



IPSWITCH

Using WhatsUp IP Address Manager 1.0

 **IPSWITCH**
WhatsUpGold

Table of Contents

Welcome to WhatsUp IP Address Manager

Finding more information and updates	1
Sending feedback.....	2

Installing and Licensing IP Address Manager

System Requirements	3
Installation overview	3
Activating IP Address Manager.....	4
Exceeding your license	4

Discovering Networks in IP Address Manager

Getting Started with IP Address Manager	6
About network discovery	7
Configuring network discovery	7
About network discovery scan types	8
About discovery settings	9
Configuring discovery settings	9
About discovery IP scopes	10
Configuring network protocols and credentials.....	11
Using the SNMP protocol and credentials	12
Using the SSH protocol	16
Using the Telnet protocol	17
Using the Windows (WMI) Protocol.....	18
About IP Address Manager Discovery Tasks	19
Configuring Discovery Tasks	19
Configuring and scheduling Subnet Scan Tasks.....	21
Configuring and scheduling DHCP Scan Tasks	23
About the Discovery Task Log	25
Merging Devices	27
Importing Device Attributes.....	27

Using the IP Address Manager console

About the IP Address Manager console	28
About the IP Address Manager console shortcut menu	30
About network discovery files	30

Managing network discovery files.....	30
Creating a new discovery file	31
Opening a discovery file	31
Opening a recently used discovery file	31
Using Merge Devices	31
Using Save.....	31
Using Save As.....	32
Collecting Device MIBs	32

Viewing network data

About network data views	33
About data grid views	33
Column filtering.....	34
Edit Device Category.....	34
Remove selected devices	35
Print and Print Preview.....	35
Copying to clipboard	35
About Device List View	36
About Device List columns	37
About Device List filters	37
Viewing Device List details	38
About the Device List View right-click menu	39
About Subnets View	40
About the Subnets View right-click menus	43
About DHCP View	44

Using IP Address Manager Tools

About IP Address Manager Tools.....	48
Using the Subnet Calculator	48
About the IP History Log	49
Classify Devices.....	51

Configuring IP Address Manager

About configuration settings	52
Configuring Discovery Settings.....	52
Configuring Protocol Settings/Credentials	53
Configuring Device Filters	54
Configuring Device Type Mappings	57

WhatsUp Gold Server Endpoint Library (Remote Servers).....	58
Configuring Email Settings	59
Configuring Thresholds.....	60

Viewing IP Address Manager Reports

About IP Address Manager reports	61
About the Available IPs report	62
About the Managed IPs report	62
About the Leased IPs report	63
About the Reserved IPs report	63
About the Duplicate IPs report.....	64
About the IP History report	64
About the DHCP Scope report.....	65
About the DNS Record report	66
About the DNS Zone report.....	66
About the Subnet Report.....	67

Scheduling Reports

About the Scheduled Reports Library	68
Configuring Scheduled Reports	68

Copyright notice

Welcome to WhatsUp IP Address Manager

In This Chapter

Finding more information and updates..... 1

Sending feedback..... 2

WhatsUp IP Address Manager is an automated solution to the cumbersome and error prone task of inventorying network address usage. IP Address Manager's discovery scans to find devices on your network and provides you with an extensive breakdown of your network's subnets, DHCP, and DNS servers. Discovery scans can be scheduled to run automatically to gather up-to-date inventory information on a daily basis. Discovery Alerts notify you when changes are detected in your discovery files and allow you to merge and sync changes. The IP Address History Log offers chronological event history, such as allocation and status change, for IP addresses, MAC addresses, and hostnames.

The IP Address Manager's network views allow you to see information about your network's subnets and servers from one central location. IP Address Manager's main view, the Subnets View, allows you to manage your network subnets, without having to leave the IP Address Manager console. IP Address Manager's DNS server view gives you in-depth inventory information for your network DHCP servers. Configurable thresholds alert you when your servers are nearing full capacity, allowing you to make hardware or configuration changes if and when conflicts arise.

Inventory information can be saved, exported, and distributed in multiple formats as reports. Scheduled Reports can be configured to send inventory information on a regularly scheduled basis.

IP Address Manager can share a server with Ipswitch WhatsUp Gold, or can be installed as a standalone application on a separate server.

Finding more information and updates

The following are information resources for IP Address Manager. This information may be periodically updated and available on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/support/index.aspx>).

- **Release Notes.** The release notes provide an overview of changes, known issues, and bug fixes for the current release. The release notes are available on the *WhatsUp Gold web site* (<http://www.whatsupgold.com/IPAM1relnotes>).
- **Application Help.** The console help contains dialog assistance, general configuration information, how-to's that explain how to use IP Address Manager's features. The Table of Contents is organized by functional area, and can be accessed from the main menu or by clicking **Help** in IP Address Manager dialogs.

- **Additional WhatsUp Gold resources.** For a listing of current and previous guides and help available for WhatsUp Gold products, see the *WhatsUp Gold web site* (<http://www.whatsupgold.com/support/guides.aspx>).
- **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/support/index.aspx>).

Sending feedback

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

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

CHAPTER 2

Installing and Licensing IP Address Manager

In This Chapter

System Requirements.....	3
Installation overview	3
Activating IP Address Manager	4
Exceeding your license.....	4

System Requirements

Refer to the *Release Notes* (<http://www.whatsupgold.com/IPAM1relnotes>) for IP Address Manager product features, system requirements, fixed in this release, known issues, and other information.

Installation overview

IP Address Manager can share a server with Ipswitch WhatsUp Gold, or can be installed as a standalone application on a separate server. In either case, IP Address Manager is licensed separately, and is installed using the IP Address Manager installation program. The IP Address Manager *Release Notes* (<http://www.whatsupgold.com/IPAM1relnotes>) contain the most up-to-date information about installing.

Before installing, we recommend that you read the IP Address Manager *Release Notes* (<http://www.whatsupgold.com/IPAM1relnotes>) 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 IP Address Manager, visit the *MyIpswitch portal* (<http://www.myipswitch.com>). For more information, see *Activating IP Address Manager* (on page 4).

Activating IP Address Manager

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

To activate IP Address Manager 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 IP Address Manager > Manage IP Address Manager License**. The activation program appears.
- 2 Follow the onscreen instructions to complete the product activation.



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

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

Exceeding your license

Your license dictates how many IP addresses you can manage with IP Address Manager. If you have exceeded your license, many features and menu options are disabled. By default, all discovered subnets and addresses are manageable, so you must decrease the number of managed IP addresses in the event that you exceed your license count. You can choose which IP addresses to manage from the IP Address Manager Subnet View. Additionally, you can upgrade your license to enable you to manage more IP addresses with IP Address Manager.

Managing subnets from the Subnet View

Using the Subnet View right-click menu, you can select to unmanage and manage subnets.

To unmanage a subnet:

Right-click a subnet, then select **Unmanage**. The subnet becomes inactive, indicated with a strike through.

Upgrading your license

If you need to upgrade your license to manage more IP addresses, you can do so from your *MyIpswitch* (<http://www.myipswitch.com/>) licensing portal.

CHAPTER 3

Discovering Networks in IP Address Manager

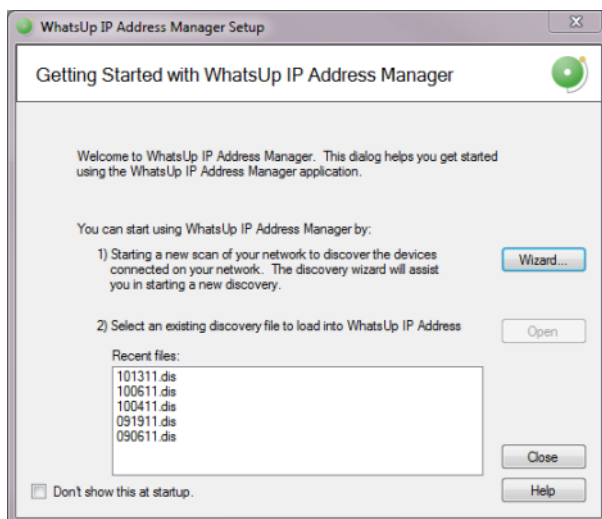
In This Chapter

Getting Started with IP Address Manager	6
About network discovery	7
Configuring network discovery	7
About network discovery scan types	8
About discovery settings	9
About IP Address Manager Discovery Tasks	19
About the Discovery Task Log	25
Merging Devices	27
Importing Device Attributes	27

Getting Started with IP Address Manager

To start IP Address Manager:

From the Windows Start Menu, select **Ipswitch IP Address Manager**.



To begin gathering and viewing network information:

- Start a new network scan to discover devices connected on the network. Click **Wizard** to start the Wizard discovery process.
- or -
- If you have saved IP Address Manager discovery files previously, you can select an existing discovery file in the **Recent files** list, then click **Open**.

Select **Don't show this at startup** to prevent this dialog from appearing each time you start IP Address Manager.

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

About network discovery

IP Address Manager discovers the devices on your network to gather detailed inventory information about each device, including device system information, IP and MAC addresses for all device interfaces, and detailed history, status, use, and type information for network addresses.

There are several ways to add devices with Network Discovery:

- Through the Network Discovery option in the IP Address Manager console **Discover > Network** menu. For more information, see Run Discovery in the Help.
- Through the single device discovery option in the IP Address Manager console **Discover > Device** menu. For more information, see Add New Device in the Help.
- Through the Getting Started with IP Address Manager Wizard that appears when you start IP Address Manager. For more information, see *Getting started with IP Address Manager* (on page 6).

Configuring network discovery

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 Network Discovery scan types* (on page 8).
- The network protocols and credentials used during the network scan. For more information, see the *Configuring network protocols and credentials* (on page 11) section.

