variables are useful for giving names to values referenced in a script, especially values that are referenced multiple times. For example,

```
CommandTerminator = "\r\n"
TFTPServerAddress = 192.168.10.50
TransferFileName= startup-config.txt
@login
@write "copy tftp start"
@write $(CommandTerminator)
@write "$(TFTPServerAddress)"
@write "(TransferFileName)"
@write $(CommandTerminator)
```

Variable definitions

A variable definition must appear on a line by itself, in the following form:

Name = Value

In the example above, Name is the variable's title, and Value is the variable's value.

Variable names must begin with an alphabetic character or an underscore (a-z, A-Z, _), and subsequent characters can be any alphanumeric character or an underscore (a-z, A-Z, 0-9, _).



Note: Spaces are not allowed in variable names.

The variable's value consists of all text on the right side of = with leading and trailing whitespace removed. For example,

```
FirstUSPresident =           The Honorable George Washington
```

The example above defines a variable named "FirstUSPresident" with the value "The Honorable George Washington".

A variable's value can be referenced anywhere in the script after the variable is defined. A variable reference consists of '\$' immediately followed by the variable's name in parentheses, as shown below.

```
$(FirstUSPresident)
```

A variable reference is replaced by the variable's value. If the variable is defined multiple times in the script, the most recent definition is used. In the example above, the variable reference "`$(FirstUSPresident)`" would be replaced by "The Honorable George Washington".

Accessing protocol settings

When a WhatsConfigured script runs, it executes against a particular device. The script uses the device's SSH or Telnet credentials to login to the device. Sometimes it is necessary for a script to directly access the protocol settings being used in a set of credentials. The protocol settings can be accessed through the variables listed in the following table.



Note: The values of these variables are read-only and cannot be modified by scripts, though scripts are free to reference their values.

| Name | Description | Example |
|-----------------------------|---|-------------|
| Settings.UserName | The SSH or Telnet username. | admin |
| Settings.Password | The SSH or Telnet password. | secret |
| Settings.PrivilegedPassword | The enable or privileged mode password. | supersecret |

Using reserved WhatsConfigured variable names

Script authors can use any names they want for their variables. However, the variables listed below are used internally by WhatsConfigured. As a general rule, script authors should avoid using these variable names in their scripts.

- AccessPrivilege
- CommandPrompt
- CommandTerminator
- LoginTerminator
- MorePrompt
- MoreResponse
- NewPassword
- NewPrivilegedPassword

- NewUserName
- Password
- PasswordPrompt
- PrivilegedPassword
- TFTPServerAddress
- TransferFileName
- UserName
- UserNamePrompt

Occasionally, a script may need to re-define one or more of these variables to affect the internal operation of WhatsConfigured commands. The section on WhatsConfigured commands describes the meanings and uses of these variables, and how scripts can re-define them to modify the behavior of WhatsConfigured commands.

Using WhatsConfigured Commands

In This Chapter

| | |
|---|------|
| About commands..... | 1141 |
| About basic WhatsConfigured command syntax..... | 1141 |
| About strings and regular expressions in WhatsConfigured..... | 1142 |
| Storing WhatsConfigured command output in the WhatsUp Gold database | 1144 |
| Editing WhatsConfigured command output..... | 1144 |
| Using WhatsConfigured commands with queries..... | 1145 |
| About WhatsConfigured command layout..... | 1145 |
| WhatsConfigured script variables affecting command execution | 1147 |
| About WhatsConfigured command types | 1147 |

About commands

Beyond commands and variables definitions, the other lines in a script contain the commands to be executed by the script.

Examples

```
@login
```

```
@enable
```

```
config t
```

```
line vty 0 4
```

```
login local
```

```
exit
```

```
username $(NewUserName) password $(NewPassword)
```

```
exit
```

```
[-] exit
```

About basic WhatsConfigured command syntax

There are two types of commands that can be included in a WhatsConfigured custom script:

- WhatsConfigured commands
- Device commands

WhatsConfigured commands are executed by WhatsConfigured itself. Device commands are executed by the device. WhatsConfigured commands begin with @ to distinguish them from device commands. Any command whose text begins with @ is a WhatsConfigured command, while any other command is a device command. In the previous example script, the @login and @write commands are WhatsConfigured commands, while all other commands are device commands.

WhatsConfigured defines the following commands:

- @login
- @connect
- @write
- @read
- @read-more

The syntax for each of these commands is defined by WhatsConfigured. In contrast, Device commands are written using the native CLI commands supported by the device (IOS or CasOS commands for Cisco devices, Linux commands for Linux devices, etc.) These commands can use whatever syntax is required by the device's CLI command set.

In its simplest form, a command is just a string specifying the name of a command along with any parameters it requires. For example, the following script contains two simple commands:

```
@ login
```

```
username $(NewUserName) password $(NewPassword)
```

About strings and regular expressions in WhatsConfigured

WhatsConfigured commands make use of two specific types of values, strings and expressions.

Strings are used to represent literal text values; string values are sequences of characters delimited by double quotes, such as:

```
"Four score and seven years ago"
```

Escape sequences (used to define special characters within strings) may be any of the following:

| Escape sequence | Represents |
|-----------------|---------------------------|
| \0 | Null character |
| \' | Single quote |
| \" | Double quote |
| \? | Literal question mark |
| \\ | Backslash |
| \a | Bell alert (audible bell) |
| \b | Backspace |
| \f | Formfeed |
| \n | New line |
| \r | Carriage return |
| \t | Horizontal tab |
| \v | Vertical tab |

Additionally, the \x escape sequence can be used to include arbitrary characters in strings, including unprintable and control characters. \x should be followed by one to four hexadecimal digits which specify the value of the desired character. For example,

```
"This is Control-S: \x13"
```

Regular expressions are used for matching patterns in the output of script commands. Regular expression values are .NET regular expression strings delimited by forward slashes. For example, the following regular expression might be used to match the command prompt on a particular device (i.e., one or more characters followed by > or #):

```
/ .+(>|#)/
```

Because forward slashes are used to delimit regular expression values, including a forward slash as part of the regular expression itself, requires the use of the // escape sequence. For example, the following regular expression matches one or more characters followed by a forward slash followed by one or more characters followed by #:

```
/ .+// .+#/
```



Note: All regular expression matching is case-insensitive.

Storing WhatsConfigured command output in the WhatsUp Gold database

Most WhatsConfigured script commands return the output received from the device when the command was executed. For example, the `show run` command on Cisco devices displays the running configuration of the device. Or, on a Linux device, the `ls -al` command displays the contents of the current working directory. It is sometimes desirable to capture the output of the WhatsConfigured command and store it in the WhatsUp Gold database. To facilitate the storage of command output in the WhatsUp Gold database, a command can be preceded by a KEY which specifies the key under which the command's output should be restored in the WhatsUp Gold database. For example, the following command stores its output under the `running-config` key in the WhatsUp Gold database.

```
[running-config] show run
```

This means, execute the `show run` command and store its output in the WhatsUp Gold database under the `running-config` key.



Note: Key names can include dashes, underscores, and alphanumeric characters (-,_,a-z, A-Z). However, spaces are not allowed in key names.

