IPSWITCH
WhatsUpGold
v2.1

WhatsConnected User Guide

IPSWITCH

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 depict and visualize their 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 be able to discover, map, search, and document their networks.

Discovery

The WhatsConnected discovery process uses industry-standard protocols, such as ICMP and SNMP, to find devices on your network. Information about discovered devices is available as a simple device list view, a device category view, and a detailed topology view.

Mapping

After WhatsConnected knows about the devices on your network, it can generate a map that shows the physical connections between all of the devices. Standard and custom maps provide an easy way to browse the network infrastructure. With the 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 generate reports that contain detailed information about the devices on your network.

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/wugtechsupport).

- **Release Notes**. The release notes provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for installing and configuring WhatsConnected. The release notes are available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wugWC21relnotes).

- **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**.

- **WhatsUp Gold optional plug-ins**. You can extend the core features of WhatsUp Gold by installing plug-ins. For information on available plug-ins and to see release notes for each plug-in, see *WhatsUp Gold plug-ins documentation* (http://www.whatsupgold.com/support/guides.aspx).

- **Licensing Information**. Licensing and support information is available on the *MyIpswitch licensing portal* (http://www.myipswitch.com/). The web portal provides enhanced web-based capabilities to view and manage Ipswitch product licenses.

- **Technical Support**. Use the WhatsUp Gold Support Site for a variety of WhatsUp Gold product help resources. From here you can view product documentation, search Knowledge Base articles, access the community site for help from other users, and get other Technical Support information. The Support Site is available on the *WhatsUp Gold web site* (http://www.whatsupgold.com/wugtechsupport).

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

The minimum software and hardware requirements are based on the Ipswitch WhatsUp Gold requirements. For more information, see the *WhatsUp Connected Release Notes* (http://www.whatsupgold.com/wc21relnotes).

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 WhatConnected installation program. The *WhatsUp Connected Release Notes* (http://www.whatsupgold.com/wc21relnotes) contain the most up-to-date information about installing. Please read the release notes to ensure that you are aware of all installation requirements.

Before installing, we recommend that you read the 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.myipswitch.com). For more information, see *Activating WhatsConnected licenses* (on page 3).

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 WhatsUp Gold 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 WhatsUp Gold 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 more help and information about licensing, go to the *Mypswitch licensing portal* (http://www.myipswitch.com/).

Discovering Networks

In This Chapter

Getting started with WhatsConnected

To start WhatsConnected:

▪ From the WhatsUp Gold console, click **Tools > WhatsConnected**. WhatsConnected starts.

When you start the WhatsConnected application, the WhatsConnected Startup dialog helps you begin using the WhatsConnected application.
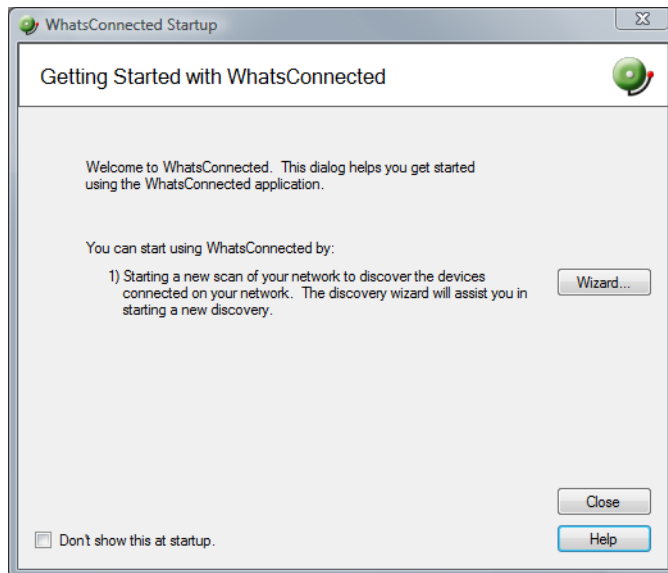
There are two Getting Started options to help you begin gathering and viewing Layer 2 network information:

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

▪ 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 6).

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 5).

- Through the Discovery Tasks option in the WhatsConnected console **Configure > Discovery Tasks**. For more information, see *Configuring Discovery Tasks* (on page 73).

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 6).

- The network protocols and credentials used during the network scan. For more information, see the *Configuring network protocols and credentials* (on page 10) 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 9).

Advanced Discovery Settings

You can acccess the Advanced Discovery Settings dialog using the **Advanced** button. This 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. Discovery settings are grouped by a general name that describes the area of the network that the settings scan.

Configuring discovery settings

To add discovery settings:

1 From the main menu of the WhatsConnected console, select **Configure > 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 6).
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 9).
14 If you want to use Advanced IP Scoping options, click **Advanced** and enter the **Include IP Scope**. For more details, see *About Include IP Scope* (on page 10). You can also enter the **Exclude IP Scope**. For more details, see *About Exclude IP Scope* (on page 10). Click **OK** to complete the advanced options, then click **Next**.

15 Click **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 Network Discovery Setup.

To rename discovery settings:

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

2 The dialog displays all previously defined discovery settings. To rename a collection of discovery settings, right-click the collection that you would like to rename, then click **Rename**. The Rename Discovery Settings dialog appears.

3 Enter a new **Name** for the collection of discovery settings.

4 Click **OK**.

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

To delete discovery settings:

1 From the main menu of the WhatsConnected console, select **Configure > 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 a 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 now also supports discovery through a Virtual Machine Interface (VMI).

The following section describes how to manage each protocol and its settings.

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 protocol properties 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.

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, SNMPv3, SSH, or VMWare protocol settings for successful network discovery.

SNMPv1 credentials

To add a new set of SNMPv1 protocol 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 set of SNMPv1 credentials is removed.

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

SNMPv2 credentials

To add a new set of SNMPv2 protocol 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 set of SNMPv2 credentials is removed.

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

SNMPv3 credentials

To add a new set of SNMPv3 protocol 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 set of SNMPv3 credentials is removed.

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

The SSH Protocol

The SSH protocol allows the discovery engine to query detailed device information from Linux and UNIX devices. The correct SSH user name and password are required to query information from your Linux/UNIX devices. This protocol is not required; it is needed only if you wish to discovery of Linux/UNIX systems. Leave empty if you do not want to use this protocol.

To add an SSH protocol setting:

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**.

