IPSWITCH

WhatsConnected v3.1
User Guide

IPSWITCH
WhatsUpGold

Welcome to WhatsConnected

Installing and Configuring WhatsConnected

Discovering Networks

Using the WhatsConnected console

Configuring WhatsConnected

Viewing WhatsConnected reports

Welcome to WhatsConnected

In This Chapter

WhatsConnected is a layer 2 and layer 3 network discovery and visualization application that equips network managers with a comprehensive tool set to accurately discover, inventory, configure, document, and visualize device connectivity, including VLAN overlays, down to the individual port. Layer 2 discovery and mapping accesses the physical infrastructure information embedded in devices to provide significantly more detailed topology information than Layer 3 discovery mechanisms. In addition to widely used IP discovery protocols, such as ICMP, ARP, and SNMP, Layer 2 discovery leverages a number of other mechanisms to discover devices including industry standard Link Layer Discovery Protocol or LLDP, as well as equipment manufacturer proprietary discovery protocols.

With Layer 2 information available about how devices in your network are connected, their interdependencies, and their locations, you can locate problems and resolve them more easily. WhatsConnected helps you understand your network from top to bottom and focus on keeping it running securely and at peak performance.

WhatsConnected provides the key functions network professionals need to discover, map, search, document, and troubleshoot networks.

Discovery

The WhatsConnected discovery process uses industry-standard protocols, such as ICMP, SNMP, and Windows (WMI), to find devices on your network. Information about discovered devices is available in seven network views, including six data grids and a graphical topolopy map.

Mapping

After WhatsConnected discovers the devices on your network, it can generate a map that shows the physical connections between all devices. Standard and custom maps provide an easy way to browse the network infrastructure. With connectivity data readily available, managing the day-to-day complexities of a network is simplified.

Any topology map in WhatsConnected can be exported to WhatsUp Gold, automating custom map views and active monitor creation for the interfaces on the map's devices. WhatsConnected integrates with WhatsUp Gold to identify and create powerful monitoring strategies for your network.

Searching

The WhatsConnected detailed device views allow for simple browsing of connectivity for any device on the network. You can use the Layer 2 Trace and IP/MAC Finder tools to easily discover the location of any device on the network.

Documenting

WhatsConnected makes it easy to share network details. You can export your topology maps to Microsoft Visio and Adobe `.pdf` as well as generate reports that contain detailed information about the hardware and software on your network. Using WMI credentials, you can view Windows inventory report information such as installed software, software updates, warranty, OS, and more.

Troubleshooting

WhatsConnected includes troubleshooting tools that help you drill into network device information and resolve issues. The WhatsConnected Capture Config tool captures the *running* and *startup* configurations for network devices, providing a tool to analyze and compare the differences between device configurations. Real-time polling and monitoring network tools let you test, analyze, and troubleshoot network device performance with monitors such as ping status and latency, interface status and utilization, CPU utilization, and memory utilization.

Finding more information and updates

The following are information resources for WhatsConnected. This information may be periodically updated and available on the *WhatsUp Gold Web site* (http://www.whatsupgold.com/support/index.aspx).

- **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 and configuring WhatsConnected. The release notes are available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/WC31relnotes).

- **Application Help for the console**. The console help contains dialog assistance, general configuration information, and how-to's that explain how to use the features. The Table of Contents is organized by functional area, and can be accessed from the main menu or by clicking **Help**.

- **Licensing Information**. Licensing and support information is available on the *MyIpswitch licensing portal* (http://www.whatsupgold.com/wugCustPortal). 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/support/index.aspx).

Sending feedback

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

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

Installing and Configuring WhatsConnected

In This Chapter

System requirements

Refer to the *Release Notes* (http://www.whatsupgold.com/WC30relnotes) for WhatsConnected product features, system requirements, fixed in this release, known issues, and other information.

Installation overview

WhatsConnected can share a server with WhatsUp Gold, or can be installed as a standalone application on a separate server. In either case, WhatsConnected is licensed separately, and is installed using the WhatsConnected installation program. The WhatsConnected Release Notes contain the most up-to-date information about installing.

Before installing, we recommend that you read the WhatsConnected Release Notes for possible application update details and review the system requirements information to ensure that the system, on which you are attempting to install, meets the base-level requirements.

To update your license to purchase WhatsConnected, visit the *MyIpswitch portal* (http://www.whatsupgold.com/wugCustPortal). For more information, see *Activating WhatsConnected licenses* (on page 4).

Activating WhatsConnected licenses

If WhatsConnected is installed using the installation application downloaded from the Web link provided in the purchase confirmation email, the program is fully functional immediately after installation.

If the WhatsConnected license is not automatically activated during installation, you can manually activate WhatsConnected using the activation program in the WhatsConnected group on the Windows Start menu.

To activate WhatsConnected manually:

Note: Before you begin the manual activation process, make sure that you have your product serial number available to use in the activation program.

1 Click **Start > Programs > Ipswitch WhatsConnected > Manage WhatsConnected License**. The activation program appears.

2 Follow the onscreen instructions to complete the product activation.

Note: When activation completes, a confirmation page indicates that the license has been activated. If activation does not complete successfully, you may be behind a proxy or firewall that is blocking the activation request. In this case, click **Offline** and follow the onscreen instructions.

For additional help and information about managing your product license, go to the *MyIpswitch licensing portal* (http://www.whatsupgold.com/wugCustPortal).

CHAPTER 3

Discovering Networks

In This Chapter

Getting started with WhatsConnected

To start WhatsConnected:

- From the Windows Start Menu, select **Ipswitch WhatsConnected > WhatsConnected**. WhatsConnected starts.

When you start the WhatsConnected application, the WhatsConnected Startup dialog helps you begin using the WhatsConnected application.
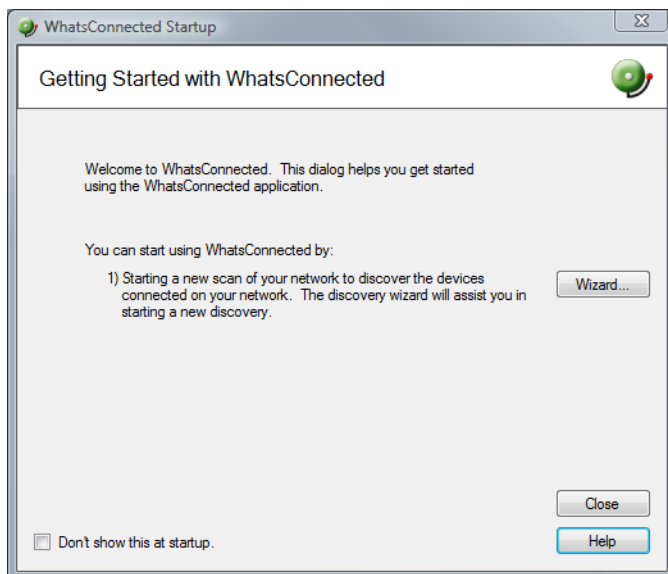
To begin gathering and viewing Layer 2 network information:

- Start a new network scan to discover devices connected on the network. Click **Wizard** to start the Wizard discovery process.

- or -

- If you have saved WhatsConnected discovery files previously, you can select an existing discovery file in the **Recent files** list, then click **Open**.

Click **Do not show this at startup** to prevent this dialog from appearing each time you start WhatsConnected.

For more information about other methods to do network discovery, see *About Layer 2 Network Discovery* (on page 7).

About Layer 2 Network Discovery

WhatsConnected discovers the devices on your network and displays a topological map of the network's physical structure. WhatsConnected also captures detailed information about each device, including IP and MAC addresses for all interfaces on the device, information about software installed on the device, and more.

There are several ways to add devices with the Layer 2 Network Discovery:

- Through the Layer 2 Network Discovery option in the WhatsConnected console **Discover > Network** menu. For more information, see Run Discovery.

- Through the single device discovery option in the WhatsConnected console **Discover > Device** menu. For more information, see Add New Device in the WhatsConnected Help.

- Through the Getting Started with WhatsConnected Wizard that appears when you start WhatsConnected. For more information, see *Getting started with WhatsConnected* (on page 6).

- Through the Discovery Tasks option in the WhatsConnected console **Discovery > Discovery Tasks**. For more information, see *Configuring Discovery Tasks* (on page 22).

Configuring Layer 2 Network Discovery

Layer 2 Network Discovery can run with a minimal amount of configuration. The discovery settings can be specific and point to a certain part of your network, or more general and pertain to the entire network. In both cases, network settings are key to successful network scans.

There are two main elements to configure for each network scan.

- A base discovery configuration that includes a discovery scan type and IP scope. For more information, see *About Layer 2 Network Discovery scan types* (on page 8).

- The network protocols and credentials used during the network scan. For more information, see the *Configuring network protocols and credentials* (on page 11) section.

Layer 2 Network Discovery setup is accomplished by using the Discovery Setup wizard or manually through several WhatsConnected dialogs. This section describes how you can manage both the discovery settings and protocol settings manually.

About Layer 2 Network Discovery scan types

An important part of Layer 2 Network Discovery is understanding the different methods by which a network can be discovered. There are two Layer 2 Network Discovery methods.

ARP Cache Discovery

Address Resolution Protocol (ARP) Cache discovery locates network devices by reading SNMP information on your network. This scan type uses SNMP enabled devices (usually routers) to identify devices that are active on your network. In addition to using the ARP cache on each network device, ARP Cache discovery also uses many proprietary discovery protocols to find additional devices connected to the network.

The Discovery Setup wizard prompts you to enter a Seed IP Scope (IP addresses, IP address ranges – including IP subnets) that indicates where you would like the discovery to start. These devices are used as the seed of the network discovery.

> **Important**: We recommend that you use ARP Cache discovery as your primary discovery method.

Ping Sweep discovery

Ping Sweep discovery scans a range of IP addresses and finds the devices that respond to the ICMP or SNMP protocol.

The Network Discovery Setup wizard prompts you to enter a Seed IP Scope (IP addresses, IP address ranges including subnets) that indicates where you would like to focus your network scan.

> **Note**: The Ping Sweep discovery method is used for very specific discovery scans. If you are unsure of your network configuration, including any of its subnetworks, ARP Cache discovery is a more appropriate method for discovering your network.

For more information about how Seed IP Scopes work in each Layer 2 discovery method, see *About Seed IP Scope* (on page 10).

Advanced Discovery Settings

Access Advanced Discovery Settings using the **Advanced** button on the Discovery Name/Method dialog. The Advanced Discovery Settings dialog sets the maximum number of threads to use during the discovery scan, allows you to configure WhatsConnected to ping

devices first, ping discovered subnets, resolve hostnames using a Domain Name System (DNS), and exclude device categories from the discovery scan.

> **Note**: When setting the number of threads used during a scan, increasing the number of threads allows WhatsConnected to simultaneously open more connections with network devices, possibly reducing the time needed to perform the scan, however this may negatively impact network performance as the number of open connections increases.

About Layer 2 discovery settings

Each network scan requires several base-level settings that guide the discovery scan of your network. These discovery settings are grouped by a general name that describes the area of the network that the settings scan. Discovery Settings are accessible from the Discovery Settings dialog (**Discover > Discovery Settings**) and the Discovery Wizard.

Configuring discovery settings

To add discovery settings:

1   From the main menu of the WhatsConnected console, select **Discover > Discovery Settings**. The Discovery Settings dialog appears.
2   The dialog displays all previously defined discovery settings. To create a new collection of discovery settings, right-click in the left list, a right-click menu appears.
3   Click **New**. The New Discovery Settings dialog appears.
4   Enter a **Name** that gives context to the discovery settings you are creating (i.e. TestLab, Production Network). This name is stored so that it can be reused for later network scans.
5   Click **OK**.
6   On the Discovery Settings dialog, a new entry appears in the left pane list for the new collection of discovery settings. Select the new collection name from the list.
7   Select the discovery method for the network scan from **Method**. For more information about the discovery types, see *About Layer 2 Network Discovery scan types* (on page 8).
8   If you use the Advanced Discovery Settings, click **Advanced** and enter the number of **Max Threads** to use while running the discovery scan. This indicates the number of separate threads to run in the background as WhatsConnected attempts to communicate with the devices on the network.

> **Note**: If you are concerned about the load discovery could place on the network, you can reduce the Max Threads to cut back on the concurrent network communication.

9   Select whether the discovery engine should try to **Ping Devices First** before attempting any other protocol.
10 Select whether the discovery engine should attempt to **Ping Discovered Subnets** to provide a more complete scan during an **ARP Cache** type of discovery.

> **Note**: This option tells the engine to take each discovered subnet and run a ping sweep through it to ensure all devices are discovered in the defined subnet.

11 Select the **Resolve DNS names** option to resolve DNS names to their IP addresses.

12 Select the **Exclude Device Categories** option if you want to exclude specific device categories from discovery. This option allows you to narrow the range of devices that are discovered. Click **OK** to complete the advanced options, then click **Next**.

13 Enter the **Seed IP Scope**. For more details in regards to the Seed IP Scope, see *About Seed IP Scope* (on page 10).

14 If you want to use Advanced IP Scoping options, click **Advanced** and enter the **Include IP Scope**. For more information, see *About Include IP Scope (WhatsUp Gold Help and User Guide)* (on page 10). You can also enter the **Exclude IP Scope**. For more information, see *About Exclude IP Scope (WhatsUp Gold Help and User Guide)* (on page 11). Click **OK** to complete the advanced options, then click **Next**.

15 lick **Next**, then enter Discovery Protocol Settings as required. Refer to the help for more information.

16 Click **Finish** to save all changes made in the Discovery Settings dialog. From the main menu of the WhatsConnected console,

To delete discovery settings:

1 From the main menu of the WhatsConnected console, select **Discover > Discovery Settings**. The Discovery Settings dialog appears.

2 The dialog displays all previously defined discovery settings. To delete a collection of discovery settings, right-click the collection that you would like to delete, then click **Delete**. The selected collection of discovery settings is deleted.

3 Click **OK**.

4 Click **OK** to save all changes made in the **Discovery Settings** dialog.

About discovery IP scopes

Discovery IP scopes are a means by which discovery is configured to understand the area(s) of the network that it scans, or excludes from a scan.

IP scopes can be:

- A single IP address (i.e. 10.0.0.1)
- A range of IP addresses (i.e. 10.0.0.1-10.0.0.100)
- A subnet range of IP addresses (i.e. 10.0.0.1/24 or 10.0.0.1/255.255.255.0)

The following is a description of how these IP scopes are used in WhatsConnected discovery settings.

About Seed IP Scope

Seed IP Scope defines the range of IP addresses where network discovery starts a scan.

- For Ping Sweep discovery, these addresses are contacted with an initial ICMP request.
- For ARP Cache discovery, these addresses are queried for additional data. The discovery engine reads SNMP data from these devices and continues to scan the network for additional devices based on the SNMP responses from the seed devices.

About Include IP Scope

Include IP Scope defines the range of IP addresses in which to include in the network scan.

- For Ping Sweep Discovery, Include IP Scope is the same as the Seed IP Scope.

- For ARP Cache Discovery, Include IP Scope indicates an IP address range that the network scan should restrict itself to during discovery.

> **Note**: In order for an Include IP Scope scan to find devices, the Seed IP Scope must intersect with the Include IP Scope. For example, if you enter a Seed IP Scope of 188.311.5.1 and an Include IP Scope of 188.311.4.10-188.311.4.160, the scan is unable to locate devices because the two IP scopes do not intersect.

Example

- A single IP address (i.e. 10.0.0.1)
- A range of IP addresses (i.e. 10.0.0.1-10.0.0.100)
- A subnet range of IP addresses (i.e. 10.0.0.1/24 or 10.0.0.1/255.255.255.0)

About Exclude IP Scope

Exclude IP Scope defines the range of IP addresses to exclude from in the network scan.

- For Ping Sweep Discovery, Exclude IP Scope might be an IP range of servers or workstations that are a subnet of the Seed IP Scope.
- For the ARP Cache Discovery, Exclude IP Scope indicates an IP address range that network scan should not attempt to discover.

Configuring network protocols and credentials

Several industry-standard protocols are used in Layer 2 Network Discovery. The two main protocols used in Layer 2 discovery are ICMP and SNMP; the SSH protocol can also be used to enhance discovery of Linux and UNIX devices. WhatsConnected also supports discovery through a Virtual Machine Interface (VMI) and Windows systems (WMI). Windows (WMI) credentials are used to collect software inventory information from Windows systems.

Additionally, the WhatsConnected credentials library provides support for Telnet and SSH. Telnet and SSH credentials are used to communicate with network devices and capture device configurations. The Capture Config tool, available in a topology map's device right-click menu, lets you backup running configurations and backup startup configurations on devices such as routers and switches. For more information, see *Capturing device configurations* (on page 70).

The following information describes how to manage each protocol/credential settings.

Using the ICMP protocol

The ICMP protocol allows the discovery engine to test whether a particular IP address is active and responding on the network. Depending on network latency, this protocol can be adjusted to meet the configuration on your network.

> **Note**: You can only edit the default ICMP settings; you cannot create a new set of ICMP credentials.

To change the ICMP settings for the discovery engine:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Select **ICMP**, then click **Edit**. The Edit ICMP Settings dialog appears.

3 Increase or decrease the **Timeout** settings. The default timeout is 500 milliseconds.

> **Note**: If you are discovering across a WAN link, increase the timeout.

4 Increase or decrease the number of ICMP **Retry counts**. The default number of one retry is recommended for most networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

5 Click **OK** to save the protocol changes.

Using the SNMP protocol and credentials

The SNMP protocol allows the discovery engine to query detailed device information from each SNMP-enabled device. The correct SNMP Read community names, along with the appropriate timeout and number of retries are required for successful network queries.

This section describes how to add and maintain the appropriate SNMPv1, SNMPv2, or SNMPv3 protocol settings for successful SNMP network device discovery.

SNMPv1 credentials

To add a new set of SNMPv1 credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Click **New**.

3 Select **SNMPv1**, then click **OK**. The protocol properties dialog appears.

4 Enter a **Name** for the set of SNMPv1 credentials.

5 Enter the new **SNMP read Community** name.

6 Optionally, enter a new **SNMP write Community** name.

7 Increase or decrease the SNMP **Timeout**. This setting is dependent on the latency and load on your network devices. Longer timeouts can cause discovery to slow down. However, if the network is experiencing a lot of network traffic, a longer timeout is recommended. A default of 1000 milliseconds is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, allow for a longer timeout.

8 Increase or decrease the SNMP **Retry count**. This setting is dependent on the latency and load on your network devices. More retries allow for SNMP failures or heavy network loads. However, more retries slow down the discovery process. One or two retries is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

9   Click **OK** to save the protocol changes.

To edit a set of SNMPv1 credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of SNMPv1 credentials, then click **Edit**. The protocol properties dialog appears.

3   Modify the existing settings.

- Edit the SNMP **Read Community** name.

- Edit the SNMP **Write Community** name.

- Increase or decrease the SNMP **Timeout**. This setting is dependent on the latency and load on your network devices. Longer timeouts can cause discovery to slow down. However, if the network is experiencing a lot of network traffic, a longer timeout is recommended. A default of 1000 milliseconds is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

- Increase or decrease the SNMP **Retry count**. This setting is dependent on the latency and load on your network devices. More retries allow for SNMP failures or heavy network loads. However, more retries slow down the discovery process. One or two retries is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, allow for a longer timeout.

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

To delete a set of SNMPv1 credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of SNMPv1 credentials, then click **Delete**. The SNMPv1 credentials are removed.

3   Click **OK** to save the protocol changes.

SNMPv2 credentials

To add a new set of SNMPv2 credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Click **New**.

3   Select **SNMPv2**, then click **OK**. The protocol properties dialog appears.

4   Enter a **Name** for the set of SNMPv2 credentials.

5   Enter the new **SNMP read Community** name.

6   Optionally, enter a new **SNMP write Community** name.

7 Increase or decrease the SNMP **Timeout**. This setting is dependent on the latency and load on your network devices. Longer timeouts can cause discovery to slow down. However, if the network is experiencing a lot of network traffic, a longer timeout is recommended. A default of 1000 milliseconds is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, allow for a longer timeout.

8 Increase or decrease the SNMP **Retry count**. This setting is dependent on the latency and load on your network devices. More retries allow for SNMP failures or heavy network loads. However, more retries slow down the discovery process. One or two retries is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

9 Click **OK** to save the protocol changes.

To edit a set of SNMPv2 credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Select an existing set of SNMPv2 credentials, then click **Edit**. The protocol properties dialog appears.

3 Modify the existing settings.

- Edit the **Name**.

- Edit the SNMP **Read Community** name.

- Edit the SNMP **Write Community** name.

- Increase or decrease the SNMP **Timeout**. This setting is dependent on the latency and load on your network devices. Longer timeouts can cause discovery to slow down. However, if the network is experiencing a lot of network traffic, a longer timeout is recommended. A default of 1000 milliseconds is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

- Increase or decrease the SNMP **Retry count**. This setting is dependent on the latency and load on your network devices. More retries allow for SNMP failures or heavy network loads. However, more retries slow down the discovery process. One or two retries is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, allow for a longer timeout.

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

To delete a set of SNMPv2 credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Select an existing set of SNMPv2 credentials, then click **Delete**. The SNMPv2 credentials are removed.

3 Click **OK** to save the protocol changes.

SNMPv3 credentials

To add a new set of SNMPv3 credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Click **New**.

3 Select **SNMPv3**, then click **OK**. The protocol properties dialog appears.

4 Enter a **Name** for the set of SNMPv3 credentials.

5 Enter the **Username** that is configured for the SNMP agent. This username is included in every SNMP packet in the authentication header. An SNMP device, upon reception of a packet, uses this username to look for configured authentication and encryption parameters and applies them to the received message.

6 Optionally, enter the **Context** needed to identify specific SNMP instances on your network.

7 If required, select the **Protocol** used for **Authentication**. Additionally, enter the **Password** used for authentication.

8 If supported, select the **Protocol** used for **Encryption**. Additionally, enter the **Password** used for encryption.

9 Increase or decrease the SNMP **Timeout**. This setting is dependent on the latency and load on your network devices. Longer timeouts can cause discovery to slow down. However, if the network is experiencing a lot of network traffic, a longer timeout is recommended. A default of 1000 milliseconds is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, allow for a longer timeout.

10 Increase or decrease the SNMP **Retry count**. This setting is dependent on the latency and load on your network devices. More retries allow for SNMP failures or heavy network loads. However, more retries slow down the discovery process. One or two retries is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

11 Click **OK** to save the protocol changes.

To edit a SNMPv3 set of credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Select an existing set of SNMPv3 credentials, then click **Edit**. The protocol properties dialog appears.

3 Modify the existing settings.

- Edit the **Name**.

- Edit the **Description**.

- Edit the SNMP **Write Community** name.
- Edit the **Protocol** and **Password** used for **Authentication**.
- Edit the **Protocol** and **Password** used for **Encryption**.
- Increase or decrease the SNMP **Timeout**. This setting is dependent on the latency and load on your network devices. Longer timeouts can cause discovery to slow down. However, if the network is experiencing a lot of network traffic, a longer timeout is recommended. A default of 1000 milliseconds is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, increase the number of retries.

- Increase or decrease the SNMP **Retry count**. This setting is dependent on the latency and load on your network devices. More retries allow for SNMP failures or heavy network loads. However, more retries slow down the discovery process. One or two retries is recommended for small to medium size networks.

> **Note**: If you are discovering across a WAN link, allow for a longer timeout.

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

To delete a set of SNMPv3 credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of SNMPv3 credentials, then click **Delete**. The SNMPv3 credentials are removed.

3   Click **OK** to save the protocol changes.

Using the SSH Protocol

The SSH protocol allows the discovery engine to query detailed device information from Linux and UNIX devices. The SSH user name and password are required to query information from your Linux/UNIX devices. This protocol required only if you want to discover Linux/UNIX systems.

To add a new set of SSH credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Click **New**.

3   Select **SSH**, then click **OK**. The protocol properties dialog appears.

4   Enter a new SSH **Username**.

5   Enter a new SSH **Password** and the **Confirm Password**.

> **Note**: SSH passwords are encrypted.

6   Enter a defined SSH port. The default port number is 22.

7   Click **OK** to save the protocol changes.

To edit a set of SSH credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of SSH credentials, then click **Edit**. The protocol properties dialog appears.

3   Modify the existing settings.

   - Enter a new SSH **Username**.

