IPSWITCH
WhatsUpGold
v15.0

Getting Started Guide

IPSWITCH

CHAPTER 1 Welcome

Welcome to WhatsUp Gold

About WhatsUp Gold

Available editions

CHAPTER 2 Deploying

CHAPTER 3 More information

Welcome

Welcome to WhatsUp Gold

Network and application infrastructures have become 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 or 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 always know the pulse of the network 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 Premium, WhatsUp Flow Monitor, WhatsConnected, 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 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° 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/WUG15relnotes).

Available 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** manages devices and applications on a single-location network. Intuitive web-enabled dashboard views provide drill-down access to alerts and issues in real-time, and access to more than 200 reports that document device, bandwidth, and application-related activity.

- **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.

WhatsUp Gold optional plug-ins

WhatsUp Gold optional applications are available for use with 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/).

- **WhatsConnected** 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, connectivity report view, asset/inventory report view, WMI (Windows) inventory information, bridge port utilization report view, a detailed topology view, and more. 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, IP/MAC Finder, polling and monitoring, and interface status and utilization 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).

- **WhatsVirtual** plug-in provides additional capabilities to discover, map, monitor, alert, and report on virtual environments in WhatsUp Gold. With WhatsVirtual, one discovery scan can discover both virtual and physical devices. In Device View, virtual devices are displayed alongside physical devices. For each virtual host discovered, a group is created for the virtual host and all of its associated virtual machines. Leveraging the VMWare vSphere APIs, WhatsVirtual enables the same mapping, reporting, predictive monitoring, and powerful alerting and notification capabilities of WhatsUp Gold to keep you informed when issues arise and to keep the network infrastructure running smoothly. For more information, see the *WhatsUp Gold web site* http://www.whatsupgold.com/WhatsVirtual.

- **WhatsUp Gold Flow Monitor** plug-in for WhatsUp Gold leverages Cisco NetFlow, sFlow, and J-Flow data from switches, routers, and Adaptive Security Appliances (ASA) 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 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 web site* (http://www.whatsupgold.com/NetFlowMonitor).

- **WhatsConfigured** 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.

The WhatsConfigured plug-in reduces the time and effort spent maintaining device configurations and changes while providing increased security, compliance, and visibility. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/).

- **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).

- **WhatsUp Gold Failover Manager** provides user-configurable criteria to determine if WhatsUp Gold is in a failed state. You can choose to have the primary system go down if *all* services are disabled, or if *any* specified service is disabled. For example, if you select all services, the services used by WhatsUp Gold must go down on the primary service for the secondary system to take over. If you select only the Polling Engine and Web Server, and both are disabled on the primary system for any reason, the secondary system takes over WhatsUp Gold network management duties until the primary system has been restored. The WhatsUp Gold Failover Manager ensures a high availability operation for WhatsUp Gold. For more information, see the *WhatsUp Gold web site* (http://www.whatsupgold.com/products/FailoverMgr).
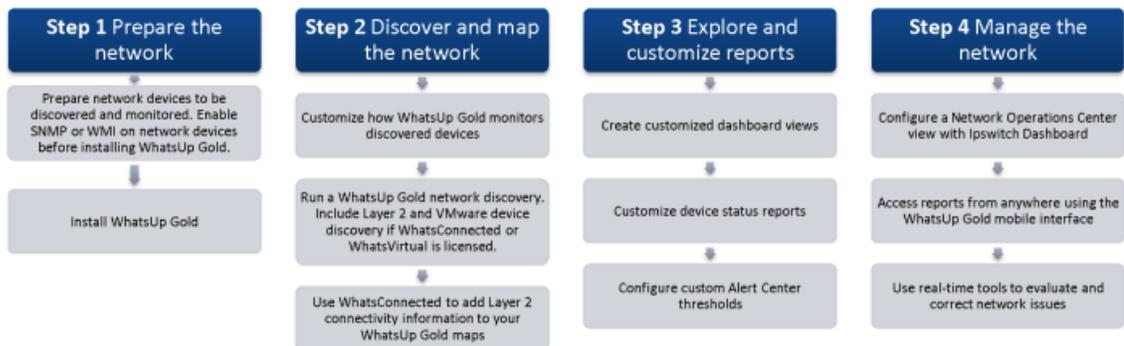
Deploying

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

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 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 in the help.

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 *MyIpswitch portal* (http://www.myipswitch.com) 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 2005 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 configure IIS 7; however, IIS 6 must be enabled prior to the WhatsUp Gold installation. For more information, see the *Installing and Configuring WhatsUp Gold v15* (http://www.whatsupgold.com/wugiis_15) and the *Release Notes* (http://www.whatsupgold.com/WUG15relnotes).

The installer provides three levels of install options. Use the install option that best fits your install situation:

- **I administer the devices on my network. I know some (or all) of the SNMP, VMWare, Windows, and other credentials for these devices**. Use this option if you know the network devices credentials for your SNMP communities and other credential types, such as VMware for the WhatsVirtual plug-in, and TFTP and SSH credentials. This information will help you accomplish better device discovery results in WhatsUp Gold. You also have the opportunity to enter email settings for the email address you want to have email action notifications sent to. After you select the network discovery method, the discovery process starts and notifies you when the discovery is finished.