> **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 SHH protocol setting:

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 SHH credentials, then click **Edit**. The protocol properties dialog appears.
3   Modify the existing settings.

   ▪   Enter a new SSH **Username**.

   ▪   Enter a new SSH **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 SSH protocol setting:

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 set of SSH credentials is removed.

The VMware (VIM) protocol

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** 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** 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**.

- Enter the defined VMware **Port**. The default port number is 443 (HTTPS).

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 is 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.
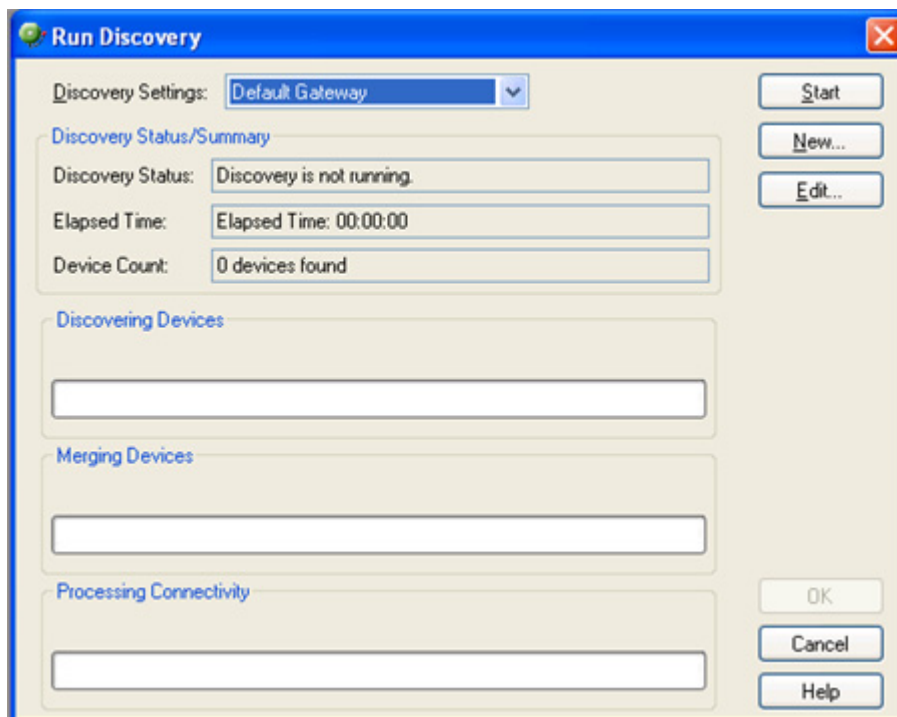
To run a Layer 2 Network Discovery:

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 6).

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 6).

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 Define the SNMP and ICMP settings required to discover your network. Enter the **SNMP read communities** as well as any **Timeout** and **Retry** information for the SNMP or ICMP requests.

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

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

11 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 24).

For more information, see Example: Using the Discovery Setup Wizard.

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.

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 6)
- *Network Device* (on page 60) and *Topology Maps View* (on page 38)
- *Exporting Topology Maps to WhatsUp Gold* (on page 44)
- *Exporting Topology Maps to Microsoft Visio™* (on page 46)

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, click **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 17).

Opening a discovery file

After starting the WhatsConnected console, you may want to open an existing discovery file.

To open an existing discovery file:

1 From the console, click **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 may open these files at any time from the console File menu.

To open a recently used discovery file:

- From the console, click **File**. At the bottom of the menu, any recently opened/saved files are listed. Select the network discovery file that 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 console, click **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 will be replaced with the devices from the selected file. The topology maps will not be 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 console, click **File > Merge Devices**. The Open Discovery File dialog appears.
2   Browse to locate the discovery file that you want to open, then Click **Open**.

The device set from the selected file will be merged with the current set of devices. The topology maps will not be 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 console, click **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 will replace 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 console, click **File > Merge Maps**. The **File Open** dialog appears.
2   Browse to locate the discovery file that you would like to open. Click **Open**.

The topology maps from the external discovery file will be 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 console, click **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 console, click **File > Save As**. The Save Discovery File dialog appears.
2   Give the discovery file a name, then click **Save**. The network data will be 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:

- *The Device Categories view* (on page 28)
- *The Device List view* (on page 34)
- *The Topology Map view* (on page 38)
- *The Subnets view* (on page 50)
- *The Links view* (on page 52)

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 base-level functions of the data grid view:

- *Column filtering* (on page 25)
- *Edit Device Category* (on page 25)
- *Show in Device Categories* (on page 26)
- *Remove selected devices* (on page 26)
- *Print and Print Preview* (on page 27)
- *Save CSV (comma-separated value file)* (on page 27)
- *Copying to clipboard* (on page 27)

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.

- Firewalls
- Routers
- Switches
- Hubs
- Wireless Access Points
- Printers
- Macintosh
- Windows
- Windows Servers
- Linux
- Unix
- IP Phone Managers
- IP Phones
- Power/UPS
- Unknown

> **Note**: Any device that is either not categorized or does not support SNMP will be 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 CTRL 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.