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

About network discovery scan types

An important part of Network Discovery is understanding the different methods by which a network can be discovered. There are two 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 discovery method, see About Seed IP Scope.

Advanced Discovery Settings

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

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

Configuring discovery settings

To add discovery settings:

- 1 From the main menu of the IP Address Manager console, select **Configure > Discovery Settings**. The Discovery Settings dialog appears.
- 2 Click **New**. The New Discovery Settings dialog appears.
- 3 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.
- 4 Select the discovery method, either **ARP Cache Discovery** or **PING Sweep Discovery**. For more information, see About Network Discovery scan types.
- 5 Click **Advanced** to set Advanced Discovery Settings.
 - 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 IP Address Manager 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.

- Select whether the discovery engine should try to **Ping Devices First** before attempting any other protocol.
- 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.

- Select the **Resolve DNS names** option to resolve DNS names to their IP addresses.
- 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,
- 6** On the Discovery/Name Method dialog, click **Next**.
- 7** Click **Gateway** to enter the **Seed IP Scope**. For more details in regards to the Seed IP Scope, see *About Seed IP Scope* (on page 11).
- 8** If you want to use Advanced IP Scoping options, click **Advanced**.
 - Enter the **Include IP Scope**. For more information, see *About Include IP Scope* (on page 11).
 - You can also enter the **Exclude IP Scope**. For more information, see *About Exclude IP Scope* (on page 11).
 - Click **OK** to complete the advanced options.
- 9** On the Discovery Starting Point(s) dialog, click **Next**.
- 10** Enter Discovery Protocol Settings as required. For more information, see *Configuring network protocols and credentials* (on page 11).
- 11** Click **Finish** to save all changes made in the Discovery Settings dialog.

To rename discovery settings:

- 1** From the main menu of the IP Address Manager 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 IP Address Manager 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 IP Address Manager 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 network discovery. The three main protocols used in discovery are ICMP, SNMP, and WMI.

Additionally, the IP Address Manager Credentials Library provides support for Telnet and SSH. Telnet and SSH credentials are used to communicate with network devices and capture device configuration information.

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

Using the ICMP protocol

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



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

To change the ICMP settings for the discovery engine:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select **ICMP**, then click **Edit**. The Edit ICMP Settings dialog appears.
- 3 Increase or decrease the **Timeout** settings. The default timeout is 500 milliseconds.



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

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



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

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

Using the SNMP protocol and credentials

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

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

SNMPv1 credentials

To add a new set of SNMPv1 credentials:

- 1 From the main menu of the IP Address Manager 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 IP Address Manager 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 IP Address Manager console, select **Settings > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of SNMPv1 credentials, then click **Delete**. The SNMPv1 credentials are removed.
- 3 Click **OK** to save the protocol changes.

SNMPv2 credentials

To add a new set of SNMPv2 credentials:

- 1 From the main menu of the IP Address Manager 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 IP Address Manager 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 IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of SNMPv2 credentials, then click **Delete**. The SNMPv2 credentials are removed.
- 3 Click **OK** to save the protocol changes.

SNMPv3 credentials

To add a new set of SNMPv3 credentials:

- 1 From the main menu of the IP Address Manager 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 IP Address Manager 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 IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of SNMPv3 credentials, then click **Delete**. The SNMPv3 credentials are removed.
- 3 Click **OK** to save the protocol changes.

Using the SSH protocol

IP Address Manager stores the SSH authentication data you provide below so that IP Address Manager can use whenever authentication is needed to connect to and gather data from a device.

To add a new set of SSH credentials:

- 1 From the main menu of the IP Address Manager 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 unique **Name**.
- 5 Optionally, enter a short **Description**.
- 6 Enter a new SSH **Username**.
- 7 Enter a new SSH **Password** and the **Confirm Password**.



Note: SSH passwords are encrypted.

- 8 Enter a defined SSH port. The default port number is 22.
- 9 Click **OK** to save the protocol changes.

To edit a set of SSH credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of SSH credentials, then click **Edit**. The protocol properties dialog appears.
- 3 Modify the existing settings.
 - Enter a new **Name** and **Description**, if needed.
 - Enter a new SSH **Username**.
 - Enter a new SSH **Password** and the **Confirm Password**.



Note: SSH user names and passwords are encrypted.

- Enter the defined SSH port. The default port number is 22.
- 4 Click **OK**, to save the protocol changes.

To delete a set of SSH credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of SSH credentials, then click **Delete**.
- 3 Click **OK** to save the protocol changes. The SSH credentials are removed.

Using the Telnet protocol

Telnet credentials can be assigned to devices for DHCP discovery, however, Telnet credentials cannot be assigned to IP Address Manager discovery tasks.

To add a new set of Telnet credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Click **New**.
- 3 Select **Telnet**, then click **OK**. The protocol properties dialog appears.
- 4 Enter a unique **Name**.
- 5 Optionally, enter a short **Description**.
- 6 Enter a new Telnet **Username**.

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



Note: Telnet passwords are encrypted.

- 8 Enter a defined Telnet port. The default port number is 23.
- 9 Click **OK** to save the protocol changes.

To edit a set of Telnet credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of Telnet credentials, then click **Edit**. The protocol properties dialog appears.
- 3 Modify the existing settings.
 - Enter a new **Name** and **Description**, if needed.
 - Enter a new Telnet **Username**.
 - Enter a new Telnet **Password** and the **Confirm Password**.



Note: SSH user names and passwords are encrypted.

- Enter the defined SSH port. The default port number is 23.
- 4 Click **OK** to save the protocol changes.

To delete a set of Telnet credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of Telnet credentials, then click **Delete**.
- 3 Click **OK** to save the protocol changes. The Telnet credentials are removed.

Using the Windows (WMI) Protocol

The WMI Domain\UserID and Password are required to connect to Windows systems. This protocol is required if you want to collect inventory information for Windows devices.

To add a set of Windows (WMI) credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Click **New**.
- 3 Select **Windows**, then click **OK**. The protocol properties dialog appears.
- 4 Enter a **Name** and **Description** for the credential.
- 5 Enter a new Windows **Domain\UserID**. You may enter `. \` for the domain or enter a specific domain name.
- 6 Enter a new Windows **Password** and **Confirm password**.



Note: Windows passwords are encrypted.

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

To edit a set of Windows credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of Windows credentials, then click **Edit**. The protocol properties dialog appears.
- 3 Modify the existing settings.
 - Enter a new Windows **Domain\UserID**. You may enter `.\` for the domain or enter a specific domain name.
 - Enter a new Windows **Password** and **Confirm password**.



Note: WMI user names and passwords are encrypted.

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

To delete a set of Windows credentials:

- 1 From the main menu of the IP Address Manager console, select **Configure > Protocol Settings/Credentials**. The Protocol Settings/Credentials dialog appears.
- 2 Select an existing set of Windows credentials, then click **Delete**.
- 3 Click **OK** to save the protocol changes. The set of Windows credentials are removed.

About IP Address Manager Discovery Tasks

IP Address Manager Discovery Tasks allow you to schedule discovery scans of your network, subnets, and DHCP servers.

Configuring 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 IP Address Manager Wizard, and the schedule is created during the creation of the discovery task. You can schedule a task to run daily, weekly, monthly, yearly or on some other defined time interval.

To add a new discovery task:

- 1 Click **Discover > Discovery Tasks**. The Discovery Task dialog appears.
- 2 Click **Add** to add a new discovery tasks to the list. The Select a Discovery Task Type dialog appears.
- 3 Select **Network Discovery Task**, then click **OK**. The New Discovery Task dialog appears.
- 4 Enter a **Name** and **Description** for the task.
- 5 From the **Discovery Settings** list, select the discovery file (`.dis`) you want to use for the discovery task. This file defines 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.

- 6 From the **Discovery Filename** list, select or create the filename you want to use to save the details of the discovery task. This file is used to save the results of the scheduled discovery task.
- 7 To enable a schedule for the task, on the **Schedule** tab, select **Enable this schedule**. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run. For more information, see the New Discovery Task dialog Help.
- 8 To receive notifications for the task, click the **Alerts** tab and select **Enable alerts on changes**. Select the alert criteria and enter the email address to which notifications should be sent. For more information see the New Discovery Task dialog Help.
- 9 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 Modify the task's **Name** and **Description** as needed.
- 3 From the **Discovery Settings** list, 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 From the **Discovery Filename** list, modify the discovery file (.dis) you want to use with the discovery task. This file is used to save the results of the scheduled discovery task.
- 5 To edit a schedule for the task, on the **Schedule** tab, ensure **Enable this schedule** is selected. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run. For more information, see the New Discovery Task dialog Help.
- 6 To receive notifications for the task, click the **Alerts** tab and ensure **Enable alerts on changes** is selected. Modify alert criteria as needed and enter the email address to which notifications should be sent. For more information see the New Discovery Task dialog Help.
- 7 Click **OK**. The New Discovery Task dialog closes and the modified task appears in the **Discovery Tasks** list.

To copy an existing discovery task:

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

To check the current status of a discovery task:

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

To start a discovery task:

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

To stop a running discovery task:

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

To close the dialog:

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

Configuring and scheduling Subnet Scan Tasks

Subnet scan tasks are tasks that have been created to run discovery scans on a schedule for your network subnets. The subnet scans are created using the Discovery Settings dialog or the Getting Started with IP Address Manager 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 subnet scan task:

- 1 Click **Discover > Discovery Tasks**. The Discovery Task dialog appears.
- 2 Click **Add** to configure a new Subnet Scan Task. The Select a Discovery Task Type dialog appears.
- 3 Select **Subnet Scan Task**, then click **OK**.
- 4 The New Subnet Scan Task dialog appears.
- 5 Enter a **Name** and **Description** for the task.
- 6 From the **Discovery Filename** list, select the discovery file (.dis) you want to use with the task. This file is used to save the results of the scheduled discovery task.



