IPSWITCH

WhatsUp Gold

Getting Started Guide

v16.4

WhatsUpGold

IT MANAGEMENT MADE SIMPLE

CHAPTER 1

Welcome

Deploying

CHAPTER 1

Welcome

In This Chapter

Welcome to WhatsUp Gold

Network and application infrastructures are some of the most critical elements in business strategy. High reliance on network or application availability requires that all businesses—from SMBs to Enterprises—take a proactive approach to preventing and resolving outages with minimal impact to productivity and revenue. The Ipswitch WhatsUp Gold product family leverages a powerful, yet affordable, easy-to-deploy and use, network tools suite that ensures you know the pulse of the network at all times so you can respond quickly to changes. When combining your network hardware with the value of WhatsUp Gold, you can be confident that you have the tools to manage your network easily and reliably.

This WhatsUp Gold Getting Started guide provides overview information about the WhatsUp Gold products—WhatsUp Gold, WhatsUp Flow Monitor, WhatsConfigured, and WhatsVirtual—and suggests other network tools to increase visibility and access to real-time network performance data.

About WhatsUp Gold

WhatsUp Gold monitors, reports, alerts, and takes action on the status of network devices, the system, and services. WhatsUp Gold installs, discovers, and maps topology and network connected assets in minutes. Leveraging SNMP v1/2/3 and WMI, it enables monitoring in combination with powerful alerting and notification capabilities to keep the network infrastructure running and you informed when issues arise. Intuitive web-enabled dashboard reports provide quick navigation to over 200 reports, documenting all device, bandwidth and application-related activity. WhatsUp Gold ensures network managers have 360-degree visibility, actionable intelligence, and complete control to make smarter decisions faster. For more information about what's new in WhatsUp Gold, see the *WhatsUp Gold release notes* (*http://www.whatsupgold.com/support/index.aspx*).

WhatsUp Gold Editions

WhatsUp Gold is available in three primary editions. Each edition tailors features to meet the diverse network management needs, from small networks to those spanning multiple geographic locations. Learn more about WhatsUp Gold on the WhatsUp Gold web site.

WhatsUp Gold also offers a variety of optional products to provide a full-line of advanced network monitoring tools:

Optional plug-ins

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

WhatsUp Gold WhatsConfigured. This configuration management plug-in enables effective management of one of the most critical assets on your network—device configurations. It automates the key configuration and change management tasks required to backup, compare, and upload configuration files for networking devices. WhatsConfigured maintains and controls configuration files and alerts when any configuration changes are detected. For more information, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/WhatsConfigured*).

WhatsUp Gold Flow Monitor. This plug-in for WhatsUp Gold leverages Cisco NetFlow, NetFlow v9 (Lite), sFlow, J-Flow, IPFIX, and Border Gateway Protocol (BGP) data from switches, routers, and Adaptive Security Appliances (ASA). It gathers, analyzes, reports, and alerts on LAN/WAN network traffic patterns and bandwidth utilization in real-time. It highlights not only overall utilization for the LAN/WAN, specific devices, or interfaces; it also indicates users, applications, and protocols that are consuming abnormal amounts of bandwidth, giving you detailed information to assess network quality of service and quickly resolve traffic bottlenecks. WhatsUp Flow Monitor protects network security by detecting unusual activity, such as that exhibited by viruses, worms, DOS attacks, and other rogue activity directed at your network. Comprehensive reporting takes the raw real-time network traffic data from routers and switches and presents you with useful information to understand trends, utilization, and where network bandwidth is consumed. For more information, see the WhatsUp Gold Flow Monitor User Guide on the *WhatsUp Gold web site* (*http://www.whatsupgold.com/NetFlowMonitor*).

WhatsUp Gold WhatsVirtual. This plug-in lets you monitor virtual environments using WhatsUp Gold. The WhatsVirtual plug-in provides WhatsUp Gold with the ability to discover, map, monitor, alert, and report on virtual environments. For more information, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/WhatsVirtual*).

WhatsUp Gold VoIP Monitor. This plug-in for WhatsUp Gold measures your network's ability to provide the quality of service (QoS) necessary for your VoIP calls on your LAN and WAN links. After a simple setup, the VoIP Monitor accesses Cisco IP SLA (service level agreement) enabled devices to monitor VoIP performance and quality parameters including jitter, packet loss, latency, and other performance values. The plug-in's full integration with WhatsUp Gold allows you to easily view graphs and metrics for bandwidth and interface utilization and troubleshoot network issues that affect VoIP performance. For more information, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/products/Voip_Monitor*).

Optional applications

WhatsUp Gold WhatsConnected. This application is a Layer 2/3 network mapping tool that discovers, maps and documents your network down to the individual port, making it simple to visualize the physical topology and understand device interconnections. This application is a standalone and is used separately from an instance of WhatsUp Gold. For more information, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/products/WhatsConnected*).

WhatsUp Log Management. This application suite provides comprehensive event and Syslog log collection, monitoring, analysis, reporting and storage for your network. The suite includes Event Analyst, Event Archiver, Event Alarm and Event Rover. For more information, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/LogManagement*).

AlertFox End-User Monitor. This application provides comprehensive synthetic web transaction monitoring capabilities from an end-user perspective. With just a push of a button, a browser-based recorder captures all the steps involved in a web transaction, so you can periodically exercise and measure mission-critical transactions as often as you need to. AlertFox EUM is offered as Software-as-a-Service (SaaS), has minimal software to install, and requires no long-term financial commitments. For more information, see the *WhatsUp Gold web site* (*http://www.whatsupgold.com/AlertFoxEUM*).

WhatsUp Gold Failover Manager. The WhatsUp Gold Failover Manager is designed to make your network monitoring and management tasks more resilient for high availability operation. It ensures continuous visibility into the health of the monitored infrastructure when the performance or connectivity of the primary WhatsUp Gold server is impaired. In such cases a secondary 'failover' server can be automatically set to take over monitoring tasks. WhatsUp Gold Failover Manager is integrated into the Alert Center for appropriate notifications and escalations. For more information, see the *WhatsUp Gold site* (*http://www.whatsupgold.com/FailoverMgr*).

WhatsUp Gold Flow Publisher. This application provides a unique insight and visibility into your network traffic for every device, whether they natively support flow monitoring or not. Flow Publisher makes flow monitoring possible for every network segment and for literally every device. By capturing raw traffic from the network and converting it into standard NetFlow records, Flow Publisher puts you in complete control and conversing in a language your users understand. For more information, see the *WhatsUp Gold site* (*http://www.whatsupgold.com/FlowPublish*).

IP Address Manager. This application provides an automated solution to the cumbersome and error prone task of inventorying network address usage. IP Address Manager discovery scans provide you with an extensive breakdown of your network's subnets, DHCP, and DNS servers. These discovery scans can be scheduled to run automatically to gather up-to-date inventory information on a daily basis. Inventory information can be saved, exported, and distributed in multiple formats as reports. For more information, see the *WhatsUp Gold site* (*http://www.whatsupgold.com/IPAMsite*).

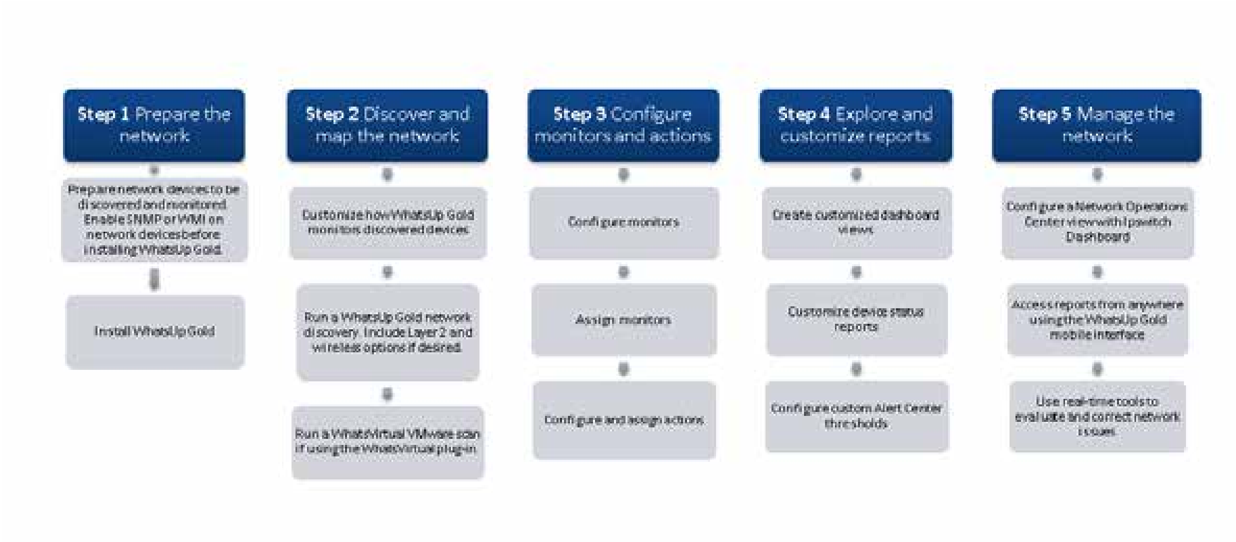
CHAPTER 2

Deploying

In This Chapter

Deploying WhatsUp Gold

WhatsUp Gold makes it easy to deploy and be running quickly so you can get started monitoring and managing your network. Use the following guideline to deploy WhatsUp Gold and WhatsUp Gold plug-ins, then begin managing your network.


Step 1 Prepare the network
Prepare network devices to be discovered and monitored. Enable SNMP or WMI on network devices before installing WhatsUp Gold.
Install WhatsUp Gold
Step 2 Discover and map the network
Customize how WhatsUp Gold monitors discovered devices
Run a WhatsUp Gold network discovery. Include Layer 2 and wireless options if desired.
Run a WhatsVirtual VMware scan if using the WhatsVirtual plug-in.
Step 3 Configure monitors and actions
Configure monitors
Assign monitors
Configure and assign actions
Step 4 Explore and customize reports
Create customized dashboard views
Customize device status reports
Configure custom Alert Center thresholds
Step 5 Manage the network
Configure a Network Operations Center view with Ipswitch Dashboard
Access reports from anywhere using the WhatsUp Gold mobile interface
Use real-time tools to evaluate and correct network issues

STEP 1: Prepare the network

Preparing devices for discovery

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

Preparing devices to be discovered

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

- Ping (ICMP)
- Scanning for open TCP ports

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

Preparing devices to be identified

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

Enabling SNMP on devices

We recommend that important devices be configured to respond to SNMP requests; SNMP v2/v2c credentials are preferred. For information about how to enable SNMP on a specific device, see Enabling SNMP on Windows devices in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*) or consult the network device documentation.