   - Enter a new SSH **Password** and the **Confirm Password**.

> **Note**: SSH user names and passwords are encrypted.

   - Enter the defined SSH port. The default port number is 22.

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

To delete a set of SSH credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of SSH credentials, then click **Delete**.

3   Click **OK** to save the protocol changes. The SSH credentials are removed.

Using the Telnet Protocol

Telnet credentials are used for the Capture Config tool that starts Backup Running Configurations and Backup Startup Configurations. The Telnet user name, password, and port are required to connect and run configurations for devices such as routers and switches. This protocol is required only if you want to run the configuration tool for devices.

To add a set of Telnet credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Click **New**.

3   Select **Telnet**, then click **OK**. The protocol properties dialog appears.

4   Enter a new Telnet **Username**.

5   Enter a new Telnet **Password** and the **Confirm Password**.

> **Note**: Telnet passwords are encrypted.

6   Enter a defined Telnet port. The default port number is 23.

7   Click **OK** to save the protocol changes.

To edit a set of Telnet credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of Telnet credentials, then click **Edit**. The protocol properties dialog appears.

3   Modify the existing settings.

- Enter a new Telnet **Username**.

- Enter a new Telnet **Password** and the **Confirm Password**.

> **Note**: Telnet user names and passwords are encrypted.

- Enter the defined Telnet port. The default port number is 23.

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

To delete a set of Telnet credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Select an existing set of Telnet credentials, then click **Delete**.

3 Click **OK** to save the protocol changes. The Telnet credentials are removed.

Using the VMware (VIM) protocol

The VMware protocol allows the discovery engine to query detailed device information from VMware host and vCenter servers. The correct VMware user name and password are required only to query information from your VMware devices.

To add a set of VMware (VIM) credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Click **New**.

3 Select **VMware (VIM)**, then click **OK**. The protocol properties dialog appears.

4 Enter a **Name** and **Description** for the set of VMware (VIM) credentials.

5 Enter a new **Username** for the VMware (VIM) credentials. This username is used to authenticate to the web service.

6 Enter a new **Password** and the **Confirm Password** for the VMware (VIM) credentials. This password is used with the above username to authenticate to the web service.

7 Enter a defined **Port**. The default port number is 443 (HTTPS). This port is used when communicating via the VIM protocol.

8 Click **OK** to save the protocol changes.

To edit a set of VMware (VIM) credentials:

1 From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2 Select an existing set of VMware (VIM) credentials, then click **Edit**. The protocol properties dialog appears.

3 Modify the existing settings.

- Enter a **Name** for the set of VMware (VIM) credentials.

- Enter a new VMware **Username**.

- Enter a new VMware **Password** and the **Confirm Password**.

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

To delete a set of VMware (VIM) credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of VMware (VIM) credentials, then click **Delete**.

3   Click **OK** to save the protocol changes. The set of VMware (VIM) credentials are removed.

Using the Windows (WMI) Protocol

Windows (WMI) credentials are used to collect software inventory information, such as applications installed, on Windows systems. The WMI Domain\UserID and Password are required to connect to Windows systems. This protocol is required only if you want to collect inventory information for Windows devices.

To add a set of Windows (WMI) credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Click **New**.

3   Select **Windows**, then click **OK**. The protocol properties dialog appears.

4   Enter a **Name** and **Description** for the credential.

5   Enter a new Windows **Domain\UserID**. You may enter `.\` for the domain or enter a specific domain name.

6   Enter a new Windows **Password** and **Confirm password**.

> **Note**: Windows passwords are encrypted.

7   Click **OK** to save the protocol changes.

To edit a set of Windows credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of Windows credentials, then click **Edit**. The protocol properties dialog appears.

3   Modify the existing settings.

- Enter a new Windows **Domain\UserID**. You may enter `.\` for the domain or enter a specific domain name.

- Enter a new Windows **Password** and **Confirm password**.

> **Note**: Windows passwords are encrypted.

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

To delete a set of Windows credentials:

1   From the main menu of the WhatsConnected console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.

2   Select an existing set of Windows credentials, then click **Delete**.

3   Click **OK** to save the protocol changes. The set of Windows credentials are removed.

Running a Layer 2 Network Discovery

Layer 2 Network Discovery scans your network for devices, using the protocol(s) and settings you selected. After devices are found, you may view the new discovery results in the WhatsConnected console.

To run a Layer 2 Network Discovery:

1 From the console click **Discover > Network**. The Run Discovery dialog appears.

2 From the **Discovery Settings** list, select the discovery configuration that you want to run. To learn more about discovery configurations, see *Configuring Layer 2 Network Discovery* (on page 7).

3 Click **New**. The Network Discovery Setup wizard appears.
- or -
Select an existing profile in the **Discovery Settings** list, then click **Edit**. The Network Discovery Setup wizard appears.
- or -
Select an existing profile in the **Discovery Settings** list, then click **Start**. The Network Discovery for the selected profile runs. Go to step 11.

4 In the **Name** box, enter a discovery configuration name that identifies the network (or part of the network) you want to discover. If you are editing an existing profile, the name is entered by default.

5 Select a method for discovering the network. Either **ARP Cache** or **Ping Sweep** discovery, then click **Next**. For more information about discovery types, see *About Layer 2 Network Discovery scan types* (on page 8).

6 Enter an **IP Seed Scope** to define the starting point of either the ARP Cache discovery, or the IP ranges to use in the Ping Sweep discovery.

 ▪ Click **Add Default Gateway** to add your default network gateway to the **IP Seed Scope**.

 ▪ Click **Advanced** to further define the IP scope configuration of the discovery process.

 To learn more about Advanced IP scope settings, see Discovery Advanced IP Scoping in the WhatsConnected Help.

7 Click **Next**. The Discovery Protocol Settings dialog appears.

8 Select the credentials you want to use in the discovery process. Click **Settings** to add new or edit existing credentials. Enter the **SNMP read communities** as well as any **Timeout** and **Retry** information for the SNMP and ICMP requests.

> **Note**: You can add SNMP, SSH, Telnet VMWare, and Windows credentials from the Protocol Settings/Credentials dialog. Add credentials based upon the types of network devices you want to discover. For more information, see *Configuring network protocols and credentials* (on page 11).

9 If needed, collect Windows Inventory Information. Select one of the options to determine whether you want basic or detailed information extracted from WMI devices found during the discovery process:

 ▪ **Basic Windows inventory (OS, BIOS, Memory, Disk Drive...)**.

 ▪ **Detailed Windows inventory (Basic + Software and Windows Updates)**.

10 Select the credential discovery priority:

- Select a credential in the list, then click **Move Up** to increase the priority for the selected set of protocol settings/credentials in the list. The first protocol settings/credentials in the list have priority for the discovery scan and the subsequent protocol settings/credentials have priority in the order listed.
  - or -

- Select a credential in the list, then click **Move Down** to lower the discovery scan priority for the selected protocol settings/credentials.

> **Tip**: As the network discovery runs, each protocol/credential setting is used, in the order listed in the Discovery Protocol Settings dialog, until a successful community name is found. Consider keeping the number of community names to a minimum to increase the efficiency of the network scan. Use the **Move Up** and **Move Down** options to move the most preferred credentials to the top of the list.

11 Click **Finish**. The wizard closes and the new discovery configuration is automatically added to the **Discovery Settings** list in the Run Discovery dialog.

12 Click **Start** to run the discovery process.

13 When the discovery progress is complete, click **OK**. The Device Categories dialog appears. You can view network device information in this dialog or use the **View** menu for other network viewing options. For more information, see *Viewing Network Data* (on page 32).

Adding a device manually

There are two ways to add a single device:

- From the main menu of the WhatsConnected console, select **Discover > Device**.

- On the WhatsConnected console toolbar, click ➕ **Plus**.

To manually add a device to the network data:

1 From the WhatsConnected console, select **Discover > Device** (or select the Plus image from the console toolbar). The Add Device dialog appears.

2 Enter the **IP Address/Hostname** for the device into the appropriate field.

3 Click **OK**. The Run Discovery dialog appears.

4 Click **Start Discovery**.

5 After the discovery process is complete, click **OK** to add the device to the network data. The Device Categories View appears and the newly added device is automatically selected.

Refreshing network connectivity

After a network is discovered, you can update connectivity data with a single discovery process.

To refresh the connectivity of a network:

1 From the main menu of the WhatsConnected console, select **Discovery > Refresh Connectivity**. The Run Discovery dialog appears and the discovery process begins to

examine all networking devices to update their sighting and connectivity information. The progress indicators display the status of the discovery process.

2   Click **OK**. The updated information is automatically be added to the current network data.

Configuring and scheduling Discovery Tasks

Discovery Tasks are tasks that have been created to run discovery scans on a schedule. The discovery scans are created using the Discovery Settings dialog or the Getting Started with WhatsConnected Wizard, and the schedule is created during the creation of the discovery task. You can schedule a task to run daily, weekly, monthly, yearly or on some other defined time interval.

To add a new discovery task:

1   Click **Discover > Discovery Tasks**. The Discovery Task dialog appears.

2   Click **Add** to add a new discovery tasks to the list. The New Discovery Task dialog appears.

3   Enter a **Name** and **Description** for the task.

4   Select the **Discovery Settings** you want to use for the discovery task. These settings define the discovery method, starting point in the network, protocols to be used, and credentials needed for the discovery scan. To add new discovery settings, click **Settings**. The Discovery Settings dialog appears.

5   For the **Discovery Filename**, select or create the filename you want to use to save the details of the discovery task. This file is used to save the results of the scheduled discovery task.

6   Optionally, enable the **Keep ___ backup/discovery histories** feature and enter a coinciding value for the number of backups you would like WhatsConnected to save.

7   On the Schedule tab, you can enable and configure a schedule on which the task will run.

-   **Enable this schedule**. Select this option to run the discovery scan on the schedule created in the Schedule section.

-   **Run this Task**. Select the **Repeat Interval**, **Start Time**, and other variables to create the schedule on which you want the discovery scan to run.

8   On the Alerts tab, you can enable and configure email alerts.

-   **Enable alerts on changes**. Select this option to receive email alerts when WhatsConnected detects changes in a discovery file. After you select to enable this feature, select the criteria for which you want to be alerted.

    -   **New devices discovered**. Select this option to be alerted when WhatsConnected discovers new devices.

    -   **Lost/missing devices discovered**. Select this option to be alerted when WhatsConnected discovers devices that were initially discovered, but were not discovered again in a subsequent discovery scan.

    -   **Connectivity/link changes discovered**. Select this option to be alerted when WhatsConnected discovers device connectivity/link changes.

- **Send email alerts to**. Select the email address to which alerts will be sent. This list is populated with email addresses saved in the Email Settings dialog. If this list is empty, or you do not see the appropriate email address, click **Email Settings** to configure a new set of email settings for this alert.

9 On the WhatsUp Gold tab, you can select to **Update Exported WhatsUp Gold Devices** that have already been exported to WhatsUp Gold with any changes that are found during the discovery scan.

10 Click **OK**. The New Discovery Task dialog closes and the new task appears in the **Discovery Tasks** list.

To edit an existing discovery task:

1 Select an existing discovery task, then click **Edit**. The Edit Discovery Task dialog appears.

2 Edit the name and description for the task in the **Name** and **Description** boxes.

3 Select the **Discovery Settings** you want to use for the discovery task. These settings define the discovery method, starting point in the network, protocols to be used, and credentials needed for the discovery scan. To add new discovery settings, click **Settings**. The Discovery Settings dialog appears.

4 For the **Discovery Filename**, select or create the filename you want to use to save the details of the discovery task. This file is used to save the results of the scheduled discovery task.

5 Optionally, enable the **Keep ___ backup/discovery histories** feature and enter a coinciding value for the number of backups you would like WhatsConnected to save.

6 On the Schedule tab, you can enable and configure a schedule on which the task will run.

- **Enable this schedule**. Select this option to run the discovery scan on the schedule created in the Schedule section.

- **Run this Task**. Select the **Repeat Interval**, **Start Time**, and other variables to create the schedule on which you want the discovery scan to run.

7 On the Alerts tab, you can enable and configure email alerts.

- **Enable alerts on changes**. Select this option to receive email alerts when WhatsConnected detects changes in a discovery file. After you select to enable this feature, select the criteria for which you want to be alerted.

  - **New devices discovered**. Select this option to be alerted when WhatsConnected discovers new devices.

  - **Lost/missing devices discovered**. Select this option to be alerted when WhatsConnected discovers devices that were initially discovered, but were not discovered again in a subsequent discovery scan.

  - **Connectivity/link changes discovered**. Select this option to be alerted when WhatsConnected discovers device connectivity/link changes.

- **Send email alerts to**. Select the email address to which alerts will be sent. This list is populated with email addresses saved in the Email Settings dialog. If this list is empty, or you do not see the appropriate email address, click **Email Settings** to configure a new set of email settings for this alert.

8 On the WhatsUp Gold tab, you can select to **Update Exported WhatsUp Gold Devices** that have already been exported to WhatsUp Gold with any changes that are found during the discovery scan.

9 Click **OK**. The New Discovery Task dialog closes and the new task appears in the **Discovery Tasks** list.

To copy an existing discovery task:

Select an existing discovery task, then click **Copy**. The New Discovery Task dialog appears with information from the copied task in the fields and *Copy of* and the name of the copied task in the **Name** box.

To check the current status of a discovery task:

Select a discovery task, then click **Status**. The Discovery Task Status dialog will appear.

To start a discovery task:

Select a discovery task, then click **Run Now**. The status of the selected task will change to *Running*. If the task completes successfully, the status will change to *Succeeded*.

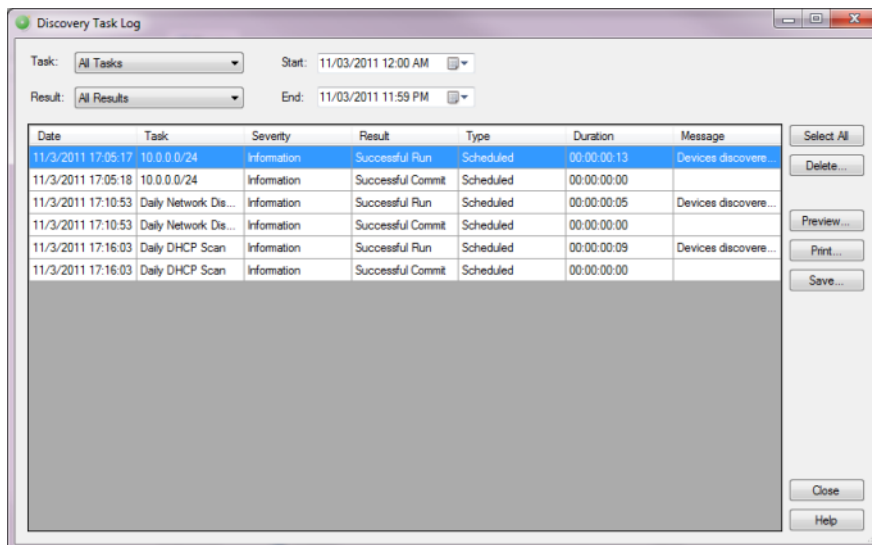**To stop a running discovery task:**

Select a running discovery task, then click **Stop**. The status changes from *Running* to *Canceled*.

To close the dialog:

Click **Close** to close the dialog. The Discovery Tasks dialog closes.

About the Discovery Task Log

The WhatsConnected Discovery Task Log displays the results of Discovery Tasks that attempted to run, whether successfully or unsuccessfully, during the specified time period.

To use the Discovery Task Log:

1   From the WhatsConnected main menu, select **Discover > Discovery Task Log**. The Discovery Task Log dialog appears displaying logs for the default time period that begins on the current day at midnight and ends on the current day at 11:59 p.m.

2   Use the dialog options to select the log data you want to view. As you make selections, the log dynamically updates to display appropriate log information based on your selections.

- Use the **Task** list to select to view log data for either a specific task or for all tasks. This list is populated with Discovery Tasks currently configured and stored in the Discovery Task Library.

- Use the **Results** list to select to view log data for a specific task result or for all task results. This list is populated with all possible Discovery Task results. You can select to view *All Results*, *Canceled*, *Failed Commit*, *Failed Initialization*, *Failed Run*, *Successful Commit*, *Successful Initialization*, and *Successful Run*.

- Use the **Start** and **End** option calendars to choose a beginning and end date for the time period for which you want to view discovery logs.

Log information

The Discovery Task Log displays the following log information:

- **Date**. The date the task attempted to run.

- **Task**. The name of the scheduled task that attempted to run. Discoveries run from the Run Discovery dialog also display in the Discovery Task Log and are listed as console Discoveries.

- **Severity**. The task's severity level; can be *Error*, *Information*, *Detail*, or *Diagnostic*.

- **Result**. The task's result.

  - *All Results* - all possible task results are displayed

  - *Canceled* - tasks canceled by the user

  - *Successful Initialization* or *Failed Initialization* - the success or failure of the steps taken to setup the discovery task (locating the discovery settings/credentials, loading the discovery file, etc.)

  - *Successful Run* or *Failed Run* - the success or failure of the discovery scan

  - *Successful Commit* or *Failed Commit* - the success or failure of the steps taken to save the discovery results and updating the log and any configurations

> **Note**: The Discovery Task Log displays only those task results that you have selected to view; if you have selected to view all task results, tasks with all results are displayed.

- **Type**. The task type. The Discovery Task Log displays only those task types that you have selected to view; if you have selected to view all task types, all task types are displayed.

- **Duration**. The elapsed time of the discovery scan.

- **Message**. If an error occurred, its details display here. If a task ran successfully, the message displays high level details about the task's results, such as the number of devices and subnets discovered.

Removing logs

The Discovery Task Log keeps all log information until you choose to remove it.

To remove logs from the selected time period:

Click to select specific logs, or click **Select All** to highlight all logs, then click **Delete**. The selected logs are removed.

Previewing and printing logs

To print preview the Task Discovery Log:

Click **Preview**. The Print Preview dialog appears.

To print the Task Discovery Log:

1   Click **Print**. The Print dialog appears.
2   Select the network printer on which to print the log, then click **OK**.

Saving logs

To save the Task Discovery Log as a .csv file:

1   Click **Save**. The Save CSV File dialog appears.
2   Specify a name for the file and the location to which to save the file, then click **Save**.

Show Discovery Alerts

The Discovery Alerts dialog provides information about devices that were discovered, but may have had issues being fully accessible. The information provided in this dialog helps you identify the details to check on the device to make it fully discoverable.
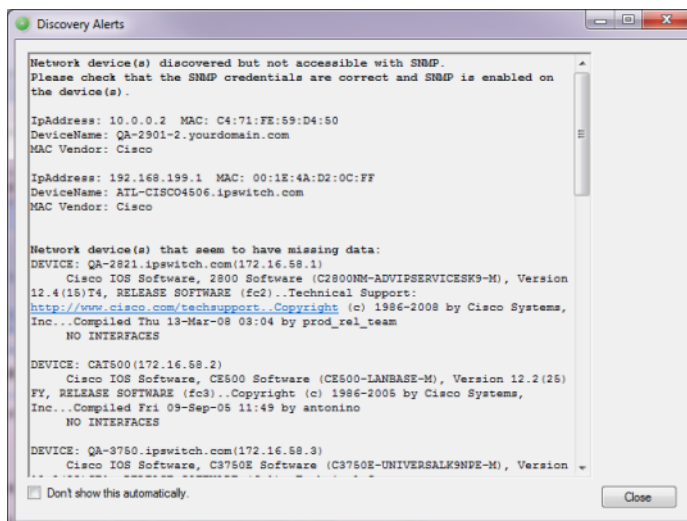
This dialog automatically appears each time changes are detected in the current discovery file. To change this default selection, select **Don't show this automatically** at the bottom left of the dialog.

To access the Discovery Alerts dialog:

On the WhatsConnected console, go to **Discover > Show Discovery Alerts**. The Discovery Alerts dialog appears.

Using the WhatsConnected console

In This Chapter

About the console

The WhatsConnected console is a Windows application used for discovering, visualizing, and exporting network data. The console has the following components:

- *Layer 2 Network Discovery* (on page 7)
- *Network Device* (on page 89) and *Topology Maps View* (on page 46)
- *Exporting Topology Maps to WhatsUp Gold* (on page 52)
- *Exporting Topology Maps to Microsoft Visio™* (on page 53)

About Layer 2 Network Discovery Files

WhatsConnected saves the information from a network discovery in a discovery file (.dis file extension). This flat file format makes it easy to share and move network data between computers with WhatsConnected installed. The size of these files is dependent on the number of devices saved in each discovery run and can be managed as part of the general file system.

Managing Layer 2 Network Discovery Files

At the end of a network discovery scan, the network data is loaded into the WhatsConnected console. At this point, there a several features available for you to manage the discovery (.dis) files. You can:

- Create a new discovery file.
- Open an existing discovery file.
- Replace devices in a current discovery file with devices from another discovery file.
- Merge devices in a current discovery file with devices from another discovery file.

- Replace topology maps in a current discovery file with maps from another discovery file.
- Merge maps in a current discovery file with maps from another discovery file.
- Save a discovery file.
- Save an existing discovery file to another discovery file.

Creating a new discovery file

At the end of a network discovery run, the network data is updated in the WhatsConnected console. At this point, you can save this network data to a discovery file. This file can be later used when the WhatsConnected console is opened.

To create a new discovery file:

- From the console, select **File > New**. This clears any existing network data so that you can perform a new network discovery.

For an example of using network discovery, see *Running a Layer 2 Network Discovery* (on page 20).

Opening a discovery file

After starting the WhatsConnected console, you can open an existing discovery file.

To open an existing discovery file:

1 From the WhatsConnected console, select **File > Open**. The File Open dialog appears.
2 Browse to a network discovery file, then click **Open**. The network data is loaded into the WhatsConnected console.

Opening a recently used discovery file

The WhatsConnected console keeps track of any recently opened/saved discovery files. You can open these files at any time from the WhatsConnected console File menu.

To open a recently used discovery file:

1 From the WhatsConnected console, click **File**. At the bottom of the menu, recently opened/saved files are listed.
2 Select the network discovery file you want to open.

Using Replace Devices

The WhatsConnected console provides the capability to replace the set of devices in the current network data model with those from another discovery file.

To replace the current set of devices:

1 From the WhatsConnected console, select **File > Replace Devices**. The Open Discovery File dialog appears.
2 Browse to locate the discovery file that you want to open, then click **Open**.

The current device set is replaced with the devices from the selected file. The topology maps are not modified.

Using Merge Devices

The WhatsConnected console provides the capability to merge the current set of devices with the devices from another discovery file.

To merge the current set of devices:

1   From the WhatsConnected console, select **File > Merge Devices**. The Open Discovery File dialog appears.
2   Browse to locate the discovery file you want to open, then click **Open**.

The device set from the selected file is merged with the current set of devices. The topology maps are not modified.

Using Replace Maps

The WhatsConnected console provides the capability to replace the topology maps with the current discovery file with those of another discovery file.

To replace the current topology maps with those from an external data file:

1   From the WhatsConnected console, select **File > Replace Maps**. The Open Discovery File dialog appears.
2   Browse to locate the discovery file that you want to open, then click **Open**.

The topology maps from the external file replaces those maps of the current discovery file.

Using Merge Maps

The WhatsConnected console provides the capability to merge the topology maps in the current discovery file the with those of another discovery file.

To merge topology maps from an external data file with the current set of maps:

1   From the WhatsConnected console, select **File > Merge Maps**. The File Open dialog appears.
2   Browse to locate the discovery file that you would like to open, then click **Open**.

The topology maps from the external discovery are merged with those of the current discovery file.

Using Save

The WhatsConnected console provides the capability to save the current network data model to a discovery file (.dis). Any modifications made to a network data model, such as added devices through discovery or added/modified topology maps, need to be saved much like a standard document after it has been modified.

> **Note**: A discovery file can only be saved after it has received an initial discovery file name. Therefore, use **File > Save As** to assign a file name to the network model the first time.

To save network data to a discovery file:

From the WhatsConnected console, select **File > Save**. The file is saved.

Using Save As

The WhatsConnected console provides the capability to save the current network data model to a discovery file. After an initial discovery, or if you want to save the network model to a different discovery file name, you can use the Save As feature.

To save network data to a discovery file:

1   From the WhatsConnected console, select **File > Save As**. The Save Discovery File dialog appears.
2   Give the discovery file a name, then click **Save**. The network data is saved to the file.