Note: If you select to use a discovery file (.dis) that is not the currently loaded discovery file, the selected discovery file must be loaded before you continue to configure the subnet scan task.

- 7 To select the subnet(s) to include in the task, on the **Subnets** tab, click **Add**. The Select Subnets dialog appears.
- 8 Select a single or multiple subnets, then click **OK**. The subnet(s) is added to the task.
- 9 To enable a schedule for the task, on the **Schedule** tab, select **Enable this schedule**. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run. For more information, see the New Subnet Scan Task dialog Help.
- 10 To receive notifications for the task, click the **Alerts** tab and select **Enable alerts on changes**. Select the alert criteria and enter the email address to which notifications should be sent. For more information see the New Subnet Scan Task dialog Help.
- 11 Click **OK**. The New Subnet Scan Task dialog closes and the new task appears in the **Discovery Tasks** list.

To edit an existing subnet scan task:

- 1 Select an existing subnet scan task, then click **Edit**. The Edit Subnet Scan Task dialog appears.
- 2 Modify the task's **Name** and **Description** as needed.
- 3 In the **Discovery Filename** box, edit the filename you want to use to save the details of the discovery task. This file is used to save the results of the scheduled discovery task.



Note: If you select to use a discovery file (.dis) that is not the currently loaded discovery file, the selected discovery file must be loaded before you continue to configure the subnet scan task.



Note: You cannot modify existing subnets; you must select and **Remove** irrelevant subnets and add new, relevant subnets.

- 4 To edit a schedule for the task, on the **Schedule** tab, ensure **Enable this schedule** is selected. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run. For more information, see the New Discovery Task dialog Help.
- 5 Optionally, add an **Exclude Scope** of IP address not to be included in the Subnet Scan. You can exclude single or multiple subnets, specific devices, or an IP scope. For more information, see the New Subnet Scan Task dialog Help.
- 6 To modify the task schedule, on the **Schedule** tab, ensure **Enable this schedule** is selected. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run. For more information, see the New Subnet Scan Task dialog Help.
- 7 To modify notifications for the task, click the **Alerts** tab and ensure **Enable alerts on changes** is selected. Select the alert criteria and enter the email address to which notifications should be sent. For more information see the New Subnet Scan Task dialog Help.
- 8 Click **OK**. The Edit Subnet Scan Task dialog closes and the modified task appears in the **Discovery Tasks** list.

To copy an existing subnet scan task:

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

To check the current status of a subnet scan task:

Select a subnet scan task, then click **Status**. The Discovery Task Status dialog appears.

To start a subnet scan task:

Select a subnet scan task, then click **Run Now**. The status of the selected task changes to *Running*. If the task completes successfully, the status changes to *Succeeded*.

To stop a running subnet scan task:

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

To close the dialog:

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

Configuring and scheduling DHCP Scan Tasks

DHCP scan tasks are tasks that have been created to run discovery scans on a schedule for your network DHCP servers. The DHCP scans are created using the Discovery Settings dialog or the Getting Started with IP Address Manager 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 subnet scan task:

- 1 Click **Discover > Discovery Tasks**. The Discovery Task dialog appears.
- 2 Click **Add** to configure a new DHCP Scan Task. The Select a Discovery Task Type dialog appears.
- 3 Select **DHCP Scan Task**, then click **OK**.
- 4 The New Subnet Scan Task dialog appears.
- 5 Enter a **Name** and **Description** for the task.
- 6 From the **Discovery Filename** list, select the discovery file (.dis) you want to use with the task. This file is used to save the results of the scheduled DHCP scan task.



Note: If you select to use a discovery file (.dis) that is not the currently loaded discovery file, the selected discovery file must be loaded before you continue to configure the subnet scan task.

- 7 To select the DHCP server(s) to include in the task, on the **Servers** tab, click **Add**. The Select Devices dialog appears displaying all currently discovered DHCP servers.
- 8 Select a single or multiple servers, then click **OK**. The server(s) is added to the task.
- 9 To enable a schedule for the task, on the **Schedule** tab, select **Enable this schedule**. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the DHCP scan to run. For more information, see the New DHCP Scan Task dialog Help.
- 10 To receive notifications for the task, click the **Alerts** tab and select **Enable alerts on changes**. Select the alert criteria and enter the email address to which notifications should be sent. For more information see the New DHCP Scan Task dialog Help.
- 11 Click **OK**. The New DHCP Scan Task dialog closes and the new task appears in the **Discovery Tasks** list.

To edit an existing subnet scan task:

- 1 Select an existing subnet scan task, then click **Edit**. The Edit DHCP Scan Task dialog appears.
- 2 Modify the task's **Name** and **Description** as needed.
- 3 In the **Discovery Filename** box, edit the filename you want to use to save the details of the discovery task. This file is used to save the results of the scheduled DHCP scan task.



Note: If you select to use a discovery file (.dis) that is not the currently loaded discovery file, the selected discovery file must be loaded before you continue to configure the subnet scan task.



Note: You cannot modify existing servers; you must select and **Remove** irrelevant servers and add new, relevant servers.

- 4 To edit a schedule for the task, on the **Schedule** tab, ensure **Enable this schedule** is selected. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the DHCP scan to run. For more information, see the New Discovery Task dialog Help.
- 5 To modify the task schedule, on the **Schedule** tab, ensure **Enable this schedule** is selected. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the DHCP scan to run. For more information, see the New DHCP Scan Task dialog Help.
- 6 To modify notifications for the task, click the **Alerts** tab and ensure **Enable alerts on changes** is selected. Select the alert criteria and enter the email address to which notifications should be sent. For more information see the New DHCP Scan Task dialog Help.
- 7 Click **OK**. The Edit Subnet Scan Task dialog closes and the modified task appears in the **Discovery Tasks** list.

To copy an existing subnet scan task:

Select an existing subnet scan task, then click **Copy**. The New DHCP Scan Task dialog appears with information from the copied task in the dialog fields, and *Copy of* and the name of the copied task in **Name**.

To check the current status of a subnet scan task:

Select a subnet scan task, then click **Status**. The Discovery Task Status dialog appears.

To start a subnet scan task:

Select a subnet scan task, then click **Run Now**. The status of the selected task changes to *Running*. If the task completes successfully, the status changes to *Succeeded*.

To stop a running subnet scan task:

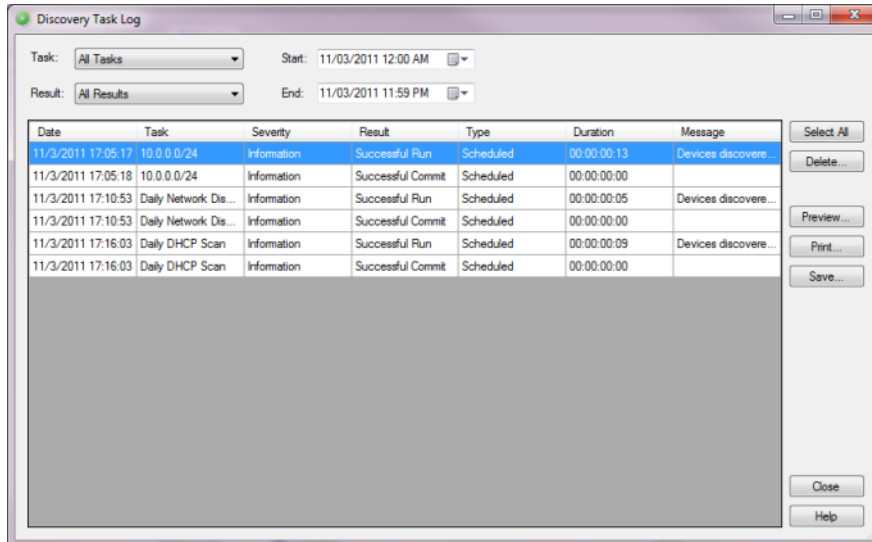
Select a running subnet scan task, then click **Stop**. The status changes from *Running* to *Canceled*.

To close the dialog:

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

About the Discovery Task Log

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



To use the Discovery Task Log:

- 1 From the IP Address Manager main menu, select **Discover > Discovery Task Log**. The Discovery Task Log dialog appears displaying logs for the default time period that begins on the current day at midnight and ends on the current day at 11:59 p.m.
- 2 Use the dialog options to select the log data you want to view. As you make selections, the log dynamically updates to display appropriate log information based on your selections.
 - Use the **Task** list to select to view log data for either a specific task or for all tasks. This list is populated with Discovery Tasks currently configured and stored in the Discovery Task Library.
 - Use the **Results** list to select to view log data for a specific task result or for all task results. This list is populated with all possible Discovery Task results. You can select to view *All Results*, *Canceled*, *Failed Commit*, *Failed Initialization*, *Failed Run*, *Successful Commit*, *Successful Initialization*, and *Successful Run*.
 - Use the **Start** and **End** option calendars to choose a beginning and end date for the time period for which you want to view discovery logs.

Log information

The Discovery Task Log displays the following log information:

- **Date.** The date the task attempted to run.
- **Task.** The name of the scheduled task that attempted to run. Discoveries run from the Run Discovery dialog also display in the Discovery Task Log and are listed as console Discoveries.
- **Severity.** The task's severity level; can be *Error*, *Information*, *Detail*, or *Diagnostic*.