Access Device Categories view on the WhatsConnected console from **View > Device Categories**.
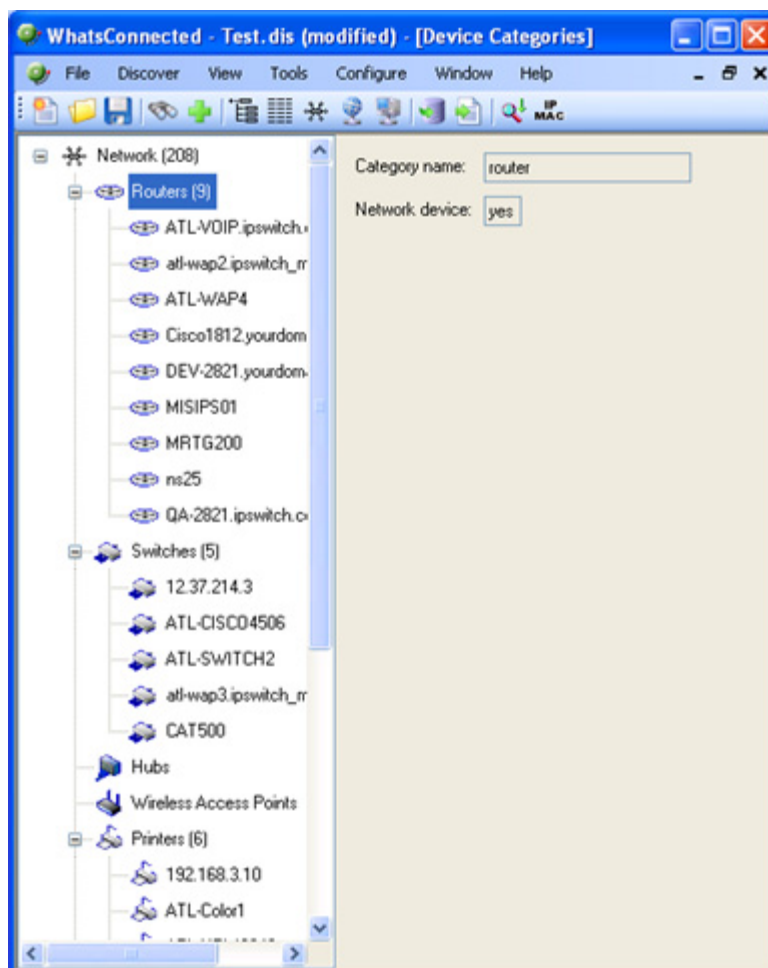
The Device Categories view also provides a tabular view of the inventory and configuration data that is gathered from each network device. For more information, see *About Device Details tab view* (on page 30).

> 💡 **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 24).

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.

- **Bridge Ports**. Provides Bridge Port and VLAN name and index information.

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

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

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

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

- **IP Routes**. Provides IP route configuration data information.

- **Spanning Tree (STP)**. Provides spanning tree configuration and status information.
- **ARP Cache**. Provides Address Resolution Protocol (ARP) table information.
- **Forwarding**. Provides Layer 2 forwarding information.
- **Protocol Profile**. Provides information about successful protocol matches for this device.
- **HSRP**. Provides information about the Hot Standby Router Protocol (HSRP) on the device. The information relates to the standby nature of routers.
- **IP Phone**. Provides information about the selected (individual) IP phone.
- **IP Phone Manager**. Provides information about the IP phones that are registered or are communicating with a call manager.
- **IP Routes**. Provides information about the IP routes configured for this device.
- **VRRP**. Provides information about the Virtual Router Redundancy Protocol (VRRP) on the device. The information relates to the standby nature of routers.
- **STP**. Provides information about Spanning Tree Protocol entries discovered on this device.
- **Software**. Provides information about installed software discovered on this device.

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 24). 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 menu

The Device Categories right-click menu allows you to manage your device categories. From the right-click menu you can add a device category, edit an existing category, delete a category, or show and/or hide a category from the device category list.

To add a device category:

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   Anywhere inside of the Device Categories list, right-click. The right-click menu appears.
3   Select **Add Category.** The Device Category Configuration dialog appears.
4   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, and after they have been created cannot be edited.

- 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.

5   Click **OK** to save changes.

To edit a device category:

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   In the Device Categories list, right-click the category you want to modify. The right-click menu appears.

3   Select **Edit Category.** The Device Category Configuration dialog appears.

> 📝 **Note**: You cannot edit default device categories.

4   Enter or select the appropriate information in the dialog fields.

- 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.

5   Click **OK** to save changes.

To delete a device category:

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   In the Device Categories list, right-click the category you want to remove. The right-click menu appears.

**3**   Select **Delete Category**. The category is removed from the device category list.

> 📝 **Note**: You cannot delete default device categories.

To hide a device category:

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   In the Device Categories list, right-click the category you want to hide, then click **Hide Category**. The device category is hidden and no longer appears in the category list.

To show a hidden device category:

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   At the top of the device category list, right-click **Network**. The right-click menu appears.

3   Under **Show Hidden Category**, select the hidden category that you want to show. If there are several hidden categories, select **Show All** to show all of the hidden categories. The selected device categories appear in the device category list.

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 24).

> 💡 **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:

- 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 30).

About Device List columns

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

The columns of the 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.
- **NetBios Name**. The windows NetBios name (if supported and known).
- **NetBios Domain**. The windows NetBios domain (if supported and known).
- **System Name**. The MIB II system name.
- **System Description**. The MIB II system description.
- **System OID**. The MIB II system object ID.
- **Vendor**. The network device manufacturer.
- **Model**. The network device model number.

Using Device List filters

You can use Device List filters to locate specific network devices and subnets. These filtering tools let you to find devices that match your specified search criteria.

To filter the device list by device type in the list view grid:

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 Click the **Device Filter** list, then select the device type you want to view in the device list. The filtered devices appear in the device list.
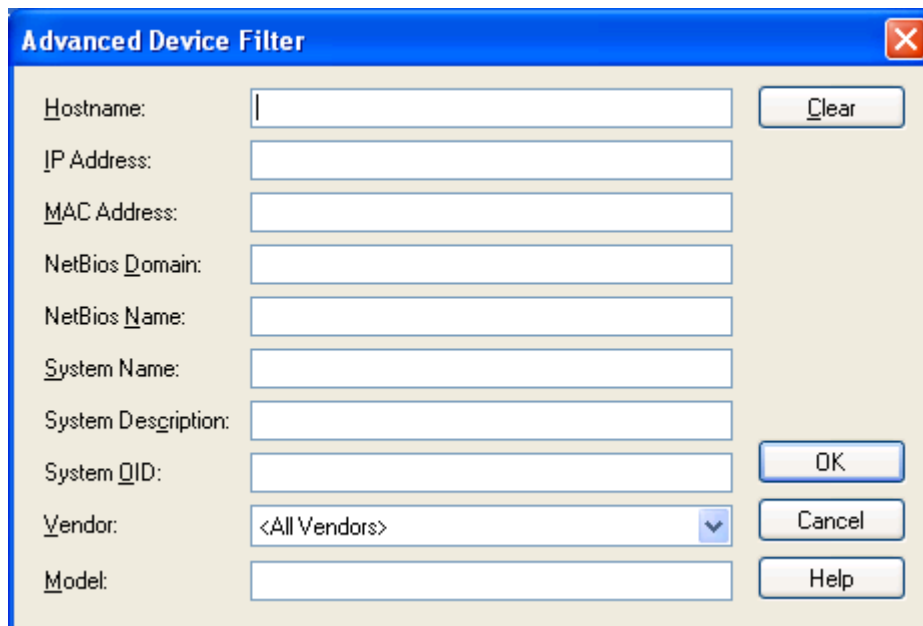
To filter the device list by search criteria:

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   Click **Advanced**. The Advanced Device Filter dialog appears.