Editing WhatsConfigured command output

Before storing a command's output in the WhatsUp Gold database, it is sometimes desirable to edit the output. For example, a command might place empty lines at the beginning or end of its output, and you may want to remove these empty lines before putting the output into the database. For situations like this, several operators are provided for editing command output. These operators are specified as part of the command's KEY. For example, the following command specifies that 4 lines should be trimmed from the output of the `ls -al` command before the output is stored in the WhatsUp Gold database under the key, `file-list`.

```
[file-list, trim-start-lines = "4"] ls -al
```

The following output editing operators are provided:

| Name | Value | Meaning | Example |
|------------------|------------------------------|--|------------------------|
| trim-start-lines | Integer | Trim the first N lines from the commands output | trim-start-lines="1" |
| trim-end-lines | Integer | Trim the last N lines from the commands output | trim-end-lines="1" |
| trim-start | String or regular expression | Trim all output before and including the first match of the specified string or regular expression | trim-start="#\n#\n#\n" |
| trim-end | String or regular expression | Trim all output including and after the last match of the specified string or regular expression | trim-end="#\n#\n#\n" |

| Name | Value | Meaning | Example |
|--------------|------------------------------|--|------------------------------|
| trim-before | String or regular expression | Trim all output before the first match of the specified string or regular expression | trim-before="!" |
| trim-after | String or regular expression | Trim all output after the last match of the specified string or regular expression | trim-after"!" |
| remove-lines | String or regular expression | Remove all lines that match the specified string or regular expression | remove-lines=/system time.+/ |

If multiple editing operators are used in the same command, they are applied in the order shown in the previous table.

```
[file-list, trim-start-lines = "4", trim-end="\n\n\n"]  ls -al
```

Using WhatsConfigured commands with queries

Some Device commands require users to answer a question before the command is executed. For example, the `enable` command on Cisco devices queries the user for a password before executing the command. For this reason, a command can optionally specify a QUERY which specifies the question asked by the device and the answer that should be given to the question. The QUERY is specified after the command within curly braces. For example,

```
shutdown { "Are you sure? ", "Y" }
```

The first value inside the curly braces is a String or Regular Expression describing the query prompt displayed by the device. The second value inside the curly braces is a String specifying the query response that should be entered in response to the query prompt. When the script interpreter executes this command, it will first send `shutdown` to the device. Next, it will wait until it receives the "Are you sure? " query prompt. Then, it will send `Y` to the device as the query response. Finally, the device will execute the command.



Note: Only Device commands can have a QUERY. WhatsConfigured commands do not need a QUERY, and, in fact, may not have one.

For example,

```
enable { $(PasswordPrompt), "${Settings.PrivilegedPassword}" }
```

About WhatsConfigured command layout

The general format of a script command is:

KEY COMMAND QUERY

For example,

```
[last-words]  shutdown  { "Are you sure? ", "Y" }
```

As previously explained, KEY specifies the key to use when storing the command's output in the WhatsUp Gold database, and possibly operations for trimming the command output. COMMAND is the text for the command itself. QUERY specifies the query prompt and query response for commands that ask a question. COMMAND is required, while KEY and QUERY are optional.

Since commands can become long, it is legal to put the KEY, COMMAND, and QUERY parts of a command on different lines. For example, the following commands are equivalent:

```
[last-words] shutdown { "Are you sure? ", "Y" }
```

```
[last-words]
```

```
shutdown
```

```
{ "Are you sure? ", "Y" }
```

```
[last-words]
```

```
shutdown { "Are you sure? ", "Y" }
```

```
[last-words] shutdown
```

```
{ "Are you sure? ", "Y" }
```

While the KEY, COMMAND, and QUERY can be on different lines from each other, each of these individual elements must start and end on the same line (i.e., they cannot span multiple lines). For example, the following commands are not valid:

```
[
```

```
last-words
```

```
] shutdown { "Are you sure? ", "Y" }
```

```
[last-words] shut
```

```
down { "Are you sure? ", "Y" }
```

```
[last-words]
```

```
shutdown
```

```
{
```

```
"Are you sure? ",
```

```
"Y"
```

WhatsConfigured script variables affecting command execution

When running a script, WhatsConfigured defines several script variables that contain information necessary to execute the script's commands. For example, the `CommandPrompt` variable contains a pattern (i.e., string or regular expression) that describes the command prompt string used by the device. This pattern is used to detect when the device is prompting for a command. Several other variables are also defined. A complete list of all script variables affecting command execution are listed in the following table.

WhatsConfigured's assigns default values to each of these variables. If a script author wants to override WhatsConfigured's default behavior, he or she may do so by re-defining one or more of these variables. For example, if a script wants to override the command prompt pattern used to run the script, it can re-define the `CommandPrompt` variable to contain the pattern of choice.

| Name | Value | Meaning | Example |
|--------------------------------|------------------------------|---|----------------------------------|
| <code>UserNamePrompt</code> | String or regular expression | Pattern describing the username prompt displayed by the device when a user logs in | "login as:" |
| <code>PasswordPrompt</code> | String or regular expression | Pattern describing the password prompt displayed by the device when a user logs in | "password:" |
| <code>CommandPrompt</code> | String or regular expression | Pattern describing the command prompt displayed by the device when prompting the user for a command | <code>/.+(# >)/</code> |
| <code>MorePrompt</code> | String or regular expression | Pattern describing the "more" prompt displayed by the device when displaying paged output | <code>/--More-- --More--/</code> |
| <code>MoreResponse</code> | String | String to be entered in response to a "more" prompt | "" |
| <code>LoginTerminator</code> | String | Line termination sequence to be used with logging in | <code>"\r\n"</code> |
| <code>CommandTerminator</code> | String | Line termination sequence to be used when executing commands | <code>"\n"</code> |

About WhatsConfigured command types

There are two types of commands in a WhatsConfigured script: device commands and WhatsConfigured commands. Device commands can be any CLI command supported by a device, and are executed by the device. WhatsConfigured commands start with '@' and are executed by WhatsConfigured rather than by the device. The following sections describe the available commands and explain when and how to use them. Most scripts will use a combination of Device commands and WhatsConfigured commands, although it is possible to write scripts using only WhatsConfigured commands.

@login

Typically, the first step in any WhatsConfigured script is to login to the device. This is typically done with the WhatsConfigured `@login` command. The `@login` command can be used to login to devices that use a traditional user-name/password login procedure that works as follows:

- 1 The device prompts the user for their user name
- 2 The user enters their user name
- 3 The device prompts the user for their password
- 4 The user enters their password
- 5 If login is successful, the device displays a command prompt and waits for the user to run commands

The `@login` command has no parameters, and is invoked as follows:

```
@login
```

When the `@login` command is executed, it does the following:

- 1 When it detects `UserNamePrompt`, it sends `Settings.UserName` to the device followed by `LoginTerminator`.
- 2 When it detects `PasswordPrompt`, it sends `Settings.Password` to the device followed by `LoginTerminator`.
- 3 When it detects `MorePrompt`, it enters `MoreResponse`.
- 4 After entering the user name and password, if `@login` detects `CommandPrompt`, it assumes that login was successful. Otherwise, it assumes that login failed.

If at any time the device's output stalls for more than `Settings.ReadTimeout` seconds, it is assumed that something is wrong, and the script returns failure.