Enabling WMI on devices

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

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

Install and enable 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. Use one of the following procedures to install SNMP Services on your network Windows systems. Refer to the device hardware documentation for specific instructions on enabling SNMP Services for the product.

Install SNMP Service on Windows devices

To install SNMP Service on Windows Server 2012:

1 From the Server Manager Dashboard, click **Add roles and features**. The Add Roles and Features Wizard appears.

2 Click **Next**. The Installation Type page appears.

3 Select **Role-based or feature-based installation**, then click **Next**. The Server Selection page appears.

4 Select **Select a server from the server pool**, then click **Next**. The Server Roles page appears.

5 Select **File and Storage Services**, then click **Next**. The Features page appears.

6 Select **SNMP Service**. The Add features that are required for SNMP Service dialog appears.

7 Click **Add Features**, then click **Next**. The Confirm installation selections page appears.

8 Select **Restart the destination server automatically if required**, then click **Yes > Install**. The SNMP Service installs.

9 After successful installation, click **Close**.

To install SNMP Service on Windows Server 2008:

1 In the Windows Control Panel, click **Programs and Features**.

2 Click **Turn Windows features on or off**.

3 Select **Server Manager** in the left panel. The Server Manager option appears on the right panel.

4 Under **Features Summary**, click **Add Features**. The Add Features Wizard appears.

5 Select **SNMP Services**, then click **Next**.

6 On the Confirm Installation Selections dialog, click **Install**.

7 After successful installation, click **Close**.

To install SNMP Service on Windows Server 2003:

1 In the Windows Control Panel, click **Programs and Features**.

2 Click **Add/Remove Windows Components**. The Windows Components Wizard appears.

3 From the Components list, select **Management and Monitoring Tools**.

4 Click **Details** to view the list of Subcomponents.

5 Select **Simple Network Management Protocol**, then click **OK.**

6 Click **Next** to install the components.

7 After the install wizard is complete, click **Finish** to close the window.

Enable SNMP Service on Windows devices

After the Windows SNMP Service has been installed, make sure that the service is enabled to run on the device.

To enable SNMP Service on Windows systems:

1 In the Windows 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 Network Performance Monitor 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.

Enable WMI on Windows devices

Before you can collect performance data on a Windows computer using Windows Management Instrumentation (WMI), you must first enable the WMI Monitoring Service. WMI is automatically installed on Windows systems, but is not automatically enabled. Use the following procedure to enable the WMI Monitoring Service on Windows systems.

To enable the WMI service on Windows devices and servers:

1 In the Windows Control Panel, click **Administrative Tools**. If you have trouble locating this in your Control Panel, enter `Administrative Tools` in the Search box, then press ENTER.

2 Double-click **Computer Management**. The Computer Management console appears.

3 Expand **Services and Applications**, then click **Services**.

4 Scroll down to the **Windows Management Instrumentation** service. Right-click the service name to Start the service if it is not running.

5 If the Startup Type is not set to Automatic, right-click the service name, then click **Properties**. On the Properties dialog, set the Startup Type to *Automatic*, then click **OK**.

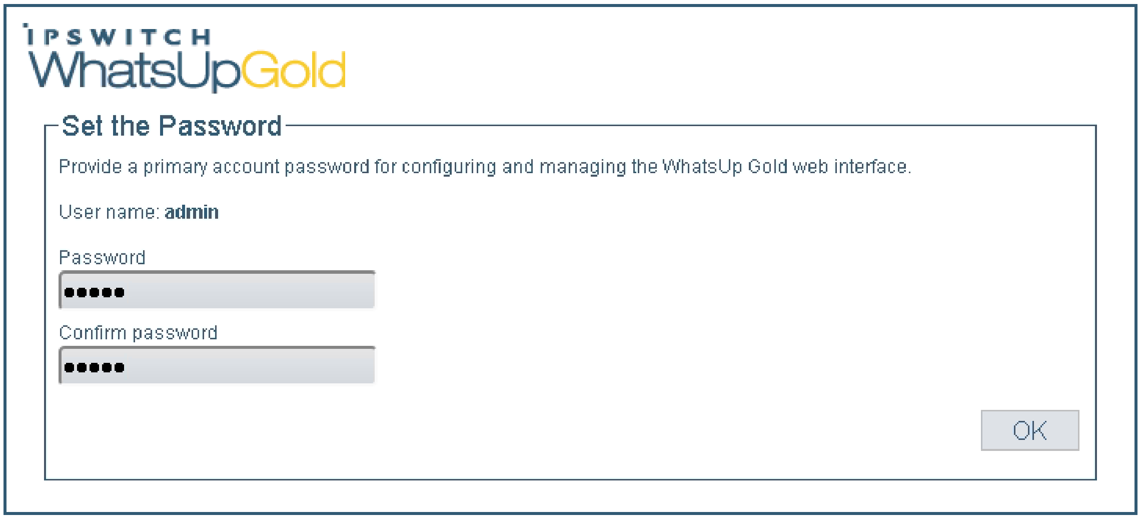
Download and install WhatsUp Gold

Download WhatsUp Gold and any WhatsUp Gold plug-ins from the links provided in the product license email from Ipswitch or visit the *WhatsUp Customer Portal* (*http://www.whatsupgold.com/wugCustPortal*) to download your software. If you are evaluating, use the evaluation license to activate WhatsUp Gold.

The WhatsUp Gold installation program bundles and delivers prerequisites for the application, including Microsoft .NET Framework 4.0 and Microsoft SQL Server 2008 R2 Express Edition. Because of the need for a more robust and feature rich web platform, Microsoft IIS 6 or Microsoft IIS 7 has become the web server for supporting the WhatsUp Gold Web Interface and its associated web services. The installation program automatically configures IIS 7; however, IIS 6 must be enabled prior to the WhatsUp Gold installation. For more information, see Installing and Configuring WhatsUp Gold v16.3 and the Release Notes on the *Support Site* (*http://www.whatsupgold.com/support/index.aspx*).

When you start the WhatsUp Gold installation, the setup wizard is launched. This setup workflow allows you to:

- Create the login password for the primary WhatsUp Gold administrator account.



Set the Password

Provide a primary account password for configuring and managing the WhatsUp Gold web interface.

User name: **admin**

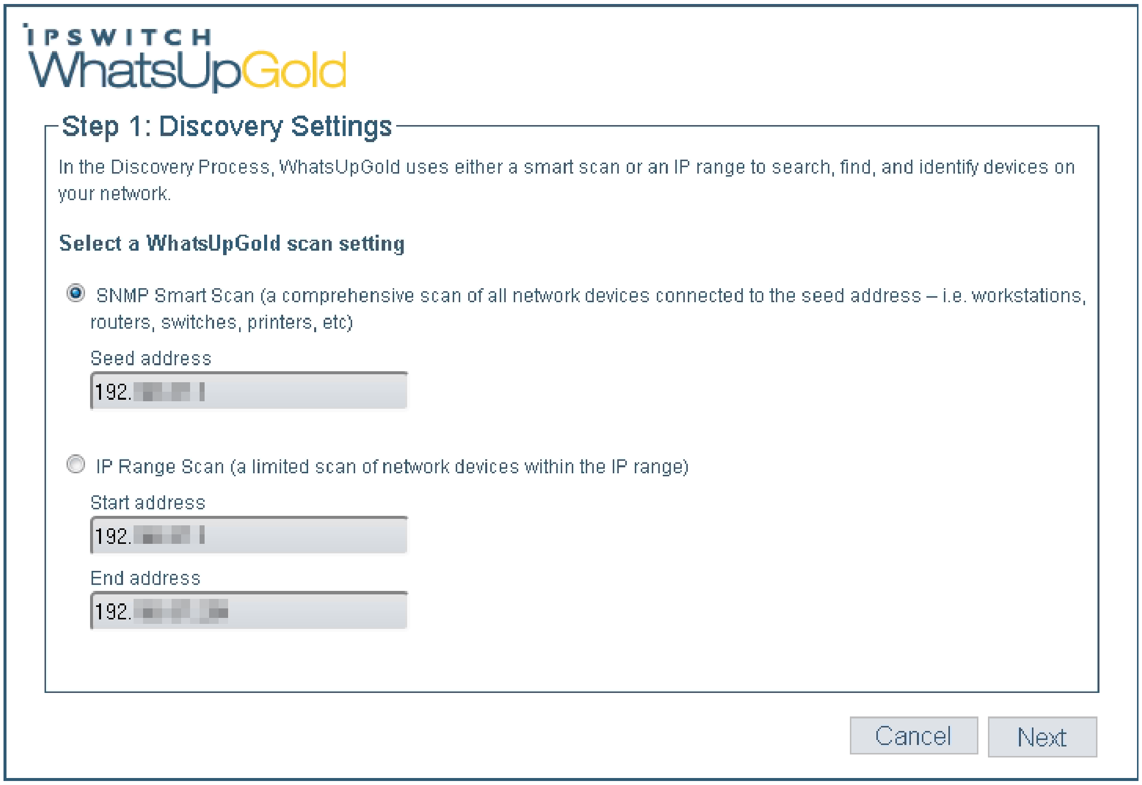
Password

●●●●●

Confirm password

●●●●●

- Specify either a range of IP addresses or a single seed address from which to initiate an SNMP smart scan for your initial device discovery.



Step 1: Discovery Settings

In the Discovery Process, WhatsUpGold uses either a smart scan or an IP range to search, find, and identify devices on your network.