3   Enter the desired search criteria in the provided fields. Use a wild card in any text box. For example, Hostname: device1*.

4   After the device filter search criteria are entered, click **OK.** The list displays only the devices that match the search criteria.

5   Click **Advanced** to further refine the search criteria, then click **OK**. Only the current list of devices is compared against the current set of search criteria to show a refined set of devices.

6   Click **Clear**, then click **OK** to clear all search criteria and return to the complete device list.

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.
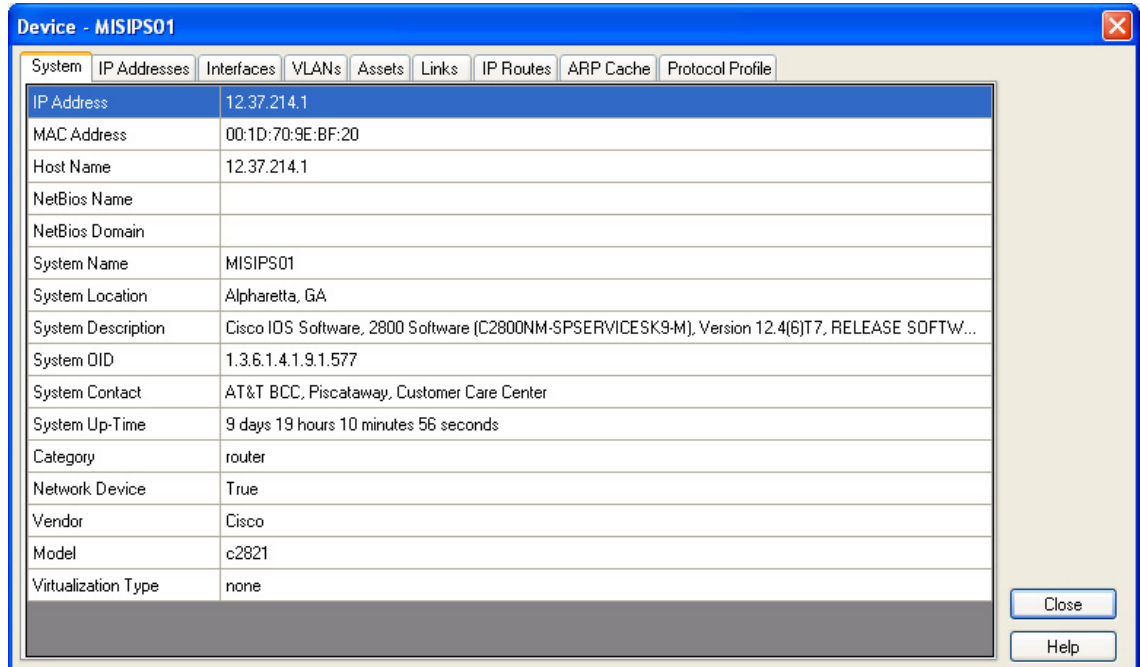
To view the device list details:

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.

Device - MISIPS01	
System | IP Addresses | Interfaces | VLANs | Assets | Links | IP Routes | ARP Cache | Protocol Profile	
IP Address	12.37.214.1
MAC Address	00:1D:70:9E:BF:20
Host Name	12.37.214.1
NetBios Name	
NetBios Domain	
System Name	MISIPS01
System Location	Alpharetta, GA
System Description	Cisco IOS Software, 2800 Software (C2800NM-SPSERVICESK9-M), Version 12.4(6)T7, RELEASE SOFTW...
System OID	1.3.6.1.4.1.9.1.577
System Contact	AT&T BCC, Piscataway, Customer Care Center
System Up-Time	9 days 19 hours 10 minutes 56 seconds
Category	router
Network Device	True
Vendor	Cisco
Model	c2821
Virtualization Type	none

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.

- **Bridge Ports**. Provides Bridge Port and VLAN name and index information.

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

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

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

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

- **IP Routes**. Provides IP route configuration data information.

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

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

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

- **Protocol Profile**. Provides information about successful protocol matches for this device.

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

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

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

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

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

- **STP**. Provides information about Spanning Tree Protocol entries discovered on this device.

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

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 24). These views allow you to browse, sort, and export (print) the data that is shown for each device.

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.
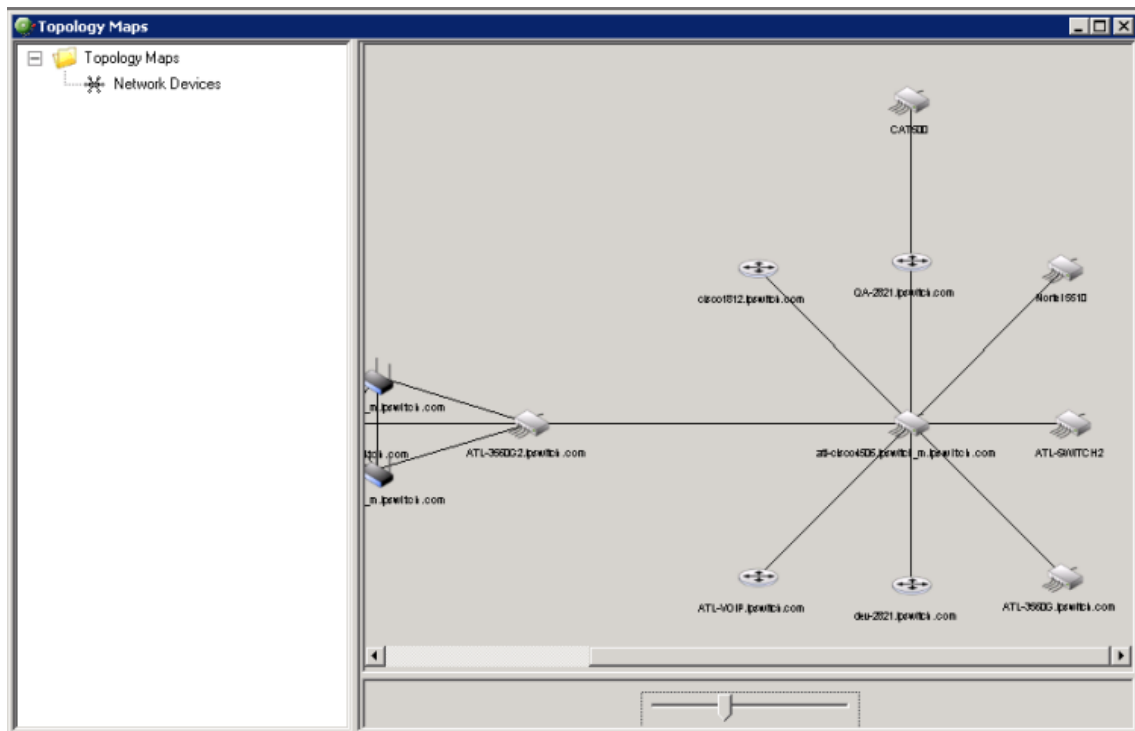
With the topology data, you can build custom topology views that display important elements of your network infrastructure.