- **Result.** The task's result.
 - *All Results* - all possible task results are displayed
 - *Canceled* - tasks canceled by the user
 - *Successful Initialization* or *Failed Initialization* - the success or failure of the steps taken to setup the discovery task (locating the discovery settings/credentials, loading the discovery file, etc.)
 - *Successful Run* or *Failed Run* - the success or failure of the discovery scan
 - *Successful Commit* or *Failed Commit* - the success or failure of the steps taken to save the discovery results and updating the log and any configurations



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

- **Type.** The task type. The Discovery Task Log displays only those task types that you have selected to view; if you have selected to view all task types, all task types are displayed.
- **Duration.** The elapsed time of the discovery scan.
- **Message.** If an error occurred, its details display here. If a task ran successfully, the message displays high level details about the task's results, such as the number of devices and subnets discovered.

Removing logs

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

To remove logs from the selected time period:

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

Previewing and printing logs

To print preview the Task Discovery Log:

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

To print the Task Discovery Log:

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

Saving logs

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

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

Merging Devices

You can merge devices from a previously discovered `.dis` file with the currently loaded `.dis` file.

To merge devices:

- 1 From the IP Address Manager main menu, go to **File > Merge Devices**.
- 2 Select the discovery file (`.dis`) you would like to merge with the currently loaded `.dis` file.

Importing Device Attributes

When you add device attributes to devices in one discovery file (`.dis`) and merge with another `.dis` file, device attributes are not automatically carried over. However, you can import device attributes.

To import device attributes:

- 1 From the IP Address Manager main menu, go to **File > Import Device Attributes**.
- 2 Select the discovery file (`.dis`) from which you would like to import device attributes to the currently loaded `.dis` file.

CHAPTER 4

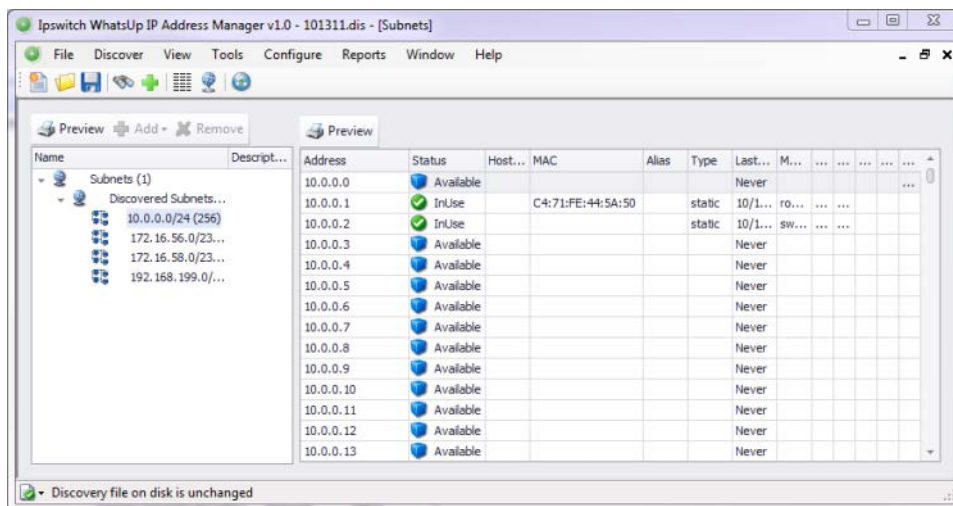
Using the IP Address Manager console

In This Chapter

About the IP Address Manager console.....	28
About network discovery files	30
Managing network discovery files	30
Collecting Device MIBs	32

About the IP Address Manager console

The IP Address Manager console is a Windows application used for discovering, configuring, and exporting network data.



The IP Address Manager console has the following components:

- Discovery through which you can discover networks or single devices

For more information on Discovery, see the *Discovering Networks in IP Address Manager* (on page 6) section.

- Several views by which to view network device data:
- Device List View
- Subnets View
- DHCP View

Using IP Address Manager

For more information on the views included in the IP Address Manager console, see the *Viewing Network Data* (on page 33) section.

- Tools to help you configure and monitor your network addresses
- Subnet Calculator
- IP Address History Event Viewer

For more information on the tools included in the IP Address Manager console, see the *Using IP Address Manager Tools* (on page 48) section.

- Configuration settings and libraries to help you configure IP Address Manager for your network
- Protocol Settings/Credentials Library
- Device Filters Library
- Device Type Mappings Library
- WUG Server Endpoint Library
- Email Settings
- Threshold Settings

For more information on the configuration settings and libraries included in the IP Address Manager console, see the *Configuring IP Address Manager* (on page 52) section.

- Reports on which you can view inventory information
- Available IPs
- Managed IPs
- Reserved IPs
- Duplicate IPs
- Leased IPs
- IP History
- DHCP Scopes
- DNS Records
- DNS Zones
- Subnets

For more information on the reports included in the IP Address Manager console, see the *Viewing IP Address Manager Reports* (on page 61) section.









- Scheduled Reports that send IP Address Manager reports on a regularly scheduled basis to the email addresses you specify

For more information on how to schedule reports, see the *Scheduling Reports* (on page 68) section.

About the IP Address Manager console shortcut menu

Use the IP Address Manager console shortcut menu to create, open, and save discovery files; to perform a network discovery; to discover single devices; and to access the Device List, Subnet, and DHCP views.



Icon	Action
	Click to create a new discovery file.
	Click to open a previously saved discovery file.
	Click to save the currently loaded discovery file.
	Click to perform a network discovery.
	Click to discover a single device.
	Click to access the Device List View.
	Click to access the Subnets View.
	Click to access the DHCP view.

About network discovery files

IP Address Manager 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 on which IP Address Manager is 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 network discovery files

There are several features available for you to manage discovery (.dis) files:

- Create a new discovery file
- Open an existing discovery file

- Merge devices in a current discovery file with devices 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, network data is loaded in the IP Address Manager console. You can save this network data to a discovery file that can be viewed and modified later.

To create a new discovery file:

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

Opening a discovery file

After starting the IP Address Manager console, you can open an existing discovery file.

To open an existing discovery file:

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

Opening a recently used discovery file

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

To open a recently used discovery file:

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

Using Merge Devices

The IP Address Manager console provides the capability to merge the current state of devices with the devices from another discovery file.

To merge the current set of devices:

- 1 From the IP Address Manager console, select **File > Merge Devices**. The Open Discovery File dialog appears.
- 2 Browse to locate the discovery file you want to open, then click **Open**. The device set from the selected file is merged with the current set of devices.

Using Save

The IP Address Manager console provides the capability to save the current network data model to a discovery file (.dis). Any modifications made to the network, such as added

Using IP Address Manager

devices through discovery, 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, if you did not do so already during discovery.

To save network data to the currently loaded discovery file:

From the IP Address Manager console, select **File > Save**. The file is saved.

Using Save As

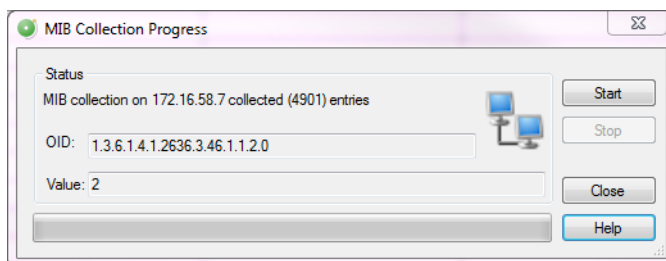
The IP Address Manager console provides the capability to save the current network data model to a discovery file. After an initial discovery, or if you want to save the network model to a different discovery file name, you can use the Save As feature.

To save network data to a discovery file:

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

Collecting Device MIBs

The MIB Collection Progress dialog displays IP Address Manager's progress as it collects MIB information from your network device.



To collect MIB information for a device:

- 1 In the Device List view, right-click the device for which you want collect MIB information. The right-click menu appears.
- 2 Select **Collect MIB data**. The MIB Collection Progress dialog appears.
- 3 Click **Start**. IP Address Manager begins collecting data for the device. The collection progress displays along the top and bottom of the dialog as the collection process takes place.



Tip: If you need to stop the scan before it completes, click **Stop**.

- 4 After the collection process completes, click **Close** to exit the dialog.

CHAPTER 5

Viewing network data

In This Chapter

About network data views	33
About Device List View.....	36
About Subnets View	40
About DHCP View.....	44

About network data views

The IP Address Manager console provides the capability of browsing network discovery results using a number of different views. The following views are provided in the IP Address Manager console:

- *Device List view* (on page 36)
- *Subnets view* (on page 40)
- *DHCP View* (on page 44)

The following sections describe how each view displays your network data.

About data grid views

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

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

Column filtering

Certain data grid views, such as the IP Address Manager Device List view, allow 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 IP Address Manager. When you close the current session of IP Address Manager, 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.

Remove selected devices

IP Address Manager 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 IP Address Manager.

To remove selected devices from a data grid view:

- 1 In a data grid view, select the devices you want to remove from the device list.
 - Press **Control** then select multiple non-contiguous devices in the list.
 - Press **Shift** to select multiple contiguous devices in the list.
- 2 Right-click in the data grid view. The right-click menu appears.
- 3 Click **Remove selected devices**. A confirmation dialog appears and asks if you are sure you want to delete the selected devices.
- 4 Click **Yes** to delete the selected devices or **No** to cancel the device deletion. If you clicked **Yes**, the selected devices are removed from the device list.

Print and Print Preview

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



Note: The print capability is disabled in the trial version of IP Address Manager.

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.

Copying to clipboard

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

To copy data items to the clipboard:

- 1 Click any item in the 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 clipboard contents paste into the application.