- **I do not know the credentials for devices on my network. I want to evaluate the product anyway, although I realize that I will not be able to access many product features without device credentials**. Use this option if you do not know the network device credentials, but want to get WhatsUp Gold installed and running so you can evaluate and use WhatsUp Gold features. Note that when you do not enter network device credentials, WhatsUp Gold will be more limited on device information. The wizard starts immediately following the WhatsUp Gold installation and discovers network devices that use *public* credentials.

- **I am an experienced WhatsUp Gold user. I already know where to enter my information and how to perform a network discovery. Let me skip the configuration wizard and go straight to WhatsUp Gold**. Use this option to bypass credentials configuration and go directly to WhatsUp Gold when the install is complete.

Configure Flow Monitor on key devices (optional for Flow Monitor 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, sFlow, or J-Flow data exported from network routers and switches. If you use the WhatsUp Gold plug-in, Flow Monitor, 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.
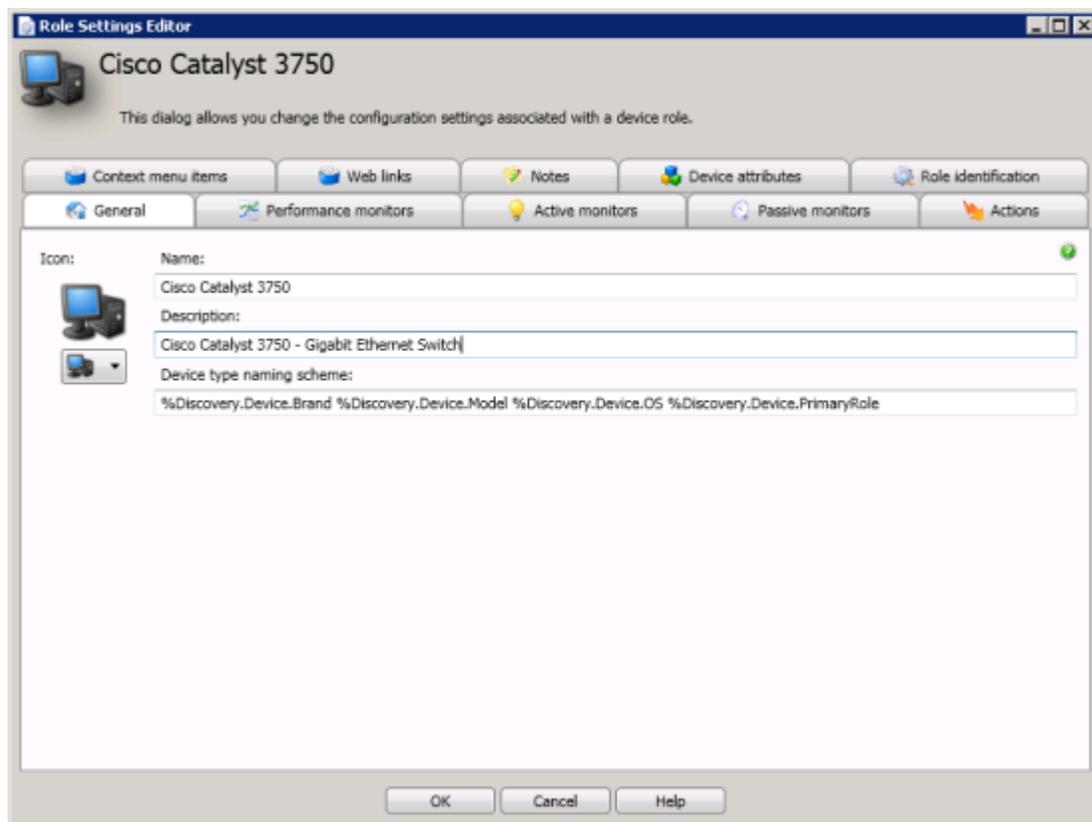
WhatsUp Gold provides several default device roles that are used to identify most common network devices. These default roles should correctly identify the majority of devices on the network, but you can modify the device roles to customize what is monitored on each device and what action policy is applied. Device Roles are managed in the WhatsUp Gold console (**File > Discover Devices > Advanced > Device role settings**).
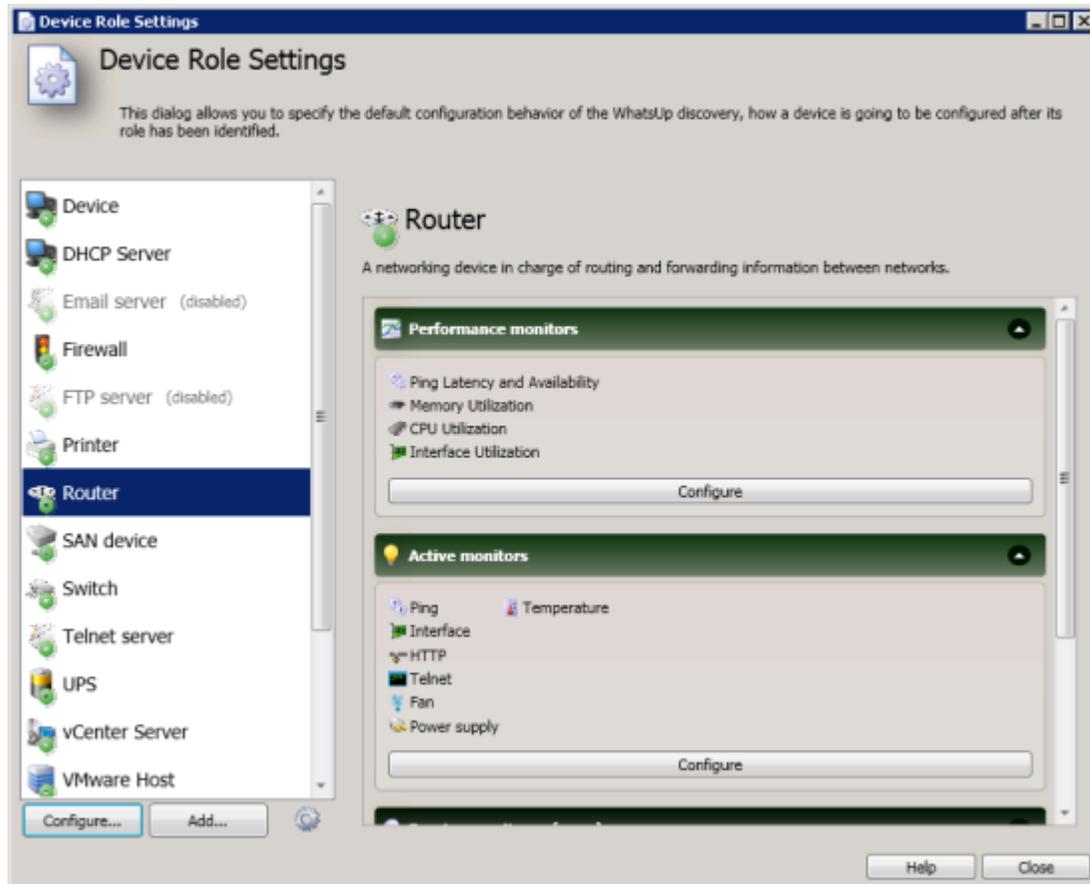
In addition, you can create new device roles to specify how WhatsUp Gold monitors and reports on devices it does not natively recognize. For more information, see Using Device Roles in the *WhatsUp Gold Online Help* (http://www.whatsupgold.com/wug15webhelp).