@enable

Many device configuration tasks require a script to enter a privileged mode in order to execute the necessary device commands. On many devices, privileged mode is entered using the `enable` command. Typically, running the `enable` command on a device requires the user to enter a user name and/or password. For devices that implement this style of `enable` command, scripts can use the WhatsConfigured `@enable` command to easily enter privileged mode. The `@enable` command has no parameters, and is invoked as follows:

```
@enable
```

When the `@enable` command is executed, it does the following:

- 1 It sends `enable` to the device followed by `CommandTerminator`.
- 2 If it detects `UserNamePrompt`, it sends `Settings.UserName` to the device followed by `CommandTerminator`.
- 3 If it detects `PasswordPrompt`, it sends `Settings.PrivilegedPassword` to the device followed by `CommandTerminator`. If `Settings.PrivilegedPassword` is empty, it uses `Settings.Password` instead.

- 4 After entering the user name and password (if necessary), if `@enable` detects `CommandPrompt`, it assumes that enable was successful. Otherwise, it assumes that enable failed.

If at any time the device's output stalls for more than `Settings.ReadTimeout` seconds, it is assumed that something is wrong, and the script returns failure.

Device commands

After invoking the `@login` command (and possibly `@enable` as well), most scripts contain a sequence of Device commands that are sent to the device for execution. A typical Device command is shown below:

Device commands are executed as follows:

```
[last-words] shutdown { "Are you sure? ", "Y" }
```

The script sends the command text to the device. It terminates the command with `CommandTerminator`.

If the command has a query, the device returns the query to the script. When it detects the query prompt, the script sends the query response to the device.

Next, the device executes the commands, and sends its output back to the script.

If the command's output is long enough to result in more prompts, when the script detects a `MorePrompt`, it sends `MoreResponse` to the device.

The script consumes the command's output until it detects `CommandPrompt`, at which point it assumes that the command's output is complete.

If at any time the device's output stalls for more than `Settings.ReadTimeout`, it is assumed that something is wrong, and the script returns failure.

If the command succeeds, and it has a KEY, its output is saved in the WhatsUp Gold database.

The following script is typical:

```
@login

enable { "password: ", "${Settings.PrivilegedPassword}" }

[running-config] show run

[-] logout
```

This script first logs in with the `@login` command, then enters privileged mode with the `@enable` command.

Next, the script sends the `show run` command to the device. The output of this command is saved in the WUG database under the `running-config` key.

Finally, the script sends the `logout` command to the device, at which point the device closes the network connection.

The `[-]` key on the `logout` command tells WhatsConfigured not to expect any output from the command, because the command causes the device to close the network connection. Typically, receiving no output from a command indicates failure, but in the case of `exit` or `logout` commands (or any other command that closes the connection), a lack of output does not indicate failure. Script authors can use the `[-]` key to indicate such commands and prevent WhatsConfigured from returning failure when the device closes the connection.

Low-level commands

Many scripts will use only `@login`, `@enable`, and `Device` commands to implement their functionality. However, some devices have non-standard Telnet or SSH interfaces that won't work with `@login` and `Device` commands. For example, some devices have non-standard login procedures for which the `@login` command will not work. Other devices have menu-driven interfaces rather than a standard command-prompt-style interface. For whatever reason, if `@login`, `@enable`, or `Device` commands do not work for a particular device, WhatsConfigured provides a set of low-level commands that can be used to interact with virtually any device, no matter how non-standard its interface might be.

The `@connect` command allows a script to precisely control the process of logging in to a device. The `@write` command allows a script to control exactly what input is sent to a device. The `@read` command allows a script to read output from a device and optionally store it in the WhatsUp Gold database.

`@connect`

The `@connect` command is an alternative to `@login` in cases where a script needs to precisely control the login process (e.g., in cases where `@login` doesn't work for a particular device). The `@connect` command connects to a device without trying to log in. After connecting to a device with `@connect`, if the device requires users to login, the script can control the login process precisely using the `@write` and `@read` commands, which are described later.

When calling `@connect`, scripts can specify one or more patterns (i.e., strings or regular expressions) that specify the output the script expects to receive from the device when it connects. These patterns are used by `@connect` to detect the end of the device output. `@connect` will assume that device output is complete when either the output matches one of the specified patterns, or no new output has been received from the device for `Settings.ReadTimeout` seconds. For example,

```
@connect "login as: ", "user name: "
```

When executed, `@connect` connects to the device, and reads whatever output comes back from the device. If the output matches one of the specified patterns, the command succeeds. If the connection attempt fails entirely, or the output received from the device does not match any of the specified patterns, the command fails (as well as the entire script). As with any other command, a KEY can be specified to capture the command's output in the

WhatsUp Gold database, although one would rarely want to store the output of an `@connect` command.

If no patterns are specified (as shown below), `@connect` connects to the device, and returns whatever output comes back from the device. In this case, the command succeeds as long as a connection is successfully established with the device.

@connect-more

Some devices return paged output that requires `more` prompts when you initially connect to them. If a script needs to handle `more` prompts during the connection process, it can use the `@connect-more` command instead of `@connect`. `@connect-more` works just like `@connect`, except that it handles `more` prompts during the connection process, while `@connect` does not. Specifically, if `MorePrompt` is detected during the connection process, `@connect-more` sends `MoreResponse` to the device.

```
@connect-more "login as: ", "user name: "
```

@write

The `@write` command can be used to send a string of characters to the device. This command allows a script to precisely control what input is being sent to the device. For example, the following script sends the `show run` command to the device, followed by the `CommandTerminator` (typically `\n` or `\r\n`).

```
@write "show run"
```

```
@write $(CommandTerminator)
```

@read

The `@read` command can be used by scripts to read the output coming back from the device. Typically, a call to `@read` will immediately follow a call to `@write`. When calling `@read`, scripts can specify one or more patterns (i.e., strings or regular expressions) to help `@read` detect the end of the device output. `@read` will assume that device output is complete when either: the output matches one of the specified patterns, or no new output has been received from the device for `Settings.ReadTimeout` seconds. Often, the output will end with `CommandPrompt`, so `"@read $(CommandPrompt)"` is a common way to call `@read`. If desired, the output received from the device can be stored in the WhatsUp Gold database, as shown below:

```
@write "show run"
```

```
@write $(CommandTerminator)
```

```
[running-config, trim-end-lines = 1] @read $(CommandPrompt)
```

When executed, `@read` will read whatever output comes back from the device. If the output matches one of the specified patterns, the command succeeds. If the output received from the device does not match one of the specified patterns, the command fails (as well as the entire script).

If no patterns are specified (as shown below), `@read` will return whatever output comes back from the device. In this case, the command will succeed as long as the connection to the device is still open.

`@read-more`

Some devices return paged output that requires `more` prompts. If a script needs to handle `more` prompts during a read operation, it can use the `@read-more` command instead of `@read`. `@read-more` works just like `@read`, except that it handles `more` prompts during the reading process, while `@read` does not. Specifically, if `MorePrompt` is detected during the reading process, `@read-more` will send `MoreResponse` to the device.