About Device List View

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

Host Name	IP Address	MAC Address	System Name	System Description	System OID	Device Category	Vendor	Model
	172.16.58.1	00:1...	QA-2821 ips...	Cisco IOS S...	1.3.6.1.4.1....	router	Cisco	Cisco 2821
	172.16.58.2	00:1...	CAT500	Cisco IOS S...	1.3.6.1.4.1....	switch	Cisco	cisco WS-C...
	172.16.58.3	C4:7...	QA-3750 ips...	Cisco IOS S...	1.3.6.1.4.1....	switch	Cisco	cisco WS-C...
	172.16.58.4	C4:7...	QA-2901.yo...	Cisco IOS S...	1.3.6.1.4.1....	router	Cisco	Cisco 2901 ...
	172.16.58.5	00:0...	QA-MSM320	MAP-330 - ...	1.3.6.1.4.1....	wireless-ap	HP/Colubris...	CN330
	172.16.58.6	00:0...	QA-X350	ExtremeXO ...	1.3.6.1.4.1....	switch	Extreme	summitX350...
	172.16.58.7	84:1...	QA-J2224	J2224 Switch	1.3.6.1.4.1....	switch	Juniper	EX2200
	172.16.58.8	F0:6...	QA-ProCurv...	ProCurve S...	1.3.6.1.4.1....	unknown	HP	
	172.16.58.13	00:1...	QA-Dell3324	Ethernet St...	1.3.6.1.4.1....	unknown	Dell	
	172.16.58.16	00:1...	QA-Enteras...	Enterasys N...	1.3.6.1.4.1....	unknown	Enterasys	
QAUPGRA...	172.16.59.1...	B8:A...	QAUpgrade...	Hardware: I...	1.3.6.1.4.1....	windowsser...	Microsoft	

You can filter data displayed in the view by using the **Device Filter** list.

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 33).




Tip: You can double-click any device in the Device List view. The *Device Details tab* (on page 38) view opens with more details about the device.

To view Device List:

From the main menu of the IP Address Manager console, select **View > Device List**. The Device List view appears.



Tip: You can also view device list from the IP Address Manager 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 *Viewing Device List details* (on page 38).

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). This column is not displayed by default.
- **NetBios Domain.** The windows NetBios domain (if supported and known). This column is not displayed by default.
- **SNMP Device.** Indicates whether the device is SNMP enabled by displaying either *Yes* or *No*. This column is not displayed by default.
- **System Name.** The MIB II system name.
- **System Description.** The MIB II system description.
- **System OID.** The MIB II system object ID.
- **Network Device.** A flag indicating whether this device is a network infrastructure device (i.e. routing, switching, forwarding network traffic). This column is not displayed by default.
- **Virtualization Type.** Indicates whether the device is a virtual representation of a real device; possible values are *VMWare* or *VirtualPC*. This column is not displayed by default.
- **Device Category.** Indicates to which category the device belongs (i.e. router, switch, hub, etc.).
- **Vendor.** The network device manufacturer.
- **Model.** The network device model number.

For information about adding columns that are not displayed by default, see *Column filtering* (on page 34).


About 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 IP Address Manager console, select **View > Device List**. The Device List view appears.




Tip: You can also view device list from the IP Address Manager 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 IP Address Manager console, select **View > Device List**. The Device List view appears.



Tip: You can also view device list from the IP Address Manager 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 IP Address Manager console, select **View > Device List**. The Device List view appears.



Tip: You can also view device list from the IP Address Manager 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.

- or -

Double-click a device. The Device Details list appears.

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

- **System**. Provides IP Address/MAC Address, MIB II information, product vendor, and other system information.
- **IP Addresses**. Provides IP Address configuration information.
- **Credentials**. Provides information about discovery protocol settings configured for this device.

- **DNS.** If the device is a DNS server, provides information about DNS zones.

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 33).

About the Device List View right-click menu

Right-clicking on a device in the device list provides the user with the following options:

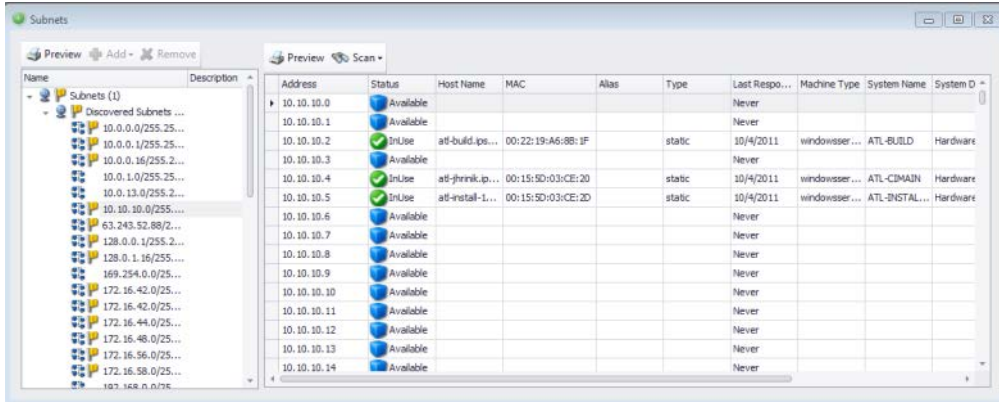
- **Edit Device Type Mapping(s).** Launches the SNMP OID to Device Type Configuration dialog displaying current settings. Add, edit, or delete OID maps as needed, then click **OK**.
- **Re-Discover Device.** Refreshes the network connection and updates any device information in the device list.
- **Remove selected devices.** Deletes selected device(s) from the device list.
- **Assign OID.** Launches the System OID assign dialog. Enter a System OID in the field provided, select **Reclassify device after assignment completion** if desired, then click **OK**.
- **Connect.** Allows you to connect to the device remotely using Telnet, SSH, Browse (Internet Explorer), or Remote Desktop Connection.
- **Ping.** Launches a command prompt window displaying data packets sent to the device and returned to the sender to verify network connectivity.
- **Send Wake-On-LAN.** Sends a special UDP message or sequence to the selected device to activate it.
- **Traceroute.** Launches a command prompt window displaying the path of data packets sent to the device and the length of time required for each hop.
- **Show IP History for.** Launches the IP Address History Log dialog. You can select options from the right-click menu directing the dialog to display historical data by **IP Address**, **MAC Address**, or **Hostname** and for a predetermined time interval of **Last 24 hours**, **Last 7 days**, **Last 30 days**, or for a **Custom** time interval.
- **Print Preview.** Generates and displays a device list report in DevExpress.
- **Print.** Launches the Print dialog in order to print a hardcopy of the Device List.
- **Save to CSV.** Launches the Save CSV File dialog in order to save an electronic copy of the device list.



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

About Subnets View

Use the IP Address Manager Subnets View for a visual representation of network subnets and to manage the IPs in discovered subnets.




The left side of the view displays the grouping of network subnets. The right side of the pane displays the subnets and IPs associated with their respective subnet group or subnet. The data grid view can be column sorted, print previewed, and printed. For more information about data grid views, see *About data grid views* (on page 33).

To view Subnets:

- 1 From the main menu of the IP Address Manager console, select **View > Subnets**. The Subnets View appears.



Tip: You can also view subnets from the IP Address Manager console shortcut menu. Click  (Subnets icon) to bring up the Subnets View.

- 2 Select a subnet in the left pane to view its information in the right pane.

Subnet View data

The Subnet View displays the following information for subnet groups.






- **Display Name.** The subnet's display name.
- **Address.** The subnet's IP address.
- **Mask.** The subnet mask.
- **CIDR.** The subnet CIDR.
- **Total IPs.** The total number of IP addresses in the subnet.
- **Managed.** The number of managed IP addresses in the subnet.
- **Last Discover.** The date and time the last subnet scan was performed for the subnet.
- **Location.** The physical location of the subnet.
- **VLAN.** The VLAN associated with the subnet.

Using IP Address Manager

- **Description.** Any subnet description.
- **IPs % used.** The percentage of total subnet IPs used.
- **IPs Available.** The number of IPs available on the subnet.
- **IPs Reserved.** The number of IPs currently defined as reserved via a DHCP reservation.
- **IPs Transient.** The number of IPs recently in use that were unresponsive as of the last subnet scan.
- **IPs In Use.** The percentage of IPs currently managed on the subnet.

The Subnet View displays the following information for individual subnets.

- **Address.** The subnet IP address.
- **Status.** The IP address status; see the table below for status possibilities and status icons.

Icon	Status
	Available - currently not in use; does not respond to ping.
	InUse - currently in use; marked as <i>Reserved</i> or <i>Leased</i> on a DHCP server and responds to ping.
	Leased - currently leased; marked as <i>Leased</i> on a DHCP server and responds to ping.
	Reserved - currently reserved; marked as <i>Reserved</i> on a DHCP server and responds to ping.
	Transient - recently in use but was unresponsive at last ping.

- **Host Name.** The host name associated with the subnet IP address.
- **MAC.** The MAC address associated with the subnet IP address.
- **Alias.** The alias associated with the subnet IP address.
- **Type.** The subnet IP address type; either *dynamic* or *static*.
- **Last Response.** The last time IP Address Manager received a response from the device assigned to the subnet IP address during a subnet scan.
- **Machine Type.** The machine type of the device associated with the subnet.
- **System Name.** The system name of the device associated with the subnet.
- **System Description.** The system description of the device associated with the subnet.
- **System Location.** The system location of the device associated with the subnet.
- **System Contact.** The system contact of the device associated with the subnet.
- **Comment.** Any comments listed for the subnet and/or its associated device.

Managing subnets

Using the Subnet View right-click menu, you can select to unmanage and manage subnets. By default, all discovered subnets are manageable; in order to comply with your IP Address Manager license, you may be required to unmanage addresses.

To unmanage a subnet:

Right-click a subnet, then select **Unmanage**. The subnet becomes inactive, indicated with a strike through.

To manage a subnet:

Right-click a subnet, then select **Manage**. The subnet becomes active.

Overwriting discovered data

You can overwrite discovered data by double-clicking in a field and entering new information. Information that has been manually updated is indicated in bold type. Data that is overwritten is not updated in subsequent subnet scans. If after manually updating information you decide to revert to discovered data, clear the field and the field repopulates with previously discovered data.