Viewing Network Data

In This Chapter

About network data views

The WhatsConnected console provides the capability of browsing network discovery results using a number of different views. The views that WhatsConnected provides are:

- *Device Categories view* (on page 37)
- *Device List view* (on page 41)
- *Topology Map view* (on page 46)
- *Subnets view* (on page 76)
- *VLAN view* (on page 78)
- *Links view* (on page 80)

The following section describes how each view is used to visualize your network data.

About data grid views

An important feature of the WhatsConnected console is its capability to show network data in a data grid, or spreadsheet-like form. These *data grid views* provide a number of user functions that are beneficial to creating multiple views of your network data. The following section describes the functions available in the data grid views. Available features vary dependent upon the data grid:

- *Column filtering* (on page 33)
- *Edit Device Category* (on page 33)
- *Show in Device Categories* (on page 34)

- *Remove selected devices* (on page 35)
- *Print and Print Preview* (on page 35)
- *Save CSV (comma-separated value file)* (on page 35)
- *Copying to clipboard* (on page 36)

Column filtering

Each data grid view allows you to show and hide its columns. This feature provides a powerful filtering capability so that you may structure your views in a way that brings the data into a form that you find most useful as a network administrator.

To show and hide columns in a data grid view:

1   Right-click a column heading in the data grid view. A list displaying all the columns that are displayed in that data grid appears; only columns with checks are displayed in the data grid.
2   To show a column, click the name of the column that you want to display in the grid. The data grid updates automatically.
3   To hide a column, clear the check from column that you would like to remove from the grid. The data grid updates automatically.
4   To close the column list options, click anywhere outside of the list box.

Note: Show and hide selections are not persistent between different sessions of WhatsConnected. When you close the current session of WhatsConnected, data grid views return to their default display settings.

Edit Device Category

Use the Device Types dialog to create or modify a custom device type mapping. To do this, enter an SNMP OID (sysObjectID) and select a device category for which to map a device. For more information about SNMP OIDs, refer to your device documentation or the *Internet Assigned Numbers Authority (IANA) web site* (http://www.iana.org/assignments/enterprise-numbers).

Use the Device Types dialog to create or modify a custom device type mapping. To do this, enter an SNMP OID (sysObjectID) and select a device category for which to map a device. For more information about SNMP OIDs, refer to your device documentation or the *Internet Assigned Numbers Authority (IANA) web site* (http://www.iana.org/assignments/enterprise-numbers).

Use the following options to create and edit device types:

- **sysObject ID (OID)**. Enter the SNMP OID (sysObjectID) for which you want to map a device. For more information about SNMP OIDs, refer to your device documentation or the *Internet Assigned Numbers Authority (IANA) web site* (http://www.iana.org/assignments/enterprise-numbers).
- **Include Subtree**. Select this option to include a subtree for the device type category.
- **Category**. Select a device type category for which to map the device.
- **Vendor/Manufacturer**. Enter the vendor or manufacturer name.

- **Model**. Enter the vendor or manufacturer model.
- **Description**. Enter the vendor or manufacturer description.
- Click **OK** to save changes.

Show in Device Categories

The Device Categories View is an explorer-type view with a Device Category tree view on the left, and a Device Details tab view on the right. The Device Categories view automatically categorizes and groups network devices so they can be viewed by their functional characteristics. The following is a list of all the categories that are supported by the WhatsConnected console.

- Routers
- Switches
- Wireless LAN Controllers
- Wireless Access Points
- Printers
- Windows
- Macintosh
- Windows Servers
- Unknown
- Linux
- Unix
- Power/UPS
- Firewall
- Virtual Servers
- Hubs
- IP Phone Managers
- IP Phones
- Probe
- KVM

Note: Any device that is either not categorized or does not support SNMP is placed in the Unknown category.

To view a Device Category:

1 From the main menu of the WhatsConnected console, select **View > Device Categories**. The Device Categories view appears.
2 Click a category to expand it and view more information and the devices belonging to the category.
3 Click a device to display device details on the right side of the page.

Remove selected devices

WhatsConnected allows you to customize device lists by removing devices from a data grid device list. This feature lets you select devices that you want to manage with WhatsConnected.

To remove selected devices from a data grid view:

1   In a data grid view, select the devices you want to remove from the device list.

- Press `Control` then select multiple non-contiguous devices in the list.
- Press `Shift` to select multiple contiguous devices in the list.

2   Right-click in the data grid view. The right-click menu appears.

3   Click **Remove selected devices**. A confirmation dialog appears and asks if you are sure you want to delete the selected devices.

4   Click **Yes** to delete the selected devices or **No** to cancel the device deletion. If you clicked Yes, the selected devices are removed from the device list.

Print and Print Preview

Each data grid can produce printable reports of the items in the data grid view.

Note: The print capability is disabled in the trial version of WhatsConnected.

To print items in a data grid view:

1   Right-click any item in the data grid view. A right-click menu appears.

2   Select **Print**. The standard Print dialog appears.

3   Select the print options, then click **OK**.

To print preview items in a data grid view:

1   Right-click any item in the data grid view. A right-click menu appears.

2   Select **Print Preview**. The standard Print Preview view appears. You may use this view to preview how the report will look when printed.

Tip: You can print the document by clicking **Print** in the Print Preview toolbar.

Save to a Comma-Separated Value (CSV) file

Each data grid can be saved to a comma-separated text file. This allows data to be extracted from the WhatsConnected data files and imported into other applications, such as Microsoft Excel.

Note: This capability is disabled in the trial version of WhatsConnected.

To save to a Comma-Separated Value (CSV) file:

1   Right-click any item in the data grid view. A right-click menu appears.

2   Click **Save to CSV**. The Save to CSV file dialog appears.

3 Browse to the location where you want to save the CSV file, then enter a **File name** for the data grid view.

4 Click **Save**.

Copying to clipboard

Each data grid can be copied to the windows clipboard and then pasted into another application.

> **Note**: This capability is disabled in the trial version of WhatsConnected.

To copy data items to the clipboard:

1 Click any item in the data grid view to ensure the correct view is selected.

2 Press `Control + C`. The data grid view items copy to the clipboard.

3 Open any application to which you can paste the clipboard data; for example Microsoft Excel™.

4 Press `Control + V`. The contents of the clipboard copy into the application.

About Device Categories View

Device Categories View automatically categorizes and groups network devices so they can be viewed by their functional characteristics. Categories include networking groups such as Routers, Switches, Hubs, and Wireless Access Points. This view also helps distinguish between desktop and server operating systems such as Macintosh, Windows, Windows Servers, Linux, and UNIX. Additional device categories, such as Printers and IP Phones, help organize your network data. Any device that is either not categorized, nor supports SNMP, is placed in the Unknown category.
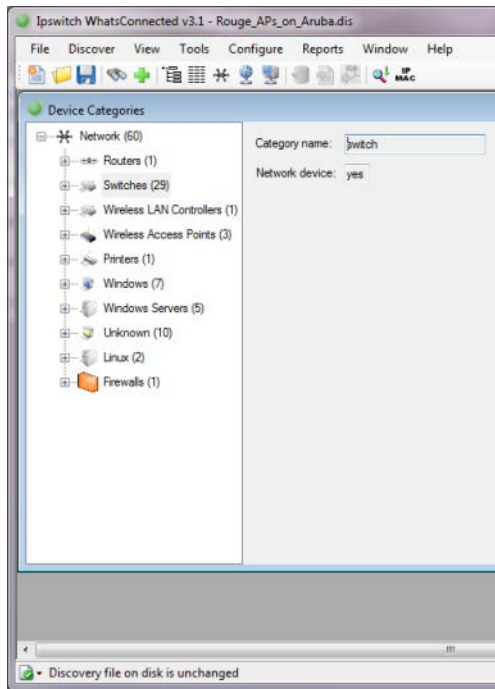
The Device Categories view also provides a tabular view of the inventory and configuration data that is gathered from each network device. For more information, see *About Device Details tab view* (on page 38).

💡 **Tip**: The actual device categories may be rearranged within the Device Categories view by clicking and dragging a category from one location in the list to another.

Data displayed in this view can be removed, printed, print previewed, or saved to a comma-separated-value (CSV) file for use in Microsoft Excel or other reporting applications. For more information, see *About data grid views* (on page 32).

To view Device Categories:

1   From the main menu of the WhatsConnected console, select **View > Device Categories**. The Device Categories view appears.
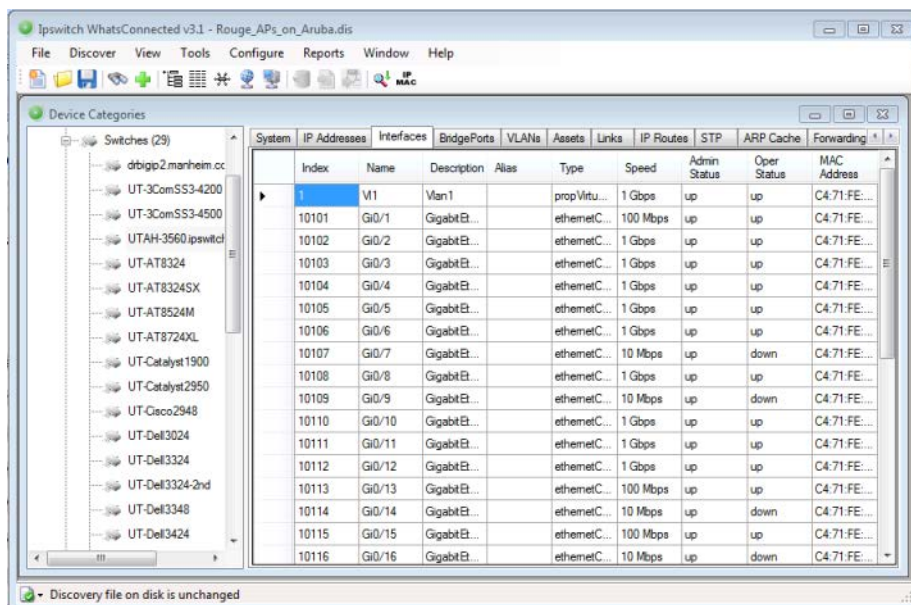
> 💡 **Tip**: You can also view device categories from the WhatsConnected console shortcut menu. Click ▤ (Device Categories shortcut icon). The Device Categories dialog appears.

2   Click a category to expand it and view more information about the devices in the category.

3   Click a device to display device details on the right side of the page.

About Device Details tab view

Associated with the Device Categories view, the Device Details tab provides a tabular view that displays detailed network device information. When a device is selected in the Device Categories view, the details of the device are shown in the Device Details tab view.

Tabs are only shown if a device has data that can be displayed. Possible tab views that may be associated with each device are:

- **System**. Provides IP Address/MAC Address, MIB II information, product vendor, and other system information.

- **IP Addresses**. Provides IP Address configuration information.

- **Interfaces**. Provides name entries (IF information) for each device interface and other interface information.

- **BridgePorts**. Provides Bridgeport and VLAN name and index information.

- **VLANs**. Provides Virtual LAN configuration information.

- **LAG Trunks**. Provides Link Aggregation Group information.

- **Assets**. Provides inventory information about the device components.

- **Access Points**. Provides information about network wireless access points.

- **Rogue Access Points**. Provides information about wireless access points not on the network.

- **AP Clients**. Provides information about AP client devices.

- **Links**. Provides physical connectivity information from this device to other network devices.

- **Spanning Tree (STP)**. Provides spanning tree configuration and status information.

- **ARP Cache**. Provides Address Resolution Protocol (ARP) table information.

- **Forwarding**. Provides Layer 2 forwarding information.

- **Credentials**. Provides information about successful credential/protocol matches for this device.

- **HSRP**. Provides information about the Hot Standby Router Protocol (HSRP) on the device. The information relates to the standby nature of routers.

- **IP Phone**. Provides information about the selected (individual) IP phone.

- **IP Phones**. Provides information about the IP phones that are registered or are communicating with a call manager.

- **IP Routes**. Provides information about the IP routes configured for this device.

- **VRRP**. Provides information about the Virtual Router Redundancy Protocol (VRRP) on the device. The information relates to the standby nature of routers.

- **Software**. Provides information about installed software discovered on this device.

- **Windows**. Provides information about the Windows system software and hardware.

- **Config**. Provides information about device config files.

- **VM Host**. Provides information about virtual servers.

- **Virtual Machines**. Provides information about the virtual machines on a virtual server.

- **Virtual Machine**. Provides information about virtual machines.

Each of the Device Details tabs is built with the data grid views that were described previously. For more information about the data grid views, see *About data grid views* (on page 32). These views allow you to browse, sort, and export (print) the data that is shown for each device.

About the Device Categories View right-click menus

Right-click **Network** in the Device Categories explorer view for the following options:

- **Add Category**. Opens the Device Category Configuration dialog, which allows you to add a new device category.

- **Show Hidden Category**. Select this option to show a hidden category.

- **Remove All Devices**. Select this option to delete all discovered devices from the network file.

Right-click a category in the Device Categories explorer view for the following options:

- **Add Category**. Opens the Device Category Configuration dialog, which allows you to add a new device category.
- **Edit Category**. Opens the Device Category Configuration dialog, which allows you to configure a device category.

Note: You cannot edit system generated categories.

- **Delete Category**. Allows you to delete a category from the Device Categories explorer view.

Note: You cannot delete system generated categories.

- **Hide Category**. Hides the category from the Device Categories explorer view.
- **Remove All <Category Name>**. Removes all devices associated with the selected category from the Device Category explorer view.
- **Send Wake-On-LAN**. If the category has Windows or Windows Servers with a MAC address, this feature sends a UDP message or sequence to the selected device to activate it.

Right-click a device in the Device Categories explorer view for the following options:

- **Add Category**. Opens the Device Category Configuration dialog, which allows you to add or configure a device category.
- **Edit Device Type/Category**. Opens the Device Type Configuration dialog, which allows you to edit a device type's configuration.
- **Edit Device Type Mapping(s)**. Opens the SNMP OID to Device Type Configuration dialog, which allows you to create or modify a custom device type mapping.
- **Show on Topology Map**. Opens the Topology Map view, which displays a graphical representation of the device.
- **Re-Discover Device**. Opens the Run Discovery dialog, which allows you to refresh the network connection and update device information in the device list.
- **Remove Device**. Deletes the device from the Device Categories explorer view.
- **Connect**. Allows you to connect to the device remotely using Telnet, SSH, Browse (e.g. Internet Explorer), or Remote Desktop Connection.
- **Ping**. Opens a command prompt window, which displays data packets sent to the device and returned to the sender to verify network connectivity.
- **Send Wake-On-LAN**. If the device has Windows or Windows Servers with a MAC address, this feature sends a UDP message or sequence to the selected device to activate it.
- **Trace Route**. Opens a command prompt window, which displays the path of data packets sent to the device and the length of time required for each hop.
- **Assign OID**. Opens the System OID dialog, which allows you to assign a system OID to the selected device.
- **Capture Config**. Opens the Capture Config dialog, which allows you to *view and backup the running and startup configurations for the selected device* (on page 70).

- **Edit MIB II Information**. Opens the Change System Info dialog, which allows you to edit the MIB II system settings for the selected device.

Right-click a device in the Device Categories *data grid view* (on page 32) for the following options:

- **Print Preview**. Opens the Print Preview dialog, which shows a preview of the information to be printed.
- **Print**. Opens the Print dialog, which allows you to print a hardcopy of the device list.
- **Save to CSV**. Opens the Save CSV File dialog, which allows you to save an electronic copy of the device list.

> **Note**: Menu options appear inactive in the right-click menu if it is not possible for the user to perform the action.

Right-click a credential in the Credentials tab for the following options:

- **Add**. Opens the Protocol Settings/Credentials dialog, which allows you to configure the protocol credentials to use for network discovery.
- **Remove**. Removes the selected credentials from the device.

About Device List View

Device List View is a spreadsheet-like view that helps you organize, filter, and find network devices and data.

You can filter data displayed in the view by using the Device Filter and Advanced features.

Data displayed in this view can be filtered, edited by device category, shown in device categories, removed, printed, print previewed, or saved to a comma-separated-value (CSV) file for use in Microsoft Excel or other reporting applications. For more information, see *About data grid views* (on page 32).

💡 **Tip**: You can double-click any device in the Device List view. The Device Details tab view opens with more details about the device.

To view Device List:

1   From the main menu of the WhatsConnected console, select **View > Device List**. The Device List view appears.

💡 **Tip**: You can also view device list from the WhatsConnected console shortcut menu. Click ▦ (Device List shortcut icon). The Device List dialog appears.

To view Device Details:

- With the device list open, double-click a device in the list. The Device Details appear. For more information, see *About Device Details tab view* (on page 38).

About Device List columns

The device list shows all matching devices in the data grid view. There are a number of columns that display the respective data for each device.

The default columns of the Device List grid view are:

- **Hostname**. The DNS hostname for the device.
- **IP Address**. The IP address that the device was discovered by.
- **MAC Address**. The MAC address associated with the main IP address.
- **System Name**. The MIB II system name.
- **System Description**. The MIB II system description.
- **System OID**. The MIB II system object ID.
- **Device Category**. Indicates to which category the device belongs (i.e. router, switch, hub, printer, etc.).
- **Vendor**. The network device manufacturer.
- **Model**. The network device model number.

The following additional columns can also be displayed in the Device List:

- **NetBios Name**. The windows NetBios name (if supported and known).
- **NetBios Domain**. The windows NetBios domain (if supported and known).
- **SNMP Device**. A flag indicating whether the device is SNMP enabled.
- **Network Device**. A flag indicating whether this device is a network infrastructure device (i.e. routing, switching, forwarding network traffic).

- **Virtualization Type**. Indicates whether the device is a virtual representation of a real device—possible values are VMware or VirtualPC.

Viewing Device List details

Associated with the Device List view, the Device Details tab provides a tabular view that displays detailed network device information. When a device is selected in the Device List view, the details of the device are shown in the Device Details tab view.
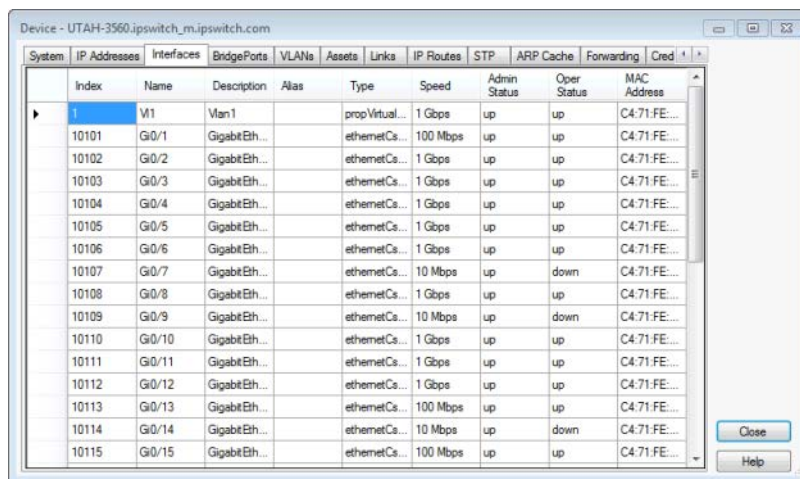
To view the device list details:

1 From the main menu of the WhatsConnected console, select **View > Device List**. The Device List view appears.

> 💡 **Tip**: You can also view device list from the WhatsConnected console shortcut menu. Click ▦ (Device List shortcut icon). The Device List dialog appears.

2 In the device list, select a device for which to view more details, then click **Details**. The Device Details list appears.

Tabs are only shown if a device has data that can be displayed. Possible tab views that may be associated with each device are:

- **System**. Provides IP Address/MAC Address, MIB II information, product vendor, and other system information.

- **IP Addresses**. Provides IP Address configuration information.

- **Interfaces**. Provides name entries (IF information) for each device interface and other interface information.

- **BridgePorts**. Provides Bridgeport and VLAN name and index information.

- **VLANs**. Provides Virtual LAN configuration information.

- **LAG Trunks**. Provides Link Aggregation Group information.

- **Assets**. Provides inventory information about the device components.

- **Access Points**. Provides information about network wireless access points.

- **Rogue Access Points**. Provides information about wireless access points not on the network.

- **AP Clients**. Provides information about AP client devices.

- **Links**. Provides physical connectivity information from this device to other network devices.

- **Spanning Tree (STP)**. Provides spanning tree configuration and status information.

- **ARP Cache**. Provides Address Resolution Protocol (ARP) table information.

- **Forwarding**. Provides Layer 2 forwarding information.

- **Credentials**. Provides information about successful credential/protocol matches for this device.

- **HSRP**. Provides information about the Hot Standby Router Protocol (HSRP) on the device. The information relates to the standby nature of routers.

- **IP Phone**. Provides information about the selected (individual) IP phone.

- **IP Phones**. Provides information about the IP phones that are registered or are communicating with a call manager.

- **IP Routes**. Provides information about the IP routes configured for this device.

- **VRRP**. Provides information about the Virtual Router Redundancy Protocol (VRRP) on the device. The information relates to the standby nature of routers.

- **Software**. Provides information about installed software discovered on this device.

- **Windows**. Provides information about the Windows system software and hardware.

- **Config**. Provides information about device config files.

- **VM Host**. Provides information about virtual servers.

- **Virtual Machines**. Provides information about the virtual machines on a virtual server.

- **Virtual Machine**. Provides information about virtual machines.

Each of the Device Details tabs is built with the data grid views that were described previously. For more information about the data grid views, see *About data grid views* (on page 32). These views allow you to browse, sort, and export (print) the data that is shown for each device.

About the Device List View right-click menu

Right-click a device in the Device List *data grid view* (on page 32) for the following options:

- **Edit Device Type/Category**. Opens the Device Type Configuration dialog, which allows you to edit a device type's configuration.

- **Edit Device Type Mapping(s)**. Opens the SNMP OID to Device Type Configuration dialog, which allows you to create or modify a custom device type mapping.

- **Show in Device Categories**. Opens the Device Categories view, which displays detailed network device information for the selected device.

- **Show on Topology Map**. Opens the Topology Map view, which displays a graphical representation of the device.

- **Re-Discover Device**. Opens the Run Discovery dialog, which allows you to refresh the network connection and update device information in the device list.

- **Remove selected devices**. Deletes selected device(s) from the Device List data grid view.

- **Connect**. Allows you to connect to the device remotely using Telnet, SSH, Browse (e.g. Internet Explorer), or Remote Desktop Connection.

- **Ping**. Opens a command prompt window, which displays data packets sent to the device and returned to the sender to verify network connectivity.

- **Send Wake-On-LAN**. If the device has Windows or Windows Servers with a MAC address, this feature sends a UDP message or sequence to the selected device to activate it.

- **Traceroute**. Opens a command prompt window, which displays the path of data packets sent to the device and the length of time required for each hop.

- **Poll/Monitor**. Allows you to view ping status/latency, interface statistics/utilization, *CPU utilization* (on page 66), and *memory utilization* (on page 67) information for the devices in the Device List view.

- **Assign OID**. Opens the System OID dialog, which allows you to assign a system OID to the selected device.

- **Capture Config**. Opens the Capture Config dialog, which allows you to *view and backup the running and startup configurations for the selected device* (on page 70).

- **Edit MIB II Information**. Opens the Change System Info dialog, which allows you to edit the MIB II system settings for the selected device.

- **Print Preview**. Opens the Print Preview dialog, which shows a preview of the information to be printed.

- **Print**. Opens the Print dialog, which allows you to print a hardcopy of the device list.

- **Save to CSV**. Opens the Save CSV File dialog, which allows you to save an electronic copy of the device list.

> **Note**: Menu options appear inactive in the right-click menu if it is not possible for the user to perform the action. If multiple devices are selected, menu options applicable to a single device are disabled.