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 39).

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 or map:

1 Right-click on topology group or map 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 or map 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.

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 modify 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 47).

> **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.

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 machnies 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 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.

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 Click **View > Topology Map**, then select a topology map. The topology map 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 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.

Exporting topology maps to WhatsUp Gold

You can use the right-click menu to export the WhatsConnected topology map details to WhatsUp Gold v12.3 or later. When the 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.

> 📓 **Note**: WhatsConnected tools are enabled in the WhatsUp Gold console. For more information about WhatsConnected tools, see *Using WhatsConnected Tools* (on page 53).

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.

  - **Whats Connected 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**.

7 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 export the 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 Click **Export To**. The right-click menu appears.

5 Click **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.

6 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.

7 Click **OK**. The topology map is exported to a Visio document.

About Topology layout modes

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 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. You can also change the root device.

To change 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.

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 48).

- ▪ **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 48).

- ▪ **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 49).

To change a topology map layout settings:

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 the topology map, then select Layout Settings. The Layout Settings dialog appears.
4   Use the Layout Settings dialog to adjust the layout options. For more information about auto-layout settings, see Layout Settings in the WhatsConnected Help.
5   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 48) or *hierarchy* (on page 48) 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.
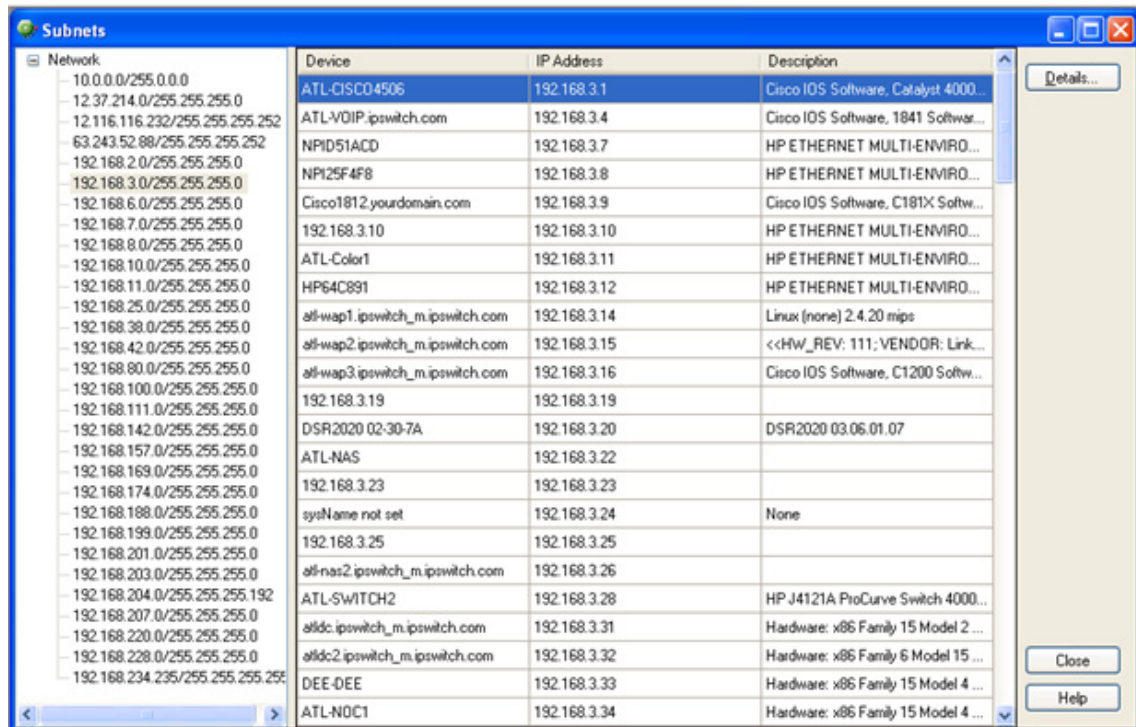
> **Tip**: You can also view topology maps from the WhatsConnected console shortcut menu. Click ✳ (Topology maps shortcut icon). The Topology Maps dialog appears.

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.

About Subnets View

Subnets View is an explorer-type view that shows the grouping of network devices based on their respective subnets (or IP addressing information).

The device list on the right side of the pane is a data grid view and therefore supports all sorting, exporting, and column filtering options. For more information about data grid views, see *About data grid views* (on page 24).