Select a WhatsUpGold scan setting

● SNMP Smart Scan (a comprehensive scan of all network devices connected to the seed address – i.e. workstations, routers, switches, printers, etc)

Seed address

192.[redacted]

○ IP Range Scan (a limited scan of network devices within the IP range)

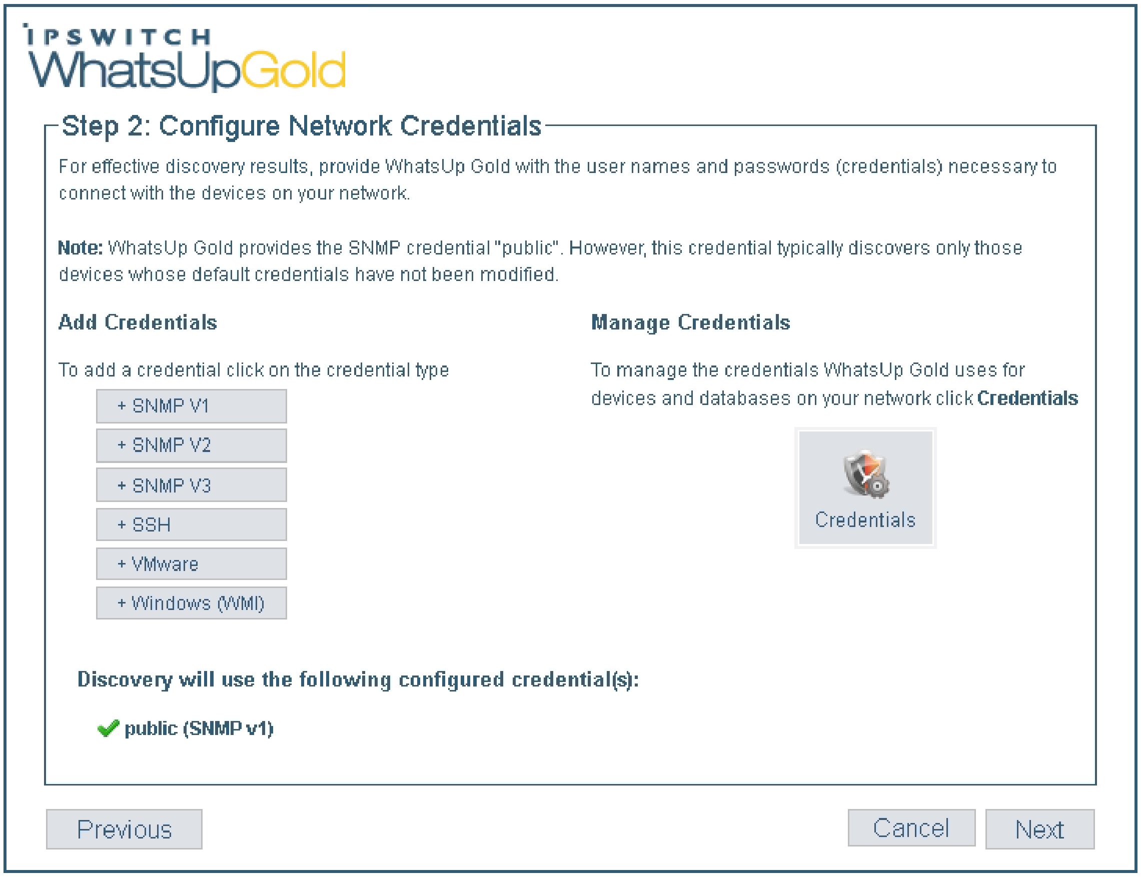
Start address

192.[redacted]

End address

192.[redacted]

- Add network *device credentials* for your SNMP communities, WMI, and other credential types, such as VMware for the WhatsVirtual plug-in and SSH credentials for the WhatsConfigured plug-in. This information helps you accomplish better device discovery results in WhatsUp Gold.



Step 2: Configure Network Credentials

For effective discovery results, provide WhatsUp Gold with the user names and passwords (credentials) necessary to connect with the devices on your network.

Note: WhatsUp Gold provides the SNMP credential "public". However, this credential typically discovers only those devices whose default credentials have not been modified.

Add Credentials

To add a credential click on the credential type

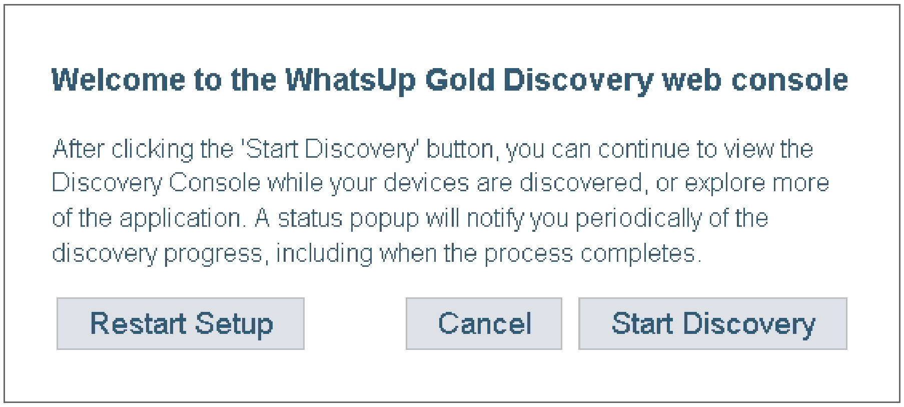
Manage Credentials

To manage the credentials WhatsUp Gold uses for devices and databases on your network click **Credentials**

Discovery will use the following configured credential(s):

✓ **public (SNMP v1)**

- *Start discovery* and notify you when the discovery is finished.



Welcome to the WhatsUp Gold Discovery web console

After clicking the 'Start Discovery' button, you can continue to view the Discovery Console while your devices are discovered, or explore more of the application. A status popup will notify you periodically of the discovery progress, including when the process completes.

Configure Flow Monitor on key devices (optional for Flow Monitor plug-in users)

✓ **Important**: The following information is an overview example. The process for configuring a device to export Flow data varies widely from device to device and is dependent upon your network configuration. Please see your router or switch documentation to determine the correct steps for configuring your device.

WhatsUp Flow Monitor collects NetFlow, NetFlow-Lite, sFlow, or J-Flow data exported from network routers and switches. If you use the WhatsUp Gold Flow Monitor plug-in to monitor network bandwidth utilization, the following example shows the command line interface commands required to enable NetFlow exports for devices on which you want to enable network bandwidth monitoring:

```
ip flow-export version 9
```

```
ip flow-export destination 192.168.28.4 9999
```

Tip: Instead of 192.168.28.4 9999, use the IP address of your WhatsUp Gold server.

In addition, configure each interface to export data to WhatsUp Flow Monitor.

```
ip flow ingress
```

- or –

```
ip flow egress
```

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 displayed in Flow Monitor reports. Any other configuration results in all private addresses reporting as the public addresses of the device performing the network address translation.

WhatsUp Flow Monitor automatically begins tracking network bandwidth utilization when it receives flow data. For more detailed Flow Monitor configuration information, see the WhatsUp Gold Flow Monitor Help and the documentation for the router/switch that is exporting data to WhatsUp Flow Monitor.

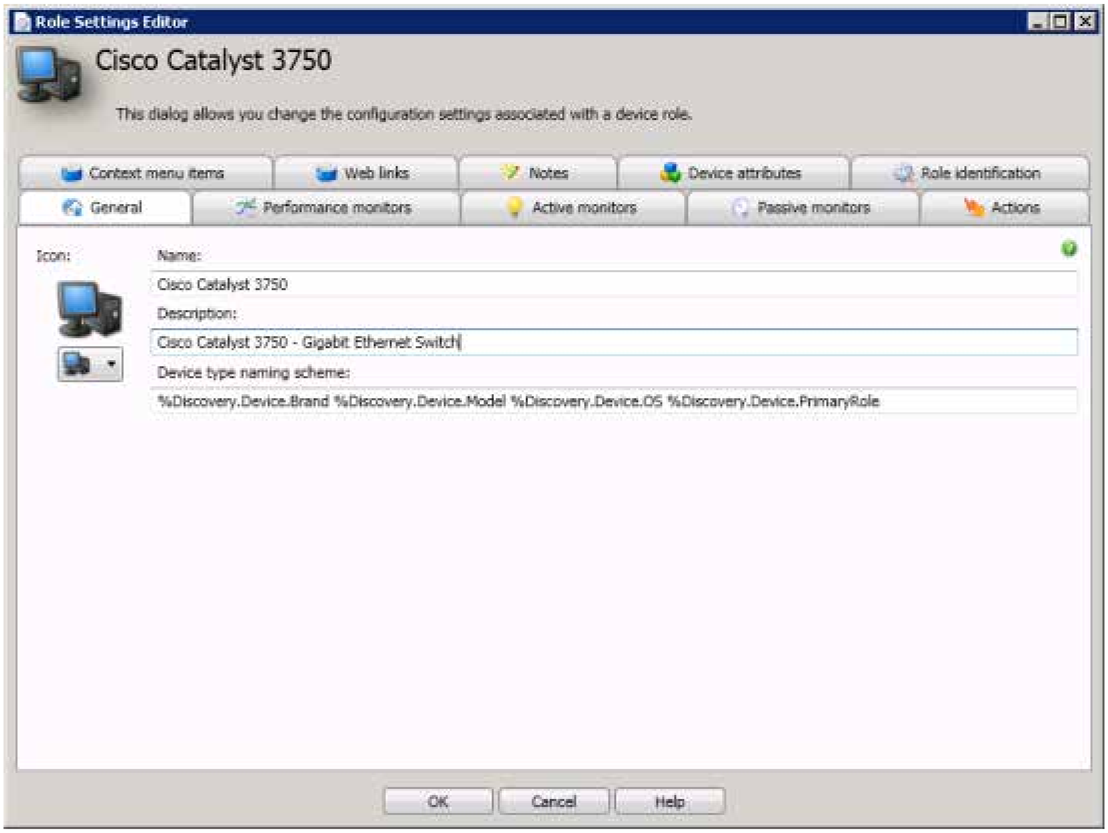
STEP 2: Discover and map the network

Customize device roles

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

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.