About Topology Maps View

Topology Maps view displays the layer 2, or physical topology, of your networking devices. Topology maps can be organized by groups or individually. By default, WhatsConnected builds a *Network Devices* view that displays the topology of your core network device infrastructure.
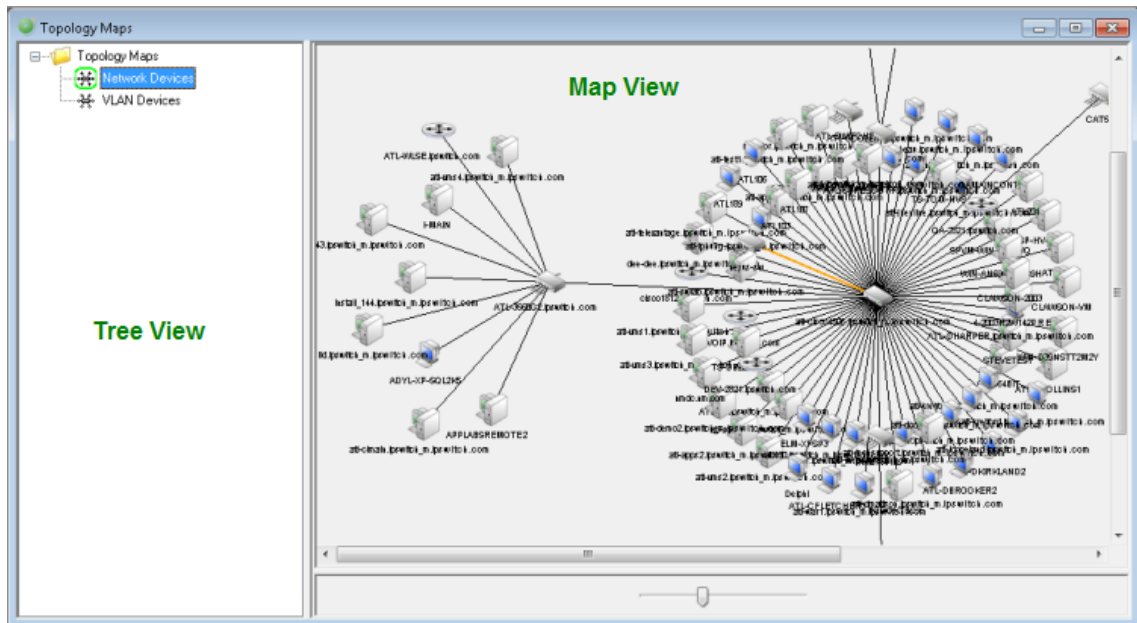
With the topology data, you can build custom topology views that display important elements of your network infrastructure. Use the:

- **Topology Map Tree View** (left). Right-click on a folder or map name to add, delete, edit, and rename maps and map groups.

> 💡 **Tip**: The ⊕ icon shown next to the Topology Map name, in the tree view, indicates that the map is configured as a dynamic topology map. For more information, see *Managing dynamic topology map updates* (on page 55).

- **Topology Map View** (right). Right-click on a map to add, connect, remove, and link devices. You can also export maps to Microsoft Visio and WhatsUp Gold, configure dynamic map updates, and use the poll and monitor tools to check performance for devices on a map. Right-click on individual devices on a map to add and remove connected devices, remove devices, select root devices, link to devices, view device properties, capture device configurations (for devices such as routers and switches), browse devices that are serving web pages, connect to devices via Telnet or SSH, Remote Desktop Connect (RDP) to Windows devices, Ping devices, and run Trace Route on the path to a device.

About Topology Tree View

Topology Maps View is an explorer-type view that allows you to organize and view network data in a graphical format. The topology viewer provides the capability to visually represent the relationships between each network device based on either its physical network connectivity or on your preferences. The left tree view allows you to organize topology groups and maps while the right view displays a graphical topology view of the network devices. To learn more about topology maps and using the topology maps view, see *Managing and customizing topology groups and maps* (on page 47).

Managing and customizing topology groups and maps

The topology tree view allows you to manage your topology maps through the right-click menu. WhatsConnected allows you to create your own custom topology maps. Using the layer 2 connectivity data, you can interactively place devices on a topology map and then use the right-click menu for that device to add/remove connected devices.

To add a new topology map:

1   Right-click on any topology group in the topology tree view. The right-click menu appears.
2   Select **Add Map**. The Add Map dialog appears.
3   Enter a name for the new topology map in **Name**.

> **Note**: Topology map names must be unique.

4   Click **OK**. The topology map is added to the selected group.

To add a new topology group:

1   Right-click on topology group in the topology tree view. The right-click menu appears.
2   Select **Add Group**. The Add Group dialog appears.
3   Enter the name of the new topology group in **Name**.

> **Note**: Topology group names must be unique.

4   Click **OK**. The topology group is added as a subfolder under the selected group.

To rename a topology group:

1   Right-click on a non-default, user created topology group in the topology tree view. The right-click menu appears.
2   Select **Rename**. The Rename Group/Map dialog appears.
3   Enter the new name of the topology group in **Name**.
4   Click **OK**. The topology group or map is updated to reflect the new name.

To delete a topology group or map:

1   Right-click on a topology group or map in the topology tree view. The right-click menu appears.
2   Click **Delete**. The group/map will be removed from the topology tree view.

To cut and paste a topology group or map:

1   Right-click on topology group or map in the topology tree view. The right-click menu appears.

2   Select **Cut**. The group or map is removed from the topology tree view.

3   Right-click on the topology group that you would like to place the topology item under in the tree view. The right-click menu appears.

4   Select **Paste**. The group or map is placed under the selected topology group.

About adding individual or connected devices to a topology map

WhatsConnected allows you to customize topology maps by adding devices to the topology map.

There are two methods by which to add devices to a topology map:

- Adding an individual device to a topology map.

- Adding a connected device to a topology map.

The following steps describe how to accomplish both methods.

> **Tip**: You can also update topology maps dynamically, as scheduled or manual discoveries occur. For more information, see *Managing dynamic topology map updates* (on page 55).

To add device(s) to a topology map:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ✳ (Topology maps shortcut icon). The Topology Maps dialog appears.

2   Select a topology map you want to view in the topology tree view.

3   Right-click in the topology map area. The right-click menu appears.

4   Select **Add Devices**. The Select Devices dialog appears.

5   Select the devices from the list that you want to add to the topology map. You can:

- Double-click a device to select it and return to the previous dialog.

- Press Ctrl and click to select multiple non-contiguous devices in the list.

- Press Shift and click to select multiple contiguous devices in the list.

6   Click **OK**. The selected devices are placed on the topology map. The layout settings (for example, radial or hierarchy) determine how the new devices are displayed in the topology map. To learn more about topology layout modes, please see *About Topology layout modes* (on page 57).

> **Note**: The topology map shows the relationships between devices on the map based on their Layer 2 connectivity—if two devices are physically connected, the topology view illustrates their connection.

To add connected devices to a topology map:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> 💡 **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ❄ (Topology maps shortcut icon). The Topology Maps dialog appears.

2   Right-click on a device in a topology map. The right-click menu appears.

3   Select **Add Connected**. The following options are displayed.

- **Network Devices**[x/y]. Add all connected network devices to the topology map.

- **Servers**[x/y]. Add all connected servers to the topology map.

- **Workstations**[x/y]. Add all connected workstations to the topology map.

- **Printers**[x/y]. Add all connected printers to the topology map.

- **All Devices**[x/y]. Add all connected devices to the topology map.

- **Virtual Machines [x/y]**. Add all virtual machines to the topology map.

> 📝 **Note**: [x/y] represents the following:
> y = the number of devices of that type connected to the device you have selected.
> x = the number of connected devices that are already on the topology map.

- **Select**. Use the Select Devices dialog to individually select which connected devices are added to the topology map.

4   By clicking on any of the displayed options, the topology map is updated with the selected devices.

About removing devices from a topology map

WhatsConnected allows you to customize topology maps by removing devices from a topology map.

There are four methods to remove devices from a topology map:

- Remove all devices from a topology map.

- Remove a single device from a topology map.

- Remove select devices from a topology map.

- Remove connected devices from a topology map.

> 💡 **Tip**: You can also update topology maps dynamically, as scheduled or manual discoveries occur. For more information, see *Managing dynamic topology map updates* (on page 55).

The following steps describe the methods to remove devices.

To remove all devices from a topology map:

1   Select the topology map in the topology tree view.

2   Right-click in the topology map area. The right-click menu appears.

3   Select **Remove All**. All devices are removed from the topology map.

To remove a single device from a topology map:

1   Select the topology map in the topology tree view.

2   Right-click on a device on the topology map. The right-click menu appears.

3   Select **Remove Device**. The device is removed from the topology map.
    - or -
    Select a device on the topology map.

4   Press DELETE. The device is removed from the topology map.

To remove selected devices from a topology map:

1   Select the topology map in the topology tree view.

2   Right-click in the topology map area. The right-click menu appears.

3   Click **Remove Devices**. The Select Devices dialog appears.

4   Use the Select Devices dialog to select the devices that you would like removed from the topology map.

- Press CTRL to select multiple non-contiguous devices in the list.

- Press SHIFT to select multiple contiguous devices in the list.

5   Click **OK**. The selected devices are removed from the topology map.

To remove connected devices from a topology map:

1   Select the topology map in the topology tree view.

2   Right-click on a device on a topology map. The right-click menu appears.

3   Select **Remove Connected**. The following options are displayed.

- **Network Devices** [x/y]. Remove all the connected network devices from the topology map.

- **Servers** [x/y]. Remove all the connected servers from the topology map.

- **Workstations** [x/y]. Remove all the connected workstations from the topology map.

- **Virtual Machines** [x/y]. Remove all virtual machines from the topology map.

- **Printers** [x/y]. Remove all the connected printers from the topology map.
- **All Devices** [x/y]. Remove all connected devices from the topology map.

> **Note**: [x/y] represents the following:
> y = number of devices of this type connected to the device you have selected.
> x = number of connected devices that are already on the topology map.

- **Select**. Click to use the Select Devices dialog to individually select the connected devices to remove from the topology map.

4 The selected devices are removed from the topology map.

Viewing link or multi-linked properties from the topology map

From the Topology Map, you can use the right-click menu to view link properties for each link on the map.

To view link properties on the topology map:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click (Topology maps shortcut icon). The Topology Maps dialog appears.

2 Select a topology map you want to modify in the topology tree view.
3 Right-click a link line between connected devices, then select **Link Properties**. The Link Properties dialog appears.
4 View the information about the two linked devices. If viewing a Multi-Link properties dialog, you can scroll or click the page bar to select the device connection point you want to view.
- or -
Click **Remove Link** to remove the link between the devices on the topology map.

Exporting network data

With your network data and topology maps in place, you are ready to start monitoring and exporting your Layer 2 network devices. One of the key features of the WhatsConnected solution is the capability to export network data into platforms outside of the WhatsConnected console. Sharing the details of your network through Microsoft Visio™ documents or creating topology maps in WhatsUp Gold provide flexible tools to document and monitor your network.

You can use the topology map right-click menu to export WhatsConnected data to WhatsUp Gold or Microsoft Visio and you can export maps to WhatsUp Gold each time a scheduled discovery task runs.

Exporting topology maps to WhatsUp Gold

You can use the topology map right-click menu to export WhatsConnected map details to WhatsUp Gold. When a topology map is exported, the devices discovered with WhatsConnected are automatically created as new devices (or merged with existing devices) in the WhatsUp database.

The following are created by the WhatsConnected export:

- The device collection and Map View are created to represent the WhatsConnected topology map.

- Active and statistical monitors are created for topology connections on each Map View.

- Device Inventory attributes are created in the WhatsUp database. Device attributes, such as Name, Description, Contact, Location, Serial Number, Model, and VLAN, are created on each exported device.

During the export, WhatsConnected compares devices in the WhatsUp Gold database with those in the WhatsConnected network data. Matches are made based on device attributes to avoid duplicate devices exporting to WhatsUp Gold.

To export a topology map to Ipswitch WhatsUp Gold:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.
2 Select the topology map, in the topology tree view, that you want to export.
3 Right-click in the topology map area. The right-click menu appears.
4 Click **Export To**. The right-click menu appears.
5 Click **WhatsUp Gold**. The WhatsUp Gold Export dialog appears.

> **Tip**: You can also select the topology map you want to export, then from the shortcut menu of the WhatsConnected console, click (Export topology to WhatsUp Gold icon). The WhatsUp Gold Export dialog appears.

6 Enter the appropriate information:

> **Important**: If you have enabled the FIPS 140-2 mode in WhatsUp Gold and want to export devices from WhatsConnected to WhatsUp Gold, make sure the device has credentials that support FIPS 140-2 (SNMP v3 with SHA-1 authentication and AES-128 encryption).
> **Important**: If you received an error during the WhatsConnected to WhatsUp Gold export process, you need to remove credentials for devices that used non-compliant FIPS 140-2 SNMP v3 credentials (MD5 authentication or DES56 encryption) and create FIPS 140-2 compliant SNMP v3 credentials (SHA-1 authentication and AES-128 encryption), then run the WhatsConnected network discovery again.

- **WhatsUp Gold Settings**

  - **Server**. Select a WhatsUp Gold Server (endpoint) to which WhatsConnected will export the topology map. You can click browse (**...**) to open the WhatsUp Gold Remote Servers dialog and Add, Edit, Copy, or Delete WhatsUp Gold remote servers that maps can be exported to.

- **WhatsUp Gold nodes**. Indicates the number of monitored devices and the maximum number of nodes available on the current WhatsUp Gold license.

- **WhatsConnected nodes**. Indicates the number of WhatsConnected nodes that have been exported to WhatsUp Gold and the maximum number of nodes available on the current WhatsConnected license.

- **Nodes to export count**. Indicates the number of new nodes that will be added to WhatsUp Gold by this export and the total nodes to be added to WhatsUp Gold by this export.

Important: WhatsConnected does not allow you to export devices to the WhatsUp database that exceed the available device count in the license. If prompted, you must reduce the number of devices that you are attempting to export. Remove the devices from the WhatsConnected topology map.

- **Layer 2 / Topology Export Settings**. Use the following options to describe the information and types of monitors to create during the export.

  - **Enable Exported Ping/SNMP Interface Active Monitors**. Select this option to enable Ping and SNMP Interface Active Monitors. This mode activates the polling engine to immediately begin polling the new monitors upon their creation.

  - **Create Ping Latency and Availability Performance Monitors**. Select this option to create Ping Latency and Availability Monitors for the exported devices.

  - **Create Interface Utilization Performance Monitors**. Select this option to create Interface Utilization Performance Monitors for the interfaces that connect the exported devices on the topology map.

Note: Only the interfaces that connect devices are exported.

  - **Enable Exported Performance Monitors**. Select this option to enable Performance Monitors for the exported devices. This mode activates the polling engine to immediately begin polling the new monitors upon their creation.

  - **Create Device Dependencies**. Select this option to create an up dependency for each child device in a parent-child relationship in the exported devices. The child device will not be actively polled when the parent device is down.

After all export settings are configured, click **Export**.

The **Status** field and progress bar displays the progress of the export.

To view the export results, open WhatsUp Gold console and find the device collection with the same name as the WhatsConnected topology map. The default topology map is named *Network Devices*.

Exporting topology maps to Microsoft Visio

You can use the topology map right-click menu to export WhatsConnected network data to Microsoft Visio 2003 or 2007 where you can further view and edit the network map. The following information describes the steps to export your topology maps to Visio from WhatsConnected.

To export a topology map to Microsoft Visio from WhatsConnected:

1 From the main menu of the WhatsConnected console, click **View > Topology Maps**. The Topology Maps tree appears.

2 Select the topology map, in the topology tree view, that you want to export.

3 Right-click in the topology map area. The right-click menu appears.

4 Select **Export To > Visio**. The Visio Export dialog appears.

> 💡 **Tip**: You can also select the topology map you want to export, then from the shortcut menu of the WhatsConnected console, click (Export topology to Microsoft Visio icon). The Visio Export dialog appears.

5 Enter the appropriate information in the following fields:

- **Document Dimensions**

  - **Sheet(s) across**. Defines the width of the document.

  - **Sheet(s) down**. Defines the height of the document.

- **Include in export**

  - **Custom Properties**. Each shape on the Visio document can be populated with custom properties. Select this option to indicate that you want custom properties placed on the Visio shape.

> 📝 **Note**: Custom properties include: IP address, MAC address, Host name, NetBIOS name, NetBIOS domain, System name, System description, System OID, System contact, System up-time, Vendor, Model, Serial Number, Hardware revision, Firmware revision, and Software revision.

  - **Link Labels**. Select this option to indicate that labels should be placed on the Visio links that attach devices to one another. In most cases, this represents the interface names that connect the devices.

  - **Multi-Link Labels**. Select this option to indicate that a multi-link label should be displayed in the Visio document. Multi-link labels are used when multiple ports/interfaces connect two devices (i.e. LAG ports).

> 📝 **Note**: The shapes that are used in the Visio document are based on the shapes that are shown in the topology view. You may change these shapes in the Application Settings dialog.

6 Click **OK**. The topology map exports to a Visio document.

Exporting topology maps to .pdf

You can use the topology map right-click menu to export WhatsConnected map details to Adobe .pdf files.

To export a topology map to an Acrobat .pdf from WhatsConnected:

1   From the main menu of the WhatsConnected console, click **View > Topology Maps**. The Topology Maps tree appears.

2   Select the topology map, in the topology tree view, that you want to export.

3   Right-click in the topology map area. The right-click menu appears.

4   Select **Export To > PDF**. The PDF Export dialog appears.

5   Enter the appropriate information in the following fields:

- Enter or **Browse** to locate the **PDF File Name**.

Document Dimensions

- **Sheet(s) across**. Enter a numerical value for the number of sheets of paper across you would like the exported map. The default value is 1 sheet across.

- **Sheet(s) down**. Enter a numerical value for the number of sheets of paper down you would like the exported map.The default value is 1 sheet down.

Margins

- **Select the Unit**. Select either *Inches* or *Centimeters*. The default unit is Inches.

- **Top**. Enter a numerical value for the top margin. The default top margin is 1 inch.

- **Bottom**. Enter a numerical value for the bottom margin. The default bottom margin is 1 inch.

- **Left**. Enter a numerical value for the left margin.The default left margin is 1 inch.

- **Right**. Enter a numerical value for the right margin.The default right margin is 1 inch.

- Select **Include Link Labels** to include link labels in the `.pdf`.

- Select **Display PDF File** to load the `.pdf` after successful export.

6   Click **OK**. The map exports to `.pdf`.

Managing dynamic topology map updates

You can apply dynamic map filters to WhatsConnected topology maps so that the maps update dynamically, each time discovery runs. Dynamic maps are updated each time a manual or scheduled discovery is performed. For more information, see *Scheduling dynamic topology map updates* (on page 62).

As a part of selecting (filtering) devices to display in the dynamic topology maps, you use Map Devices and Connected Devices selection filters to build the a custom map. For example, using the Map Devices filtering options, you can select devices in the IP range of 10.0.0.1 - 10.0.0.100 to appear on a map. Any device added to the network, within the range, will be added to the map. You can also apply Connected Devices filters to show devices connected to the core mapped devices. For example, you can filter a map to show all servers connected to switches on the topology map.

This feature helps ensure that your customized topology maps are up-to-date with the most recent network configuration. Use the Edit Map: Network Devices dialog to:

- Define the devices you want to show on the map so that each time the map is updated dynamically, any new devices that match the criteria is added to the map.

- Configure the topology layout and display settings; for example, radial, hierarchy, manual map layout options.
- Automatically export dynamic map discoveries to WhatsUp Gold.

For more information about the filtering options, see *Creating Device Filters* (on page 95).

How to get here:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> 💡 **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ⚒ (Topology maps shortcut icon). The Topology Maps dialog appears.

2 Select the topology map, in the topology tree view, that you want to export.
3 Right-click in the topology map area. The right-click menu appears.
4 Click **Layout / Display Settings**. The Edit Map: Devices dialog appears.
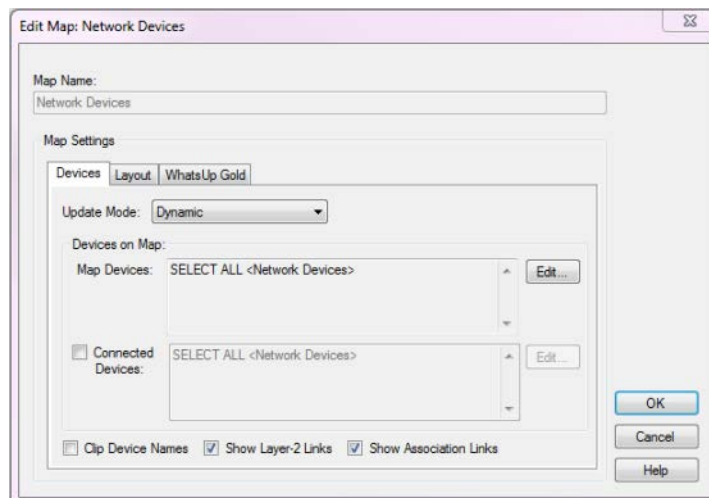
To manage topology map set the update mode and filters, set the layout format, and set the export to WhatsUp Gold option:

The Edit Map: Network Devices dialog includes three tabs to manage device maps:

- **Devices** tab. Use this tab to select the topology map update mode and filter for the devices you want to display on the map. For more information see, *Filtering devices and scheduling topology map updates* (on page 57).

- **Layout** tab. Use this tab to select the topology map layout mode format for the devices on the map: radial, hierarchy, or manual layout. For more information see, *Configuring the topology layout and display settings* (on page 57).

- **WhatsUp Gold** tab. Use this tab to select the option to export topology maps to WhatsUp Gold. If available, VLAN and inventory information exports to WhatsUp Gold. For more information see, *Automatically exporting scheduled map discoveries to WhatsUp Gold* (on page 61).

Filtering devices and dynamically updating the topology map

Use the Edit Map: Devices dialog Devices tab to select the topology map update mode (Dynamic or Manual) and filter the devices you want to display on the map.

How to get here:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> 💡 **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click �֍ (Topology maps shortcut icon). The Topology Maps dialog appears.

2   Select the topology map, in the topology tree view, that you want to export.
3   Right-click in the topology map area. The right-click menu appears.
4   Click **Layout / Display Settings**. The Edit Map: Devices dialog appears.

To filter devices for the topology map:

1   On the Edit Map: Network Devices dialog Devices tab, select the **Update Mode**:

   ▪ **Dynamic**. Select this option to apply the map filters to the topology map each time a scheduled discovery runs. The scheduled map discoveries can also be automatically exported to WhatsUp Gold each time the discovery runs. For more information, see *Automatically exporting scheduled map discoveries to WhatsUp Gold* (on page 61).

   ▪ **Manual**. Select this option to disable device filtering for maps. When the device filters are disabled, you can add devices to the map with the topology map right-click menu. For more information, see *About adding individual or connected devices to a topology map* (on page 48).

2   Use the Map Devices and Connected Devices box to design a filter for the devices you want to include on the map. Click **Edit** next to each device filter to open the Edit Devices Filter dialog and make device filter selections. For more information, see *Creating Device Filters* (on page 95). After the filter options are selected, they appear in the Map Devices and Connected Devices boxes.

3   If you want to shorten each device name on the map, select the **Clip Device Names** option. This option shortens (clips) the device's full domain names on the map. This helps display the map information in a less cluttered, easier to read view.

4   If you want to see layer-2 links for devices in the map, select the **Show Layer-2 Links** option.

5   If you want to see association links for devices in the map, select the **Show Association Links** option.

Configuring the topology layout and display settings

Use the Edit Map: Network Devices dialog Layout tab to select the topology map layout format you want to display. To understand the layout modes, you must first be familiar with the layout strategy used by the WhatsConnected topology engine. For each map, the topology viewer automatically selects a root device, which becomes the starting point of the diagrams. The root device is selected based on finding the device on the diagram with the most network connections. Additionally, you can manually select the root device. For more information, see *Changing the root device selection* (on page 60).

Using the connectivity model, the topology viewer sets the *root* as the parent and then assigns all connected devices as children. This process continues until all devices on the topology map are given a parent/child relationship.

With the parent/child relationships calculated, the WhatsConnected topology viewer provides three layout modes for any topology map. These modes describe the manner in which each child node (or device) is given its position on the topology map. The layout modes are described as follows:

- **Radial**. In this mode, each child node is connected to its parent in a radial (or circular) pattern. For more information, see *About Radial layout settings* (on page 58).

- **Hierarchy**. In this mode, each child node is given a position in a hierarchical or tree-like view with the root being either on the left, top, right or bottom. For more information, see *About Hierarchy Layout settings* (on page 59).

- **Manual**. In this mode, you can use the drag-and-drop features of the topology view to position the device on the topology map where you want to locate it. For more information, see *About Manual Layout setting* (on page 59).

How to get here:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click �֍ (Topology maps shortcut icon). The Topology Maps dialog appears.