Discover the network

As described in the *Download and install WhatsUp Gold* (on page 6) section of this guide, the install provides three install options to provide varying levels of assistance for discovering network devices. Depending on the option you selected, you may or may not have already selected a method to discover network. If you have not selected a discovery method and after you have completed any additional device role customization, if you choose to do so; you can discover network devices with WhatsUp Gold.

We recommend using the **SNMP Smart Scan** option to discover the network. 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.

Other discovery scan options are:

- **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 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.

📝 **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.
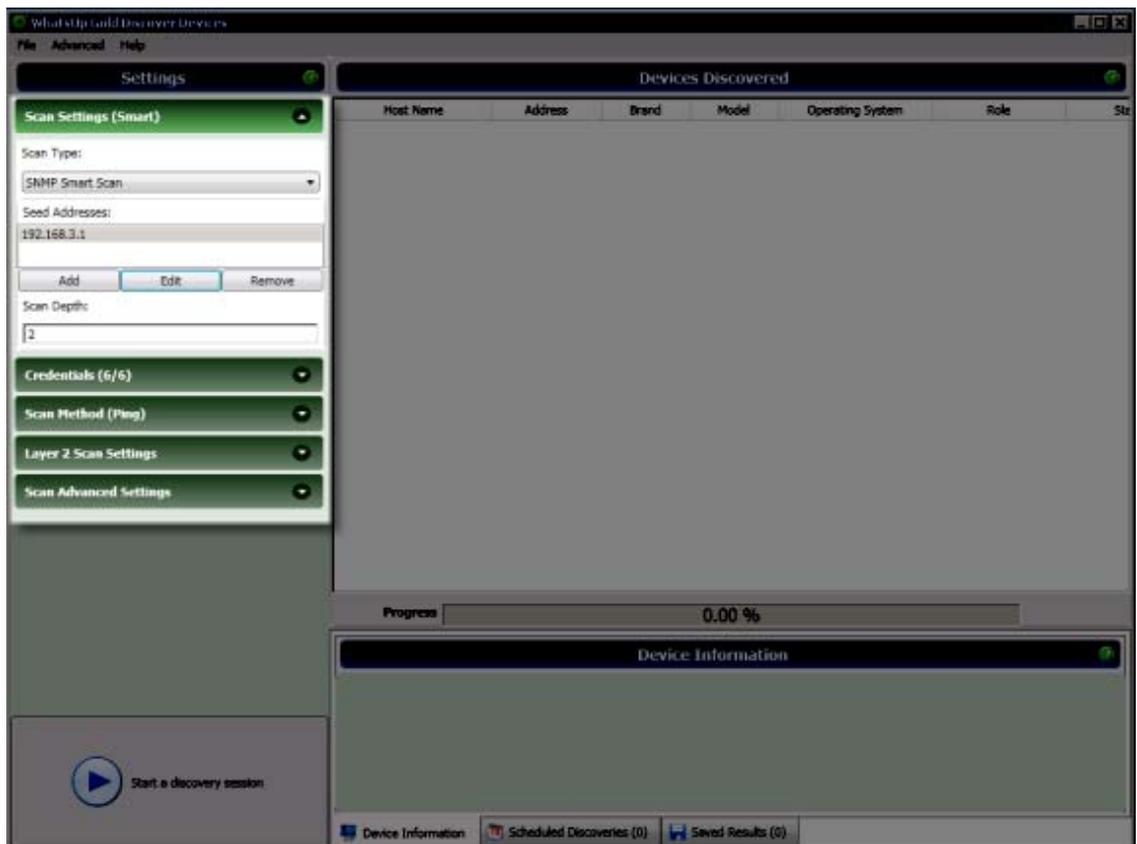
Select SNMP, Windows, and VMware Credentials