Cisco Catalyst 3750

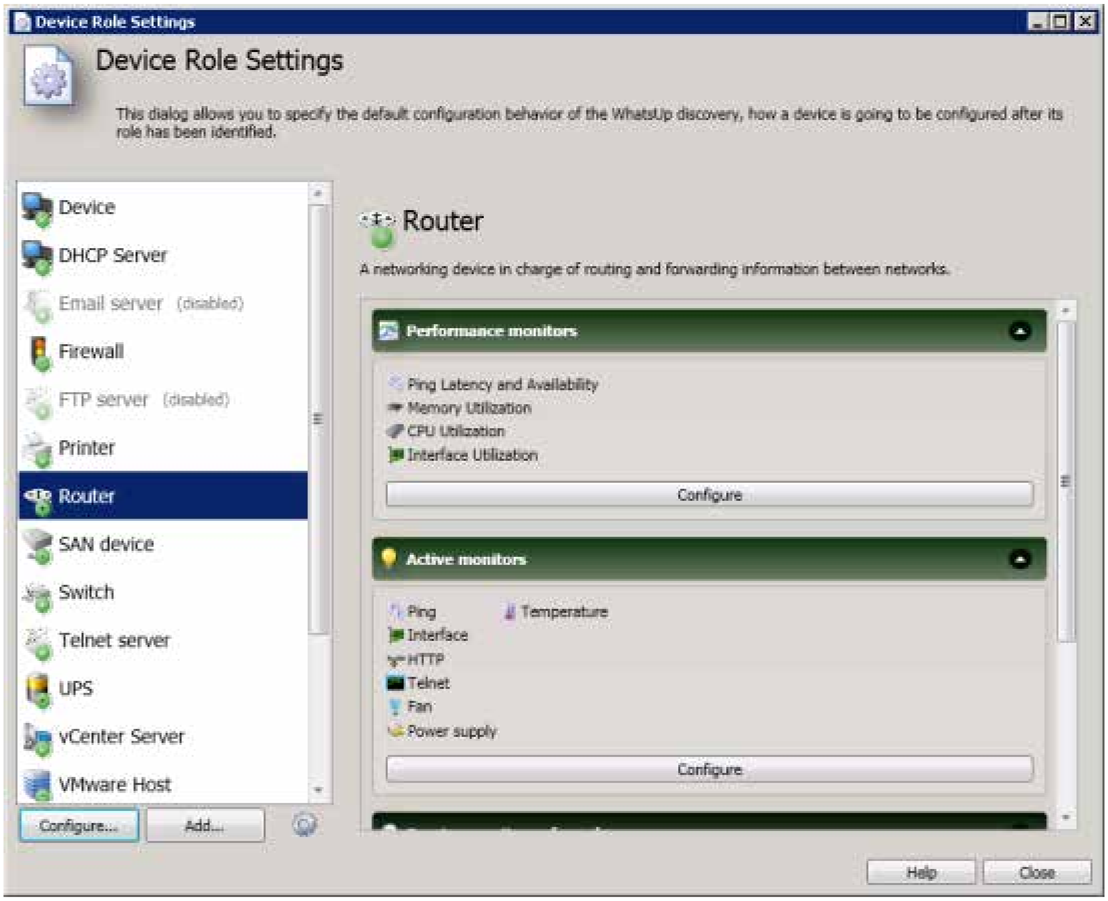
This dialog allows you change the configuration settings associated with a device role.

Name:
Cisco Catalyst 3750

Description:
Cisco Catalyst 3750 - Gigabit Ethernet Switch

Device type naming scheme:
%Discovery.Device.Brand %Discovery.Device.Model %Discovery.Device.OS %Discovery.Device.PrimaryRole

WhatsUp Gold provides several default device roles that are used to identify most common network devices. These default roles should correctly identify the majority of devices on the network, but you can modify the device roles to customize what is monitored on each device and what action policy is applied. Device Roles are managed in the WhatsUp Gold console (**File > Discover Devices > Advanced > Device role settings**).



Device Role Settings

This dialog allows you to specify the default configuration behavior of the WhatsUp discovery, how a device is going to be configured after its role has been identified.

Router

A networking device in charge of routing and forwarding information between networks.

In addition, you can create new device roles to specify how WhatsUp Gold monitors and reports on devices it does not natively recognize. For more information, see Using Device Roles in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Discover the network

As described in the *Download and install WhatsUp Gold* (on page 8) section of this guide, after the installation process, WhatsUp Gold steps through the setup workflow for the password setup, discovery settings, configuring network credentials, and starting the first discovery. If you have used this setup wizard you can proceed to STEP 3.

If you have not used the setup wizard or prefer to complete a discovery from the Discovery Console, you can use the WhatsUp Gold Discovery console (**Devices > Discovery Console**) to discover network devices. We recommend using the **SNMP Smart Scan** option to discover the network.

Discovery scan options are:

- **SNMP Smart Scan**. This scan type uses one or more SNMP-enabled devices to identify the devices and sub-networks on your network. Enter an IP address of the Core router and an IP address of each Branch router as seed addresses, and specify a Scan Depth. We recommend a Scan Depth of 2.
- **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.
- **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 addresses.

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

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

- **VMware Scan** (available for WhatsVirtual license). 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.

Select 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 in WhatsUp Gold. For more information, see Using Credentials in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

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

Configure Scan Method

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

- **Ping**. When using this method, WhatsUp Gold detects devices by issuing a ping request via ICMP and listening for a response.

§ **Advanced**. When using this method, WhatsUp Gold first detects all devices that respond to ping. Then, if a device does not respond to ping, WhatsUp Gold scans common TCP ports for a response.

§ **Ping Timeout (seconds)**. Enter the time, in seconds, for a device to respond to a ping scan. If it does not respond to the scan within this time, the scan continues on to the next IP address. The default is 2 seconds.

§ **Ping Retries**. Enter the number of times to attempt to ping a device before continuing on to the next device. The default is 1 retry.

Configure Advanced Settings

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.

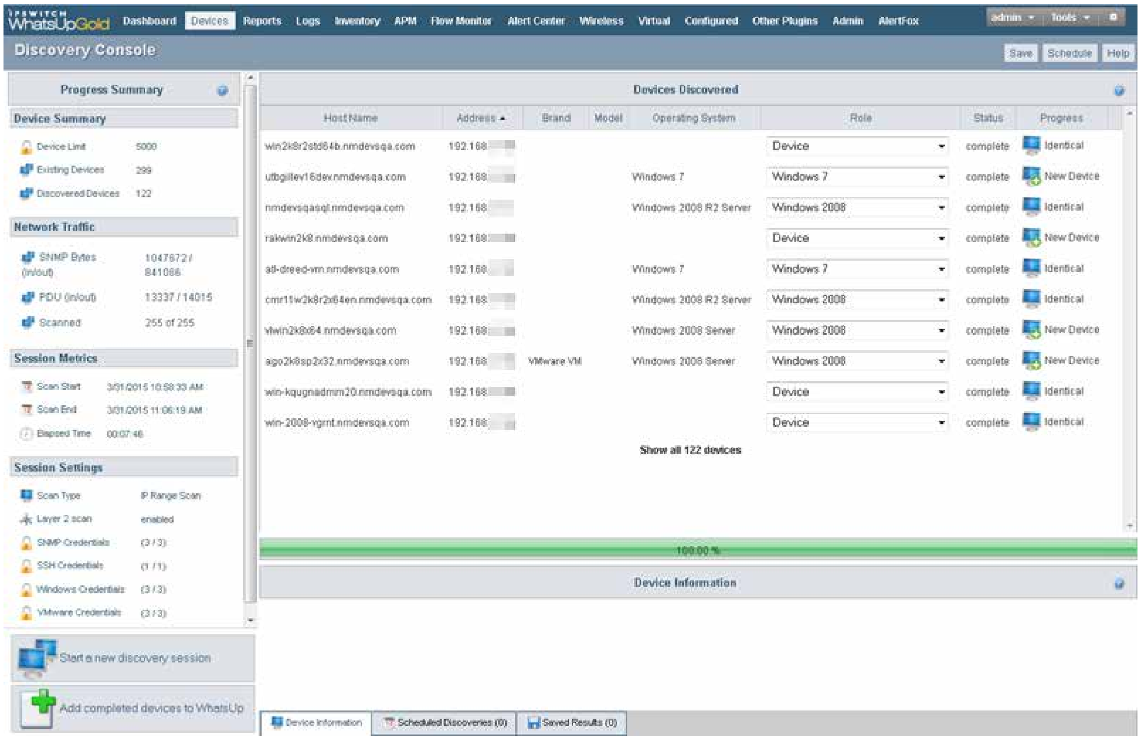
By default, WhatsUp Gold automatically scans for virtual machines hosted by discovered VMware servers. If you do not want WhatsUp Gold to scan for the virtual machines hosted by discovered VMware servers, clear **Auto scan virtual environments**.

By default, WhatsUp Gold automatically uses layer 2 discovery to generate layer 2 topology maps and inventory information available in the Device Viewer. If you do not want WhatsUp Gold to use layer 2 discovery, clear **Use layer 2 discovery and generate layer 2 topology map** to disable Layer 2 discovery.

To ensure wireless devices are found and identified during discovery, select the **Gather information for wireless topology and performance** option. Wireless device discovery is required to setup devices for use with WhatsUp Gold Wireless. You must select this option in order to manage wireless devices. For best results, please ensure the wireless option is enabled prior to discovery. Additionally, do not use single device discovery to add wireless devices to WhatsUp Gold. Devices discovered will not be recognized as wireless devices.

Start Discovery

When you start the discovery session, WhatsUp Gold begins scanning the network and identifying physical devices and virtual devices (if WhatsVirtual is installed). 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 the device brand, model, and operating system. Based on the network device attributes discovered about each device, WhatsUp Gold designates a device role.