2   Select the topology map, in the topology tree view, that you want to export.
3   Right-click in the topology map area. The right-click menu appears.
4   Click **Layout / Display Settings**. The Edit Map: Devices dialog appears.

To change a topology map layout settings:

1   From the Edit Map: Network Devices dialog, select the Layout tab.
2   Use the Layout Settings tab to adjust the layout options.
3   Click **OK**. The selected devices will be repositioned on the topology map.

About Radial Layout settings

In the radial layout mode, connected child devices are given positions in a radial (or circular) pattern around their parent device. You can modify the layout results by changing the following layout attributes:

- **Level Spacing**. This setting dictates the amount of space between the parent and child device. Increase this value to provide more spacing between the parent and children devices.

- **Node Angle**. This setting dictates the amount of space between each child (or sibling) devices. Increase this value to fan out the children.

> **Note**: When increasing the node angle, if a large number of devices are shown connected to one parent, the radial layout may overlap (make a full circle). In this case you may need to decrease the node angle and increase the level spacing.

About Hierarchy Layout settings

In the hierarchy layout mode, connected child devices are given positions in a hierarchical (or tree like) pattern in relationship to their parent. You can modify the layout results by changing the following layout attributes:

Direction. This setting indicates the placement of the root device and the direction the children will be placed from the root device.

- **Down**. The root device is placed at the top of the topology map, and children are placed respectively below the root device.

- **Up**. The root device is placed at the bottom of the topology map, and children are placed respectively above the root.

- **Left**. The root device is placed at the right of the topology map, and children are placed respectively to the left of the root.

- **Right**. The root device is placed at the left of the topology map, and children are placed respectively to the right of the root.

Alignment. This setting indicates the placement of the root (or parent) device in relationship to its children.

- **Center**. The root/parent device is centered (either vertically/horizontally) with respect to its children.

- **Left**. The root/parent device is located to the far left (either vertically/horizontally) with respect to its children.

- **Right**. The root/parent device is located to the far right (either vertically/horizontally) with respect to its children.

Level Spacing. This setting dictates the amount of space between the parent and child devices. Increase this value to provide more spacing between the parent and children devices.

Node Spacing. This setting dictates the amount of space between each child (or sibling) devices. Increase this value to create more space between sibling devices.

Straight Links. A flag that indicates whether the lines from the parent device to the children devices should be straight lines or routed (angled) lines.

About Manual Layout settings

In manual layout mode, the automatic layout methods are turned off and you are given complete control over device placement on the topology map. The topology maps provide a drag-and-drop capability to simplify creating and arranging a custom topology map. The following is a list of drag-and-drop operations in manual layout mode.

- **Left Mouse Click**. Selects a device on the topology map.

- **Shift + Left Mouse Click**. Multi-selects devices on a topology map.

- **Left Mouse Click + Mouse Move**. Selects and drags a device to a new position on the topology map.

- **Alt + Left Mouse Click + Mouse Move**. Selects and drags a device PLUS all of its children to a new position on the topology map.

You can use the manual layout mode to add new devices to the topology map. The method to add a device is the same as adding a device in radial or hierarchical layout mode. After the devices are placed on the topology map, you can manually move devices on the map or select the *radial* (on page 58) or *hierarchy* (on page 59) layout settings to readjust the map.

Layout Children

While in the manual layout mode, the WhatsConnected topology maps provide the capability to use the auto-layout algorithms to reposition child devices on a topology map.

To reposition child devices on a topology map:

Note: Make sure that the layout settings are set to Manual layout to change layout children settings. For more information see, Layout Children in the WhatsConnected Help.

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

Tip: You can also view topology maps from the WhatsConnected console shortcut menu. Click (Topology maps shortcut icon). The Topology Maps dialog appears.

2 Select a topology map you want to modify in the topology tree view.
3 Right-click a device with connected devices, then select **Layout Children**. The Layout Children dialog appears.
4 Use the Layout Settings dialog to adjust the layout options. For more information about auto-layout settings, see *Layout Children* in the WhatsConnected Help.
5 Click **OK**. The selected devices will be repositioned on the topology map.

Changing the root device selection

By default the topology map root device is selected automatically based on the topology map device with the most network connections. After discovery, you can also change the root device selection to a different device.

To manually select the root device:
1 Select any device on the topology map, then right-click. The right click menu appears.
2 Click **Select As Root Device**. This overrides the automatic root calculation and all parent/child relationships are built based on the newly selected device as the root device.

If you have manually changed the root device selection, you can revert back to auto-select the root device if preferred.

To auto-select the Root Device:
1 Select the device on the topology map that was manually selected as the root device, then right-click. The right click menu appears.
2 Click **Auto-Select Root Device**. This disables the manual root device selection and returns the selection back to the automatic root device selection.

Automatically exporting scheduled map discoveries to WhatsUp Gold

Use the Edit Map: Network Devices dialog WhatsUp Gold tab to select the option to export topology maps to WhatsUp Gold. Device attribute information, based on the device filters applied to the map, are exported to WhatsUp Gold. Dynamic maps are exported to WhatsUp Gold each time a manual or scheduled discovery is performed. For more information, see *Scheduling dynamic topology map updates* (on page 62).

How to get here:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ✳ (Topology maps shortcut icon). The Topology Maps dialog appears.

2   Select the topology map, in the topology tree view, that you want to export.
3   Right-click in the topology map area. The right-click menu appears.
4   Click **Layout / Display Settings**. The Edit Map: Devices dialog appears.

To automatically export topology map devices to WhatsUp Gold:

   ▪   On the Edit Map: Network Devices dialog WhatsUp Gold tab, select **Export map to WhatsUp Gold**.

> **Note**: After a scheduled discovery occurs, any updates that occurred during discovery must be saved to the discovery file (.dis) before the updated device information can be exported to WhatsUp Gold.

> **Note**: WhatsConnected exports will not delete devices shown in WhatsUp Gold that were previously discovered, but disappear from subsequent dynamic map updates.

   ▪   **Export Settings (Layer 2 / Topology)**. Use the following options to describe the information and types of monitors to create during the automatic export.

      ▪   **Enable Exported Ping/SNMP Interface Active Monitors**. Select this option to enable Ping and SNMP Interface Active Monitors. This mode activates the polling engine to immediately begin polling the new monitors upon their creation.

      ▪   **Create Ping Latency and Availability Performance Monitors**. Select this option to create Ping Latency and Availability Monitors for the exported devices.

      ▪   **Create Interface Utilization Performance Monitors**. Select this option to create Interface Utilization Performance Monitors for the interfaces that connect the exported devices on the topology map.

> **Note**: Only the interfaces that connect devices are exported.

      ▪   **Enable Exported Performance Monitors**. Select this option to enable Performance Monitors for the exported devices. This mode activates the polling engine to immediately begin polling the new monitors upon their creation.

- **Create Device Dependencies**. Select this option to create an up dependency for each child device in a parent-child relationship in the exported devices. The child device will not be actively polled when the parent device is down.

Scheduling dynamic topology map updates

The dynamic topology map feature updates device maps, based on map filters, each time a discovery runs. However, if you want to run updates automatically on a schedule, use Discovery Tasks to set up scheduled discoveries.

To schedule dynamic topology map updates:

1 Set up a dynamic topology map. For more information, see *Managing dynamic topology map updates* (on page 55).

2 Configure and schedule a Discovery Task. For more information, see *Configuring and scheduling Discovery Tasks* (on page 22).

Polling and Monitoring

WhatsConnected provides map-level tools to test and monitor network device performance and help provide a view of the overall network health. The following polling and monitoring tools help you view specific device performance details:

- **Ping Status/Latency**. Use to poll devices and view the up or down status and response time.
- **Interface Status/Utilization**. Use to poll devices and view interface performance information.
- **CPU Utilization**. Use to poll devices and view CPU performance information.
- **Memory Utilization**. Use to poll devices and view memory use data.

To access

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> 💡 **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ⬚ (Topology maps shortcut icon). The Topology Maps dialog appears.

2 Select the topology map, in the topology tree view, that you want to modify.
3 Right-click in the topology map area. The right-click menu appears.
4 Select the monitor you want to use. The monitor dialog appears.

To use topology map device polling and monitoring tools:

From the topology map right-click menu, select a monitor you want to use. For more information see:

- *Using Poll/Monitor tools - Ping Status/Latency* (on page 63)
- *Using Poll/Monitor tools - Interface Status/Utilization* (on page 64)
- *Using Poll/Monitor tools - CPU Utilization* (on page 66)
- *Using Poll/Monitor tools - Memory Utilization* (on page 67)

Using Poll/Monitor tools - Ping Status/Latency

Use the poll/monitor network map tool to view ping status and latency information for devices on the network map. This report provides information about the ping status (up or down device availability) and a graph of the ping latency (round-trip time over time). This tool can help you determine how a single device or multiple devices are performing and where network device bottlenecks may exist on the network.

The following is a list of the information available for the monitor. The Device, Name, and Product ID columns display by default:

- **Name**. Displays the device name.
- **IP Address**. Displays the computer IP address.
- **Ping Status**. Displays the whether the device is in an up or down state.
- **RTT**. Displays the round trip time in milliseconds; the amount of time it takes for the ping request to be returned from the remote device.

Access the Ping Status/Latency tool:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.
2 Select a topology map you want to view in the topology tree view.
3 Right-click in the topology map area. The right-click menu appears.
4 Select **Poll/Monitor > Network > Ping Status/Latency**. The Ping Status/Latency dialog appears with a list of the devices on the map.

To start a Ping Status/Latency monitor on a map:

1 Select the devices you want to include in the monitor.
2 Click **Settings** if you want to change the Poll Interval and the Ping Timeout settings.
3 Click **Start** to begin the test. The Ping Latency for each device displays in the graph and the Ping Status and Round-Trip Time (RTT) for each device displays in the respective columns in the table below.
4 Click **Stop** to end the monitor test.

To edit the columns that appear in the report:

- Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

- Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

Using Poll/Monitor tools - Interface Status/Utilization

Use the poll/monitor network map tool to view interface status and utilization information for devices on the network map. This report provides a number of interface monitor statistics and a graph of the data transmitted through the interface. This tool can help you determine a variety of information about interface traffic for a single device or aggregate data for multiple devices.

Following are the interface statistic monitors available and the information each provides:

- **In + Out Utilization**. Interfaces that use half-duplexing share the interface between In and Out octets, so the max speed limits both In and Out bytes. This information provides a better view of the total utilization of the interface this monitor by adding the in utilization with the out utilization. This monitor is not useful when viewing interfaces that use full-duplexing.

- **In Broadcast Packets (sec.)**. The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **In Bytes (sec.)**. The same as IfInOctets, from the IF-MIB, per second. renamed to "Bytes" since it is a more common term. One octet is a byte.

- **In Errors (sec.)**. For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character- oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **In Multicast Packets (sec.)**. The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **In Packets (sec.)**. The sum of In Broadcast, Multicast, and Unicast packets.

- **In Ucast Packets (sec.)**. The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **In Unknown Protocols (sec.)**. For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **In Utilization (%)**. The change in InOctets, per second, as a percentage of the max speed of the interface.

- **Out Broadcast Packets (sec.)**. The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **Out Bytes (sec.)**. To provide user with a better view of the total utilization of the interface, this monitor adds the In utilization with the Out utilization. This monitor has no value when viewing interfaces that use full-duplexing.

- **Out Discards (sec.)**. The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **Out Errors (sec.)**. For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **Out Multicast Packets (sec.)**. The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **Out Packets (sec.)**. The sum of Out Broadcast, Multicast, and Unicast packets.

- **Out Queue Length (sec.)**. The count of all packets in the out packet Queue waiting to be sent (per second).

- **Out Ucast Packets (sec.)**. The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of `ifCounterDiscontinuityTime`.

- **Out Utilization (%)**. The change in OutOctets, per second, as a percentage of the max speed of the interface.

To access the Interface Status/Utilization tool:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2 Select a topology map you want to view in the topology tree view.

3 Right-click in the topology map area. The right-click menu appears.

4 Select **Poll/Monitor > Network > Interface Status/Utilization**. The Interface Status/Utilization dialog appears with a list of the devices on the map.

To start a Interface Status/Utilization monitor on a map:

1 Select the devices you want to include in the monitor.

2 Click **Settings** if you want to change the Poll Interval settings.

3 Click **Start** to begin the test. The selected monitor data displays in the graph and the table below.

4 Click **Stop** to end the monitor test.

To edit the columns that appear in the report:

- Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

- Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

Using Poll/Monitor tools - CPU Utilization

Use the poll/monitor network map tool to view CPU utilization information for devices on the network map. This report provides information about CPU performance and a graph of the percentage of CPU utilization. This tool can help you determine how a single device or multiple devices are performing and where CPU performance issues may exist on the network.

The following is a list of the information available for the monitor. The CPU, Protocol, and Utilization% columns display by default:

- **CPU**. Displays the device name.
- **Protocol**. Displays the communication method (protocol) used to access CPU utilization information.
- **Utilization%**. Displays information about the CPU usage percentage.

To access the Interface Status/Utilization tool:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2 Select a topology map you want to view in the topology tree view.

3 Right-click in the topology map area. The right-click menu appears.

4 Select **Poll/Monitor > Network > CPU Utilization**. The CPU Utilization dialog appears with a list of the devices on the map.

To start a CPU Utilization monitor on a map:

1 Select the devices you want to include in the monitor.

2 Click **Settings** if you want to change the Poll Interval settings.

3   Click **Start** to begin the test. The CPU utilization for each device displays in the graph and the respective columns of the table.

4   Click **Stop** to end the monitor test.

To edit the columns that appear in the report:

- Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

- Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

Using Poll/Monitor tools - Memory Utilization

Use the poll/monitor network map tool to view memory utilization information for devices on the network map. This report provides information about memory performance and a graph of the percentage of memory utilization. This tool can help you determine how a single device or multiple devices are performing and where CPU performance issues may exist on the network.

The following is a list of the information available for the monitor. The Device, Total Memory, Used Memory, Free Memory, Protocol, and Utilization% columns display by default:

- **Device**. Displays the device name.
- **Total Memory**. Displays the total amount of memory available on the system.
- **Used Memory**. Displays the amount of memory currently in use by applications.
- **Free Memory**. Displays the amount of memory currently available for applications to use.
- **Protocol**. Displays the communication method (protocol) used to access memory utilization information.
- **Utilization%**. Displays information about the memory usage percentage.

To access the Memory Utilization tool:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2   Select a topology map you want to view in the topology tree view.

3   Right-click in the topology map area. The right-click menu appears.

4   Select **Poll/Monitor > Network > Memory Utilization**. The Memory Utilization dialog appears with a list of the devices on the map.

To start a CPU Utilization monitor on a map:

1   Select the devices you want to include in the monitor.

2   Click **Settings** if you want to change the Poll Interval settings.

3   Click **Start** to begin the test. The memory utilization for each device displays in the graph and the respective columns of the table.

4   Click **Stop** to end the monitor test.

To edit the columns that appear in the report:

▪   Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

▪   Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

▪   Click **Preview** to see a print preview of the entire report.

▪   Click **Print** to print the entire report.

▪   Click **Save** to save the entire report to a CSV file.

Managing individual devices on the topology map

From a topology map, you can right-click a device on the map, use the menu options to manage devices, and start tools for the device.
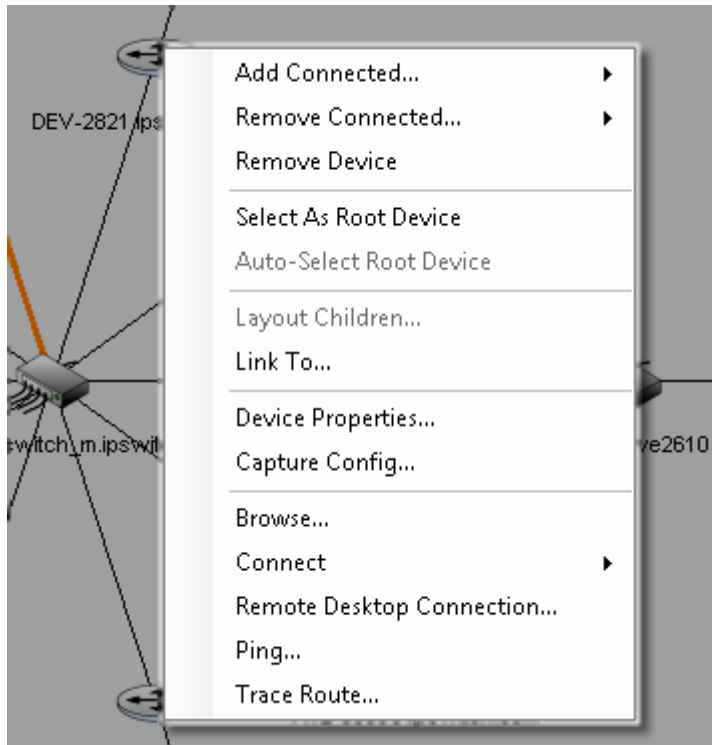
Use the following topology map tools:

▪   **Add Connected** devices. For more information, see *About adding individual or connected devices to a topology map* (on page 48).

- **Remove Connected** devices. For more information, see *About adding individual or connected devices to a topology map* (on page 48).

- **Remove Device** from the map. For more information, see *About removing devices from a topology map* (on page 49).

- **Select as Root Device**. For more information, see *Changing the root device selection* (on page 60).

- **Auto-Select Root Device**. For more information, see *Changing the root device selection* (on page 60).

- **Link To** a device. For more information, see *Adding device links manually* (on page 69).

- **Device Properties**. For more information, see *Viewing device properties from a topology map* (on page 70).

- **Capture Config** tool. For more information, see *Viewing Configuration Archives* (on page 71).

- **Browse** tool. For more information, see *Browsing a device* (on page 72).

- **Connect** tool. For more information, see *Connecting to a device with Telnet or SSH* (on page 72).

- **Remote Desktop Connection** tool. For more information, see *Connecting to a device using Remote Desktop Connection* (on page 73).

- **Ping** tool. For more information, see *Using the Ping tool* (on page 73).

- **Trace Route** tool. *Using the Trace Route tool* (on page 74).

Adding device links manually

The Manual Link dialog lets you manually manage your topology links between devices from the topology map right-click menu. In some cases, where devices cannot be automatically discovered with complete device details, WhatsConnected allows you to create manual device links. Manually defining a device's relationship with another device on the network lets you ensure that the overall topology map is accurate. When devices are linked manually, you can also select the device interfaces/ports that are linked between devices.

After a device is manually linked to another device, each time a new or scheduled discovery occurs, the manual link remains intact and unchanged as it relates to other network devices.

> **Note**: Make sure that at least one of the devices participating in the manual link is a network circuit connection device such as a switch, router, etc.

To add a manual link on the WhatsConnected topology map:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2   Right-click on a device that you want to manually link to another device. The right-click menu appears.

3   Select **Link To...**. The Manual Link dialog appears with the Link From device populated in the Device box in the Link From section of the dialog.

4   From the **Interface/Port** list, select the device interface to connect through.

5   In the **Link From...** section, click to open the Select Devices dialog and select the device to link to, then click **OK**.

6   From the **Interface/Port** list, select the device interface to connect to, then click **OK**.

Viewing device properties from a topology map

From the Topology Map, you can use the right-click menu to view device properties for each device on the map.

To view device properties on the topology map:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

> 💡 **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ⌘ (Topology maps shortcut icon). The Topology Maps dialog appears.

2   Select a topology map you want to modify in the topology tree view.

3   Right-click a device with connected devices, then select **Device Properties**. The Device Viewer appears.

4   Click the tab for the device information you want to view.

Capturing device configurations

You can right-click a device, such as a router or switch, on a topology map to view and backup the *running* and *startup* configurations for devices. This feature provides a way for you to save a backup copy of a device's startup and running configuration. The configuration backup information is stored in the WhatsConnected discovery (`.dis`) file. In addition to saving configuration backup information, you can compare multiple configurations to evaluate configuration changes between different configuration dates.

SSH or Telnet credentials are required to capture device configurations. For more information see, *Configuring network protocols and credentials* (on page 11).

WhatsConfigured provides additional comprehensive configuration management capabilities such as automated configuration task execution and monitoring, integrated alerting and reporting, secure configuration and change management, policy based monitoring, and more. For more information, see *WhatsUp Gold WhatsConfigured* (http://www.whatsupgold.com/whatsconfiguredmktg).

To capture device configurations with WhatsConnected:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2   Select a topology map you want to view in the topology tree view.

3   Right-click a device for which you want to run the Capture Config tool. The right-click menu appears.

4   Click **Capture Config**. The Capture Config dialog appears.

5   In the Config list, select one of the following options:

- **Backup Running Config**. Accesses the device's configuration that operates the device.

- **Backup Startup Config**. Accesses the device's configuration that starts the device.

6 In the Protocol Settings list, select the credentials required to communicate with the device.
- or -
Click the browse button (**...**) to create or edit existing credentials. See the help for more information about using the Protocols/Settings Credentials dialog.

7 Click **Capture** to begin the backup process. The Configuration Archives dialog opens with captured configuration information.

Viewing Configuration Archives

The Configuration Archives dialog shows the results of running the Capture Config tool and the configuration archives saved from previous captures. The Time Created and Config Key information is provided for each capture that has run.
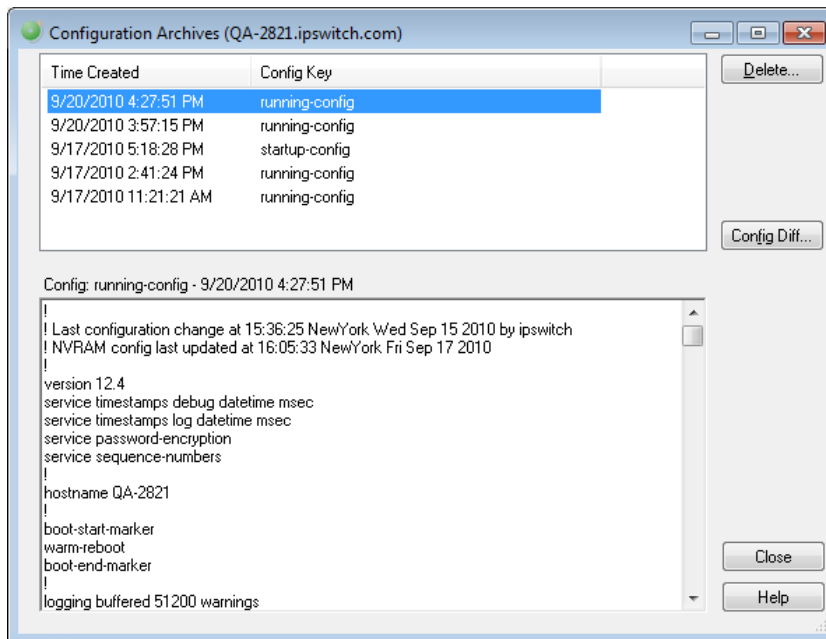

To view configuration archives:

You can select any of the captures in the list to view the detailed configuration information queried from the device. The results of the selected capture is displayed in the lower half of the dialog.