Script Examples

In This Chapter

Example Scripts 1153

Example Scripts

This example shows a typical script that uses @login to login to the device, uses @enable to enter privileged mode, and then executes several Device commands.

```
@login

@enable

[running-config] show run

[-] exit
```

This example shows how to login to a device and run a command using only low-level WhatsConfigured commands:

```
@connect "login as: "

@write "${Settings.UserName}"

@write $(LoginTerminator)

@read "password: "

@write "${Settings.Password}"

@write $(LoginTerminator)

@read $(CommandPrompt)

@write "exit"

@write $(CommandTerminator)
```

This example shows how to combine high-level commands and low-level commands in the same script as above:

```
@login

@enable

@write "copy tftp start"

@write $(CommandTerminator)
```

```
@write "$(TFTPServerAddress)"  
  
@write $(CommandTerminator)  
  
@write "$(TransferFileName)"  
  
@write $(CommandTerminator)  
  
@write $(CommandTerminator)  
  
[-] exit
```

About the WhatsConfigured Custom Script Language

The WhatsConfigured custom script language is relatively simple and consists primarily of command-line interface (CLI) commands. The language is not meant to be a full-featured scripting language, such as JavaScript or VBScript, but rather is kept simple so that is accessible to all levels of WhatsConfigured users, including those with minimal programming skills. In order to meet the standards of this target audience, the language contains no constructs for looping, branching, or creating subroutines; it only supports simple sequences of commands.

The custom script language has three possible elements:

- Comments
- Variables
- Commands

Task Status

This dialog displays the status of a task that you are attempting to run using the **Run Now** option on the WhatsConfigured Task Script Library.

After the task completes, click **Results** to view details results for the task.

About the WhatsConfigured Diff Viewer

Use this dialog to compare two archived configuration files.

Select a device

When the dialog first loads, it displays two configuration files for the same device. You can use the **Select a device** link on either side of the dialog to choose a different device from which to view configuration files.



Select a config file to view

Below the device icon and name is a list of currently archived configuration files. You can select a different configuration file to view from this list.



View diffs

The number of differences between the two configuration files are listed on the left side of the dialog. Next to the number of differences are two arrow buttons that you can use to navigate through the configuration files' diffs.



Diffs in the configuration files are highlighted in purple and green.

```
120 !  
121 interface Loopback1  
122 ip address 1.1.1.1 255.255.255.255  
123 !
```

```
120 !  
121 interface Loopback1  
122 no ip address  
123 !
```



Tip: To go back to the Device Properties dialog on the WhatsUp Gold web interface, use the **Back** button at the top left of the page.

Using WhatsConnected

In This Chapter

| | |
|------------------------------|------|
| WhatsConnected Task Log..... | 1157 |
| WUG Device Viewer | 1158 |

WhatsConnected Task Log

The WhatsConfigured Task Log displays log messages generated by WhatsConfigured tasks.

Report body

- **Date** displays the date the task ran.
- **Task** displays the name of the specific task.
- **Device** displays the network device for which the task ran.
- **Result** displays the outcome of the task.
- **Message** displays the log message that generated according to the task's result.

Filtering the report

Date range

Use the date/time picker at the top of the report to select a date range and time frame.

In the **Date range** list, some reports also allow you to specify and customize the business hour report times for reports to display. This allows you to view the network activity only for specified business hours. The date and time format for the date on this report matches the format specified in **Program Options > Regional** set in the WhatsUp Gold console.



Note: The Business Hours setting is available for group reports only.

Task

Use the Task list to select a specific task for which to view report data. This list is populated with scheduled tasks currently configured in the Scheduled Task Library.

Device

Use the Device list to select a specific network device for which to view report data. You can view data for all devices in the group.



Tip: You can change the device group you are viewing by clicking the group name in the application bar at the top of the page.

Result

Use the Result list to select a specific result for which to view report data. You can choose to view data for all results.

Navigation

You can change the group you are viewing by clicking the group name in the application bar at the top of the page.

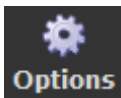
You can change to another group report by selecting one from the **More Group Reports** list.

Printing

You can print a fully formatted log through your browser by clicking the print icon in the browser's toolbar, or selecting **File > Print** from the browser's menu.

Toolbar buttons

Use the following toolbar buttons to manage report exports, schedule report emails, and get application help.



Click this icon to add the current report to:

- your Favorites list (available in full reports).
Tip: After selected, Favorite reports can be accessed from the **Reports > Favorites** folder of the **WhatsUp** section of the GO Menu.
- export the report to a file (Text, Microsoft Excel, or PDF available in full reports and PDF available in dashboard reports).
- email a report as a PDF attachment.
- schedule reports to be emailed.

Note: JavaScript must be enabled on your browser for this feature to work.



Click this icon to view help for the current report.

WUG Device Viewer

From the WhatsUp console, right click on a device in a Map View that has been exported from WhatsConnected. Select the **Device Viewer** menu option.

The **WhatsConnected Device info** that is launched from the WhatsUp Gold console gives a detailed view of the layer 2 and inventory details that have been collected for a network WhatsConnecteddevice.

The Device information type is a list of the available information types. Each information type provides a subset of the information discovered by WhatsConnected for the device. The information types available for a given device will be dependent on the information available for discovery from that device.

A brief description of available information types follows, for more information, follow the associated link:

- *System Information* (on page 1159). IP Address/MAC Address, MIB II information
- *IP Address Information* (on page 1160). IP Address configuration
- *Device Viewer - Interface Information* (on page 1160). Interface Information. Interface entries with status.
- *Bridge Port Information* (on page 1161). Bridge Port information and VLAN configuration.
- *VLAN Information* (on page 1161). Virtual LAN configuration information.
- *Asset Information* (on page 1162). Inventory information for the device components.
- *Link Information* (on page 1163). Physical connectivity from this device to other network devices.
- *IP Route Information* (on page 1163). IP route configuration data.
- *Spanning Tree Information (STP)* (on page 1163). Spanning tree configuration and status.
- *ARP Cache Information* (on page 1164). Address Resolution Protocol (ARP) table.
- *Forwarding Information* (on page 1164). Layer2 forwarding information.
- *Protocol Profile Information* (on page 1164). Successful protocol matches for this device.

Device Viewer - System Information

System Information displays a combination of basic device information from the various ICMP, SNMP, DNS, and NetBIOS protocols is displayed here.

The tab displays the following system information.

- **IP Address.** The main IP address used to discover the device.
- **MAC Address.** The MAC address associated with the main IP address.
- **Host Name.** The DNS host name for the device.
- **NetBIOS Name.** The NetBIOS name of the machine (if supported).
- **NetBIOS Domain.** The NetBIOS domain that the machine belongs to (if supported).
- **System Name.** The SNMP MIB II System Name.
- **System Description.** The SNMP MIB II System Description.
- **System OID.** The SNMP MIB II System Object ID.
- **System Location.** The SNMP MIB II System Location.
- **System Contact.** The SNMP MIB II System Contact
- **System Up-Time.** The SNMP MIB II System Up-Time (since last restart)
- **Category.** The device category that has been assigned to the system based on its functional characteristics.
- **Network Device.** Flag that indicates whether the device is performing a network device function. (i.e. Router, Switch, Hub, etc.)
- **Vendor.** Manufacturer of the device
- **Model.** Model number of the device.
- **Virtualization Type.** If the device represents a virtual device, this field indicates the type of virtual device (VMware or VirtualPC).