Viewing Subnet device details

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

To view subnet device details:

▪ From the main menu of the WhatsConnected console, select **View > Subnets**. The Subnets view appears.
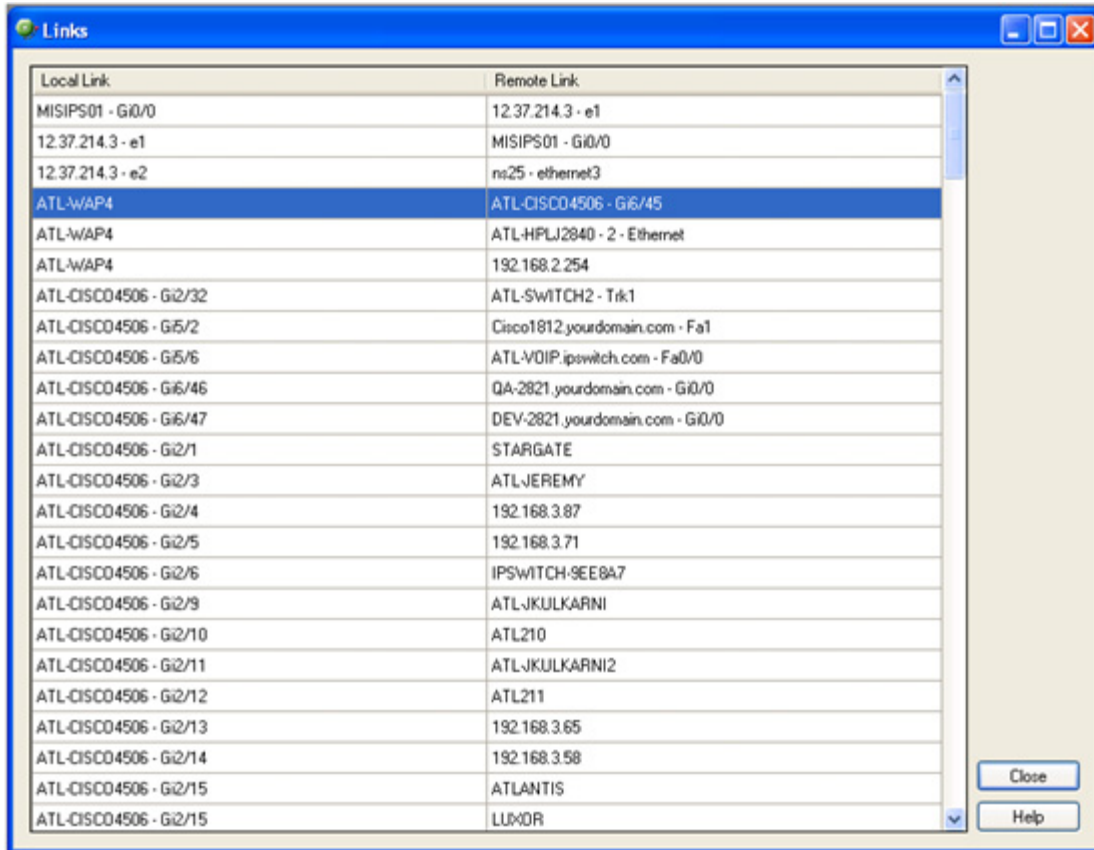
> 💡 **Tip**: You can also view subnets from the WhatsConnected console shortcut menu. Click 🌐 (Subnets icon). The Subnets dialog appears.

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 24).

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.

Using WhatsConnected Tools

In This Chapter

About WhatsConnected Tools

WhatsConnected includes network tools that are available in both the WhatsConnected and WhatsUp Gold consoles.

- Layer 2 Trace tool
- IP/MAC Finder tool
- *Export Topology to Visio* (on page 46) tool (available in WhatsConnected only)
- *Device Viewer* (on page 60) 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.
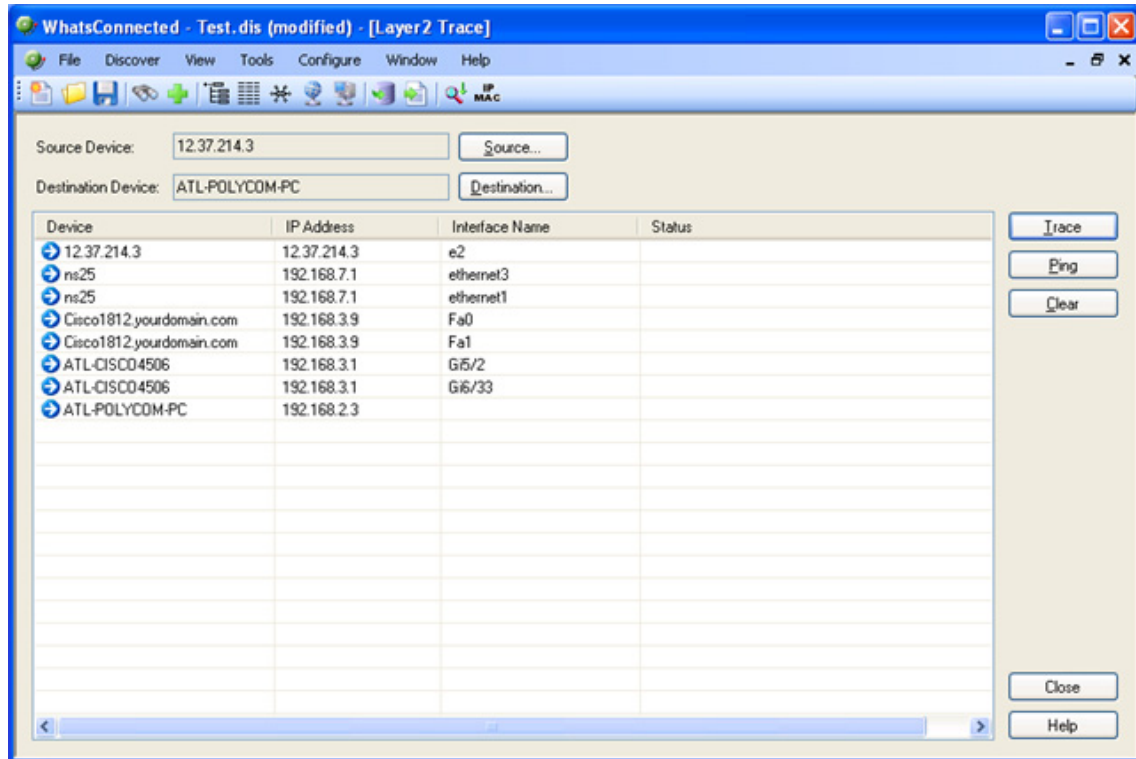
Using previously discovered network connectivity data, the Layer 2 Trace tool finds the path between the two devices and then displays each network interface that is used to build the path. The trace tool also allows for a quick check of the status and availability of each step along the layer 2 path.

The Layer 2 trace tool is accessible from the WhatsConnected and WhatsUp Gold console.

To run the Layer 2 Trace tool from WhatsConnected console:

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 WhatsConnected console shortcut menu. Click (Layer 2 Trace shortcut icon). The Layer 2 Trace dialog appears.