To compare differences between configuration archives:

`Ctrl` select two configurations, then click **Config Diff** to compare the configurations. A side-by-side view of the configuration files appears.
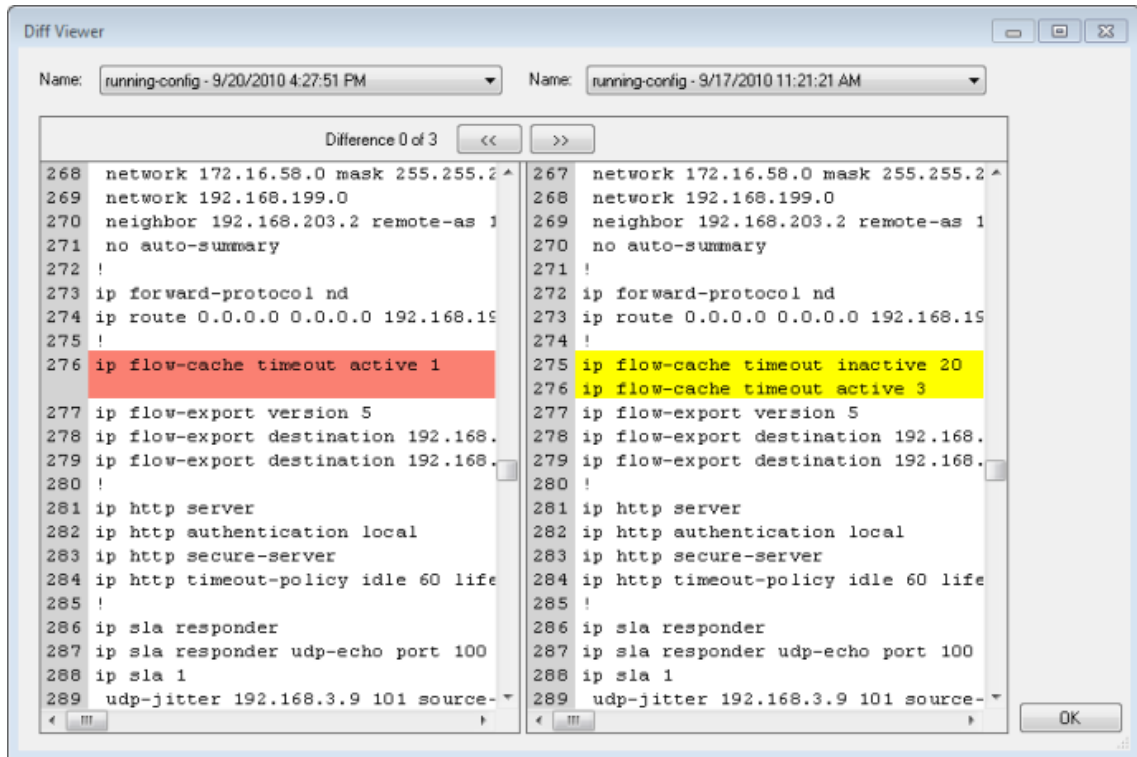
Browsing a device

You can right-click a device on the topology map to browse the web server for the device. If a web server is available on port 80, a browser opens and you connect to the device's web server. This feature provides easy access to the selected device, allowing you to view the web page being served by this device. Often, for switches and routers, the browser-based device configuration application launches.

To browse to a device's web server from WhatsConnected:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2 Right-click on a device that you want to connect to its web server. The right-click menu appears.

3 Click **Browse**. The device's web server page opens in an internet browser.

Connecting to a device with Telnet or SSH

You can right-click a device on the topology map to connect and communicate with the device using Telnet or SSH communication protocols. This feature provides easy access to devices shown on the WhatsConnected topology map view, allowing you to log in and configure the device via Telnet or SSH. You must be familiar with the Telnet or SSH commands in order to manage and configure the device.

> **Note**: The PuTTy program is used to communicate via Telnet or SSH. Refer to the Plink help for details about the Telnet or SSH commands. For more information, refer to the *PuTTY web site* (http://www.whatsupgold.com/Plink).

To connect to a device via Telnet or SSH protocols:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.
2   Select a topology map you want to view in the topology tree view.
3   Right-click on a device that you want to communicate with via Telnet or SSH. The right-click menu appears.
4   Click **Connect**, then select the communication protocol you want to use: **Telnet** or **SSH**. A command prompt opens and starts the selected communication protocol with the device.
5   Log in to the device using the required login credentials.
6   Enter the commands you want to issue to the device. When you have completed the configuration settings, make sure that you logout of the communication session.

Connecting to a device using Remote Desktop Connection

You can right-click a Windows device on the topology map to start a Remote Desktop Connection session. In order to establish the remote connection, the Windows Remote Desktop Connection feature must be enabled on the device and you need to know the login credentials for the device. This feature provides easy access to the selected device, allowing you to access and use the device remotely.

To connect to a remote device using Remote Desktop Connection:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.
2   Select a topology map you want to view in the topology tree view.
3   Right-click on a Windows device that you want to connect to using the Remote Desktop Connection. The right-click menu appears.
4   Click **Remote Desktop Connection**. The Remote Desktop Connection dialog appears.

Using the Ping tool

You can right-click a device on the topology map to ping the device and determine its status. The Ping tool sends out an ICMP (Internet Control Message Protocol) echo request to the selected network device. The following results of the ping request appear:

- **Destination**. The address specified in Address/Hostname.
- **Packets**. The number of data packets sent, received, and lost during the device ping.
- **RTT**. Round trip time in milliseconds; the amount of time it takes for the ping request to be returned from the remote device.

To ping a device:

1   From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.
2   Select a topology map you want to view in the topology tree view.

3 Right-click a device that you want to ping. The right-click menu appears.

4 Click **Ping**. The command prompt dialog appears and pings the selected device.

5 Click **X** to close the command prompt dialog.

Using the Trace Route tool

You can right-click a device on the topology map to do a trace route on a network device. This tool sends out echo requests to the selected device, then traces the path it takes to get to the device IP address or host name. This tool is often used to determine where, on the network, a data transmission interruption occurs. The results of the trace route shows the IP address of each device encountered on the path and the time it took to reach each device encountered on the path.

To run a Trace Route on a device:

1 From the main menu of the WhatsConnected console, select **View > Topology Maps**. The Topology Maps view appears.

2 Select a topology map you want to view in the topology tree view.

3 Right-click a device that you want to run a Trace Route on. The right-click menu appears.

4 Click **Trace Route**. The command prompt dialog appears and runs a trace route on the selected device.

5 Click **X** to close the command prompt dialog.

About the Topology Maps View right-click menus

Right-click a folder in the Topology Maps explorer view for the following options:

- **Add Map**. Opens the Add Map dialog, which allows you to *add a new topology map* (on page 47).

- **Add Group**. Opens the Add Group dialog, which allows you to add a new topology map group.

- **Rename**. Renames the selected folder on the Topology Maps tree view.

- **Cut**. Removes the folder from the Topology Map tree view and allows you to paste the map in another location on the Topology Map tree view.

- **Paste**. Pastes the cut folder in another location on the Topology Maps tree view.

- **Delete**. Removes the folder from the Topology Map tree view.

Right-click a topology map in the Topology Maps explorer view for the following options:

- **Edit**. Opens the Edit Map dialog, which allows you to *edit the selected topology map properties* (on page 55).

- **Cut**. Removes the topology map from the Topology Map tree view and allows you to paste the map in another location on the Topology Map tree view.

- **Delete**. Removes the topology map from the Topology Map tree view.

Right-click the Topology Maps map view for the following options:

- **Add Devices**. Opens the Select Devices to Add dialog, which allows you to browse a list of devices to add to the topology map.

- **Add Connected**. *Adds a new child device* (on page 48) to the topology map.

- **Add Associated**. *Adds a new device* (on page 48) to the topology map.
- **Remove Devices**. Opens the Select Devices to Remove dialog, which allows you to browse a list of devices to remove from the topology map.
- **Remove All**. *Remove all devices* (on page 49) from the topology map.
- **Remove Selected**. *Removes the selected devices* (on page 49) from the topology map.
- **Link Selected**. Link the selected devices on the topology map.
- **Export To**. Allows you to export the topology map to a `.pdf`, Visio file, or to WhatsUp Gold.
- **Layout/Display Settings**. Opens the Edit Map: Network Devices dialog, which allows you to *apply dynamic map filters to WhatsConnected topology maps* (on page 55) so that the maps update dynamically, each time discovery runs.
- **Poll/Monitor**. Allows you to view ping status/latency, interface statistics/utilization, *CPU utilization* (on page 66), and *memory utilization* (on page 67) information for devices on the topology map.

Right-click a device in the Topology Maps map view for the following options:

- **Add Connected**. *Adds a new child device* (on page 48) to the selected device's hierarchy on the topology map.
- **Add Associated**. *Adds a new associated device* (on page 48) to the selected device's hierarchy on the topology map.
- **Remove Connected**. *Removes a current child device* (on page 49) from the selected device's hierarchy on the topology map.
- **Remove Associated**. *Removes the associated device* (on page 49) from the selected device's hierarchy on the topology map.
- **Remove Device**. *Deletes device* (on page 49) from the topology map.
- **Select as Root Device**. Manually selects the device as the root device, or starting point of the diagram.
- **Auto-Select Root Device**. If you have manually selected a device as the root device, this option allows you to return the selection back to the automatic root device selection.
- **Layout Children**. Allows you to use the auto-layout algorithms to reposition child devices on a topology map.
- **Link To**. Opens the Manual Link dialog, which allows you to manually manage your topology links between devices from the topology map.
- **Device Properties**. Opens the Device Properties dialog, which allows you to view details for the selected device.
- **Show in Device Categories**. Opens the Device Categories view, which displays detailed network device information for the selected device.
- **Capture Config**. Opens the Capture Config dialog, which allows you to *view and backup the running and startup configurations for the selected device* (on page 70).
- **Connect**. Allows you to connect to the device remotely using Telnet, SSH, Browse (e.g. Internet Explorer), or Remote Desktop Connection.
- **Ping**. Opens a command prompt window, which displays data packets sent to the device and returned to the sender to verify network connectivity.

- **Trace Route**. Opens a command prompt window, which displays the path of data packets sent to the device and the length of time required for each hop.

- **Edit MIB II Information**. Opens the Change System Info dialog, which allows you to edit system settings (name, contact, location) for the selected device.

Note: Menu options appear inactive in the right-click menu if it is not possible for the user to perform the action. If multiple devices are selected, menu options applicable to a single device are disabled.

About Subnets View

The Subnets View is an explorer-type view that shows the grouping of network subnets on the left side of the pane.

On the right side of the pane, devices associated with their respective subnet are displayed. The data grid view can be column sorted, print previewed, printed, or saved to a comma-separated-value (CSV) file for use in Microsoft Excel or other reporting applications. For more information about data grid views, see *About data grid views* (on page 32).
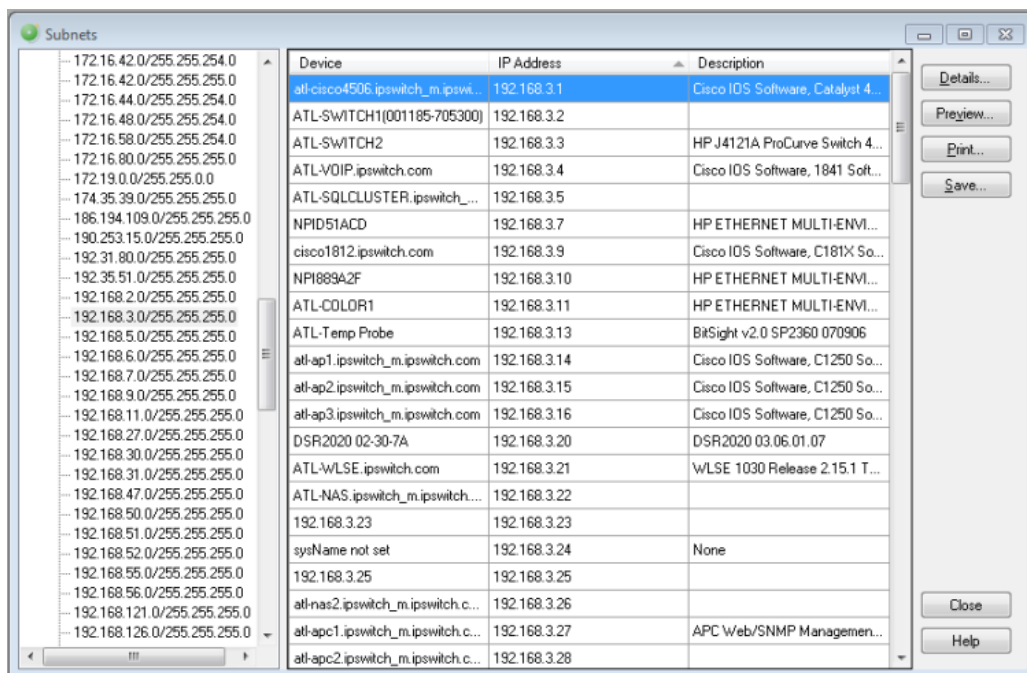
To view Subnets:

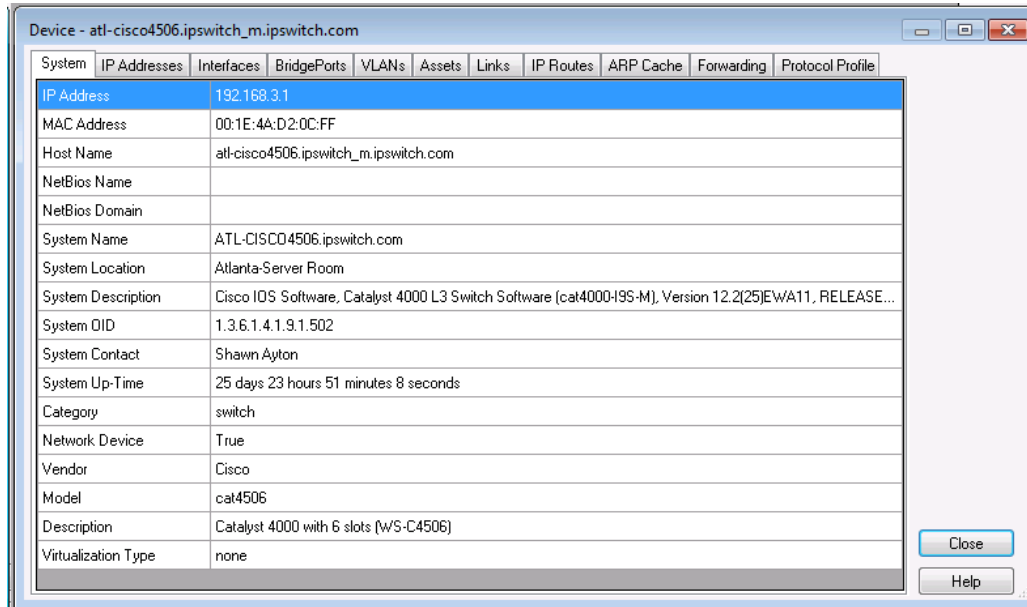1 From the main menu of the WhatsConnected console, select **View > Subnets**. The Subnets view appears.

Tip: You can also view subnets from the WhatsConnected console shortcut menu. Click (Subnets icon). The Subnets dialog appears.

Viewing Subnet device details

Associated with the Subnets view, the Device details tab provides a tabular view that displays detailed device information for a subnet device.

To view subnet device details:

1   From the main menu of the WhatsConnected console, select **View > Subnets**. The Subnets view appears.

2   Select a subnet you want to view, select the device for which you want to view details, then click **Details**. The device details appear.

> 💡 **Tip**: You can double-click any device in the Device List view. The Device Details tab view opens.

About the Subnets View right-click menus

Right-click a subnet in the Subnets explorer view for the following option:

- **Discover Subnet**. Opens the Discover Subnet dialog, which allows you to discover a subnet/mask.

Right-click a device in the Subnets *data grid view* (on page 32) for the following options:

- **Print Preview**. Opens the Print Preview dialog, which shows a preview of the information to be printed.

- **Print**. Opens the Print dialog, which allows you to print a hardcopy of the device list.

- **Save to CSV**. Opens the Save CSV File dialog, which allows you to save an electronic copy of the device list.

> 🗒️ **Note**: Menu options appear inactive in the right-click menu if it is not possible for the user to perform the action.

About VLANs View

VLANs View is an explorer-type view that shows the grouping of network devices, based on their respective VLANs (Virtual Local Area Network), on the left side of the pane

On the right side of the pane, devices associated with their respective VLANs are displayed. The data grid view can be column sorted, print previewed, printed, or saved to a comma-separated-value (CSV) file for use in Microsoft Excel or other reporting applications. For more information about data grid views, see *About data grid views* (on page 32).
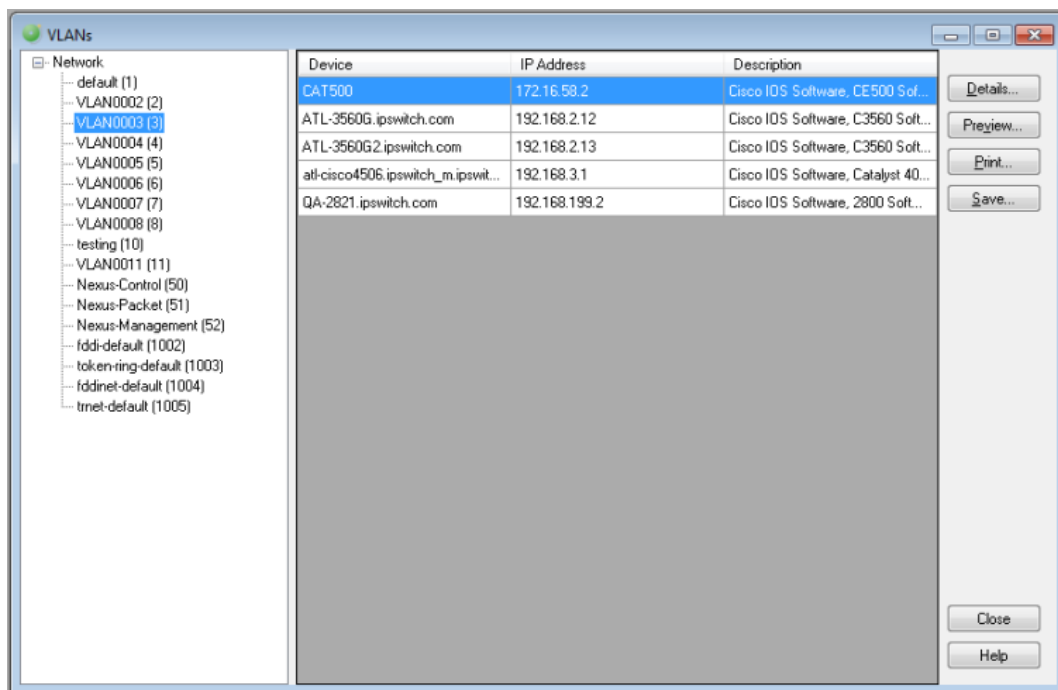
To view VLANs:

- From the main menu of the WhatsConnected console, select **View > VLANs**. The VLANs view appears.

Viewing VLAN device details

Associated with the VLANs view, the Details dialog provides a tabular view that displays detailed VLAN device information.

To view VLAN device details:

1 From the main menu of the WhatsConnected console, select **View > VLANs**. The VLANs view appears.

2 Select a VLAN you want to view, select the device for which you want to view details, then click **Details**. The device details appear.

About the VLANS View right-click menus

Right-click a device in the VLANS *data grid view* (on page 32) for the following options:

- **Print Preview**. Opens the Print Preview dialog, which shows a preview of the information to be printed.
- **Print**. Opens the Print dialog, which allows you to print a hardcopy of the device list.
- **Save to CSV**. Opens the Save CSV File dialog, which allows you to save an electronic copy of the device list.

About the Links View

The Links View is a spreadsheet-like view that displays all known topology links in the network discovery file. This view provides a concise list of all of your network connections.

Data displayed in this view can be printed, print previewed, or saved to a text file, comma-separated-value (CSV) file for use in Microsoft Excel, or a .PDF. For more information, see *About data grid views* (on page 32).

To view the Links view:

1   From the main menu of the WhatsConnected console, select **View > Links**. The Links view appears.

> 💡 **Tip**: You can also view links from the WhatsConnected console shortcut menu. Click 🖳 (Links shortcut icon). The Links dialog appears.

2   View the following information about the links:

   ▪ **Local Link**. Shows the local side of a connection. This connection is the Display Name of the device, and if available, the interface information.

   ▪ **Remote Link**. Shows the remote side of a connection. The connection is the Display Name of the remote device, and any available interface information.
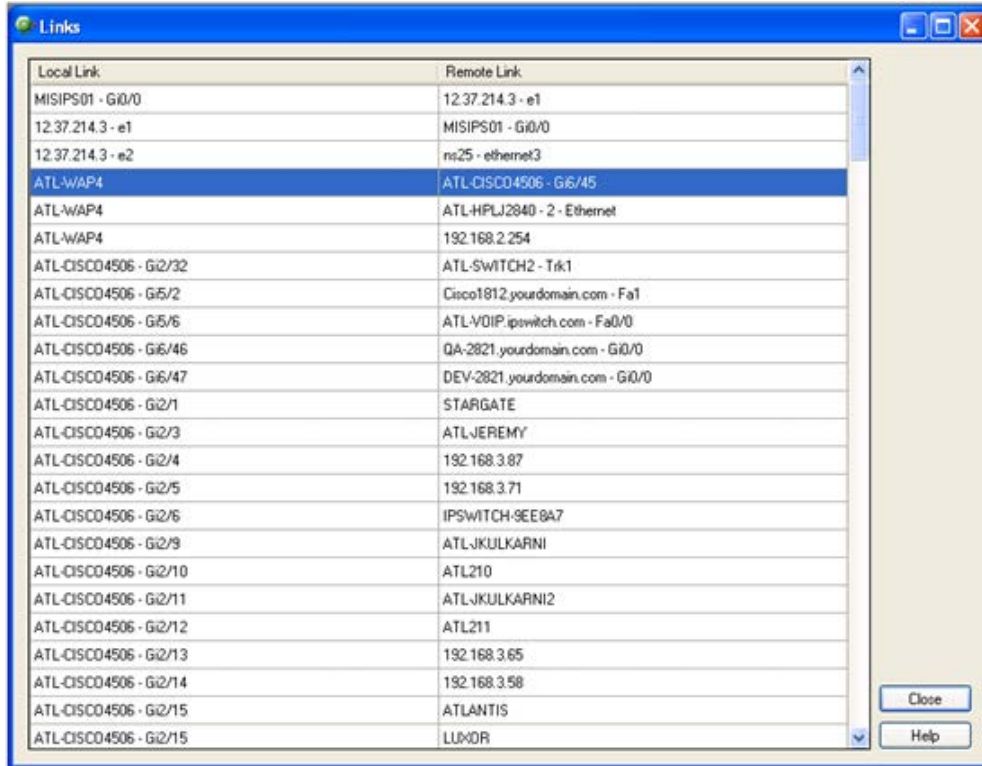
3   Click **Close** to close the Links dialog.

About the Links View right-click menu

Right-click a device in the Links *data grid view* (on page 32) for the following options:

- **Print Preview**. Opens the Print Preview dialog, which shows a preview of the information to be printed.
- **Print**. Opens the Print dialog, which allows you to print a hardcopy of the device list.
- **Save to CSV**. Opens the Save CSV File dialog, which allows you to save an electronic copy of the device list.

Using WhatsConnected Tools

In This Chapter

About WhatsConnected Tools

WhatsConnected includes network tools that are available in the WhatsConnected console.

- *Layer 2 Trace* (on page 83) tool
- *IP/MAC Finder* (on page 85) tool
- *Rebuild Connectivity* (on page 88) tool
- *Classify Devices* (on page 88) tool

Using Layer 2 Trace

In troubleshooting situations, it is often critical to understand the path that network data takes to access another network device. The Layer 2 Trace tool provides a method to trace the physical network path from one device to another.
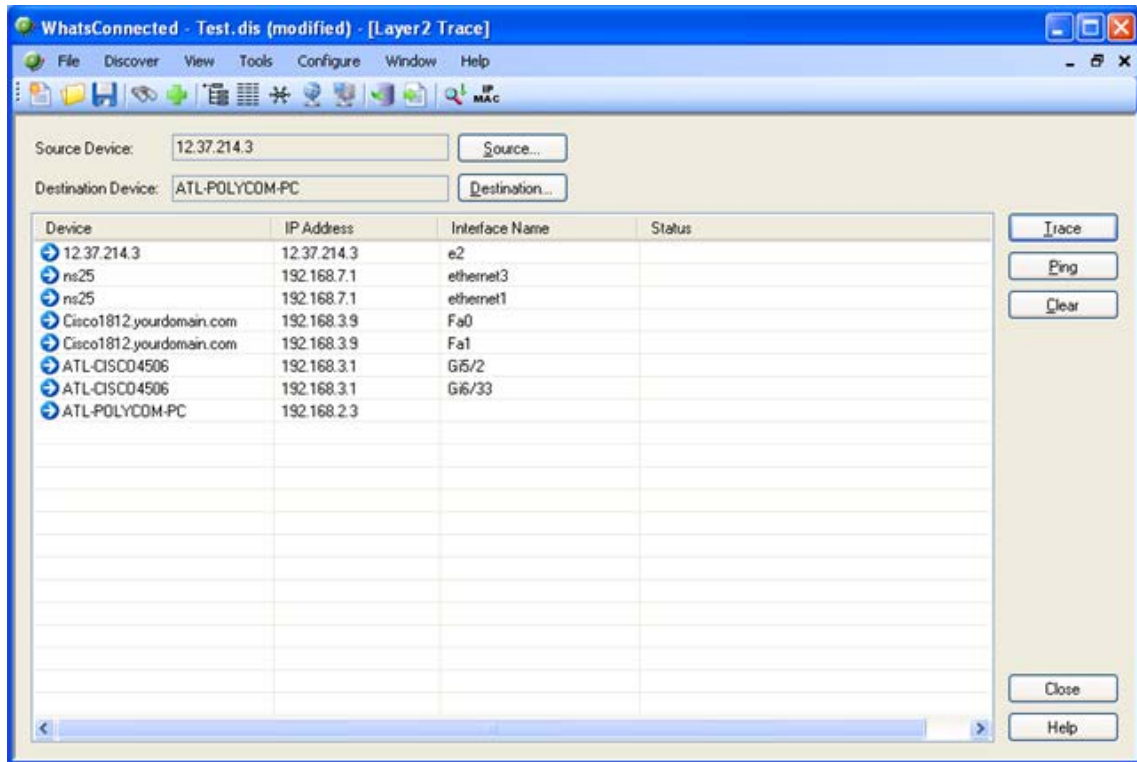
Using previously discovered network connectivity data, the Layer 2 Trace tool finds the path between the two devices and then displays each network interface that is used to build the path. The trace tool also allows for a quick check of the status and availability of each step along the layer 2 path.