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 in WhatsUp Gold. For more information, see Using Credentials in the *WhatsUp Gold Online Help* (http://www.whatsupgold.com/wug15webhelp).

> **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

> Note: The Layer 2 scan 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).

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**.

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.

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 WhatsVirtual tab in the WhatsUp Gold views dialog.

Map the network (optional for WhatsConnected users)

After device discovery is complete in WhatsUp Gold, as an alternative to using the new Layer 2 discovery option from within WhatsUp Gold, you can discover topology maps with WhatsConnected. WhatsConnected is available as a stand-alone application and you can export data to WhatsUp Gold when WhatsUp Gold servers are configured as endpoints for exchange data with WhatsConnected. Unlike other topology mapping solutions that overlay devices on a topology bitmap or Visio drawing, WhatsConnected scans your network using industry-standard protocols (such as ICMP, SNMP and LLDP) to automatically create Layer 2 topology maps of your network segments.
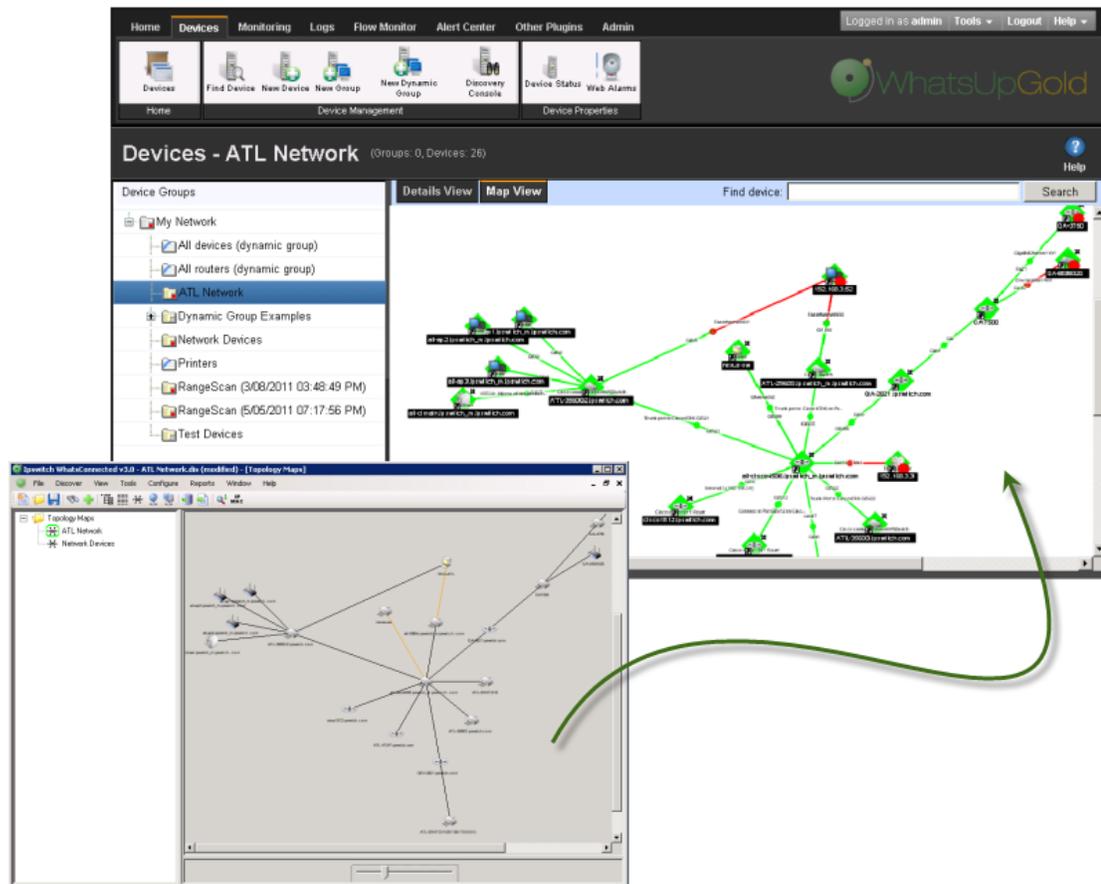
First, run a layer 2 discovery in WhatsConnected, then right-click the topology map to export the map to WhatsUp Gold and monitor the mapped devices. You can use filters to manage devices that display on WhatsConnected maps and you can schedule discoveries to dynamically update map and export to WhatsUp Gold. After exporting maps from WhatsConnected to WhatsUp Gold, you can actively monitor network devices from a topology map view. Network topology maps provide a fast easy and way to browse the network infrastructure and display physical connections between devices, simplifying the day-to-day complexities of managing and quickly resolving network issues. Additionally, you can export the topology maps to Microsoft Visio, making documenting your network topology nearly effortless.