Progress Summary

Device Summary

Device Limit	5000
Existing Devices	299
Discovered Devices	122

Network Traffic

SNMP Bytes (in/out)	1047672 / 841086
PDU (in/out)	13337 / 14015
Scanned	255 of 255

Session Metrics

Scan Start	3/01/2015 10:58:33 AM
Scan End	3/01/2015 11:06:19 AM
Elapsed Time	00:07:46

Session Settings

Scan Type	IP Range Scan
Layer 2 scan	enabled
SNMP Credentials	(3 / 3)
SSH Credentials	(1 / 1)
Windows Credentials	(3 / 3)
VMware Credentials	(3 / 3)

Start a new discovery session

Add completed devices to WhatsUp

Devices Discovered

Host Name	Address ▲	Brand	Model	Operating System	Role	Status	Progress
win2k8r2std64b.nmdevsqa.com	192.168.[redacted]				Device	complete	Identical
utbgillev16dev.nmdevsqa.com	192.168.[redacted]			Windows 7	Windows 7	complete	New Device
nmdevsqasql.nmdevsqa.com	192.168.[redacted]			Windows 2008 R2 Server	Windows 2008	complete	Identical
rakwin2k8.nmdevsqa.com	192.168.[redacted]				Device	complete	New Device
atl-dreed-vm.nmdevsqa.com	192.168.[redacted]			Windows 7	Windows 7	complete	Identical
cmr11w2k8r2x64en.nmdevsqa.com	192.168.[redacted]			Windows 2008 R2 Server	Windows 2008	complete	Identical
vlwin2k8x64.nmdevsqa.com	192.168.[redacted]			Windows 2008 Server	Windows 2008	complete	New Device
ago2k8sp2x32.nmdevsqa.com	192.168.[redacted]	VMware VM		Windows 2008 Server	Windows 2008	complete	New Device
win-kqugnadmm20.nmdevsqa.com	192.168.[redacted]				Device	complete	Identical
win-2008-vgmt.nmdevsqa.com	192.168.[redacted]				Device	complete	Identical

Show all 122 devices

100.00 %

Device Information

After all devices are discovered, click **Add completed devices to WhatsUp Gold** to add the discovered devices to a device group and map.

Tip: When VMWare hosts are discovered with the WhatsVirtual plug-in, after you click **Add completed devices to WhatsUp Gold**, the VMWare hosts are listed in the Device View, VMWareScan folder. Double-click a VMWare Host to view the associated virtual machines. You can see a graphical representation of your virtual environment from the Virtual tab in the WhatsUp Gold views dialog.

STEP 3: Configure and assign monitors and actions

Configure monitors

WhatsUp Gold uses three types of monitors to gather information about and report on your network devices. In addition to the monitors applied to devices during discovery through device roles, you can configure supplementary monitors to gather the type of information you feel is necessary to successfully gauge your network's health.

- **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. Active monitors are configured in the Active Monitor Library. For more information, see Configuring Active Monitors in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).
- **Passive monitors** listen 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 Monitors are configured in the Passive Monitor Library. For more information, see Configuring Passive Monitors in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).
- **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 device components:

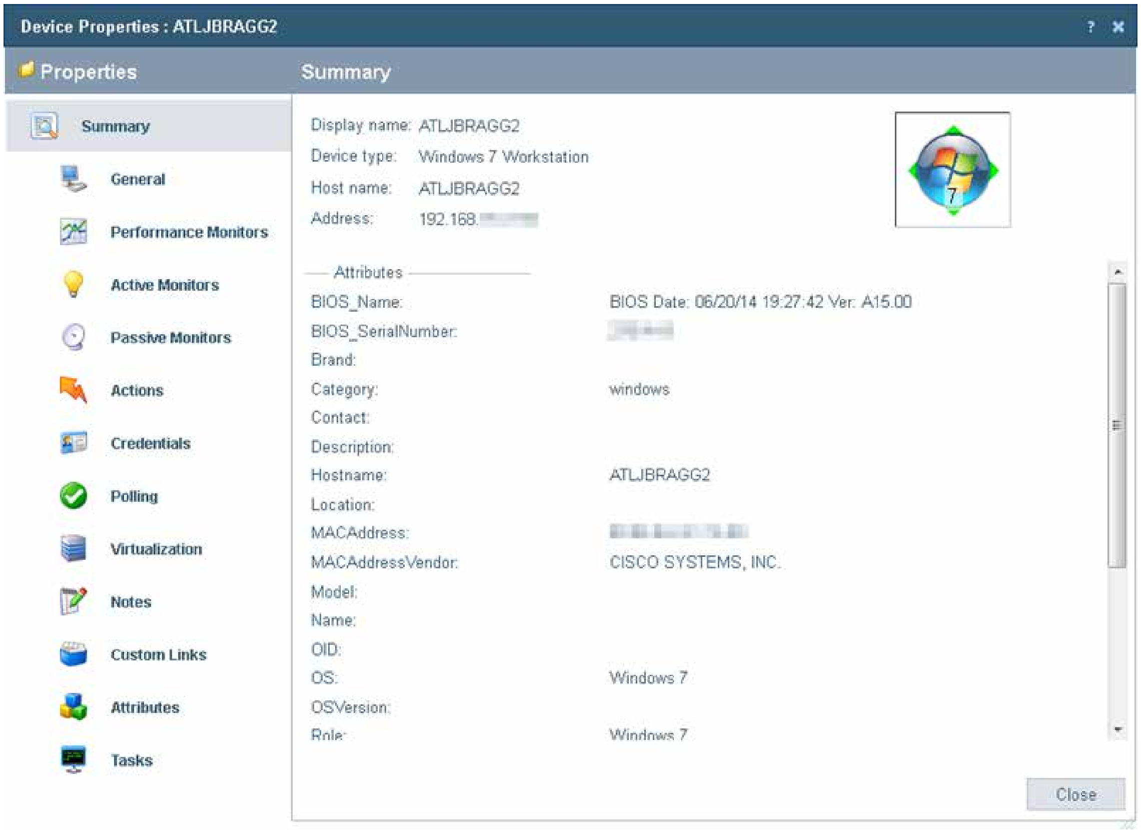
- CPU utilization
- Disk utilization
- Interface utilization
- Interface traffic
- Memory utilization
- Ping availability
- Ping response time

Additionally, you can create custom performance monitors to track specific performance monitors for Active Script, APC UPS, PowerShell Scripting, Printer, SNMP, SQL Query, SSH, WMI Formatted, and WMI performance counters.

Performance Monitors are configured in the Performance Monitor Library. For more information, see Configuring Performance Monitors in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Assign monitors

After you configure relevant monitors in their respective monitor libraries, you then need to assign these monitors to the devices from which you want to gather network data using the Device Properties dialog which is accessed by right-clicking a device in either Device or Map view and then clicking **Properties**.



Display name: ATLJBRAGG2
Device type: Windows 7 Workstation
Host name: ATLJBRAGG2
Address: 192.168.[redacted]

Attributes

BIOS_Name: BIOS Date: 06/20/14 19:27:42 Ver: A15.00
BIOS_SerialNumber: [redacted]
Brand:
Category: windows
Contact:
Description:
Hostname: ATLJBRAGG2
Location:
MACAddress: [redacted]
MACAddressVendor: CISCO SYSTEMS, INC.
Model:
Name:
OID:
OS: Windows 7
OSVersion:
Role: Windows 7

The Device Properties dialog displays all monitors that are currently configured in each of the three monitor libraries.

In addition to adding monitors on a device-by-device basis, you can add monitors to multiple devices using the Bulk Field Change feature. For more information, see Assigning a monitor to multiple devices in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Configure and assign actions

WhatsUp Gold actions are designed to perform a task as a device or monitor state change occurs.

As you configure an action, you choose the task it is to perform. Actions can try to correct the problem, notify someone of the state change, or launch an external application. Also, when you configure an action, you choose whether to assign it to a device, or to an active or passive monitor.

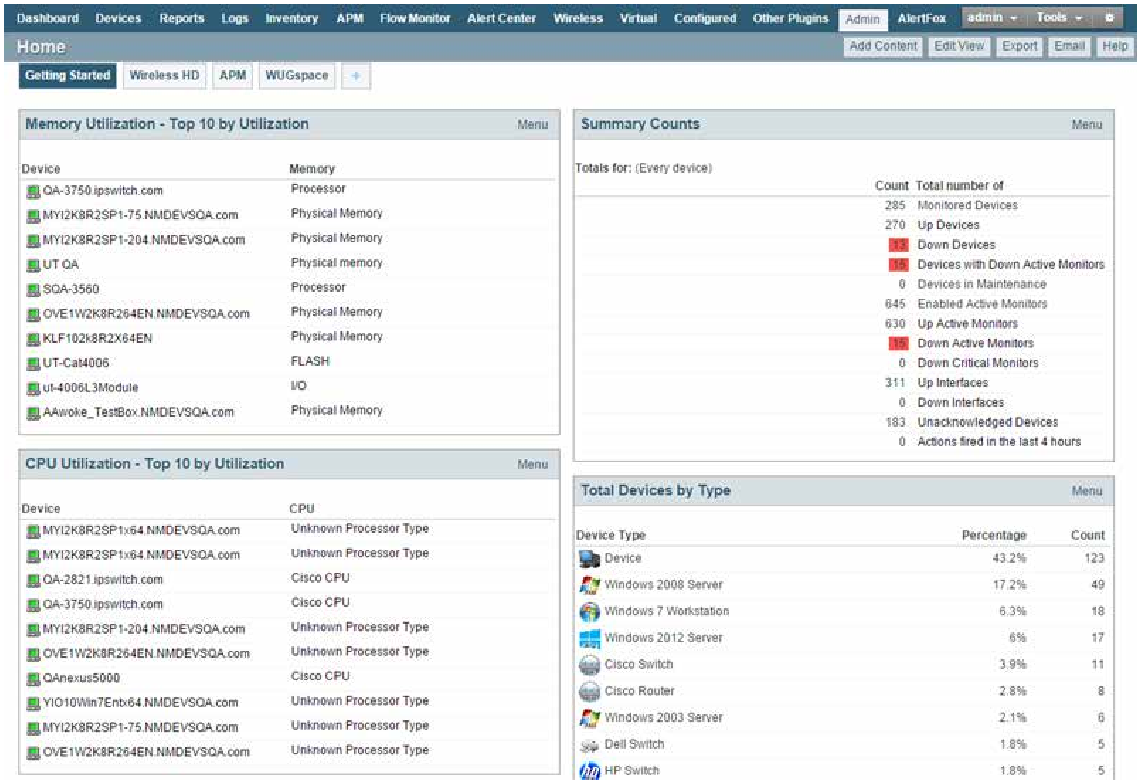
When assigned to an active monitor, actions fire according to the state changes it issues. For example, you can configure an Email Action to send an email alert when the active monitor for a Web server issues a down state change.