To run the Layer 2 Trace tool:

From WhatsConnected:

1   From the main menu of the WhatsConnected console, select **Tools > Layer 2 Trace**. The Layer 2 Trace dialog appears.

> 💡 **Tip**: You can also view Layer 2 Trace tool from the console shortcut menu. Click (Layer 2 Trace shortcut icon). The Layer 2 Trace dialog appears.

2   Click **Source**. The Select Source Device dialog appears.
3   Select a starting device for the layer 2 trace, then click **OK**. The IP address selection appears in the Source Device box.

> 💡 **Tip**: You can use the Device Filter list to view specific device types.

4   Click **Destination**. The Select Destination Device dialog appears.

5   Select a destination device for the layer 2 trace, then click **OK**. The IP address selection appears in the Destination Device box.

> 💡   **Tip**: You can use the Device Filter list to view specific device types.

6   Click **Trace**. The step-by-step layer 2 path from the source device to the destination device displays in a list format. The results of the search are displayed in the Layer2 Trace tool list columns.

- **Device**. Lists the devices that the network path traverses.

- **IP Address**. Lists the IP address of each device on the network path.

- **Interface Name**. Lists the interfaces that the network path traverses.

- **Status**. Lists the device status information.

> 📝   **Note**: After a trace is completed, you can click **Ping** to view the current status of the Layer 2 path. This tool pings each device identified in the trace and uses SNMP to query the interface for its status.

7   Click **Clear** to remove the information from the Layer 2 Trace table and start a new trace.
     - or -
     Click **Close** to close the dialog.

Using IP/MAC Address Finder

The IP/MAC Address Finder provides an easy way to locate an IP or MAC address on the network. Using the previously discovered network devices, IP/MAC Address Finder finds and displays network interfaces that have sighting information for the supplied IP or MAC address. To get the most up-to-date sighting information, you can use the Refresh button which sends SNMP requests to each network device to quickly update the sighting information.
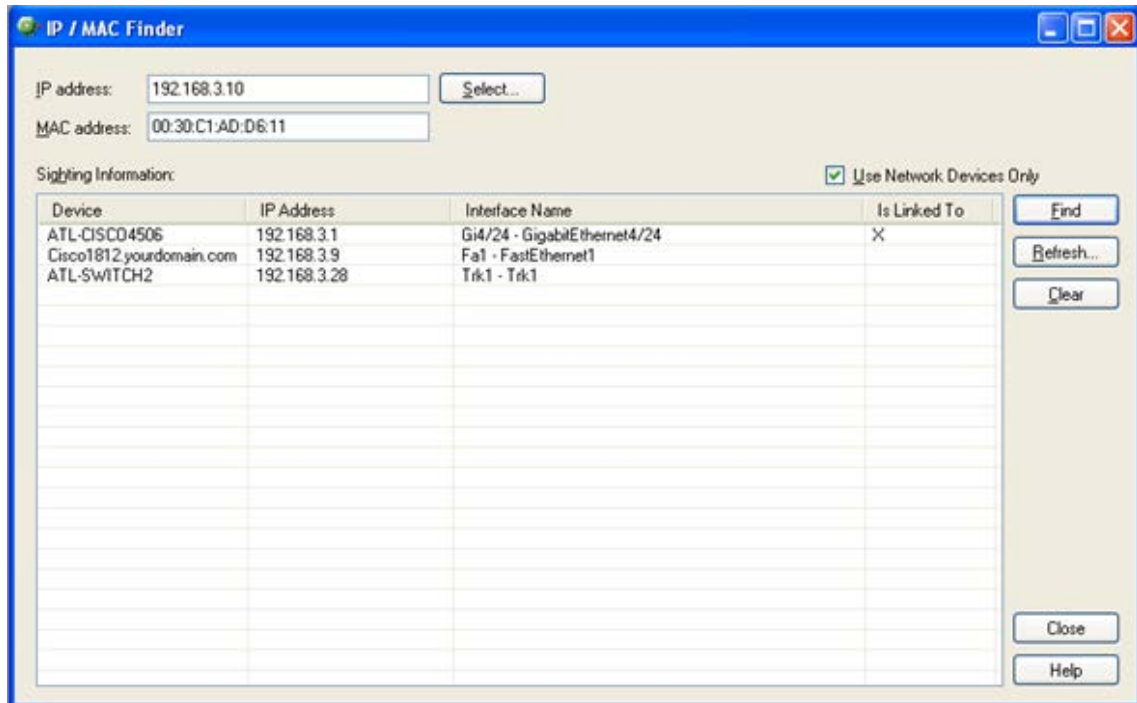
When enough network data is available, IP/MAC Finder indicates to which network interface the IP or MAC address is physically connected.

The IP/MAC Finder tool can search for either an IP or a MAC address on the network. The results of the search are displayed in the IP/MAC Finder list columns.

To use the IP/MAC Finder tool:

1   From the main menu of WhatsConnected select **Tools > IP/MAC Finder**. The IP/MAC Finder dialog appears.

💡   **Tip**: You can also view IP/MAC finder tool from the WhatsConnected console shortcut menu. Click 📷 (IP/MAC Finder shortcut icon). The IP/MAC Finder dialog appears.

2   Enter the appropriate information in the following fields.

- ▪ **IP Address**. Enter the IP address of a device for which you want to find sightings on the network. Leave this option blank if you are only scanning for a MAC address.
  - or -
  Click **Select** to select a device, in the Select Devices dialog, for which you want to

identify a MAC address. For more information, see *About the Select button* (on page 86).

> **Note**: The IP/MAC Finder tool does not support IPv6 addresses.

- **MAC Address**. Enter The MAC address for which you are scanning the network. Leave this option blank if you are only scanning for an IP address.

3   Select **Use Network Devices Only** to display the IP/MAC sightings found only on *network* device types.
- or -
Deselect **Use Network Devices Only** to display all IP/MAC sightings found on *all* device types.

4   Click **Find** to search the network to locate where the IP or MAC device is on the network. The results of the search are displayed in the Sighting Information list:

- **Device**. Lists the name of the network device that has sighting information for the IP or MAC address.

- **IP Address**. Lists the IP address of the sighting device.

- **Interface Name**. Lists the network interface that is routing or forwarding traffic to the IP or MAC address.

- **Is Linked To**. Lists the network devices to which the device is linked.

5   Click **Clear** to remove the information from the IP/MAC Finder table and start a new device sighting.
- or -
Click **Close** to close the dialog.

About the Select button

The IP/MAC Address Finder's Select button uses previously discovered network information to help you find a device, then select the device for which to search the network for sightings of its IP or MAC address.

To use the Lookup button:

1   Open the **IP/MAC Finder Address**.
2   Click **Select**. The Select Devices dialog appears. This dialog allows you to pick a device from your existing network discovery.
3   In the **Device Filter** list, select the device type you want to display in the Device List. All device devices are listed by default. The device list displays those devices that match the device filter criteria.
4   Select a device in the list, then click **OK**. The IP address and MAC address automatically fills the **IP Address** and **MAC Address** fields.

About the Refresh Connectivity button

The IP/MAC Address Finder's Refresh Connectivity button refreshes the connectivity model by sending SNMP requests to each network device to update the network data.

To use the Refresh Connectivity button:

1   Open the **IP/MAC Address Finder**.
2   Click **Refresh**. The Run Discovery dialog appears.
3   Wait for the progress information to indicate that the discovery is complete.
4   Click **OK**. The network model updates with the latest connectivity information based on this discovery run.

Using the Subnet Calculator

The Subnet Calculator is used to calculate a range of subnets for a specific IP address based on the network bits, subnet bits, and host bits when setting up a network.

To use the Subnet Calculator:

1   Access the Subnet Calculator by selecting **Tools > Subnet Calculator** from the main menu.
2   Enter the IP address of the subnet you want to discover under **IPAddress**. The Binary, Octal, and Hexadecimal forms of the IP address entered display in the respective fields within the dialog.
3   To specify the number of one bits in the binary notation of the net mask, select a number 1-31 from the **Mask Bits** list, or alternately, select a specific net mask from the **Net Mask** list. The Subnet Calculator auto-fills applicable subnet information in the remaining fields within the dialog, including the initial **Subnet Results**.
4   The following subnet characteristics can be altered by selecting from the applicable lists within the dialog. **Subnet Results** update automatically as changes are made.

   - **Subnet Bits** - The number of subnet bits can range from 1-31 when the number of mask bits is set to 1. As the number of mask bits increases, the listed options for subnet bits decreases. If the number of mask bits is set to 31, the number of subnet bits must be 31.

   - **Subnet Mask** - The available range of subnet masks that may be applied decreases as the number of mask bits increases.

   - **Number of Subnets** - The available number of subnets begins at 1. Each subsequent list option is the previous number multiplied by two and can be set as high as 536870912 when the number of mask bits is set to 1. As the number of mask bits increases, the listed options for number of subnets decreases. If the number of mask bits is set to 31, the number of subnets must be 1.

   - **Host Bits** - The number of host bits can range from 1-31. As the number of host bits increases, the number of subnets decreases. Additionally, if the number of mask bits is altered, the number of host bits automatically changes so the sum of the two numbers is equal to 32.

   - **Hosts per Subnet** - The available hosts per subnet begins with 2(RFC3021) and 2. Each subsequent list option is the previous number multiplied by 2, minus 2 (2x - 2) and can be set as high 2147483646 when the number of mask bits is set to 1. As the number of mask bits increases, the listed options for hosts per subnet decreases. If the number of mask bits is set to 31, the number of hosts per subnet must be 2(RFC3021).

> **Note**: RFC3021 designates a document which defines a scenario where there is a single host bit and the subnet and broadcast addresses double as hosts. 2(RFC3021) is only for point to point connections.

5 The following subnet characteristics are also displayed within the dialog and automatically update as changes to other fields are made, but may not be altered directly by the user:

- **Inverse (Wild Card) Mask** - The inverse mask indicates how many hosts are in a subnet and is calculated by subtracting each of the 4 sections of the subnet mask from 255. If only the last section of the inverse mask is used, it is the number of hosts per subnet plus 1.

- **Subnet Bitmap** - The subnet bitmap is a visual representation of the subnet using algebraic variables in place of numbers. 'n' represents network or mask bits which indicate the total amount of space available. 's' represents subnet bits minus network bits which indicate how many subnets are available. 'h' represents host bits which indicate the number of hosts in a subnet. If the subnet bits increase, the host bits decrease, and vice versa.

Rebuild Connectivity

The Rebuild Connectivity feature reruns the connectivity engine to rebuild all the links inside the network model. Rebuild connectivity generally happens automatically after a new discovery, but you can run Rebuild Connectivity at any time if you have merged more devices into the network using the file menu.

To run Rebuild Connectivity:

From the main menu of the WhatsConnected console, select **Tools > Rebuild Connectivity**. The Rebuild Connectivity tool runs.

Classify Devices

The Classify Devices feature reruns the device classifier after the device type configuration has been changed. With this feature, you can enter mappings into the Device Type Configuration and run Classify Devices to update all device categories.

To run Classify Devices:

From the main menu of the WhatsConnected console, select **Tools > Classify Devices**. The Classify Devices tool runs.

Using the Device Viewer

The Device Viewer allows you to view device configuration and inventory details. The information displayed in the Device Viewer is accessed from the discovery files (`.dis`) obtained during discovery.

To run the Device Viewer tool:

1   Start WhatsConnected.
2   In Device Categories view, expand a device category in the device category tree, then select a device. The WhatsConnected Device Viewer appears displaying the device details. Tabs only display if a device has data that can be displayed for that tab. Possible tab views that may be associated with each device are:

- **System**. Provides IP Address/MAC Address, MIB II information, product vendor, and other system information.

- **IP Addresses**. Provides IP Address configuration information.

- **Interfaces**. Provides name entries (IF information) for each device interface and other interface information.

- **BridgePorts**. Provides Bridgeport and VLAN name and index information.

- **VLANs**. Provides Virtual LAN configuration information.

- **LAG Trunks**. Provides Link Aggregation Group information.

- **Assets**. Provides inventory information about the device components.

- **Access Points**. Provides information about network wireless access points.

- **Rogue Access Points**. Provides information about wireless access points not on the network.

- **AP Clients**. Provides information about AP client devices.

- **Links**. Provides physical connectivity information from this device to other network devices.

- **Spanning Tree (STP)**. Provides spanning tree configuration and status information.

- **ARP Cache**. Provides Address Resolution Protocol (ARP) table information.

- **Forwarding**. Provides Layer 2 forwarding information.

- **Credentials**. Provides information about successful credential/protocol matches for this device.

- **HSRP**. Provides information about the Hot Standby Router Protocol (HSRP) on the device. The information relates to the standby nature of routers.

- **IP Phone**. Provides information about the selected (individual) IP phone.

- **IP Phones**. Provides information about the IP phones that are registered or are communicating with a call manager.

- **IP Routes**. Provides information about the IP routes configured for this device.

- **VRRP**. Provides information about the Virtual Router Redundancy Protocol (VRRP) on the device. The information relates to the standby nature of routers.

- **Software**. Provides information about installed software discovered on this device.

- **Windows**. Provides information about the Windows system software and hardware.

- **Config**. Provides information about device config files.

- **VM Host**. Provides information about virtual servers.

- **Virtual Machines**. Provides information about the virtual machines on a virtual server.

- **Virtual Machine**. Provides information about virtual machines.

Configuring WhatsConnected

In This Chapter

About WhatsConnected configuration settings

WhatsConnected provides a variety of configuration setting options to help you optimize WhatsConnected Layer 2 discovery for your network.

- *Application Settings* (on page 91)
- *Protocol Settings/Credentials* (on page 93)
- *Device Categories* (on page 94)
- *Device Filters* (on page 95)
- *Device Type Mappings* (on page 97)
- *WhatsUp Gold Server Endpoint Library (Remote Server)* (on page 98)
- *Email Settings* (on page 99)

Configuring Applications Settings

You can use the Applications Settings to select the type of shapes to use in the Topology Maps. The topology map shape options are:

- WhatsUp
- Cisco

To configure Application Settings:

1 From the main menu of the WhatsConnected console, select **Configure > Application Settings**. The Application Settings dialog appears.

2 Select the shapes you want to use in your topology maps:

- **WhatsUp**. The topology maps use the basic functional shapes from WhatsUp Gold to draw a device on the topology maps.

- **Cisco**. The topology maps use the standard Cisco icons/images for each functional collection (Router, Switch, etc) to represent a device.

3 Click **OK** to save settings.

Configuring Discovery Settings

A network discovery requires a general collection of settings to define a network discovery scope. Use the Discovery Settings to edit discovery collection settings, select a discovery configuration from the list of network discovery collections, or enter information for a new discovery collection. Discovery settings can be used in discovery tasks to schedule a scan. See *Configuring Discovery Tasks* (on page 22) for more information on discovery tasks.

Creating, editing, or deleting discovery settings

To create a new set of discovery settings:

1 From the main menu of the WhatsConnected console, select **Discovery > Discovery Settings**. The Discovery Settings dialog appears.

2 Click **New**. The Network Discovery Settings wizard appears.

3 Enter the appropriate information in the wizard dialogs.

To edit a set of discovery settings:

1 From the main menu of the WhatsConnected console, select **Discovery > Discovery Settings**. The Discovery Settings dialog appears.

2 Select an existing set of discovery settings, then click **Edit**. The Network Discovery Settings wizard appears.

3 Enter the appropriate information in the wizard dialogs.

To copy a set of discovery settings:

1 From the main menu of the WhatsConnected console, select **Discovery > Discovery Settings**. The Discovery Settings dialog appears.

2 Select an existing set of discovery settings, then click **Copy**. The Network Discovery Settings wizard appears.

3 Enter the appropriate information in the wizard dialogs.

To delete a set of discovery settings:

1 From the main menu of the WhatsConnected console, select **Discovery > Discovery Settings**. The Discovery Settings dialog appears.

2 Select an existing set of discovery settings, then click **Delete**.

3 Confirm that you are deleting the correct set of discovery settings, then click **Yes**. The discovery settings are removed from the list.

Configuring Protocol Settings/Credentials

Use the Protocol Settings/Credentials dialog to configure the protocol credentials that you want to use for network discovery.

- **SNMPv1** discovery requires the SNMP read community information, timeout settings, and retry counts.
- **SNMPv2** discovery requires the SNMP read community information, timeout settings, and retry counts.
- **SNMPv3** discovery requires the associated Username, timeout settings and retry counts. Optionally, you can select to use Authentication and Encryption.
- **SSH** requires the User Name, Password, and Port used to make an SSH connection.
- **Telnet** requires the User Name, Password, and Port information used to make a Telnet connection. Telnet credentials are used to support the Map Capture Config tool that starts Backup Running Configurations and Backup Startup Configurations.

> **Note**: Telnet credentials are not used during device discovery.

- **VMware** discovery requires the User Name, Password, and Port used to connect to a VMware host or vCenter server.
- **Windows** device discovery requires WMI information, Domain\UserID and Password, to connect to Windows devices. Windows credentials are used to collect software inventory information from Windows systems.

> **Note**: You can only edit the default ICMP settings; you cannot create a new set of ICMP settings.

To configure Protocol Settings:

- From the main menu of the WhatsConnected console, select **Settings > Protocol Settings/Credentials**. The Protocol Settings dialog appears.

To create a new set of protocol credentials:

1 Click **New**.
2 Select the type of Protocol settings that you would like to create, then click **OK**. The protocol properties dialog appears.
3 Enter the appropriate protocol settings in the protocol editor.

To edit protocol settings:

1 Select a set of protocol credentials, then click **Edit**. The protocol properties dialog appears.
2 Enter the settings you want to modify in the protocol editor.

To copy protocol settings:

1 Select a set of protocol credentials, then click **Copy**. The new copy of the credentials dialog appears.
2 Make any required changes to create new credentials, then click **OK**.

To delete a set of protocol credentials:

1   Select a set of protocol credentials, then click **Delete**. The protocol setting is deleted from the list.

2   Click **OK** to save changes.

To import protocol credentials from WhatsUp Gold:

1   Click **Import**. The Import Credentials dialog appears.

2   From the WhatsUp Gold Server list, select a WhatsUp Gold Server endpoint from which to import credentials or click browse (**...**) to open the WhatsUp Gold Remote Server dialog to Add, Edit, Copy, or Delete WhatsUp Gold remote servers from which to import credentials.

3   Click **Import**. WhatsConnected imports all of the currently configured credentials from the selected WhatsUp Gold server Credentials Library, and they appear in the Protocol Settings/Credentials dialog.

To selectively Assign or Unassign protocol credentials to device(s):

1   Select a credential you want to manually assign to device(s), then click Assign or Unassign. The Select Devices dialog appears.

2   Select one or `Ctrl +` select multiple devices to assign the credential to device(s).

3   Click **OK** to apply credentials to the selected device(s).

Configuring Device Categories

Use the Device Category Configuration dialog to configure and manage device categories. These device categories are used to organize devices found during discovery and are displayed on the WhatsConnected Device Categories View.

To configure device categories:

1   From the main menu of the WhatsConnected console, select **Configure > Device Category**. The Device Category Configuration dialog appears.

2   Click **New**. The New Device Category dialog appears.

   - or -

   Select a device category, then click **Edit**. The Edit Device Category dialog appears.

3   Enter or select the appropriate information in the dialog fields.

   ▪   Enter the **Category Name** that is displayed in the Device Category Configuration dialog.

   Note: Category names must be unique.

   ▪   Enter the **Display label** that is displayed for the category in the device category view.

   ▪   Enter or **Browse** to the **Icon filename** that is used to represent all devices in this category.

   ▪   Select **Network device** to identify the category as a network infrastructure device.

4   Click **OK** to save changes.

> 💡 **Tip**: You can also access the Device Category Configuration dialog from the Device Category View's right-click menu.

Configuring Device Filters

Device filters allow you to filter reports so that only the network information you want is displayed. You can customize the filter to display information about:

- All of your devices, including endpoint devices, such as servers and workstations.
- Only your network devices.
- Only those devices that have SNMP credentials.

You can create filters for categories of devices, individual IP addresses, IP ranges, subnets, VLANs, or combinations of these elements.

Device Categories

Device categories are used in filters to narrow your report to a specific group of network devices. The default categories list includes network devices, end devices, and devices with specific operating systems. You can add custom device categories for use in grouping devices in ways not available with the default device categories. When you create a custom device category, it will appear on the list and you will be able to select it when you are creating device filters. For more information on device categories, see *Device Category Configuration* (on page 94).

Advanced Filtering

Device filters provide advanced filtering options that allow you to filter device lists, topology maps, and reports to provide information for individual IP addresses, ranges of IP addresses, subnets and VLANs.

Click **Hosts/IPs** to add hostnames or IP addresses to the filter. You can filter your report on specific hostnames, for example you could filter a report to display only information about your payroll database server, `payroll.company.com`, or you could list a group of servers by hostname, such as the servers in a DMZ, `dmz.firewall1.company.com`, `dmz.externalweb.company.com`, and `dmz.externalweb.backup.company.com`. You can also filter using a single IP address, or multiple IP addresses. You can filter on an IP range such as 10.0.3.1 - 10.0.3.200 or a specific subnet. You can list a subnet using standard notation (192.168.5.0/255.255.255.0) or CIDR notation (192.168.5.0/24).

Click **VLANs** to add VLANs to the filter. When filtering on VLANs you can list one or more VLANs by VLAN name or index. The name of the VLAN, for example VLAN1, or the index for the VLAN, is entered in the Device Filter - VLANs dialog.

Creating, editing, copying or deleting a Device Filter

The following procedures provide instructions on how to create, edit, copy and delete device filters using the Device Filters dialog.

How to get to the Device Filters list dialog:

From the WhatsConnected menu, select **Configure > Device Filters**. The Device Filters list dialog appears.

> 💡 **Tip**: Alternatively, click the **...** browse button on any of the reports to which a device filter can be applied to get to the Device Filters list dialog.

The Device Filters list dialog displays the name of each filter and the associated pseudo code representing what the filter will return.

To create or edit a device filter:

1   If you are creating a new filter, click **New** to create a new device filter. The Device Filter definition dialog appears.

2   If you want to edit an existing device filter, select a device filter, then click **Edit** to edit an existing device filter. The Device Filter definition dialog for the selected filter appears.

3   For the **Name**, enter the name you want to use to refer to the filter. This name is displayed in the Device Filter lists on all reports and maps that have filtering available.

4   Select the range of devices you want to include in the filter in the **Include devices matching** area. This option sets the device range by restricting the devices filtered to one of the following groups of devices:

- **All Devices**. Select this option if you want the filter to be applied to all of the devices in the current discovery file.

- **SNMP Devices Only**. Select this option if you want the filter to be applied only to those devices with an SNMP credential in the credential library.

- **Network Devices Only**. Select this option if you want the filter only to be applied to network devices.

5   Use the options in the Advanced section to select specific hosts or VLANs to include in the filter.

Advanced. The Advanced filtering options filter for individual or ranges of IP addresses, host names, NetBIOS names, subnets, or VLANs. The following buttons invoke dialogs to enter values for the advanced filtering criteria.

a) To restrict the filter to specific hostnames, IP addresses, IP address ranges or subnets, click **Hosts/IPs** . The Device Filter - Host/IP Address Include Scope dialog appears. Enter the hosts, IP addresses, and subnets you want to include in your filter, then click **OK**. The Device Filter - Host/IP Address Include Scope dialog closes.