WhatsConnected also provides a variety of map-level user tools to test and monitor device performance. Real-time polling and monitoring tools, such as Interface Status/Utilization, Ping Status/Latency, and other tools help you test, analyze, and troubleshoot network device performance.

STEP 3: 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.
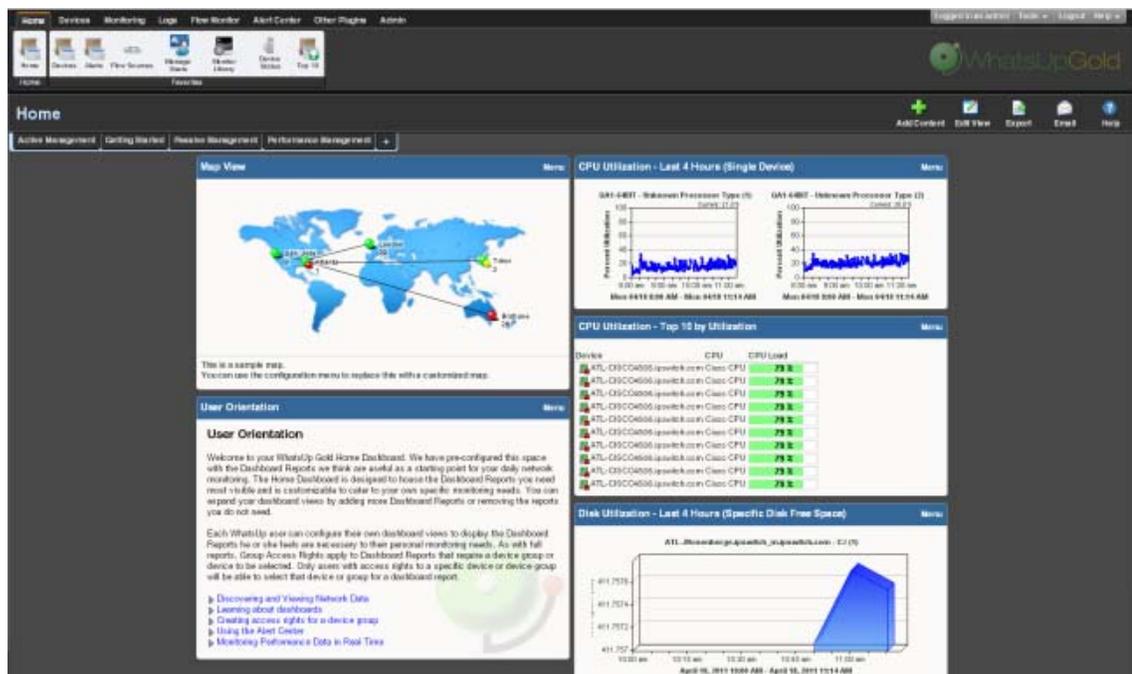
The Home Dashboard can display both Home- and Device-level dashboard reports. You can place any dashboard report on a Home dashboard; mixing and matching summary, group, and device-specific data.

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.

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/wug15webhelp).

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.
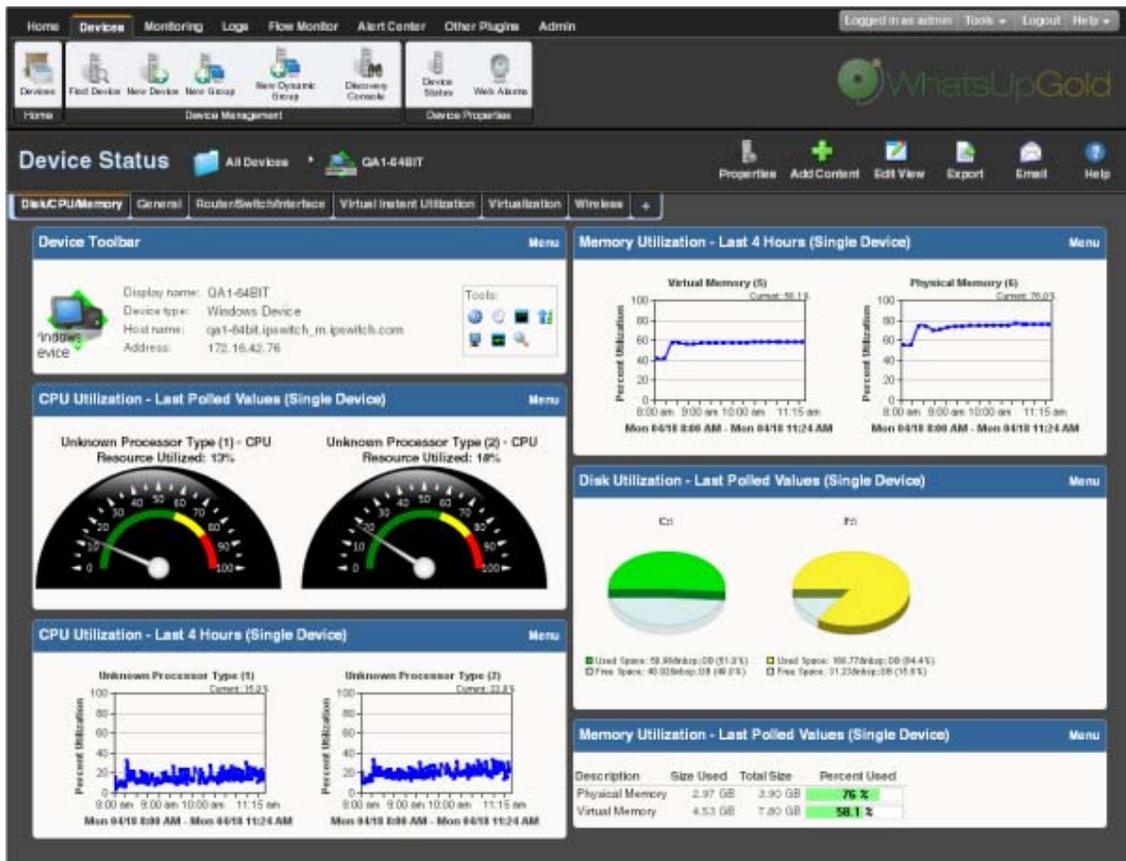
Throughout the web interface you will see links to devices, such as HP ProCurve Switch. All of these links point to the Device Status dashboard for that device. If there is a potential problem with a monitored device, the Device Status dashboard is a good place to look for more information on the device status. The Device Status dashboard includes several default dashboard views:

- Disk/CPU/Memory
- General
- Router/Switch/Interface
- Virtual Instant 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.
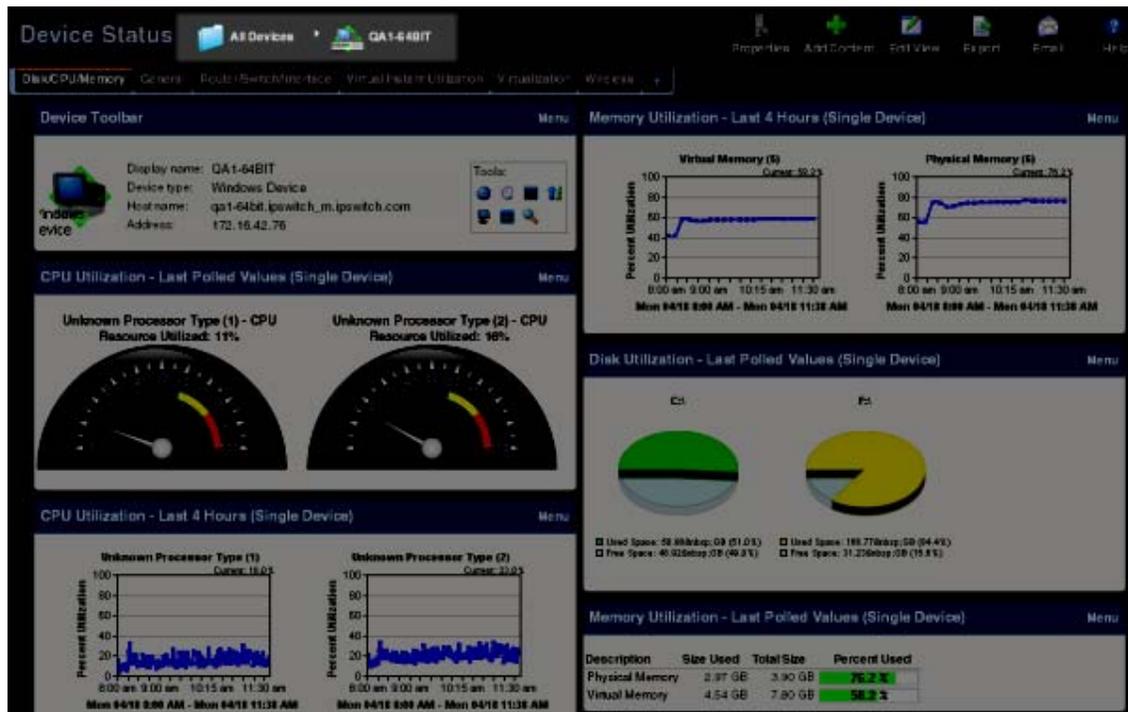
For more information, see Adding dashboard reports to a dashboard in the *WhatsUp Gold Online Help* (http://www.whatsupgold.com/wug15webhelp).

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.

You can create myriad of other thresholds to monitor other types of Performance, Passive, and System 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/wug15webhelp).


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

STEP 4: Manage the network

WUG15.0 Configure network devices (optional for WhatsConfigured users)

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.