Note: All editable Subnet View fields are limited to a maximum of 512 characters.

Adding Subnet groups and subnets

You can add subnet groups and subnets to the subnet view by using the **Add** option at the top left of the screen.

To add a group:

Select the top-level Subnets group, click the down arrow next to **Add** to expand the list, and select **Group**. The Add Subnet Group dialog appears.

To add a subnet:

Select the top-level Subnets group, click the down arrow next to **Add** to expand the list, and select **Subnet**. The Add Subnet dialog appears.

Subnet scanning

To conduct a subnet discovery scan now, select a server from the left pane, right-click, then select **Scan Now**. The Run Now dialog appears.

- or -

Click the arrow next to **Scan** to expand the list, then select **Scan Now**. The Run Now dialog appears.

To schedule a subnet server discovery task, select a server from the left pane, right-click, then select **Schedule Scan**. The New Subnet Scan Task dialog appears.

- or -

Click the arrow next to **Scan** to expand the list, then select **Schedule Scan**. The Run Now dialog appears.

Printing

To preview and print the list of subnets, click **Preview** over the list of subnets.

To preview and print the devices associated with a selected subnet, click **Preview** over the list of IP devices.

About the Subnets View right-click menus

Right-clicking on a subnet in the navigation tree provides the following options:

- **Scan Now.** Launches the discovery dialog and discovers devices on the selected subnet.
- **Schedule Scan.** Launches the New Subnet Scan Task dialog. Schedule an upcoming scan using the procedures found in *Configuring Scheduled Reports* (on page 68).
- **Unmanage.** Strikes through the subnet in the navigation tree and removes applicable data from the display. To manage the subnet again, right-click on the subnet and select **Manage**.

Right-clicking on an address in the device list provides the following options:

- **Connect.** Allows you to connect to the device remotely using Telnet, Browse, RDP, or SSH.
- **Rediscover.** Refreshes the network connection and updates any device information in the Device List.
- **Ping.** Launches a command prompt window displaying data packets sent to the device and returned to the sender to verify network connectivity.
- **Traceroute.** Launches a command prompt window displaying the path of data packets sent to the device and the length of time required for each hop.
- **WakeOnLAN.** Sends a special UDP message (or sequence) to the selected device to activate it.
- **Show In Device List.** Adds the selected device and all applicable data to the Subnet List.
- **Add Duplicate Device.** Adds a copy of the selected device to the Subnet List.
- **Remove Duplicate Device.** Deletes selected device(s) from the Subnet List.
- **Unmanage.** Strikes through the address in the address list and removes applicable data from the display. To manage the device again, right-click on the address and select **Manage**.
- **Show IP History for.** Launches the IP Address History Log dialog. You can select options from the right-click menu directing the dialog to display historical data by **IP**

Using IP Address Manager

Address, MAC Address, or Hostname and for a predetermined time interval of **Last 24 hours, Last 7 days, Last 30 days**, or for a **Custom** time interval.

- **Set Status to.** Modifies the displayed status for an address to [**Default**], **Available, In Use, Leased, Reserved** or **Transient**.



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

About DHCP View

Use the IP Address Manager DHCP View for a visual representation of network DHCP servers and associated scopes.


IP Address	Name	Descrip...	Exclud...	Reserved	Leased	In Use	% Used	Available	Total
10.0.0.2	QA-290...			2	0	0	0	252	252
172.16.58.3	QA-375...			475	1	0	2	35	35
172.16.58.4	QA-290...			3	0	0	1	251	252
172.16.59.107	QA-WI...			0	1	17	22	82	83
192.168.199.2	QA-282...			0	0	0	0	0	0
192.168.203.2	DEV-28...			51	0	0	0	11	11

The left side of the view displays the grouping of network DHCP servers and server scopes. The right side of the pane displays the server/scope properties by scope, exclusion, options, and leases. The data grid view can be print previewed and printed.

To view DHCP servers:

- 1 From the main menu of the IP Address Manager console, select **View > DHCP**. The DHCP View appears.
- 2 Select a server in the left pane to view its information in the right pane.
- 3 Click a tab (**Scopes, Exclusions, Options, Leases**) to view server or scope information for that tab.



Tip: You can also access the DHCP View from the IP Address Manager console shortcut menu. Click  (DHCP icon) to bring up the DHCP View.

DHCP View data

The DHCP View displays the following information for DHCP Server groups.

- **IP address.** The DHCP server's assigned IP address.

Using IP Address Manager

- **Name.** The DHCP server's device name.
- **Description.** The DHCP server's description.



Note: This field is editable.

- **Excluded IPs.** The total number of IP address exclusions set for the server.
- **Reserved.** The total number of IP addresses currently reserved on the server.
- **Leased.** The total number of IP addresses currently leased.
- **In use.** The total number of IP addresses currently in use.
- **% used.** The percentage of IP addresses currently in use.
- **Available.** The percentage of IP addresses currently available for use on the server.
- **Total IPs.** The total number of IP addresses—used and available for use—on the server.

The DHCP View displays the following information for individual DHCP servers.

Scopes tab

- **Name.** The scope's name.
- **Range.** The scope's IP address range.
- **Description.** The scope's description.



Note: This field is editable.

- **Excluded IPs.** The total number of IP address exclusions set for the scope.
- **Reserved.** The total number of IP addresses currently reserved.
- **Leased.** The total number of IP addresses currently leased.
- **In use.** The total number of IP addresses currently in use in the scope.
- **% used.** The percentage of IP addresses currently in use in the scope.
- **Available.** The percentage of IP addresses currently available for use in the scope.
- **Total.** The total number of IP addresses—used and available for use—in the scope.

Exclusions tab

The exclusions tab lists any IP address ranges currently set to be excluded as available IP addresses on the DHCP server. Exclusions are listed for both the Server level and the Scope level.

Options tab

The Options tab lists the following options for Cisco DHCP servers.



Note: The Options tab does not display information for Windows DHCP servers; options information can be found on the Info tab for Windows server scopes.

- **Options.** Server options are assigned to all DHCP clients that lease an IP address from any scope configured on the server and apply to all scopes on the server; can be *Router, DNS Servers, Domain Name, and Lease Time*.
- **Value.** The respective value of the option.

Leases tab

- **IP.** The leased IP address.
- **MacAddress.** The MAC address to which the IP is assigned.
- **Expiration.** The date the lease terminates.
- **Type.** The lease type; either *manual* or *automatic*.

The DHCP View displays the following information for individual DHCP server scopes.

Info tab

- **Name.** The scope's name.
- **Description.** The scope's description.



Note: This field is editable.

- **Range Low.** The lowest IP address in the scope range.
- **Range High.** The highest IP address in the scope range.
- **Subnet.** The subnet on which the scope resides.



Note: The Info tab does not display information for Cisco DHCP server scopes; options information can be found on the Options tab for Cisco servers.

- **Options.** Scope options only apply to the specific scope for which they are configured; can be *Router, DNS Servers, Domain Name, and Lease Time*.

Reservations tab

- **IP.** The reserved IP address.
- **Mac.** The MAC address to which the reserved IP is assigned.

Exclusions tab

The exclusions tab lists any IP address ranges currently set to be excluded as available IP addresses on the scope.

DHCP server scanning

To conduct a DHCP server discovery scan now, select a server from the left pane, right-click, then select **Scan Now**. The Run Now dialog appears.

Using IP Address Manager

To schedule a DHCP server discovery task, select a server from the left pane, right-click, then select **Schedule Scan**. The New DHCP Scan Task dialog appears.

Printing

To preview and print the list of subnets, click **Preview** over the list of subnets.

To preview and print the devices associated with a selected subnet, click **Preview** over the list of IP devices.

CHAPTER 6

Using IP Address Manager Tools

In This Chapter

About IP Address Manager Tools	48
Using the Subnet Calculator.....	48
About the IP History Log.....	49
Classify Devices	51

About IP Address Manager Tools

IP Address Manager includes the following tools to aid you in configuring your network and monitoring network address and host allocation.

- *Subnet Calculator* (on page 48)
- *IP History Event Viewer* (on page 49)
- *Classify Devices* (on page 51)

Using the Subnet Calculator

The Subnet Calculator is used to calculate a range of subnets for a specific IP address based on the network bits, subnet bits, and host bits when setting up a network.

To use the Subnet Calculator:

- 1 Access the Subnet Calculator by selecting **Tools > Subnet Calculator** from the main menu.
- 2 Enter the IP address of the subnet you want to discover under **IPAddress**. The Binary, Octal, and Hexadecimal forms of the IP address entered display in the respective fields within the dialog.
- 3 To specify the number of one bits in the binary notation of the net mask, select a number 1-31 from the **Mask Bits** list, or alternately, select a specific net mask from the **Net Mask** list. The Subnet Calculator auto-fills applicable subnet information in the remaining fields within the dialog, including the initial **Subnet Results**.
- 4 The following subnet characteristics can be altered by selecting from the applicable lists within the dialog. **Subnet Results** update automatically as changes are made.
 - **Subnet Bits** - The number of subnet bits can range from 1-31 when the number of mask bits is set to 1. As the number of mask bits increases, the listed options for

subnet bits decreases. If the number of mask bits is set to 31, the number of subnet bits must be 31.