- **Host / System / NetBIOS Names**. Enter the hostname, system name or NetBIOS name of the device or devices you want the filter to select. When you list a name in this box, the filter will return only those devices with that name in the box. You can use a * character as a wildcard in this box. Click **Clear** to clear the Host / System / NetBIOS Names box.

- **IP addresses / Subnets**. Enter the IP address, IP address range or subnet address (CIDR format) of the device or devices you want the filter to select. When you list one or more addresses or and address range for this option, the filter will return only those devices that match or fall within the indicated address range. Click **Clear** to clear the IP addresses / Subnets option.

b) Click **VLANs** to open the Device Filter - VLANs dialog.

Enter the VLAN name or index from which you want the filter to select devices. Click **Clear** to clear the VLAN names or indexes.

6   Select the categories of devices you want to include in your device filter.

If you select any category, only devices that match that category appears. If you have not selected any devices, all devices that meet the other filter criteria appears.

- Click **Select All** to select all of the categories. With all of the categories selected, WhatsConnected returns all devices.

- Click **Unselect All** to de-select all of the categories. With all of the categories de-selected, WhatsConnected will return all devices within the device range.

- **Filter summary**. Provides a pseudo-code representation of the filter.

7   Click **Preview** to see the list of devices returned by the filter. This list of devices appears in the map or report that uses this filter.

8   Click **OK**. The Device Filter definition dialog closes, and the device filter appears on the Device Filter list dialog.

To delete a device filter:

Select a device filter, then click **Delete** to delete an existing device filter. The selected device filter is removed from the Device Filters dialog.

To copy an existing device filter:

Select a device filter, then click **Copy** to copy an existing device filter. The Device Filter definition dialog appears with *Copy of <filter_name>* in the Name field where *<filter_name>* is the name of the filter you selected to copy. All of the filter criteria associated with the selected device filter is automatically selected.

Configuring Device Type Mappings

Use the Device Types dialog to create or modify a custom device type mapping. To do this, enter an SNMP OID (sysObjectID) and select a device category for which to map a device. For more information about SNMP OIDs, refer to your device documentation or the *Internet Assigned Numbers Authority (IANA) web site* (http://www.iana.org/assignments/enterprise-numbers).

To configure Device Types:

1   From the main menu of the WhatsConnected console, select **Configure > Device Type Mappings**. The SNMP OID to Device Type Configuration dialog appears.

2   Use the following options to create and edit device types:

- **New**. Click to create a new device type configuration (mapping).

  - **sysObject ID (OID)**. Enter the SNMP OID (sysObjectID) for which you want to map a device. For more information about SNMP OIDs, refer to your device documentation or the *Internet Assigned Numbers Authority (IANA) web site* (http://www.iana.org/assignments/enterprise-numbers).

- **Include Subtree**. Select to include the device OID subtree entries in the device type configuration.

- **Category**. Select a device type category for which to map the device.

- **Vendor/Manufacturer**. Enter the device vendor or manufacturer name.

- **Model**. Enter the device vendor or manufacturer model.

- **Description**. Enter the device vendor or manufacturer description.

- **Edit**. Select a device in the OID Maps list to modify the current settings.

- **Copy**. Select a device in the OID Maps list to copy an existing OID Map and modify it to create a new OID Map.

- **Delete**. Select a device in the OID Maps list to delete an existing OID Map.

3 Click **OK** to make changes.

WhatsUp Gold Server Endpoint Library (Remote Servers)

Data shared between WhatsUp Gold and WhatsConnected and data that is accessed using the NetworkViewerDataService in WhatsUp Gold requires that WhatsUp Gold servers (or endpoints) be defined to exchange data between the applications. WhatsConnected import/export features communicate with the data service to access the WhatsUp Gold database.

If WhatsConnected is installed on a system with WhatsUp Gold installed, then a "Local Server" endpoint is added automatically to the remote servers (endpoint library). The "Local Server" endpoint cannot be deleted but it can be edited. Other remote servers can be created and edited similar to other libraries in WhatsUp Gold and WhatsConnected. WhatsUp Gold remote servers are stored in the `netview-viewer-config-user.xml` configuration file.

The WhatsUp Gold Remote Servers dialog lets you define and manage WhatsUp Gold servers for:

- Exporting topology maps from WhatsConnected
- Exporting scheduled discovery data from WhatsConnected
- Importing credential data from a WhatsConnected server

Use this dialog to Add, Edit, Copy, and Delete WhatsUp Gold servers that will interact with WhatsConnected data.

The dialog displays the following WhatsUp Gold remote server information **Name**, Description, Host Name/IP Address, and Port.

To manage WhatsUp Gold remote servers:

- Click **New** to add a new WhatsUp Gold remote server.
- Select a WhatsUp Gold remote server, then click **Edit** to modify the server settings.

- Select a WhatsUp Gold remote server, then click **Copy** to make a duplicate of the server settings.

- Select a WhatsUp Gold remote server, then click **Delete** to remove it from the list.

Configuring Email Settings

Use The Configure SMTP Settings dialog to configure the default Email Settings for WhatsConnected.

To configure Email Settings for WhatsConnected:

1 Go to the Configure SMTP Settings dialog:

2 On the WhatsConnected console, select **Configure > Email Settings**. The Configure SMTP Settings dialog appears.

3 Specify or select the appropriate information in the dialog fields.

- **Destination email address**. Specify the address that the Email action message should be sent.

- **From email address**. Specify the address to be listed as "From" in the email sent by the Email action.

- **SMTP server**. Specify the address of the server on which SMTP is running.

- **Port**. Specify the port on which the SMTP service is listening. The standard SMTP port is 25.

- **Timeout (sec)**. Specify the amount of time (in seconds) that WhatsConnected should wait for a response from the SMTP server. If the time limit is exceeded, the email fails. The default timeout is 30 seconds.

- **Use SMTP authentication**. Select this option if your SMTP server requires user authentication.

  - **Username**. Specify the username to be used with SMTP authentication.

  - **Password**. Specify the password of the username to be used with SMTP authentication.

- **Use an encrypted connection (SSL/TLS)**. If your SMTP server supports encrypting data over a TLS connection (formerly known as SSL), select this option to encrypt SMTP traffic.

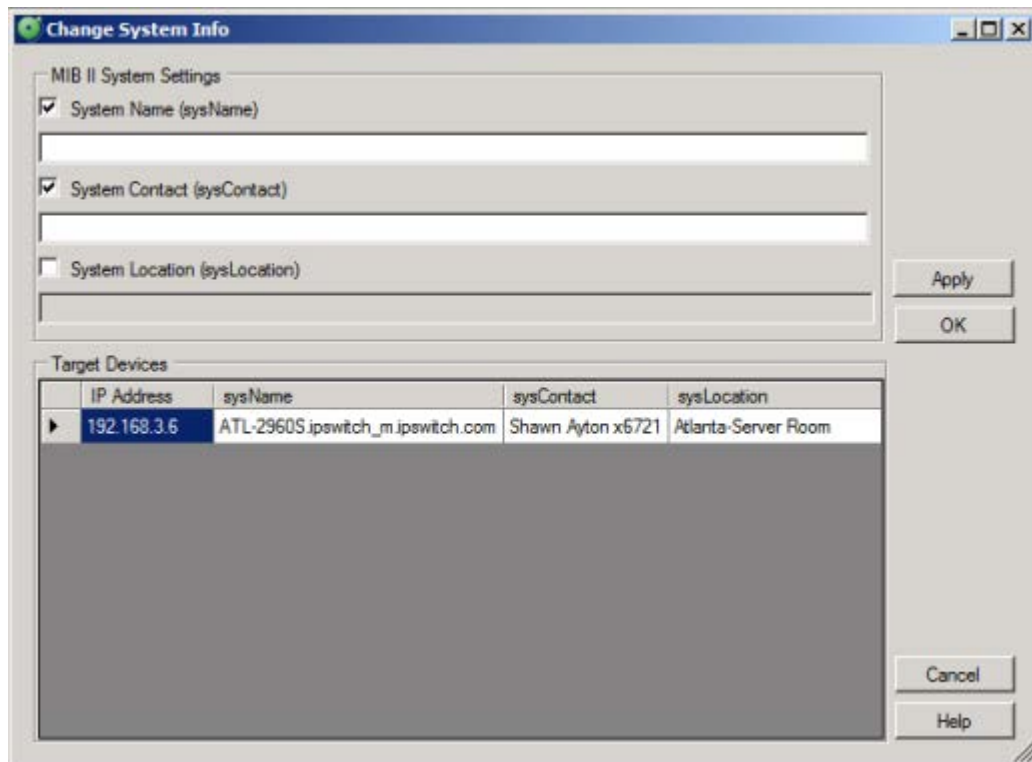**4** Click **OK** to save changes.

Changing System Info

The Edit MIB II Information option allows you to change MIB II system values (name, contact, and location) for one or more devices. This feature allows you to make system changes to multiple devices at one time, saving you the trouble of having to manually configure each device separately.

> **Note**: Any device for which you want to change system information must have valid SNMP read/write credentials. For more information, see Configuring network protocols and credentials.

To modify system information for a device, or group of devices:

1   From either the Device List view, Device Categories view, or the Topology Maps view, select one or more devices, then right-click. The right-click menu appears.

2   From the right-click menu, select Edit MIB II Information. The Change System Info dialog appears.

3   Select the system variables you want to modify for the selected device(s) to enable the system value fields for modifications. You can modify the **System Name (sysName)**, **System Contact (sysContact)**, and the **System Location (sysLocation)**.

4   Enter new values for the system variables you select.

5   Click **Apply** to save changes without closing the dialog.

   - or -

   Click **OK** to save changes and to close the dialog.

Viewing WhatsConnected reports

In This Chapter

About WhatsConnected reports

WhatsConnected reports provide information about network assets and their connectivity. The following reports are available in the WhatsConnected console in the **Reports** menu.

- **Asset/Inventory report**. Displays a list of all of the assets discovered by WhatsConnected.

- **Installed Software Inventory**. Displays a list of Windows systems and the applications operating on the systems.

> **Important**: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
> Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

- **Operating System Inventory**. Displays the Windows operating systems operating on each discovered Windows system.

- **BIOS Inventory**. Displays a list of Basic Input Output System (BIOS) for each discovered Windows system.

- **Warranty Information**. Displays the warranty service information for each discovered Windows system.

- **Device Connectivity report**. Displays a list of the devices connected to each discovered network device.

- **Bridge Port Utilization report**. Displays a list that details the bridge ports available on each discovered network device and the number of bridge ports that are currently being used.

To view a report:

On the WhatsConnected console, click **Reports,** then select the report you want to view.

About the Asset/Inventory Report

The Asset/Inventory Report provides a view of the network assets discovered by WhatsConnected as well as tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer. When an asset acts as a chassis for other assets, you can either view just the chassis, or the chassis and all of its associated assets.

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Asset/Inventory Report**.

The following is a list of the information available about individual device assets in the report.

- **Device**. Displays the device name.
- **Description**. Displays the manufacturer's description of the physical component.
- **Category**. Displays the category in which the device was placed during discovery.
- **Location**. Displays the location of the device.
- **Contact**. Displays the name of the contact associated with the device.
- **SNMP OID**. Displays the SNMP OID of the device.
- **IP Address**. Displays the IP address assigned to the device.
- **MAC Address**. Displays the MAC address assigned to the device.
- **Model**. Displays the model of the device.
- **Serial Number**. Displays the serial number of the device.
- **Service Tag**. Displays the service tag associated with the device.
- **HW Rev**. Displays the hardware revision of the device.
- **SW Rev**. Displays the software revision of the operating system used by the device.
- **FW Rev**. Displays the firmware revision of the device.
- **Vendor**. Displays the device vendor.

Configuring the Asset/Inventory report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1. To create a group, click `Ctrl` and right-click to select individual devices to add to a group.
2. On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

To display components that are housed within another device:

Select **Show all assets** to display any components that are housed within another device.

Installed Software Inventory Report (for Windows systems)

The Software Inventory Report provides a view of software installed on Windows systems that WhatsConnected discovers on the network. It also provides tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

> ✅ **Important**: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
> Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Installed Inventory Report**.

The Device, Name, and Product ID columns display by default. The following is a list of the information available for the report.

- **Device**. Displays the device name.
- **Name**. Displays the software application installed on the Windows system.
- **Product ID**. Displays the software product ID information.
- **Description**. Displays the manufacturer's description of the physical hardware.
- **Category**. Displays the category in which the device was placed during discovery.
- **Location**. Displays the device location information.
- **Contact**. Displays the name of the contact associated with the device.
- **IP Address**. Displays the IP address of the device.

Configuring the Software Inventory Report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report view:

Enter additional filtering information in the View Filter box to narrow the list of devices you want to view. For example, enter ATL in the View Filter box to find devices that include ATL in the device name. Select the **NOT** option to show matches that do not match the entry in the View Filter box.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1 To create a group, click `Ctrl` and right-click to select individual devices to add to a group.
2 On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

Software Update Report (for Windows systems)

The Software Update Report provides a view of software updates on Windows systems that WhatsConnected discovers on the network. It also provides tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

Important: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Software Updates**.

The Device, IP Address, Hot Fix, Caption, and Fix Descriptions columns display by default. The following is a list of the information available for the report.

- **Device**. Displays the device name.
- **IP Address**. Displays the IP address of the device.
- **Hot Fix**. Displays the KB article associated with the software update fix.
- **Caption**. Displays the KB article url associated with the hot fix update.

- **Fix Description**. Displays information about the type of software update that was installed. For example, a security fix or a hot fix.
- **Description**. Displays the manufacturer's description of the physical hardware.
- **Category**. Displays the category in which the device was placed during discovery.
- **Location**. Displays the device location information.
- **Contact**. Displays the name of the contact associated with the device.
- **Comments**. Displays any comments provided about the software update.
- **Installed By**. Displays the user name information for the person that installed the software.
- **Installed On**. Displays the date that the software update was installed.
- **Status**. Displays status information about the software update.

Configuring the Software Inventory Report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report view:

Enter additional filtering information in the View Filter box to narrow the list of devices you want to view. For example, enter ATL in the View Filter box to find devices that include ATL in the device name. Select the **NOT** option to show matches that do not match the entry in the View Filter box.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1 To create a group, click `Ctrl` and right-click to select individual devices to add to a group.

2 On the right-click menu:

- Click **Print Preview** to preview the selected devices.

- Click **Print** to print the selected devices

- Click **Save to CSV** to save the selected devices to a CSV file.

Operating System Inventory Report (for Windows systems)

The Operating System Inventory Report provides a view of operating system installed on Windows systems that WhatsConnected discovers on the network. It also provides tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

> **Important**: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
>
> Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Operating System Inventory Report**.

The Device, Operating System, Service Pack, and Version columns display by default. The following is a list of the information available for the report:

- **Device**. Displays the device name.

- **Operating System**. Displays information about the operating system running on the device.

- **Service Pack**. Displays information about the operating system service packs installed on the computer.

- **Version**. Displays operating system version information.

- **Device Description**. Displays the computer description information provided by the device owner.

- **Category**. Displays the category in which the device was placed during discovery.

- **Location**. Displays the device location information.

- **Contact**. Displays the contact information associated with the device.

- **IP Address**. Displays the computer IP address.
- **Memory Capacity**. Displays the computer RAM used on the device.
- **Manufacturer**. Displays the device manufacturer.
- **Serial Number**. Displays the computer serial number.

Configuring the Operating System Inventory Report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report view:

Enter additional filtering information in the View Filter box to narrow the list of devices you want to view. For example, enter ATL in the View Filter box to find devices that include ATL in the device name. Select the **NOT** option to show matches that do not match the entry in the View Filter box.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1 To create a group, click Ctrl and right-click to select individual devices to add to a group.
2 On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

BIOS Inventory Report (for Windows systems)

The Basic Input Output System (BIOS) Report provides a view of the hardware operating system information for the Windows systems that WhatsConnected discovers on the network. It also provides tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

> **Important**: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
> Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

To view the report:

On the WhatsConnected console, click **Reports,** then select the **BIOS Inventory Report**.

The Device, BIOS Name, and BIOS Description columns display by default. The following is a list of the information available for the report:

- **Device**. Displays the device name.
- **BIOS Name**. Displays the name of the BIOS manufacturer.
- **BIOS Description**. Displays additional BIOS manufacturer description information.
- **Device Description**. Displays the computer description information provided by the device owner.
- **Category**. Displays the category in which the device was placed during discovery.
- **Location**. Displays the device location information.
- **Contact**. Displays the contact information associated with the device.
- **IP Address**. Displays the computer IP address.
- **Memory Capacity**. Displays the amount of RAM used on the device.
- **Release Date**. Displays the BIOS release date information.
- **Serial Number**. Displays the computer serial number.

Configuring the BIOS Inventory Report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report view:

Enter additional filtering information in the View Filter box to narrow the list of devices you want to view. For example, enter ATL in the View Filter box to find devices that include ATL in

the device name. Select the **NOT** option to show matches that do not match the entry in the View Filter box.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1 To create a group, click `Ctrl` and right-click to select individual devices to add to a group.
2 On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

Warranty Information Report (for Windows systems)

The Warranty Information Report provides a view of the hardware warranty information for the Windows systems that WhatsConnected discovers on the network. It also provides tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

> ✅ **Important**: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
> Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Warranty Information Report**.

The Device, Description, Start and End Date columns display by default. The following is a list of the information available for the report:

- **Device**. Displays the device name.
- **Device Description**. Displays the device description.
- **Category**. Displays the category in which the device was placed during discovery.
- **Location**. Displays the device location information.
- **Contact**. Displays the contact information associated with the device.
- **IP Address**. Displays the device IP address.
- **Provider**. Displays the warranty provider information.
- **Description**. Displays a information about the software support agreement.
- **Start Date**. Displays the software support agreement beginning date.
- **End Date**. Displays the software support agreement ending date.
- **Notes**. Displays warranty provider note information.

Configuring the Warranty Information Report

To add or edit warranty information for a device in the Warranty Report:
1   Select a device in the report table for which you want to add warranty information.
2   Click **Add** or **Edit** to add information to the Warranty Report.
3   Click **OK** to save changes.

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report view:

Enter additional filtering information in the View Filter box to narrow the list of devices you want to view. For example, enter ATL in the View Filter box to find devices that include ATL in the device name. Select the **NOT** option to show matches that do not match the entry in the View Filter box.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1 To create a group, click `Ctrl` and right-click to select individual devices to add to a group.
2 On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

To select the Device Viewer a device in the report:

- Select a device in the report list, then click **Device**. The Device Viewer appears.
- Select a tab for the device information you want to view.

To view a device's service information on the vendor's web site:

- Select a device in the report list, then click **Go To**. If available, the vendor's system and service information is shown.

Windows Services Report (for Windows systems)

The Windows Services Report provides a view of Windows services that WhatsConnected discovers running on each network device. It also provides tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

> ✅ **Important**: Each Windows host device for which you want to collect software inventory, operating system inventory, BIOS inventory, and warranty inventory information must have the WMI feature enabled. For more information about enabling WMI on Windows systems, see the operating system help.
> Additionally, make sure that WMI credentials are configured in WhatsConnected. For more information, see *Configuring Protocol Settings/Credentials* (on page 93).

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Windows Services Report**.

The Device, IP Address, Service Display Name, Service Description, and State columns display by default. The following is a list of the information available for the report.

- **Device**. Displays the device name.
- **Description**. Displays the manufacturer's description of the physical hardware.
- **Category**. Displays the category in which the device was placed during discovery.
- **Location**. Displays the device location information.
- **Contact**. Displays the name of the contact associated with the device.
- **IP Address**. Displays the IP address of the device.
- **Service Display Name**. Displays the display name of the application service.
- **Service Description**. Displays a description for the application service.
- **Service Name**. Displays the name of the application service.
- **Caption**. Displays a short description of the service.
- **Path Name**. Displays the application service directory path for the executable (`.exe`) file.
- **Service Type**. Displays information about whether the application service is a unique or shared service.
- **Startup Type**. Displays information about how the service is started (Auto, Disabled, Manual).
- **Log On As**. Display information about how the type of logon used for the application service.
- **State**. Displays whether the status of the application service (Running or Stopped). This column is displayed in the report summary.
- **Status**. Displays status information about the software update.

Configuring the Software Inventory Report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report view:

Enter additional filtering information in the View Filter box to narrow the list of devices you want to view. For example, enter ATL in the View Filter box to find devices that include ATL in

the device name. Select the **NOT** option to show matches that do not match the entry in the View Filter box.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1. To create a group, click `Ctrl` and right-click to select individual devices to add to a group.
2. On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

Device Connectivity Report

The Device Connectivity Report provides a list of the devices connected to a network device as well as tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, sort on any column, and filter the report by device type. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

To access the report:

On the WhatsConnected console, go to **Reports > Device Connectivity**.

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Device Connectivity Report**.

The following is a list of the information available in the report:

- **Device**. Displays the name of the device.
- **Description**. Displays the manufacturer's description of the device.
- **Category**. Displays the assigned category based on functional characteristics.
- **Location**. Displays the physical location of the device.
- **Contact**. Displays the name of the contact associated with the device.
- **SNMP OID**. Displays the SNMP Object ID assigned to the device.
- **IP Address**. Displays the IP address of the connected device.
- **IF Name/Port**. Displays the interface name and associated port.
- **IF Index**. Displays the interface index.
- **Connected Device**. Displays the hostname of the connected device.
- **Connected IP Address**. Displays the IP address of the connected device.

Configuring the Device Connectivity report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report:

Select the device type you would like to display from the Device Filter list. The report will refresh and display only devices of the selected type. You can also click the browse (**...**) button to open the Device Filters dialog and apply an existing device filter or create a new device filter. After you apply a device filter, it affects the devices included in the report.

To filter the report on the device type of the connected devices:

Select the device type of the connected devices from the Connected Device Filter list box. The report will refresh and display only devices with connected devices of the selected type.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1   To create a group, click `Ctrl` and right-click to select individual devices to add to a group.

2   On the right-click menu:

- Click **Print Preview** to preview the selected devices.

- Click **Print** to print the selected devices

- Click **Save to CSV** to save the selected devices to a CSV file.

Bridge Port Utilization Report

The Bridge Port Utilization report provides a list of the bridge ports available on a network device as well as tools to sort and filter the assets that appear in the view. You can choose which columns you would like to display, and sort on any column. You can preview and print the report, save the report in a comma separated values (CSV) file, or view a device in the Device Viewer.

To view the report:

On the WhatsConnected console, click **Reports,** then select the **Port Utilization Report**.

The following is a list of the information available in the report:

- **Port Total**. Displays the total number of bridge ports provided by all of the discovered network devices.

- **Ports Used**. Displays the total number of bridge ports being used on all of the discovered network devices.

- **Device**. Displays the device name.

- **Description**. Displays the manufacturer's description of the physical component.

- **Location**. Displays the location of the device.

- **Contact**. Displays the name of the contact associated with the device.

- **SNMP OID**. Displays the SNMP Object ID of the network device.

- **IP Address**. Displays the IP Address of the network device.

- **Port Count**. Displays the total number of bridge ports provided by the network device.

- **Ports Used**. Displays the number of bridge ports that are being used on the network device.

Configuring the Bridge Port Utilization report

To view details on a device:

Select the device and click **Details.** A Device Viewer appears.

To edit the columns that appear in the report:

Right-click on any column heading, the column selection list appears. In the column selection list, click on the columns you would like to display.

To sort on a column:

Left-click on the column heading. The direction of the arrow indicates the direction of the sort. If the arrow is pointing down, the column is sorted in descending order. If the arrow is pointing up, the column is sorted in ascending order.

To see a print preview, print or save the report to a CSV file:

- Click **Preview** to see a print preview of the entire report.
- Click **Print** to print the entire report.
- Click **Save** to save the entire report to a CSV file.

To print preview, print or save a group of devices to a CSV file:

1 To create a group, click `Ctrl` and right-click to select individual devices to add to a group.
2 On the right-click menu:

- Click **Print Preview** to preview the selected devices.
- Click **Print** to print the selected devices
- Click **Save to CSV** to save the selected devices to a CSV file.

Copyright notice

This document was published on Friday, April 20, 2012 at 08:54.