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.
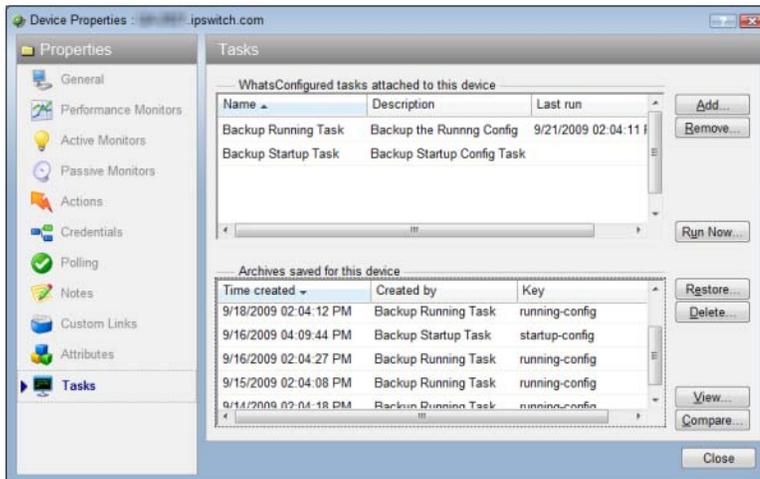

First, assign credentials for each device that you plan to manage through WhatsConfigured. Next, configure Task scripts that login to devices via SSH or Telnet to run command-line interface (CLI) commands on managed devices. Tasks can use pre-configured task scripts or you can configure your own custom 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. For more information, see *WhatsUp Gold Online Help* (http://www.whatsupgold.com/wug15webhelp).

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/wug15webhelp).
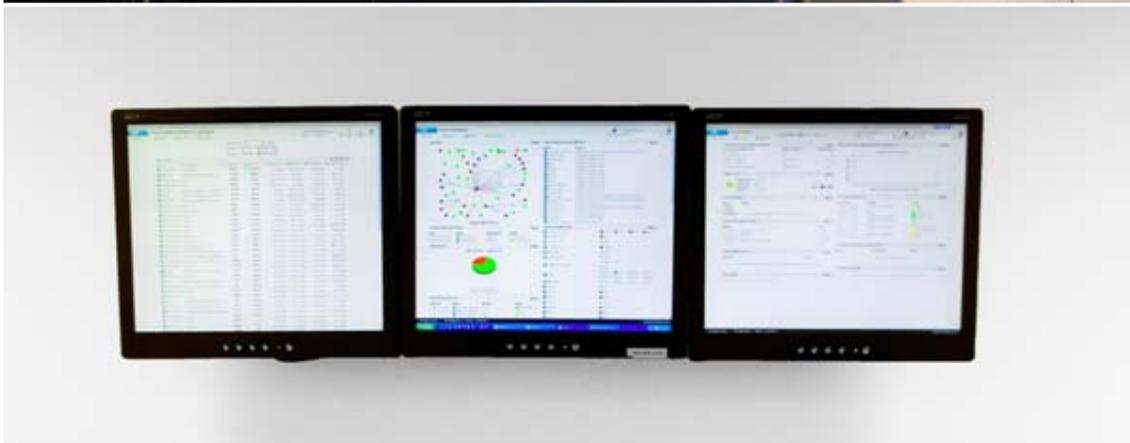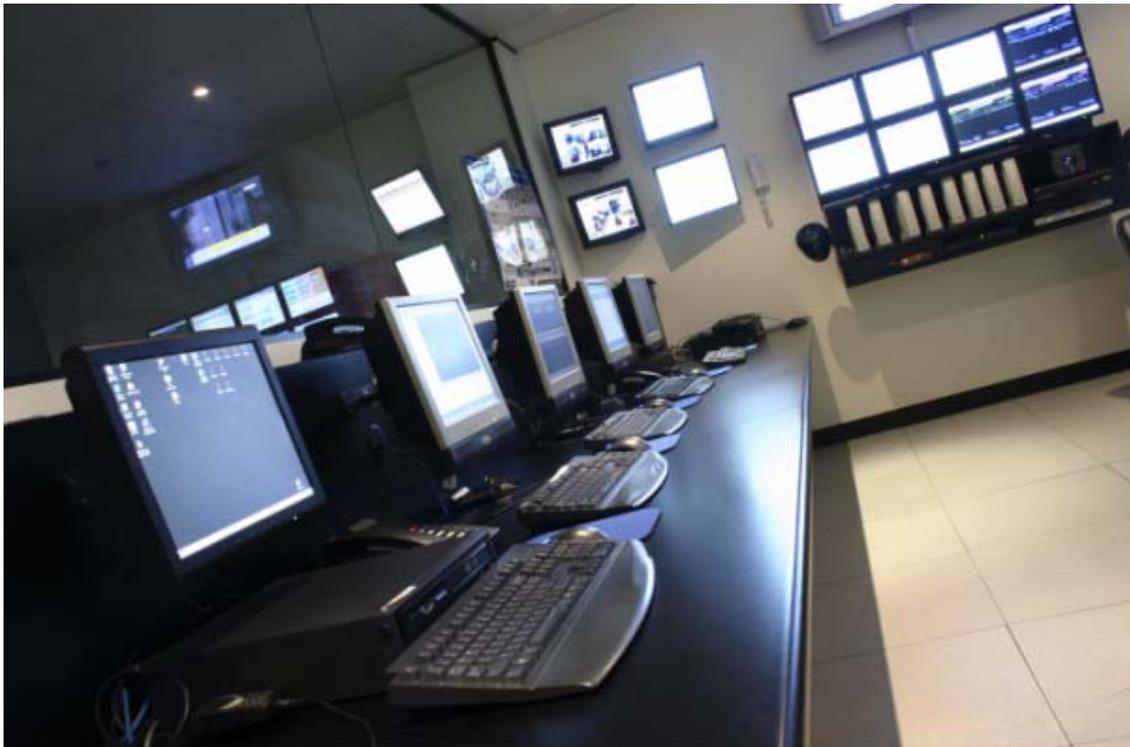
> 💡 **Tip**: If your network contains more than a couple of branch offices, consider using WhatsUp Gold Distributed Edition. WhatsUp Gold Distributed Edition extends the full functionality of WhatsUp Gold Premium Edition to each branch office, sharing network health information between a central NOC 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.