- **Subnet Mask** - The available range of subnet masks that may be applied decreases as the number of mask bits increases.
- **Number of Subnets** - The available number of subnets begins at 1. Each subsequent list option is the previous number multiplied by two and can be set as high as 536870912 when the number of mask bits is set to 1. As the number of mask bits increases, the listed options for number of subnets decreases. If the number of mask bits is set to 31, the number of subnets must be 1.
- **Host Bits** - The number of host bits can range from 1-31. As the number of host bits increases, the number of subnets decreases. Additionally, if the number of mask bits is altered, the number of host bits automatically changes so the sum of the two numbers is equal to 32.
- **Hosts per Subnet** - The available hosts per subnet begins with 2(RFC3021) and 2. Each subsequent list option is the previous number multiplied by 2, minus 2 ($2x - 2$) and can be set as high 2147483646 when the number of mask bits is set to 1. As the number of mask bits increases, the listed options for hosts per subnet decreases. If the number of mask bits is set to 31, the number of hosts per subnet must be 2(RFC3021).



Note: RFC3021 designates a document which defines a scenario where there is a single host bit and the subnet and broadcast addresses double as hosts. 2(RFC3021) is only for point to point connections.

- 5 The following subnet characteristics are also displayed within the dialog and automatically update as changes to other fields are made, but may not be altered directly by the user:
 - **Inverse (Wild Card) Mask** - The inverse mask indicates how many hosts are in a subnet and is calculated by subtracting each of the 4 sections of the subnet mask from 255. If only the last section of the inverse mask is used, it is the number of hosts per subnet plus 1.
 - **Subnet Bitmap** - The subnet bitmap is a visual representation of the subnet using algebraic variables in place of numbers. 'n' represents network or mask bits which indicate the total amount of space available. 's' represents subnet bits minus network bits which indicate how many subnets are available. 'h' represents host bits which indicate the number of hosts in a subnet. If the subnet bits increase, the host bits decrease, and vice versa.

About the IP History Log

The IP History Log displays event history, such as allocation and status change, for IP addresses, MAC addresses, and hostnames during the specified time period.

To use the IP Address History Log:

- 1 From the IP Address Manager main menu, select **Tools > IP History Event Viewer**. The IP Address History Log dialog appears. Initially, the log is empty. You must first specify

search criteria and specify a time period for which to view history information before performing a search.

- 2 Use the dialog options to select the history data you want to view.
 - Use the Search Criteria **IP Address(es)**, **Hostname**, and **MAC Address** lists to specify the criteria for which you want to view history. The IP Address list is populated with IP Addresses for which you have performed discovery scans.
 - Use the **Start** and **End** option calendars to choose a beginning and end date for the time period for which you want to view discovery logs.
- 3 After you specify appropriate search criteria and the time period for which you want to view history information, click **Search**. The IP Address History Log displays the history results according to your search criteria.

History information

The IP Address History Log displays the following log information:

- **Date/Time**. The date and time of the log.
- **Source**. The log source.
- **IP Address**. The IP address.
- **MAC Address**. The MAC address.
- **Hostname**. The device hostname.
- **Status**. The status address at the time of the log.
 - New - when a device is added to the IP binding
 - Not Found - when a previously discovered subnet is not found it is listed as not found
 - Replaced - when a device assigned to a particular IP address is replaced
 - InUse - when a device at a particular IP address responds to ping or another discovery protocol
 - Leased - when a DHCP server shows a lease for an IP address
 - Reserved - when a DHCP server shows a reservation for an IP address
- **Message**. The log message.
- **NetBios Name**. The NetBios name.
- **Name**. The device name.

Previewing, exporting, and printing logs

To print preview the IP Address History Log:

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

To export the IP Address History Log:

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

- 2 Select **File > Export Document**. A flyout menu appears. Select the format to which you want to export the log. You can select to export to *.pdf, HTML, .rtf, .xls, XLSX, .csv, text, or image*. The Export Options for the file format you selected appear.
- 3 Specify export options, then click **OK**. The Save As dialog appears.
- 4 Specify a name for the file and the location to which to save the file, then click **Save**.

To print the IP History Log:

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

Saving logs

To save the IP History Log as a .csv file:

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

Classify Devices

The Classify Devices feature reruns the device classifier after the device type configuration has been changed. With this feature, you can enter mappings into the Device Type Configuration and run Classify Devices to update all device categories.

To run Classify Devices:

From the main menu of the IP Address Manager console, select **Tools > Classify Devices**. The Classify Devices tool runs.

Configuring IP Address Manager

In This Chapter

About configuration settings.....	52
Configuring Discovery Settings.....	52
Configuring Protocol Settings/Credentials.....	53
Configuring Device Filters.....	54
Configuring Device Type Mappings.....	57
WhatsUp Gold Server Endpoint Library (Remote Servers)	58
Configuring Email Settings	59
Configuring Thresholds.....	60

About configuration settings

IP Address Manager provides a variety of configuration setting options to help you optimize IP Address Manager for your network.

- *Discovery Settings* (on page 52)
- *Protocol Settings/Credentials* (on page 53)
- *Device Filters* (on page 54)
- *WhatsUp Gold Server Endpoint Library (Remote Server)*
- *Email Settings* (on page 59)
- *Thresholds* (on page 60)

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.

Creating, editing, or deleting discovery settings

To create a new set of discovery settings:

- 1 From the main menu of the IP Address Manager 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 IP Address Manager 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 IP Address Manager 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 IP Address Manager 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 that you want to use for network discovery.

- **SNMPv1** discovery requires the SNMP read community information, timeout settings, and retry counts.
- **SNMPv2** discovery requires the SNMP read community information, timeout settings, and retry counts.
- **SNMPv3** discovery requires the associated Username, timeout settings and retry counts. Optionally, you can select to use Authentication and Encryption.
- **SSH** requires the User Name, Password, and Port used to make an SSH connection.
- **Telnet** requires the User Name, Password, and Port information used to make a Telnet connection. Telnet credentials are used to support the Map Capture Config tool that starts Backup Running Configurations and Backup Startup Configurations.
- **Windows** device discovery requires WMI information, Domain\UserID and Password, to connect to Windows devices. Windows credentials are used to collect software inventory information from Windows systems.



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

To configure Protocol Settings:

From the main menu of the IP Address Manager 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 **Copy**. The new copy of the credentials dialog appears.
- 2 Make any required changes to create new credentials, then click **OK**.

To delete a set of protocol credentials:

- 1 Select a set of protocol credentials, then click **Delete**. The protocol setting is deleted from the list.
- 2 Click **OK** to save changes.

To import protocol credentials from WhatsUp Gold:

- 1 Click **Import**. The Import Credentials dialog appears.
- 2 From the WhatsUp Gold Server list, select a WhatsUp Gold Server endpoint from which to import credentials or click browse (...) to open the WhatsUp Gold Remote Server dialog to Add, Edit, Copy, or Delete WhatsUp Gold remote servers from which to import credentials.
- 3 Click **Import**. IP Address Manager imports all of the currently configured credentials from the selected WhatsUp Gold server Credentials Library, and they appear in the Protocol Settings/Credentials dialog.

To selectively Assign or Unassign protocol credentials to device(s):

- 1 Select a credential you want to manually assign to device(s), then click Assign or Unassign. The Select Devices dialog appears.
- 2 Select one or **Ctrl** + select multiple devices to assign the credential to device(s).
- 3 Click **OK** to apply credentials to the selected device(s).

Configuring Device Filters

Device filters allow you to filter reports so that only the network information you want is displayed. You can customize the filter to display information about:

- All of your devices, including endpoint devices, such as servers and workstations.
- Only your network devices.

- Only those devices that have SNMP credentials.

You can create filters for categories of devices, individual IP addresses, IP ranges, subnets, VLANs, or combinations of these elements.

Device Categories

Device categories are used in filters to narrow your report to a specific group of network devices. The default categories list includes network devices, end devices, and devices with specific operating systems. You can add custom device categories for use in grouping devices in ways not available with the default device categories. When you create a custom device category, it will appear on the list and you will be able to select it when you are creating device filters. For more information on device categories, see [Configuring Device Categories](#).

Advanced Filtering

Device filters provide advanced filtering options that allow you to filter device lists, topology maps, and reports to provide information for individual IP addresses, ranges of IP addresses, subnets and VLANs.

Click **Name/IP Address** to add hostnames or IP addresses to the filter. You can filter your report on specific hostnames, for example you could filter a report to display only information about your payroll database server, `payroll.company.com`, or you could list a group of servers by hostname, such as the servers in a DMZ, `dmz.firewall1.company.com`, `dmz.externalweb.company.com`, and `dmz.externalweb.backup.company.com`. You can also filter using a single IP address, or multiple IP addresses. You can filter on an IP range such as `10.0.3.1 - 10.0.3.200` or a specific subnet. You can list a subnet using standard notation (`192.168.5.0/255.255.255.0`) or CIDR notation (`192.168.5.0/24`).

Creating, editing, copying or deleting a Device Filter

The following procedures provide instructions on how to create, edit, copy and delete device filters using the Device Filters dialog.

How to get to the Device Filters list dialog:

From the IP Address Manager menu, select **Settings > Device Filters**. The Device Filters list dialog appears.



Tip: Alternatively, click the browse (...) button on any of the reports to which a device filter can be applied to get to the Device Filters list dialog.

The Device Filters list dialog displays the name of each filter and the associated pseudo code representing what the filter will return.

To create or edit a device filter:

- 1 If you are creating a new filter, click **New** to create a new device filter. The Device Filter definition dialog appears.
- 2 If you want to edit an existing device filter, select a device filter, then click **Edit** to edit an existing device filter. The Device Filter definition dialog for the selected filter appears.

- 3 For the **Name**, enter the name you want to use to refer to the filter. This name is displayed in the Device Filter lists on all reports and maps that have filtering available.
- 4 Select the range of devices you want to include in the filter in the **Include devices matching** area. This option sets the device range by restricting the devices filtered to one of the following groups of devices:
 - **All Devices**. Select this option if you want the filter to be applied to all of the devices in the current discovery file.
 - **SNMP Devices Only**. Select this option if you want the filter to be applied only to those devices with an SNMP credential in the credential library.
 - **Network Devices Only**. Select this option if you want the filter only to be applied to network devices.
- 5 Use the options in the Advanced section to select specific hosts or VLANs to include in the filter.