You can configure actions on a single device or monitor, or define an Action Policy to use across multiple devices or monitors. Actions are configured in the Action Library. For more information, see Using Actions in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

STEP 4: Explore and customize reports

Set up dashboard views

From the WhatsUp Gold web interface, you can group collections of reports into pages called dashboard views. Dashboard views provide easily accessible and personalized dashboard-style overviews of the health of your network. Referred to as Home, this universal dashboard is designed to display the network information that you need most visible.



Memory Utilization - Top 10 by Utilization

Device	Memory
QA-3750.ipswitch.com	Processor
MYI2K8R2SP1-75.NMDEVSQA.com	Physical Memory
MYI2K8R2SP1-204.NMDEVSQA.com	Physical Memory
UT QA	Physical memory
SQA-3560	Processor
OVE1W2K8R264EN.NMDEVSQA.com	Physical Memory
KLF102k8R2X64EN	Physical Memory
UT-Cat4006	FLASH
ut-4006L3Module	I/O
AAwoke_TestBox.NMDEVSQA.com	Physical Memory

CPU Utilization - Top 10 by Utilization

Device	CPU
MYI2K8R2SP1x64.NMDEVSQA.com	Unknown Processor Type
MYI2K8R2SP1x64.NMDEVSQA.com	Unknown Processor Type
QA-2821.ipswitch.com	Cisco CPU
QA-3750.ipswitch.com	Cisco CPU
MYI2K8R2SP1-204.NMDEVSQA.com	Unknown Processor Type
OVE1W2K8R264EN.NMDEVSQA.com	Unknown Processor Type
QAnexus5000	Cisco CPU
YIO10Win7Entx64.NMDEVSQA.com	Unknown Processor Type
MYI2K8R2SP1-75.NMDEVSQA.com	Unknown Processor Type
OVE1W2K8R264EN.NMDEVSQA.com	Unknown Processor Type

Summary Counts

Totals for: (Every device)

Count	Total number of
285	Monitored Devices
270	Up Devices
13	Down Devices
15	Devices with Down Active Monitors
0	Devices in Maintenance
645	Enabled Active Monitors
630	Up Active Monitors
15	Down Active Monitors
0	Down Critical Monitors
311	Up Interfaces
0	Down Interfaces
183	Unacknowledged Devices
0	Actions fired in the last 4 hours

Total Devices by Type

Device Type	Percentage	Count
Device	43.2%	123
Windows 2008 Server	17.2%	49
Windows 7 Workstation	6.3%	18
Windows 2012 Server	6%	17
Cisco Switch	3.9%	11
Cisco Router	2.8%	8
Windows 2003 Server	2.1%	6
Dell Switch	1.8%	5
HP Switch	1.8%	5

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.

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.

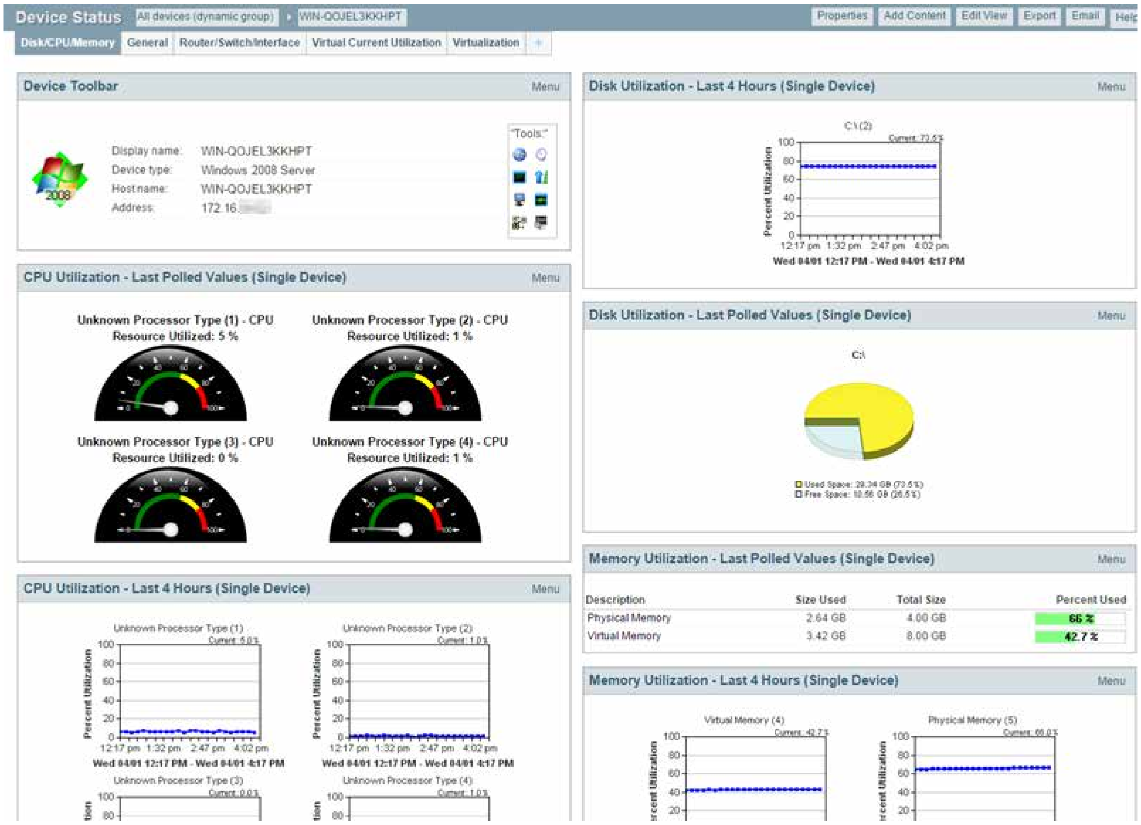
We recommend creating dashboard views to show the health of the network; for example the server room, access points, the core network, and branch offices. In addition, you may want to create dashboard views that show the statuses of devices of different types, such as a *Routers*, *Switches*, *Virtual Machines*, or *VoIP devices* dashboard view. For more information, see

Adding dashboard reports to a dashboard view in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Customize device status reports

The Device Status dashboard provides a detailed view the health of a *single* monitored device by aggregating multiple reports that apply to that device. You can view the Device Status dashboard for any device you are managing with WhatsUp Gold.

The Device Status dashboard is automatically configured to display the most commonly viewed information about a device, but you can customize it to your specific requirements.


Device Status
All devices (dynamic group)
WIN-QOJEL3KKHPT
Properties
Add Content
Edit View
Export
Email
Help
Disk/CPU/Memory
General
Router/Switch/Interface
Virtual Current Utilization
Virtualization
Device Toolbar
Menu
"Tools:"
2008
Disk Utilization - Last 4 Hours (Single Device)
C:\ (2)
Current: 73.5%
Percent Utilization
100
80
60
40
20
0
12:17 pm 1:32 pm 2:47 pm 4:02 pm
Wed 04/01 12:17 PM - Wed 04/01 4:17 PM
CPU Utilization - Last Polled Values (Single Device)
Unknown Processor Type (1) - CPU Resource Utilized: 5 %
Unknown Processor Type (2) - CPU Resource Utilized: 1 %
Unknown Processor Type (3) - CPU Resource Utilized: 0 %
Unknown Processor Type (4) - CPU Resource Utilized: 1 %
Disk Utilization - Last Polled Values (Single Device)
C:\
Used Space: 29.34 GB (73.5%)
Free Space: 10.56 GB (26.5%)
CPU Utilization - Last 4 Hours (Single Device)
Unknown Processor Type (1)
Current: 5.0%
Unknown Processor Type (2)
Current: 1.0%
Unknown Processor Type (3)
Current: 0.0%
Unknown Processor Type (4)
Current: 1.0%
Memory Utilization - Last Polled Values (Single Device)
Memory Utilization - Last 4 Hours (Single Device)
Virtual Memory (4)
Current: 42.7%
Physical Memory (5)
Current: 66.0%

Display name: WIN-QOJEL3KKHPT
Device type: Windows 2008 Server
Host name: WIN-QOJEL3KKHPT
Address: 172.16.[redacted]

Description	Size Used	Total Size	Percent Used
Physical Memory	2.64 GB	4.00 GB	66 %
Virtual Memory	3.42 GB	8.00 GB	42.7 %

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 about the device status.

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.

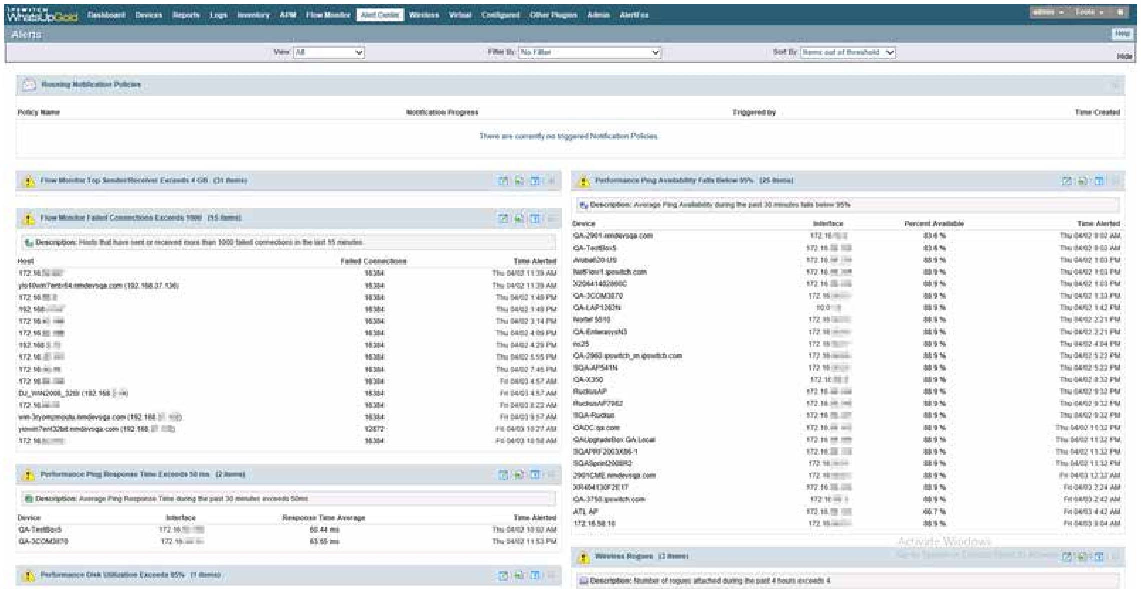
The Disk/CPU/Memory View is the most appropriate view for a Windows or UNIX host that supports the Host Resources MIB for performance monitoring. The Router/Switch/Interface View is the most appropriate view for a manageable Switch or Router that is capable of reporting Interface or Bandwidth utilization.