Device Viewer - IP Address Information

IP Address Information displays the following IP address information.

- **IP Address.** The IP address.
- **Net Mask.** The Net Mask used in association with the IP address.
- **MAC Address.** The MAC address associated with the IP address.
- **IF Index.** The IF Index that this IP address is bound to.
- **Hostname.** The hostname of the device associated with the IP address.

Device Viewer - Interface Information

Interface Information displays the following index information.

- **Index.** The interface index normally associated with the ifIndex of the RFC 1213 ifTable.
- **Name.** The interface name.

- **Description.** The interface description.
- **Alias.** The interface alias name.
- **Type.** The interface type. This field is defined by the ifType enumeration from the RFC 1213 MIB.
- **Speed.** The configured data speed of the interface.
- **Admin Status.** The administration state of the interface (i.e. up, down, unknown).
- **Oper Status.** The operational state of the interface (i.e. up, down, unknown, testing).
- **MAC Address.** The MAC address of the interface.

Device Viewer - Bridge Port Information

Bridge Port Information displays the following bridge port information.

- **Index.** The bridge port index.
- **IF Name/Descr.** The IF Name + IF Description associated with this bridge port.
- **Name.** The name of the bridge port.
- **VLAN Name.** The name of the VLAN assigned to this bridge port.
- **VLAN Index.** The VLAN index that is assigned to this bridge port.



Note: By default, the proceeding columns are not shown.

- **Vendor Index.** A proprietary index used by the vendor to associated with this bridge port.
- **IF Index.** The IF index associated with this bridge port.
- **Module Index.** The index of the module that this bridge port is contained within (used in chassis / module configurations).
- **Module Port Index.** The port number of this bridge port in relationship to the module it is contained with (used in chassis/module configurations).
- **VLAN Trunk.** A flag that indicates whether the bridge port is a VLAN truck (forwarding traffic for more than one VLAN).
- **LAG Port.** A flag that indicates whether the bridge port is a member of a Link Aggregation Group (LAG).
- **Inter-Switch Link.** A flag that indicates whether the bridge port is used in a connection between two switches (or similar devices).

Device Viewer - VLAN Information

VLAN Information displays the following information.

- **Index.** The VLAN index.
- **Name.** The VLAN name.
- **Egress Ports.** The bridge ports that are forwarding traffic for this VLAN. The VLAN traffic is transmitted as TAGGED or ENCAPSULATED unless indicated in **Untagged Ports**.
- **Untagged Ports.** The bridge ports that are forwarding traffic from this VLAN. The VLAN traffic will be transmitted "in the clear" or UNTAGGED on these bridge ports.



Note: By default, the proceeding columns are not shown.

- **Dot1q Index.** This field indicates if the Dot1q VLAN index differs from the base VLAN Index.
- **Forbidden Ports.** The bridge ports that are not allowed to forward this VLAN.
- **Subnet.** Subnet that was discovered/associated with this VLAN.

Device Viewer - Asset Information

Asset Information displays the following information.

- **Index.** A unique index for this asset entry.
- **Class.** The physical class that describes this component (i.e. chassis, module, port, fan).
- **Name.** The name of the physical component.
- **Description.** The manufacturer's description of the physical component.
- **Manufacturer.** The name of the manufacturer.
- **Model.** The model name for the physical component.
- **Serial Number.** The serial number for the physical component.
- **Hardware Version.** The hardware revision for the physical component.
- **Firmware Version.** The firmware revision for the physical component.
- **Software Version.** The software version the physical component.
- **Port Count.** The port count of the component (if it is a switch/switch module).



Note: The data that is associated with the physical components of the device can be most effectively described by the Entity constructs defined in the ENTITY MIB. Therefore, there are a number of columns not normally shown that relate directly back to the ENTITY MIB entries. These columns are shown as follows:

- **Physical Index.** The Entity MIB index.
- **Switch Index.** In the case of a stacked switch, the switch index in the stack.

- **Module Index.** In the case of an enclosed chassis/module configuration, the module index of the physical component.
- **Card Index.** In the case of an enclosed chassis/module configuration, the card index of the physical component.
- **Alias.** An alias name for the physical component.
- **Vendor Type.** A vendor index number that is specific to the hardware vendor.
- **Status.** The current status of the physical component.
- **Asset ID.** The proprietary asset ID that is assigned to the physical component.
- **Contained In.** Indicates the index of the physical component that this component is contained in.
- **Parent Relative Position.** Indicates the relative position when the component is contained in another component (for example, a module index in a chassis configuration)
- **Field Replaceable Unit.** Indicates whether the item can be replaced in the field.

Device Viewer - Link Information

Link Information displays the following information.

- **Local Link.** The local physical link, or interface. If no interface information is shown, the connection was made to the device.
- **Remote Link.** The remote physical link.

Device Viewer - IP Route Information

IP Route Information displays the following.

- **Destination.** The destination IP address of this route. Entries of 0.0.0.0 are considered to be a default route.
- **Net Mask.** The mask used in conjunction with the destination address.
- **Next Hop.** The IP address of the next hop of this route.
- **IF Index.** The index of the local interface through which the next hop of this route should be reached.
- **Type.** The type of route (i.e. local, direct, indirect)
- **Protocol.** Routing mechanism by which this route was learned.

Device Viewer - Spanning Tree Protocol (STP) Information

Spanning Tree Protocol (STP) Information displays the following.

- **Index.** The BridgePort index to which this entry applies.
- **Designated Root.** The MAC address of the designated spanning-tree root for this bridge port.
- **Designated Root Device.** The Display Name of the designated root.
- **Designated Bridge.** The MAC address of the designated bridge for this bridge port.

- **Designated Bridge Device.** The Display Name of the designated bridge device.
- **Designated Port.** The designated remote port on the designated bridge device.
- **State.** The current state of the spanning-tree protocol for this bridge port.

Device Viewer - ARP Cache Information

Address Resolution Protocol (ARP) Information displays the following.

- **IP Address.** The IP address of the ARP entry.
- **MAC Address.** The MAC address that is associated with the IP address.
- **IF Index.** The IF index of the interface that this entry was associated with.
- **Type.** The type of cache element. Each cache element is assigned one of the following values: 1 - other, 2 - invalid, 3 - dynamic, 4 - static

Device Viewer - Forwarding Information

Layer 2 forwarding Information displays the following.

- **BP Index.** The bridge port index associated with this forwarding entry.
- **IF Name.** The display name of the interface associated with the bridge port.
- **Remote MAC Address.** The MAC address that is forwarded on the identified bridge port.
- **Remote Device Name.** The display name of the remote device.



Note: A name is only shown when a remote device can be associated with the given MAC address.

- **Remote IF Name.** The display name of the remote interface.
- **Remote MAC Vendor.** The vendor name of the remote device.

Device Viewer - Protocol Profile Information

Successful protocol matches for this device.

Using ELM Reports

In This Chapter

Using Event Log Management (ELM) Reports in WhatsUp Gold . 1166

Using Event Log Management (ELM) Reports in WhatsUp Gold

In This Chapter

Event Log Management (ELM) Reports in WhatsUp Gold Overview 1166

Using the Event Log Management (ELM) Configurator 1166

Event Log Management (ELM): Plugin Reports 1171

Event Log Management (ELM) Reports in WhatsUp Gold Overview

WhatsUp Gold version 15.0 provides integration with the Event Log Management central database. For access to ELM reports and data, you must also have ELM products, specifically WhatsUp Event Archiver and / or WhatsUp Event Alarm, configured to send collected log data to a MS SQL Server. WhatsUp Gold accesses report data through stored procedures in the ELM database.