From WhatsUp Gold:

1   From the WhatsUp Gold console, select a device group map view.

2   Right-click on any device in the map view. The right-click menu appears.

> 💡 Click **Layer 2 Trace**. The WhatsConnected - Layer 2 Trace dialog appears.

3   Click **Source**. The Select Source Device dialog appears.

4   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.

5   Click **Destination**. The Select Destination Device dialog appears.

6   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.

7   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.

8   Click **Clear** to remove the information from the Layer 2 Trace table and start a new trace.
- or -
Click **Close** to close the dialog.

To run the Layer 2 Trace tool from WhatsUp Gold console:

1   From the WhatsUp Gold console, right-click a device in a Device View or Map View tab. The right-click menu appears.

2   Click **Layer 2 Trace**. The Layer 2 Trace dialog appears.

3   Click **Source**. The Select Source Device dialog appears.

4   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.

5 Click **Destination**. The Select Destination Device dialog appears.

6 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.

7 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.

8 Click **Clear** to remove the information from the Layer 2 Trace table and start a new trace.
- or -
Click **Close** to close the dialog.
- or -
Click **Save** to open the Save Up Dependency dialog. This dialog provides a list of Layer 2 paths, found in the Layer 2 trace, that can use up dependencies in WhatsUp Gold polling dependency rules. For more information, see *Dependencies overview* in the WhatsUp Gold Help.

Using IP/MAC Finder

The IP/MAC Finder tool provides an easy way to locate an IP or MAC address on the network. Using the previously discovered network devices, IP/MAC Finder will find and display 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.
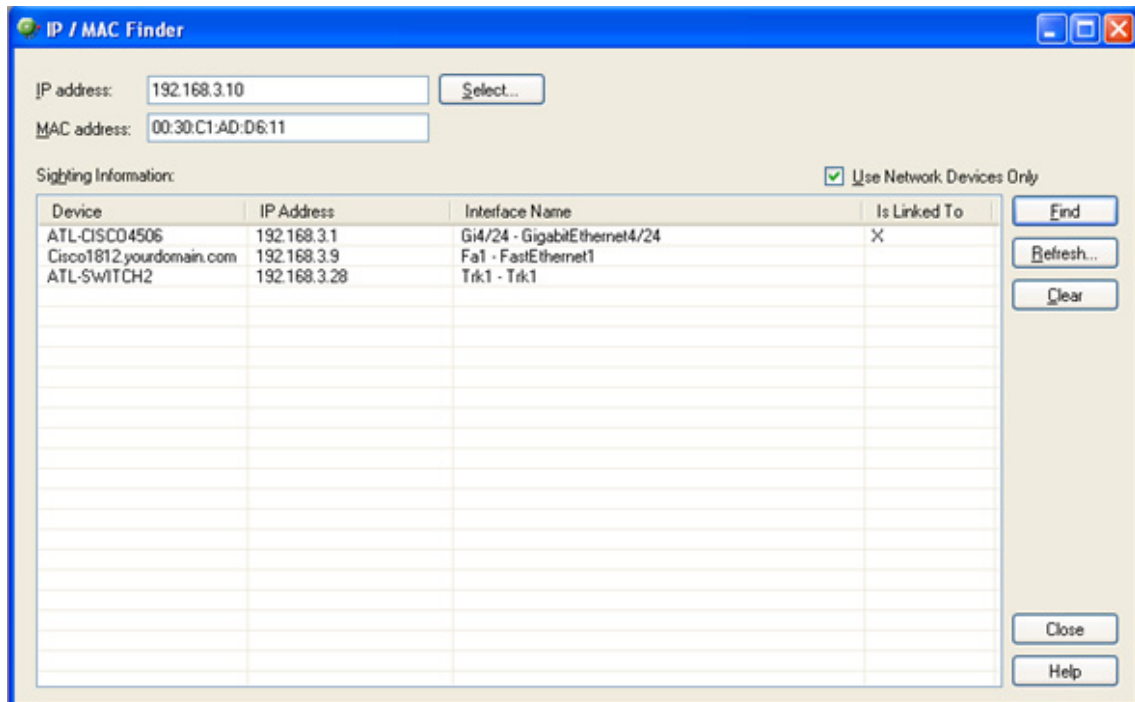
When enough network data is available, IP/MAC Finder indicates to which network interface the IP or MAC address is physically connected.

> **Note**: The IP/MAC Finder is accessible from both the WhatsConnected console and the WhatsUp Gold console.

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 on the WhatsConnected console:

From WhatsConnected:

1   From the main menu of the WhatsConnected console, 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.

From WhatsUp Gold:

1   From the WhatsUp Gold console, select a device group map view.
2   Right-click on any device in the map view. The right-click menu appears.
3   Click **IP/MAC Finder**. The WhatsConnected - IP/MAC Finder dialog appears.

4   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 59).

> **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.

5   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.

6   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.

7   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.

To use the IP/MAC Finder tool within WhatsUp console:

1   From the WhatsUp Gold console, right-click a source device in a Device View or Map View tab. The right-click menu appears.
2   Click **IP/MAC Finder**. The IP/MAC Finder dialog appears.
3   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 59).

> **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.

4 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.

5 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.

6 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 Finder tool's Select feature 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** tool from either the WhatsConnected or WhatsUp Gold console (see *Using the IP/MAC Finder* (on page 57)).

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 Finder tool's Refresh Connectivity feature 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 Finder** tool from either the WhatsConnected or WhatsUp Gold console (see *Using the IP/MAC Finder* (on page 57)).
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.

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 the 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 the Rebuild Connectivity:

▪   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 from the WhatsUp Gold console. The information displayed in the Device Viewer is accessed from the WhatsUp database.

To run the Device Viewer tool:

1   Start the WhatsUp Gold console.

2   Locate a device that has been exported from WhatsConnected to the WhatsUp database.

3   Right-click the device in the WhatsUp console. The right-click menu appears.

4   Select **Device Viewer**. The WhatsConnected Device Viewer appears displaying the device details. 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.

- **Bridge Ports**. Provides Bridge Port and VLAN name and index information.

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

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

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

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

- **IP Routes**. Provides IP route configuration data information.

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

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

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

- **Protocol Profile**. Provides information about successful protocol matches for this device.

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

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

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

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

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

- **STP**. Provides information about Spanning Tree Protocol entries discovered on this device.