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 in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Configure Alert Center Thresholds

As soon as WhatsUp Gold is installed and your network is discovered, Alert Center begins monitoring and alerting on a variety of thresholds for devices across the network. Disk, CPU, interface, and memory utilization are tracked for all devices and virtual devices (with the optional WhatsVirtual plug-in), as are ping response time and availability.



Alerts

View: All

Filter By: No Filter

Sort By: Items out of threshold

Running Notification Policies

Policy Name	Notification Progress	Triggered by	Time Created

There are currently no triggered Notification Policies.

Flow Monitor Top Sender/Receiver Exceeds 4 GB (31 items)

Flow Monitor Failed Connections Exceeds 1000 (15 items)

Description: Hosts that have sent or received more than 1000 failed connections in the last 15 minutes.

Host	Failed Connections	Time Alerted
172.16.[redacted]	16384	Thu 04/02 11:39 AM
ylo10vm7entr64.nmdevsqa.com (192.168.37.136)	16384	Thu 04/02 11:39 AM
172.16.[redacted]	16384	Thu 04/02 1:40 PM
192.168.[redacted]	16384	Thu 04/02 1:49 PM
172.16.[redacted]	16384	Thu 04/02 3:14 PM
172.16.[redacted]	16384	Thu 04/02 4:09 PM
192.168.[redacted]	16384	Thu 04/02 4:29 PM
172.16.[redacted]	16384	Thu 04/02 5:55 PM
172.16.[redacted]	16384	Thu 04/02 7:45 PM
172.16.[redacted]	16384	Fri 04/03 4:57 AM
DJ_WIN2008_32Bi (192.168.[redacted])	16384	Fri 04/03 4:57 AM
172.16.[redacted]	16384	Fri 04/03 8:22 AM
win-3ryomzmodu.nmdevsqa.com (192.168.[redacted])	16384	Fri 04/03 9:57 AM
ylowin7ent32bit.nmdevsqa.com (192.168.[redacted])	12872	Fri 04/03 10:27 AM
172.16.[redacted]	16384	Fri 04/03 10:58 AM

Performance Ping Response Time Exceeds 50 ms (2 items)

Description: Average Ping Response Time during the past 30 minutes exceeds 50ms

Device	Interface	Response Time Average	Time Alerted
QA-TestBox5	172.16.[redacted]	60.44 ms	Thu 04/02 10:02 AM
QA-3COM3870	172.16.[redacted]	63.65 ms	Thu 04/02 11:53 PM

Performance Disk Utilization Exceeds 85% (1 items)

Performance Ping Availability Falls Below 95% (25 items)

Description: Average Ping Availability during the past 30 minutes falls below 95%

Device	Interface	Percent Available	Time Alerted
QA-2901.nmdevsqa.com	172.16.[redacted]	83.6 %	Thu 04/02 9:02 AM
QA-TestBox5	172.16.[redacted]	83.6 %	Thu 04/02 9:02 AM
Aruba620-US	172.16.[redacted]	88.9 %	Thu 04/02 1:03 PM
NetFlow1.ipswitch.com	172.16.[redacted]	88.9 %	Thu 04/02 1:03 PM
X20641462860C	172.16.[redacted]	88.9 %	Thu 04/02 1:03 PM
QA-3COM3870	172.16.[redacted]	88.9 %	Thu 04/02 1:33 PM
QA-LAP1262N	10.0.[redacted]	88.9 %	Thu 04/02 1:42 PM
Nortel 5510	172.16.[redacted]	88.9 %	Thu 04/02 2:21 PM
QA-EnterasysN3	172.16.[redacted]	88.9 %	Thu 04/02 2:21 PM
rs25	172.16.[redacted]	88.9 %	Thu 04/02 4:04 PM
QA-2960.ipswitch_m.ipswitch.com	172.16.[redacted]	88.9 %	Thu 04/02 5:22 PM
SQA-AP541N	172.16.[redacted]	88.9 %	Thu 04/02 5:22 PM
QA-X350	172.1[redacted]	88.9 %	Thu 04/02 9:32 PM
RuckusAP	172.16.[redacted]	88.9 %	Thu 04/02 9:32 PM
RuckusAP7962	172.16.[redacted]	88.9 %	Thu 04/02 9:32 PM
SQA-Ruckus	172.16.[redacted]	88.9 %	Thu 04/02 9:32 PM
QADC.qa.com	172.16.[redacted]	88.9 %	Thu 04/02 11:32 PM
QAUpgradeBox.QA.Local	172.16.[redacted]	88.9 %	Thu 04/02 11:32 PM
SQAPRF2003X86-1	172.16.[redacted]	88.9 %	Thu 04/02 11:32 PM
SQASprint2008R2	172.16.[redacted]	88.9 %	Thu 04/02 11:32 PM
2901CME.nmdevsqa.com	172.16.[redacted]	88.9 %	Fri 04/03 12:32 AM
XR4041130F2E17	172.16.[redacted]	88.9 %	Fri 04/03 2:24 AM
QA-3750.ipswitch.com	172.1[redacted]	88.9 %	Fri 04/03 2:42 AM
ATL AP	172.16.[redacted]	66.7 %	Fri 04/03 4:42 AM
172.16.58.10	172.16.[redacted]	88.9 %	Fri 04/03 9:04 AM

Wireless Rogues (2 items)

Description: Number of rogues attached during the past 4 hours exceeds 4

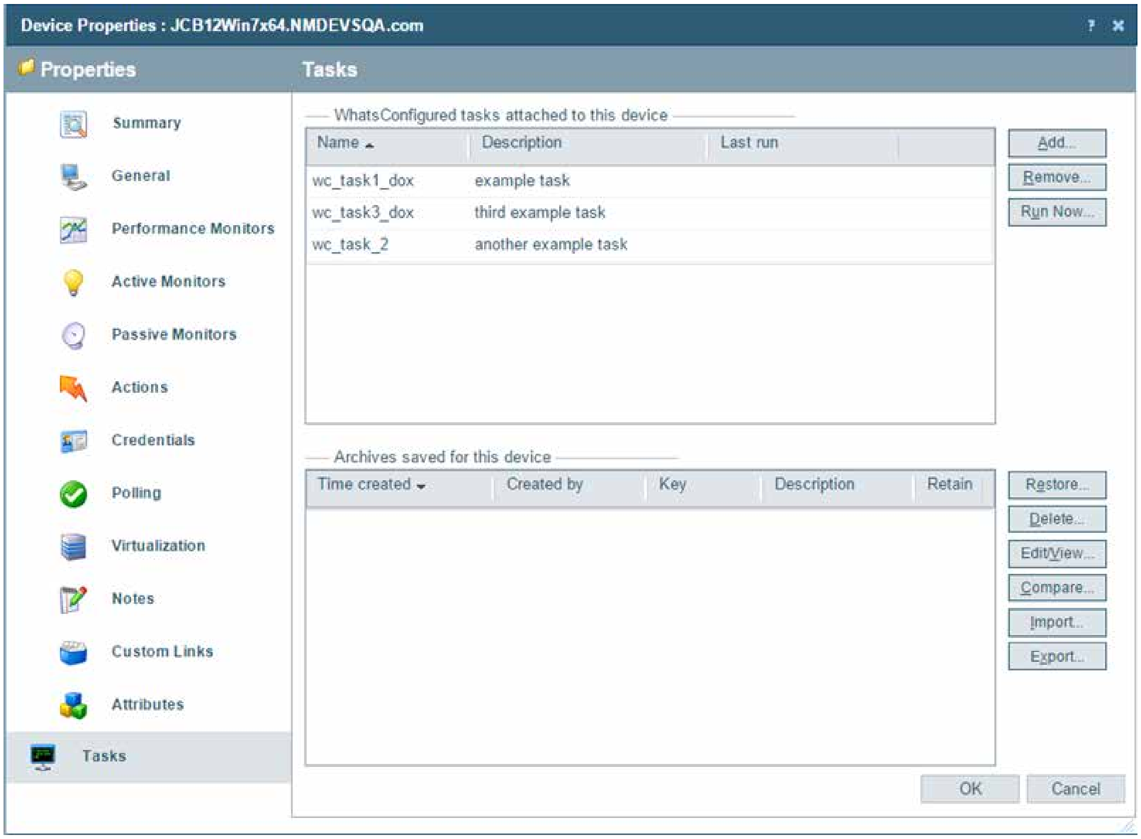
You can create variety of other thresholds to monitor other types of Performance, Passive, System, and Wireless alerts which can be applied to all devices or device groups collecting that type of data. For more information, see Using the Alert Center in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

If you use WhatsUp Gold Flow Monitor or WhatsConfigured plug-ins, additional thresholds are available to expose and alert on network traffic that could indicate a problem.

STEP 5: Manage the network

Configure network devices (optional for WhatsConfigured users)

WhatsConfigured enables effective management of one of the most critical assets on your network—device configurations. As an integrated plug-in available 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. You can leverage this automated configuration to reduce the amount of time spent ensuring network devices are configured correctly, freeing valuable time.