ELM report integration supports the following six core log types:

- Application
- Directory service
- DNS server
- File replication service
- Security
- System

To view ELM data in WhatsUp Gold, you must first use the *ELM Configuration Integration tool* (on page 1166) to add, select, or delete ELM database instances that WhatsUp Gold can access. If needed, you can use the configurator tool to work with multiple ELM database instances.

ELM data integration with WhatsUp Gold allows you to create the following types of reports:

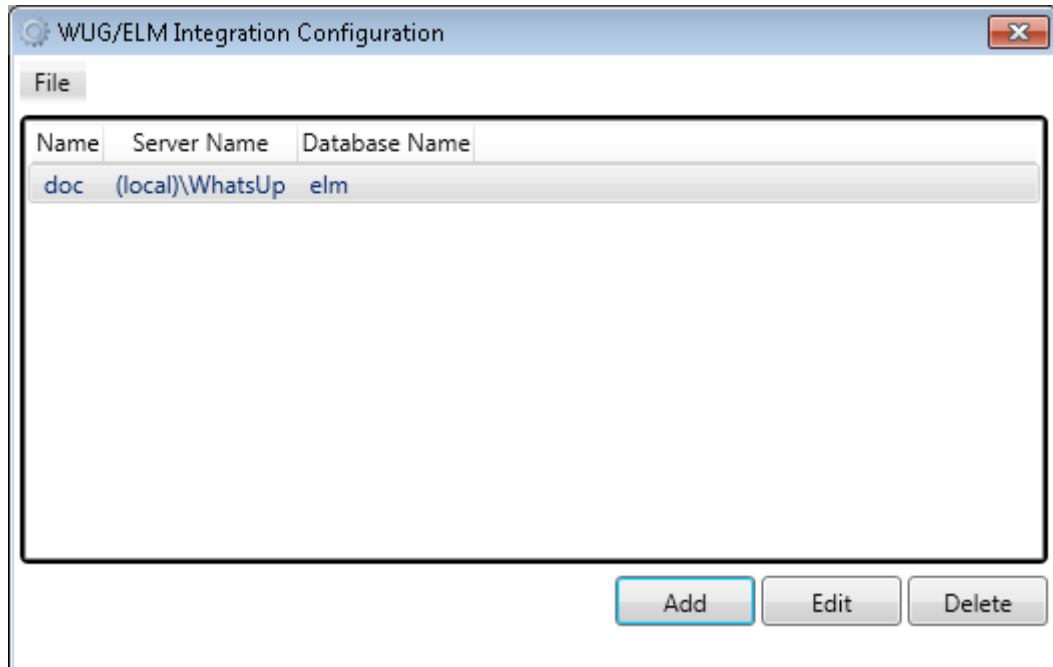
- *ELM Summary Dashboard Reports* (on page 585)
- *ELM Alarm Dashboard Reports* (on page 586)
- *ELM Plugin Full Reports* (on page 1171)

Using the Event Log Management (ELM) Configurator

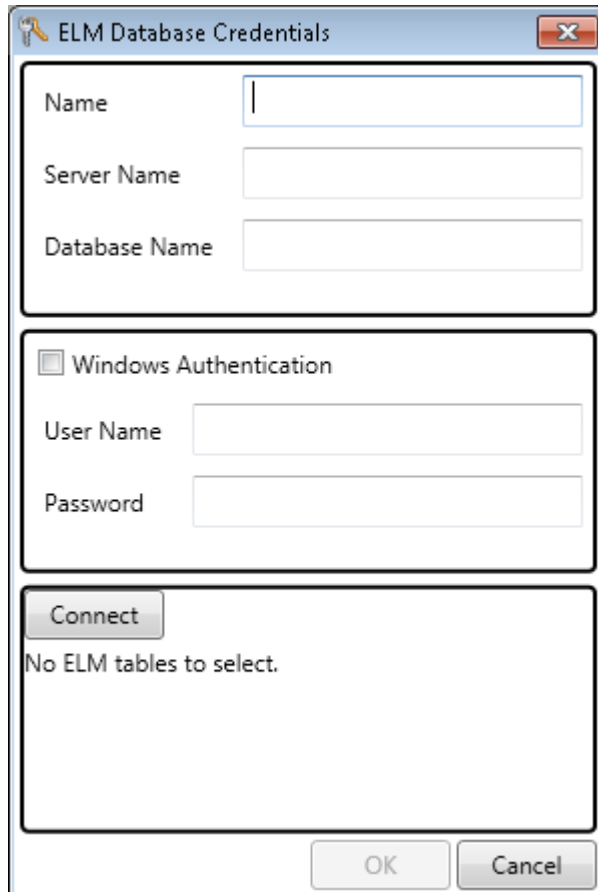
The ELM integration configuration tool allows you to manage your ELM database sources. For WhatsUp Gold to display ELM information, you must add ELM database instances to WhatsUp Gold using the ELM integration configuration tool, and then select the database instances for use in your WhatsUp Gold ELM reports.

To access the ELM integration configuration tool:

- 1 From the Windows Start menu, click **Programs** or **All Programs** > **Ipswitch WhatsUp Gold v 15.0** > **Utilities** > **WhatsUp ELM Integration Tool**. The WUG/ELM Integration Configuration tool opens.



- 2 Click **Add** to add a database. The ELM Database Credentials dialog opens.



ELM Database Credentials

Name

Server Name

Database Name

☐ Windows Authentication

User Name

Password

Connect

No ELM tables to select.

OK Cancel

- 3 Complete the following fields:
 - **Name.** Type a name for your database source.
 - **Server Name.** Type the hostname of the SQL server hosting the ELM database you want to add, as well as the instance name, if applicable.
 - **Database Name.** Type the name of the database storing your ELM data.
 - **Windows Authentication.** If you are using Windows authentication, select the check box. If deselected, the ELM Configurator connects using SQL authentication.
 - **User Name.** Type the appropriate user name.
 - **Password.** Type the password associated with the user name.
- 4 Click **Connect**. The database is accessed and any relevant ELM tables automatically display in the Integration Configuration tool interface.
- 5 Select the tables containing Event Alarm and Event Archiver data, choosing the appropriate product associated with each table.



Note: Select WhatsUp Event Archiver tables in the Event Archiver column, and select WhatsUp Event Alarm tables in the Event Alarm column. Only checked tables are automatically used to build reports within WhatsUp Gold.

- 6 Click **OK** to add the database source.



Note: To access the Summary Dashboard reports in WhatsUp Gold that display incoming detected alerts by WhatsUp Event Alarm, you must instruct WhatsUp Event Alarm to send detected events to a SQL Server database table.

To instruct WhatsUp Event Alarm to send detected events to a SQL Server database table:

- 1 Access the WhatsUp Event Alarm Control Panel.
- 2 Click the **Edit** menu, then click **Define Notifications**. The Define Notifications dialog box opens.
- 3 Select the **Database** option, **build an ODBC connection to your SQL Server**.
- 4 Type a table name for storing detected events.