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

> **Note**: The device details are the same as those displayed in the Device Details Viewer in the WhatsConnected console. For more information, see *About Device Details tab view* (on page 30).

> **Note**: You can click **Select** to open the Select Device dialog and select another device. For more information, see Select Devices in the WhatsConnected Help.

Viewing WhatsConnected reports

In This Chapter

About WhatsConnected reports

WhatsConnected reports provide information about your 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.
- **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.

Asset/Inventory report

The Asset/Inventory Report provides a view of the assets discovered by WhatsConnected. The following is a list of the information available about individual 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 of 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 see 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 pull-down box. The report will refresh and display only 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.

To display components that are housed within another device:

Select **Show all assets** to display any components that are housed within another device.

Device Connectivity report

The Device Connectivity Report provides a list of the devices connected to a network device. 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 see details on a device:

Select the device and click **Details.** A Device Viewer appears.

To filter the report on device type:

Select the device type you would like to display from the Device Filter list box. The report will refresh and display only devices of the selected type.

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.

▪ **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 see 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.

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 68)
- *Discovery Settings* (on page 69)
- *Protocol Settings/Credentials* (on page 70)
- *Device Categories* (on page 71)
- *Device Types* (on page 72)
- *Discovery Tasks* (on page 73)

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:
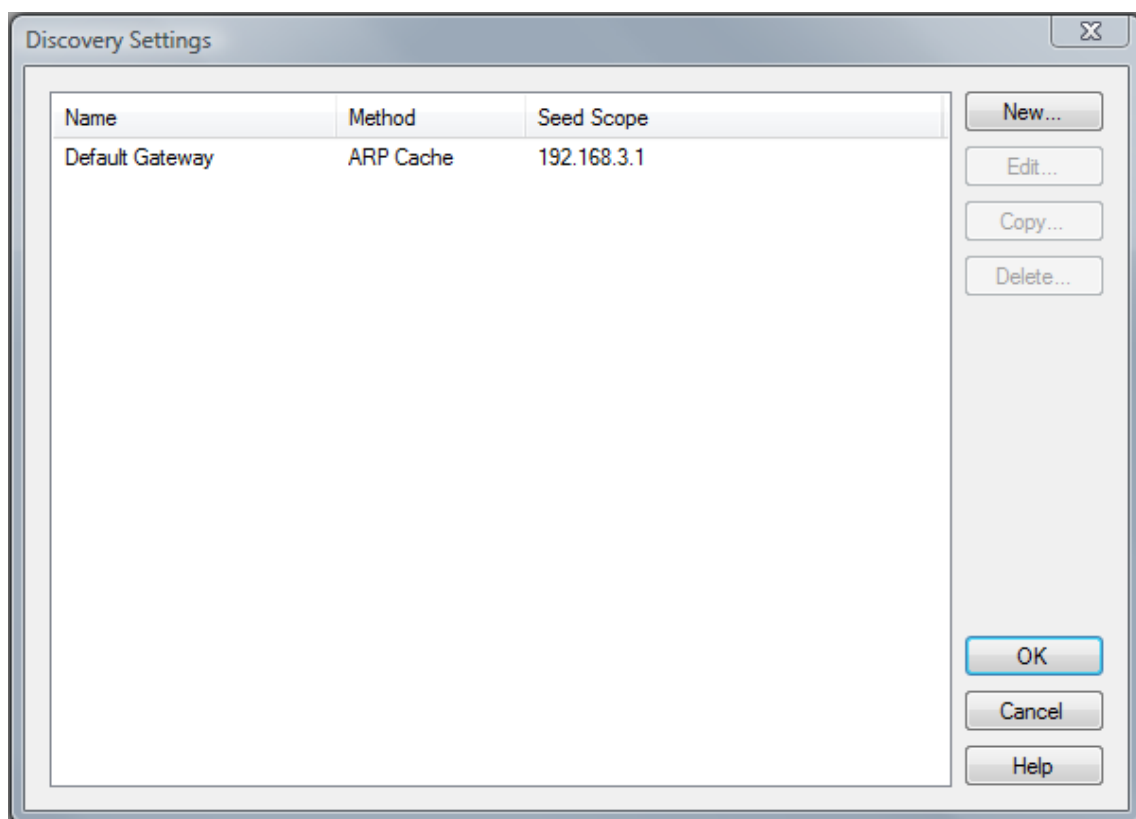
- WhatsUp
- Cisco

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 73) 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 **Configure > 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 **Configure > 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 **Configure > 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 **Configure > 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 (for ICMP, SNMPv1-v3, SSH, or VmWare) 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.

- **ICMP** discovery requires the timeout settings and retry counts.

- **SSH** discovery requires the User Name, Password, and Port used to attempt an SSH connection.

- **VMware** discovery requires the User Name, Password, and Port used to attempt a connection to a VMware host or vCenter server.

> **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 **Configure > 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 **Edit**. The protocol properties dialog appears.

2   Make any needed changes, 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 SNMPv1, SNMPv2, SNMPv3, SSH, and VMware credentials from the selected WhatsUp Gold server Credentials Library, and they appear in the Protocol Settings/Credentials dialog.

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 Types

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 vendor or manufacturer name.

    - **Model**. Enter the vendor or manufacturer model.

    - **Description**. Enter the 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.

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 **Configure > Discovery Tasks**. The Discovery Task dialog appears.

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

3 Enter the name and description for the task in the **Name** and **Description** boxes.

4 In the **Discovery Settings** box, 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 In the **Discovery Filename** box, select the filename you want to use to save the details of the discovery task. This file will be used to save the results of the scheduled discovery task.

6 Select **Update Exported WhatsUp Gold Devices** to update devices that have already been exported to WhatsUp Gold with any changes that are found during the discovery scan.

7 In the Run This Task area, select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run.

8 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 In the **Discovery Settings** box, select or edit 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 In the Discovery Filename box, edit the filename you want to use to save the details of the discovery task. This file will be used to save the reslults of the scheduled discovery task.

5 Select **Update Exported WhatsUp Gold Devices** to update devices that have already been exported to WhatsUp Gold with any changes that are found during the discovery scan. 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.

6 In the Run This Task area, edit the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run.

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

To copy an exisiting 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 will change from *Running* to *Canceled*.

To close the dialog:

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

Copyright notice

This document was published on Monday, June 28, 2010 at 10:31.