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.
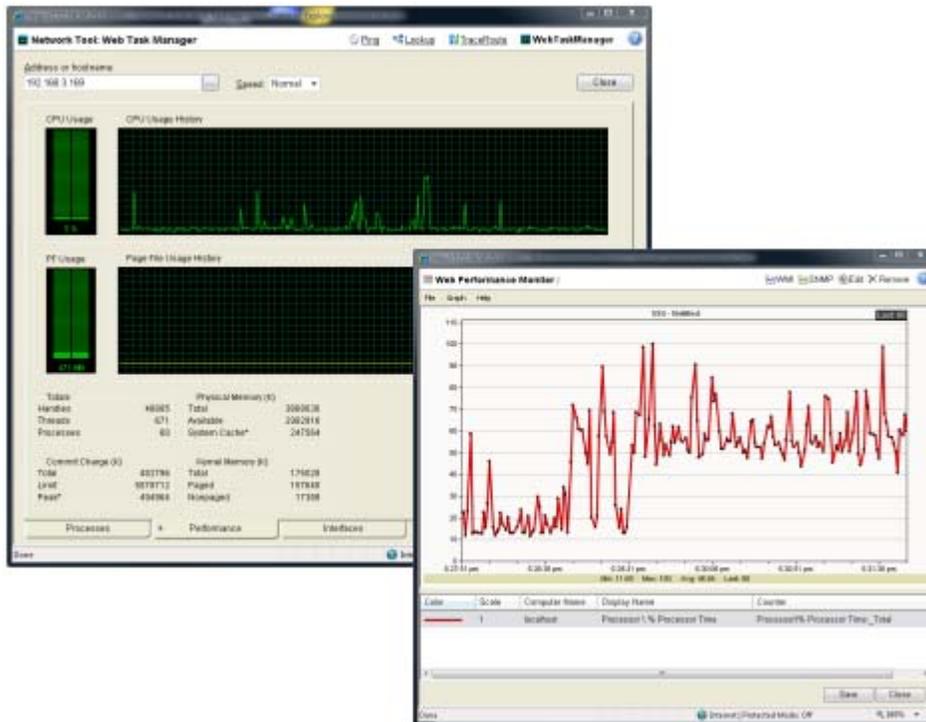
View reports on the go

With many network management solutions, the most information you can get from your cell 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 modern 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/wug15ma).
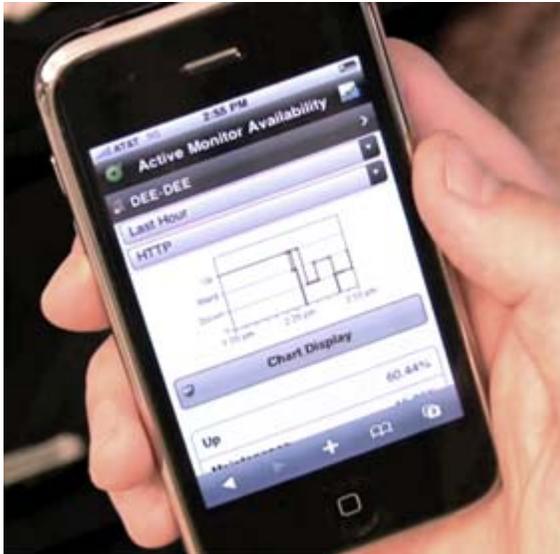
More information

In This Chapter

Common network management tasks

Refer to the information below to learn more about common network management tasks in WhatsUp Gold and the sections in the *WhatsUp Gold Online Help* (http://www.whatsupgold.com/wug15webhelp) that pertain to those tasks.

To:	See:
Use network discovery scans to discover devices you want to monitor on the network.	Learning about the Discovery Console
Use Device Roles to specify the criteria devices must match to be identified as the device role and specify the monitoring configuration applied to devices added to WhatsUp Gold.	Using Device Roles
Monitor performance (CPU, disk, memory, and interface use) for critical devices.	Using Performance Monitors
Monitor standard IP services on a device, such as HTTP, FTP, or SMTP.	Using Active Monitors
Listen for device events, such as authentication failures and Syslog messages.	Using Passive Monitors
Use reports to troubleshoot and monitor performance and historical data collected in WhatsUp Gold.	Using WhatsUp Gold monitor reports

To:	See:
Set up dashboard views for users to view custom reports.	Understanding and using dashboards
Manage user accounts and rights.	Managing users and groups
Set up and route alerts to the appropriate network administrator.	Using Actions
Customize network maps to reflect your company's network topology.	Using Maps
Group devices by type, location, services, or some other attribute.	Managing Devices, Dynamic Groups
Set up user-configured thresholds and notification policies on performance monitors, passive monitors, WhatsUp Gold system health, the Flow Monitor plug-in, and the WhatsConfigured plug-in.	Using the Alert Center

For 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.

- **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).

Copyright notice

This document was published on Friday, May 27, 2011 at 15:13.