As you add database sources, they display in the WUG/ELM Integration Configuration dialog. From here, you can:

- Add more database sources by clicking the **Add** button.
- Edit database information by selecting a database source and then clicking the **Edit** button.
- Delete a database source from the configuration tool by selecting the source and then clicking the **Delete** button.

Event Log Management (ELM): Summary Reports

ELM summary *dashboard reports* (on page 348) display ELM Event Archiver-specific database table information. There are three different ELM summary reports:

- Summary Counts
- Failure Audits By Computer
- Failure Audits By User

The Summary Counts report displays the number of events associated with monitored computer and users accounts over a user-defined time frame, including critical events, warning events, and informational events.

- Click the **Monitored Computers** link to display the ELM Events by Computer report, which lists all computers in the ELM database tables and their associated number of events.
- Click the **User Accounts** link to display the number of Success Audits and Failure Audits associated with each username in the ELM database tables.

The Failure Audits By Computer report displays a list of failure audits over a user-defined time frame, associated with each computer being monitored by ELM. Click a computer name to see report details.

The Failure Audits By User reports displays a list of failure audits associated with each user being monitored by ELM, over a user-defined time frame. Click a username to see report details.

For information about configuring ELM summary reports, see *Configuring ELM Summary Reports* (on page 1170).

For more information about dashboard reports, see the *Adding dashboard reports to a dashboard view* (on page 342) help topic.

Configuring Event Log Management (ELM) Summary Reports

You can configure how ELM Summary reports display information.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog appears.
- 2 Type or select the appropriate information for the following fields.
 - **Report name.** Type a title for the dashboard report.
 - **Date Range.** Select a date range from which you want to view report information.
 - **Select an ELM database.** Use the list to select the ELM database from which you want to view report information.
- 3 Click **OK** to save changes.

Event Log Management (ELM): Alarm Reports

ELM Alarm *dashboard reports* (on page 348) display ELM Event Alarm-specific database table information. There are three different ELM alarm reports:

- Critical Event Alarms
- Warning Event Alarms
- Informational Event Alarms

The Critical Event Alarms report displays a list of critical events along with event details present in the Event Alarm tables from a given SQL Server ELM database instance. Critical events include error and failure audit event types. To view the details associated with a critical event, click the **Event Information** link. The Event Alarm Description dialog opens, displaying a description of the critical event alarm.

The Warning Event Alarms report displays a list of warning events along with event details present in the Event Alarm tables from a given SQL Server ELM database instance. Warning events only include warning event types. To view the details associated with a warning event, click the **Event information** link. The Event Alarm Description dialog opens, displaying a description of the warning event alarm.

The Informational Event Alarms report displays a list of informational events along with event details present in the Event Alarm tables from a given SQL Server ELM database instance. Informational events include information and success audit event types.

To view the details associated with an informational event, click the **Event Information** link. The Event Alarm Description dialog opens, displaying a description of the informational event alarm.

For information on configuring ELM Alarm reports, see *Configuring ELM Alarm Reports* (on page 1171).

For more information about dashboard reports, see the *Adding dashboard reports to a dashboard view* (on page 342) help topic.

Configuring Event Log Management (ELM) Alarm Reports

You can configure how ELM Alarm reports display information.

To configure this dashboard report in WhatsUp Gold:

- 1 In the title bar of the dashboard report pane, select **Menu > Configure**. The Configure Report dialog opens.
- 2 Type or select the appropriate information for the following fields.
 - **Report name.** Type a title for the dashboard report.
 - **Column 5 width.** Type a width for the Event Information column (column 5) in pixels.
 - **Select an ELM database.** Use the list to select the ELM database from which you want to view report information.
- 3 Click **OK** to save changes.

Event Log Management (ELM): Plugin Reports

ELM Plugin reports display ELM Event Archiver-specific database information. You can access ELM plugin reports by selecting the **Other Plugins** tab. There are two different ELM plugin reports:

- ELM Events By Computer
- ELM Audits By User

The ELM Events By Computer report displays a list of computers with the total number of error events, warning events, and informational events within the selected time period. The report is sorted by computers with the most errors. This report is divided into two full reports: Errors/Warnings and Security events. You can select the report you want to view by clicking the appropriate tab located in the upper left corner of the report.

The ELM Audits By User report displays a list of user accounts and their associated total number of success audits and failure audits for the selected time period. The report is sorted by the user account with the most failure audits.

To display ELM data in the Plugin reports, you must select an ELM database by using the link located to the right of the report title. Use this link to select and view data from different ELM data sources (if you have multiple data sources saved in the configuration integration tool).

About the Dashboard Screen Manager

In This Chapter

Ipswitch Dashboard Screen Manager overview..... 1173

How does the Dashboard Screen Manager work? 1174

Installing the Dashboard Screen Manager 1175

Configuring a Dashboard Screen Manager playlist 1176

Ipswitch Dashboard Screen Manager overview

The Dashboard Screen Manager is a stand-alone application designed to display a series of Web pages, or a "playlist," on one or multiple monitors.



The Dashboard was created as a complement to the Ipswitch network monitoring application, WhatsUp Gold, and as an aid to keeping your network visible. The Dashboard application is included in the WhatsUp Gold and WhatsUp Gold Central and Remote Site installations.

The Dashboard can run on a display console and cycle through various pages from the WhatsUp Gold web interface.

Network administrators then have important and pertinent network information on display at all times, cycling and changing on its own without the need of constant configuration. It also provides the capability to view multiple networks that you are monitoring simultaneously.

Though the Dashboard Screen Manager was created to work along-side WhatsUp Gold, it can display virtually any Web page. For example, an Internet business providing service to a small town in the desert glances at one screen on the Dashboard and sees that the connectivity to the town is down. By displaying the weather for this town on another screen at the same time, the network administrator is able to see that the extreme temperatures of the day have likely caused problems for the cable transmitters.



Note: If you want to display a password protected page for another Web application, you must supply a valid username and password for the page. For more information, see the Dashboard application Help.

For more information about the Dashboard playlists, see *Configuring a Dashboard Playlist* (on page 1176).

For more information about configuring a multi-monitor network display, see *Setting up a WhatsUp Multi-Monitor Network Display*, located on the *WhatsUp Gold Support Site* (<http://www.whatsupgold.com/wugtechsupport>).

How does the Dashboard Screen Manager work?

In order for the Dashboard to work, it needs:

- 1 A monitor, or several monitors
- 2 A playlist for each monitor

The Dashboard displays a single playlist on every monitor you configure for use with the Dashboard. You can configure as many monitors as you would like for use with the Dashboard.

What is a Dashboard playlist?

On the Dashboard Screen Manager, a playlist is a list of Web pages the Dashboard displays on a single monitor. A playlist can consist of one single, or multiple Web pages. When a playlist is configured with a single Web page, this single page is refreshed on a user-specified refresh interval. When a playlist is configured with multiple Web pages, the playlist cycles through the pages also on a user-specified interval.