WhatsConfigured tasks attached to this device

Name	Description	Last run
wc_task1_dox	example task	
wc_task3_dox	third example task	
wc_task_2	another example task	

Archives saved for this device

Time created	Created by	Key	Description	Retain

If you use the WhatsConfigured plug-in, you need to configure and assign credentials to communicate with devices you plan to manage on your network, configure task scripts and tasks, and assign tasks to the appropriate devices. First, assign credentials for each device that you plan to manage through WhatsConfigured. Next, use the CLI Settings Library to define custom sets of CLI elements to override device's default CLI settings. Do this to ensure that WhatsConfigured can correctly communicate with devices as it attempts to carry out tasks. Next, configure task scripts that login to devices via SSH or Telnet to run command-line interface (CLI) commands on managed devices. Tasks can use pre-configured task scripts or you can configure your own custom task scripts with the WhatsConfigured Custom Script Language. Task scripts can perform a number of operations, such as uploading, restoring, backing up a running or startup configuration, or changing an application password. After tasks are configured and assigned, they either run on the schedule you configure, or can be run as needed from the WhatsConfigured Task Library and the WhatsUp Gold Device Properties Tasks dialog. Task scripts are stored and managed in the Task Script Library and associated to WhatsConfigured in the WhatsConfigured Task dialog.

After configuring task scripts and tasks, you can configure policies and templates. WhatsConfigured policies search through archived configuration files for strings that are either expected or not expected within files. These policies can be added to Alert Center task thresholds and you can be alerted when a policy fails due to unexpected content in a config file. WhatsConfigured templates allow you to automatically push device configurations to devices of the same type by replacing device-specific (IP address, hostname) information with variables, saving time and reducing the possibility of error that occurs with manual device configuration. For more information, see *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Configure a NOC display

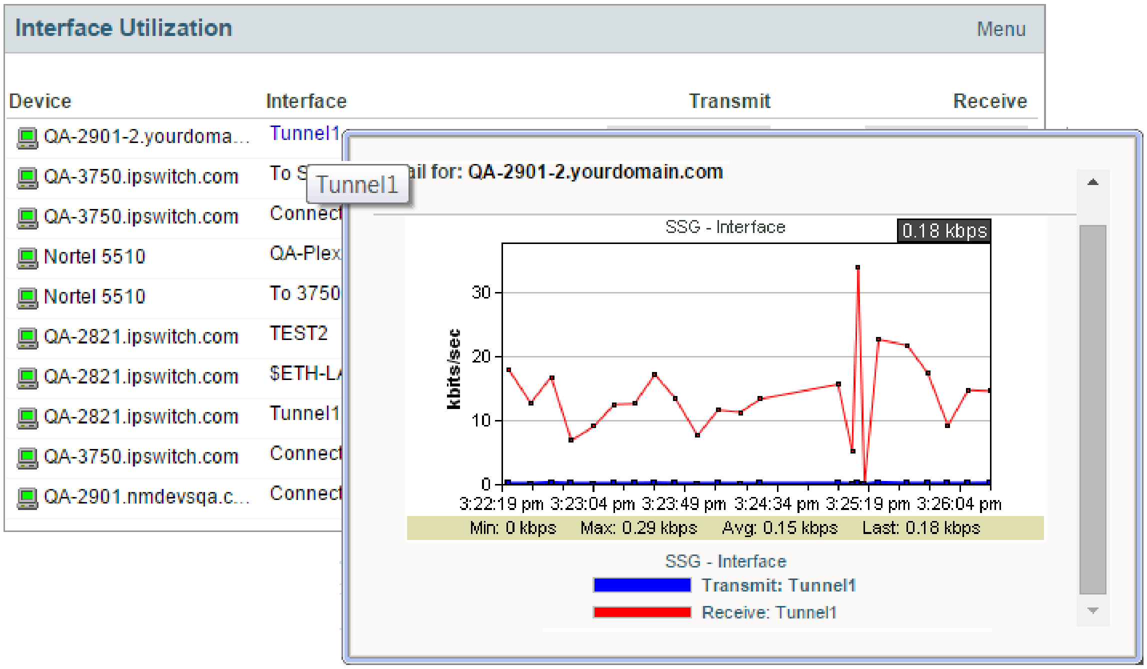
After you have discovered your network, configured WhatsUp Gold and other plug-ins, you can optionally extend the visibility WhatsUp Gold provides to your Network Operations Centers (NOC) using Dashboard.

Dashboard is a standalone application included with WhatsUp Gold Premium, Distributed, and MSP editions. Dashboard cycles through report pages on the WhatsUp Gold web interface, providing network administrators with constant insight into network health. For more information, see *About the Dashboard Screen Manager* in the *WhatsUp Gold Online Help* (*http://www.whatsupgold.com/support/index.aspx*).

Tip: If your network contains more than a couple of branch offices, consider using WhatsUp Gold Distributed Edition. WhatsUp Gold Distributed Edition extends the full functionality of WhatsUp Gold Premium Edition to each branch office, sharing network health information between a central NOC and any number of remote sites—no matter where they're located or how they’re connected.

Assess issues with real-time tools

Throughout reports in WhatsUp Gold, you can view InstantInfo popups, which let you see, in real-time, how the metric shown on a report is performing. For example, if you're viewing an interface utilization report for a device, InstantInfo popups allow you to see the real-time interface utilization. This helps you to quickly evaluate the health of the device.



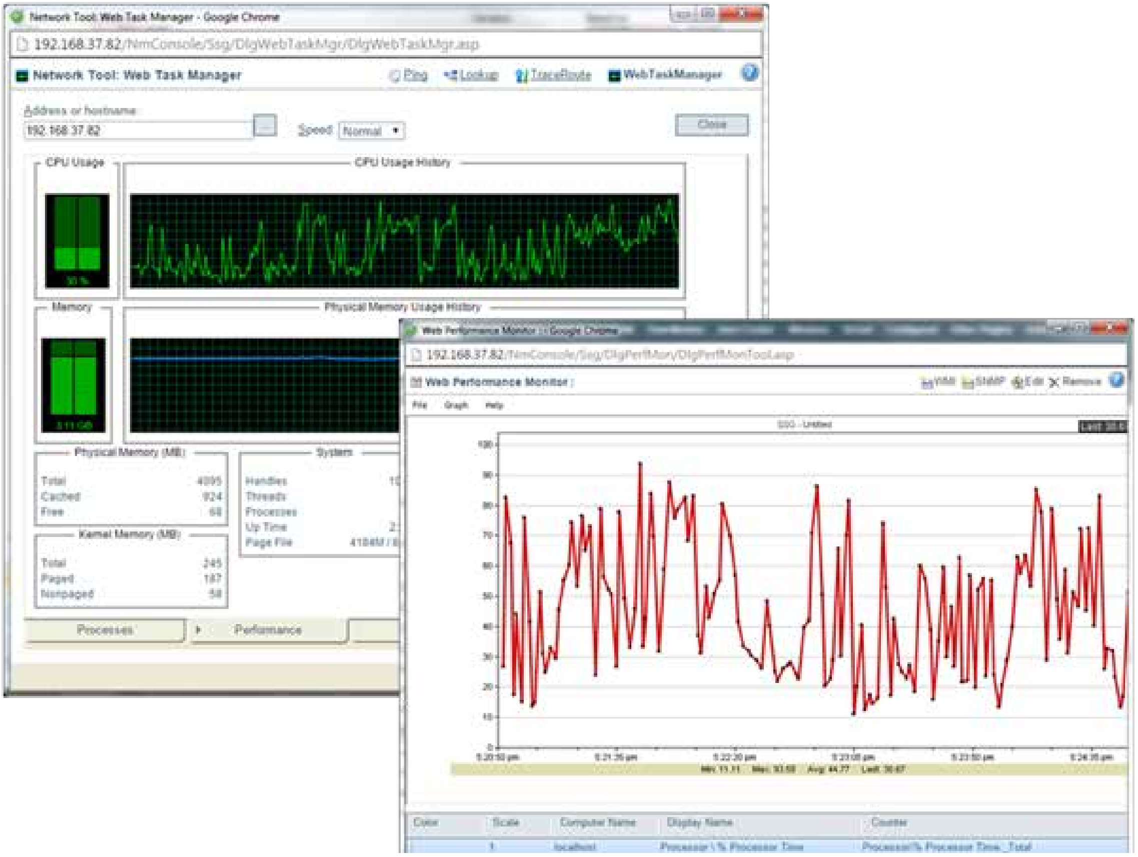
Interface Utilization

Device	Interface	Transmit	Receive
QA-2901-2.yourdoma...	Tunnel1		
QA-3750.ipswitch.com	To S		
QA-3750.ipswitch.com	Connect		
Nortel 5510	QA-Plex		
Nortel 5510	To 3750		
QA-2821.ipswitch.com	TEST2		
QA-2821.ipswitch.com	$ETH-L		
QA-2821.ipswitch.com	Tunnel1		
QA-3750.ipswitch.com	Connect		
QA-2901.nmdevsqa.c...	Connect		

il for: QA-2901-2.yourdomain.com

Min: 0 kbps Max: 0.29 kbps Avg: 0.15 kbps Last: 0.18 kbps

Similarly, you can use two network tools to view real-time data on network devices: the Web Task Manager and Web Performance Manager. Bringing the power of the Microsoft Windows Task Manager and Microsoft Windows Performance Monitor tools to the Web lets you view real-time device data directly from the WhatsUp Gold web interface.



Network Tool: Web Task Manager - Google Chrome

192.168.37.82/NmConsole/Ssg/DlgWebTaskMgr/DlgWebTaskMgr.asp

Network Tool: Web Task Manager

Address or hostname: 192.168.37.82

Speed: Normal

Physical Memory (MB)	
Total	4095
Cached	924
Free	68

Kernel Memory (MB)	
Total	245
Paged	187
Nonpaged	58

System	
Handles	1
Threads	
Processes	
Up Time	2
Page File	4184M /

Web Performance Monitor :: Google Chrome

192.168.37.82/NmConsole/Ssg/DlgPerfMon/DlgPerfMonTool.asp

Web Performance Monitor

Min: 11.11 Max: 93.58 Avg: 44.77 Last: 30.67

Color	Scale	Computer Name	Display Name	Counter
	1	localhost	Processor \ % Processor Time	Processor\% Processor Time_Total

View reports on the go

With many network management solutions, the most information you can get from your mobile phone is a notification of an issue. With WhatsUp Gold's mobile interface, you don't have to have physical access the WhatsUp Gold computer every time you get a message about network health. The mobile web interface lets you view WhatsUp Gold and Flow Monitor reports from virtually any mobile device, so you can troubleshoot issues as soon as you find out about them. For more information, see the *WhatsUp Gold Mobile Access Guide* (*http://www.whatsupgold.com/support/index.aspx*).