Installing the Dashboard Screen Manager

On the device you wish to install the Ipswitch Dashboard Screen Manager:

- 1 Log on to an Administrator account.
- 2 Start the installation program:
If you downloaded the Dashboard from the Ipswitch Web site, run the downloaded installation application.
- 3 Read the Welcome screen. Click **Next** to continue.
- 4 Read the license agreement. Select the appropriate option, then click **Next**.
- 5 Select the install directory for the Dashboard. The default is:
`C:\Program Files\Ipswitch\Dashboard`
To browse and select an install directory different than that of the default location, click **Change**.
Click **Next** to continue.
- 6 Click **Install** to install the Ipswitch Dashboard.



Note: To terminate the installation once it has begun, click **Cancel**.

- 7 Make your selection, then click **Finish**.

Disable script debugging in Internet Explorer

After you have installed the Dashboard Screen Manager, it is important that you make sure script debugging is disabled. Otherwise, a debugging program will pop-up and could crash the Dashboard. By default, script debugging is disabled, but if you are unsure or know that you have it enabled, you can check this setting in Internet Explorer.

To disable script debugging in Internet Explorer:

- 1 Open Internet Explorer and go to **Tools > Internet Options**. The Internet Options dialog appears.
- 2 Select the **Advanced** tab.
- 3 Scroll down and check the **Disable Script Debugging (Internet Explorer)** and the **Disable Script Debugging (Other)** options.
- 4 Click **OK** to save changes.

Opening the Dashboard Screen Manager

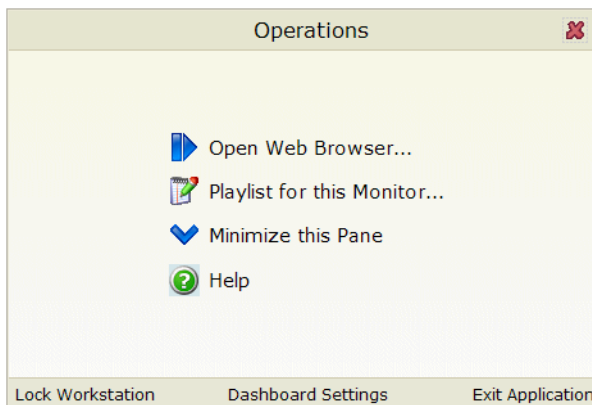
After successfully installing the Dashboard, you can access the application from your Windows Start Menu by selecting **Ipswitch Dashboard > Dashboard**.



Note: This changes if after the initial setup of the Dashboard, you choose to run the Dashboard at Startup (on the Dashboard Settings dialog). If you choose to do so, the Dashboard Screen Manager will automatically take you to the blank screen discussed below.

When the dashboard first opens, a blank screen is displayed. The blank page's title bar reads, "Ipswitch Dashboard [Configure the 'Playlist' for the Dashboard by clicking a mouse button] - aboutblank."

If you have multiple displays, you will see a Dashboard application instance for each display in the taskbar. For example, if you have three display devices, DISPLAY1, DISPLAY2, or DISPLAY3 shows in the taskbar. Select the display you want to configure first, then click a button on your mouse to open the Dashboard Operations dialog. From here, you can *configure Dashboard playlists* (on page 1176).



Configuring a Dashboard Screen Manager playlist

Keep in mind that you need to set up a playlist for each physical monitor on which you want to display Web pages through the Dashboard Screen Manager.

To configure a single Web page playlist:

If you have chosen not to run the Dashboard Screen Manager upon Startup, click **Start > Programs > Ipswitch Dashboard > Dashboard**. The Dashboard Operations dialog appears.

- or -

If you have chosen to run the Dashboard Screen Manager upon Startup, on the display you want to configure a playlist for, click on the screen and the Dashboard Operations dialog appears.

- 1 On the Dashboard Operations dialog, select **Playlist for this Monitor**. The Pane Properties dialog appears.

Pane Properties - DISPLAY1

☒ Display single Web page

Title bar text:

URL:

Refresh interval: (seconds)

Web login:
 ...

☐ Cycle through multiple Web pages

| Description | URL |
|-------------|-----|
| | |

Add...
Edit...
Remove...
Up...
Down...

OK Cancel Help

- 2 Select **Display single Web page**.
- 3 Enter the appropriate information in the following fields:
 - **Title bar text.** Enter the title bar name for the Dashboard display.
 - **URL.** Enter or paste the URL for the Web page you want to display in the following format:

```
http://www.websitename.com/webpagename
```
 - **Refresh interval (in seconds).** Enter an amount of time (in seconds) for how often you would like the Web page to refresh.
 - **WhatsUp Gold Web login.** Either select a user from the drop-down list, or click the browse (...) button to choose a user from the WhatsUp Gold Web Login Library. This user account is used for the Dashboard application to log-in to a password protected site. Without a proper user account, the application is not able to display a password-protected Web page. If you are using a non-WhatsUp Gold Web page, set the Web login to **None**.



Note: Other applications requiring a username and password to display Web pages can be used in the Dashboard Screen Manager. You can specify these other application username and passwords in the **URL** field, appended to the Web page URL.

- 4 Click **OK** to save changes.



Important: The Web Login drop-down list is empty until you populate the Web Login Library with users. You can do this via the Web Login Library dialog.

To configure a multiple Web page playlist:

If you have chosen not to run the Dashboard Screen Manager upon Startup, click **Start > Programs > Ipswitch Dashboard > Dashboard**. The Dashboard Operations dialog appears.

- or -

If you have chosen to run the Dashboard Screen Manager upon Startup, on the display you want to configure a playlist for, click on the screen and the Dashboard Operations dialog appears.

- 1 On the Dashboard Operations dialog, select **Playlist for this Monitor**. The Pane Properties dialog appears.
- 2 On the display you want to configure a playlist for, select **Playlist for this Monitor**. The Pane Properties dialog appears.
- 3 Select **Cycle through multiple Web pages**.
- 4 Click the **Add** button to add Web pages to the list. The Add URL to Playlist dialog appears.
- 5 Enter the appropriate information in the following fields:
 - **Title bar text.** Enter the title bar name for the Dashboard display.
 - **URL.** Enter or paste the URL for the Web page you want to display in the following format:
`http://www.websitename.com/webpagename`
 - **Refresh interval (in seconds).** Enter an amount of time (in seconds) for how long you would like the Web page to be on the screen.
 - **WhatsUp Gold Web login.** Either select a user from the drop-down list, or click the browse (...) button to choose a user from the WhatsUp Gold Web Login Library. This user account is used for the Dashboard application to log-in to a WhatsUp Gold Web page. Without a proper user account, the application is not able to display a password-protected Web page. If you are using a non-WhatsUp Gold Web page, set the Web login to **None**.



Note: Other applications requiring a username and password to display Web pages can be used in the Dashboard Screen Manager. You can specify these other application username and passwords in the **URL** field, appended to the Web page URL.

- 6** Click **OK** to add the new Web page to the playlist.
- 7** Edit and Remove Web pages by selecting a Web page from the list and then clicking the **Edit** or **Remove** button.
- 8** Click **OK** to save changes.

Copyright notice

©1991-2011 Ipswitch, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the expressed prior written consent of Ipswitch, Inc.

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc., also assumes no liability for damages resulting from the use of the information contained in this document.

IMail, the IMail logo, WhatsUp, the WhatsUp Gold logo, WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

This document was published on Tuesday, June 21, 2011 at 18:41.