Advanced. The Advanced filtering options filter for individual or ranges of IP addresses, host names, NetBIOS names, subnets, or VLANs. The following buttons invoke dialogs to enter values for the advanced filtering criteria.

- a) To restrict the filter to specific hostnames, IP addresses, IP address ranges or subnets, click **Hosts/IPs** . The Device Filter - Host/IP Address Include Scope dialog appears. Enter the hosts, IP addresses, and subnets you want to include in your filter, then click **OK**. The Device Filter - Host/IP Address Include Scope dialog closes.
 - **Host / System / NetBIOS Names**. Enter the hostname, system name or NetBIOS name of the device or devices you want the filter to select. When you list a name in this box, the filter will return only those devices with that name in the box. You can use a * character as a wildcard in this box. Click **Clear** to clear the Host / System / NetBIOS Names box.
 - **IP addresses / Subnets**. Enter the IP address, IP address range or subnet address (CIDR format) of the device or devices you want the filter to select. When you list one or more addresses or and address range for this option, the filter will return only those devices that match or fall within the indicated address range. Click **Clear** to clear the IP addresses / Subnets option.
- b) Click **VLANs** to open the Device Filter - VLANs dialog.

Enter the VLAN name or index from which you want the filter to select devices. Click **Clear** to clear the VLAN names or indexes.
- 6 Select the categories of devices you want to include in your device filter.

If you select any category, only devices that match that category appears. If you have not selected any devices, all devices that meet the other filter criteria appears.

 - Click **Select All** to select all of the categories. With all of the categories selected, IP Address Manager returns all devices.
 - Click **Unselect All** to de-select all of the categories. With all of the categories de-selected, IP Address Manager will return all devices within the device range.
 - **Filter summary**. Provides a pseudo-code representation of the filter.
- 7 Click **Preview** to see the list of devices returned by the filter. This list of devices appears in the map or report that uses this filter.

- 8 Click **OK**. The Device Filter definition dialog closes, and the device filter appears on the Device Filter list dialog.

To delete a device filter:

Select a device filter, then click **Delete** to delete an existing device filter. The selected device filter is removed from the Device Filters dialog.

To copy an existing device filter:

Select a device filter, then click **Copy** to copy an existing device filter. The Device Filter definition dialog appears with *Copy of <filter_name>* in the Name field where <filter_name> is the name of the filter you selected to copy. All of the filter criteria associated with the selected device filter is automatically selected.

Configuring Device Type Mappings

IP Address Manager Device Types allow you to link SNMP OID's with a specific device type, such as a Windows server. The SNMP OID to Device Type dialog displays all currently configured device types. Use this dialog to create or modify a custom device type mapping and to view device type information.

To configure a new device type:

- 1 From the main menu of the IP Address Manager console, select **Configure > Device Type Mappings**. The SNMP OID to Device Type Configuration dialog appears.
- 2 Click **New**. The Device Type Configuration dialog appears.
- 3 Enter the appropriate information into the dialog fields.
 - **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**. Optionally, enter the device vendor or manufacturer name.
 - **Model**. Optionally, enter the device vendor or manufacturer model.
 - **Description**. Optionally, enter the device vendor or manufacturer description.
- 4 Click **OK** to make changes.

To edit a device type:

- 1 From the main menu of the IP Address Manager console, select **Configure > Device Type Mappings**. The SNMP OID to Device Type Configuration dialog appears.
- 2 Select a Device Type, then click **Edit**. The Device Type Configuration dialog appears.
- 3 Enter the appropriate information into the dialog fields.
 - **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.** Optionally, enter the device vendor or manufacturer name.
 - **Model.** Optionally, enter the device vendor or manufacturer model.
 - **Description.** Optionally, enter the device vendor or manufacturer description.
- 4 Click **OK** to make changes.

To copy a device type:

- 1 From the main menu of the IP Address Manager console, select **Configure > Device Type Mappings**. The SNMP OID to Device Type Configuration dialog appears.
- 2 Select a Device Type, then click **Copy**. The Device Type Configuration dialog appears displaying the information of the Device Type you are duplicating.
- 3 Make changes as needed, then click **OK** to save changes.

To delete a device type:

- 1 From the main menu of the IP Address Manager console, select **Configure > Device Type Mappings**. The SNMP OID to Device Type Configuration dialog appears.
- 2 Select a Device Type, then click **Delete**. The Device Type is removed from the list and from any device to which it is assigned.

WhatsUp Gold Server Endpoint Library (Remote Servers)

Data that is imported from WhatsUp Gold to IP Address Manager requires that WhatsUp Gold servers (or endpoints) be defined to exchange data between the applications. Data shared between WhatsUp Gold and IP Address Manager is accessed using the `NetworkViewerDataService` in WhatsUp Gold. IP Address Manager import features communicate with the data service to access the WhatsUp Gold database.

If IP Address Manager is installed on a system with WhatsUp Gold installed, then a "Local Server" endpoint is added automatically to the remote servers (endpoint library). The "Local Server" endpoint cannot be deleted but it can be edited. Other remote servers can be created and edited similar to other libraries in WhatsUp Gold and IP Address Manager. WhatsUp Gold remote servers are stored in the `netview-viewer-config-user.xml` configuration file.

The WhatsUp Gold Remote Servers dialog lets you define and manage WhatsUp Gold servers for importing credential data from a IP Address Manager server.

Use this dialog to Add, Edit, Copy, and Delete WhatsUp Gold servers that will interact with IP Address Manager data.

The dialog displays the following WhatsUp Gold remote server information **Name**, **Description**, **Host Name/IP Address**, and **Port**.

To manage WhatsUp Gold remote servers:

- Click **New** to add a new WhatsUp Gold remote server.
- Select a WhatsUp Gold remote server, then click **Edit** to modify the server settings.
- Select a WhatsUp Gold remote server, then click **Copy** to make a duplicate of the server settings.
- Select a WhatsUp Gold remote server, then click **Delete** to remove it from the list.

Configuring Email Settings

Use The Configure SMTP Settings dialog to configure the default Email Settings for IP Address Manager.

To configure Email Settings for IP Address Manager:

- 1 Go to the Configure SMTP Settings dialog:
- 2 On the IP Address Manager console, select **Configure > Email Settings**. The Configure SMTP Settings dialog appears.
- 3 Specify or select the appropriate information in the dialog fields.
 - **Destination email address.** Specify the address that the Email action message should be sent.
 - **From email address.** Specify the address to be listed as "From" in the email sent by the Email action.
 - **SMTP server.** Specify the address of the server on which SMTP is running.
 - **Port.** Specify the port on which the SMTP service is listening. The standard SMTP port is 25.
 - **Timeout (sec).** Specify the amount of time (in seconds) that IP Address Manager should wait for a response from the SMTP server. If the time limit is exceeded, the email fails. The default timeout is 30 seconds.
 - **SMTP server requires authentication.** Select this option if your SMTP server requires user authentication.
 - **Username.** Specify the username to be used with SMTP authentication.
 - **Password.** Specify the password of the username to be used with SMTP authentication.
 - **Use an encrypted connection (SSL/TLS).** If your SMTP server supports encrypting data over a TLS connection (formerly known as SSL), select this option to encrypt SMTP traffic.
- 4 Click **OK** to save changes.



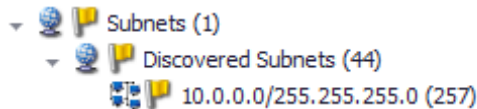
Tip: Click **Test** to send a test email to the destination email address specified above.

Configuring Thresholds

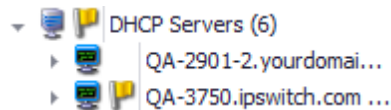
Use the IP Address Manager Thresholds dialog to configure thresholds that IP Address Manager will use to notify you when a subnet or DHCP scope is nearly full.

To configure thresholds:

- 1 Go to the IP Address Manager Threshold dialog:
- 2 On the IP Address Manager console, select **Configure > Thresholds**. The Configure SMTP Settings dialog appears.
- 3 Specify or select the appropriate information in the dialog fields.
 - **Subnet % Full.** Enter the numerical value for the percentage threshold. If a subnet reaches this value, IP Address Manager notifies you by displaying a yellow flag next to the subnet and next to the subnet group in which the subnet resides. The default threshold is 90% full.



- **DHCP % Full.** Enter the numerical value for the percentage threshold. If a subnet reaches this value, IP Address Manager notifies you by displaying a yellow flag next to the DHCP scope and next to the server on which the DHCP scope resides. The default threshold is 90% full.



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

Viewing IP Address Manager Reports

In This Chapter

About IP Address Manager reports.....	61
About the Available IPs report.....	62
About the Managed IPs report	62
About the Leased IPs report	63
About the Reserved IPs report.....	63
About the Duplicate IPs report.....	64
About the IP History report.....	64
About the DHCP Scope report.....	65
About the DNS Record report	66
About the DNS Zone report.....	66
About the Subnet Report	67

About IP Address Manager reports

The following reports display inventory information about your network devices and addresses.

- *Available IPs* (on page 62)
- *Managed IPs* (on page 62)
- *Reserved IPs* (on page 63)
- *Leased IPs* (on page 63)
- *DHCP Scopes* (on page 65)
- *DNS Records* (on page 66)
- *Subnets* (on page 67)
- *IP History* (on page 64)
- *Duplicate IPs* (on page 64)

About the Available IPs report

The Available IPs report provides a listing of IP addresses currently unassigned to any device and available for use. The report displays the following information:

- **Addresses** - Lists IP addresses on the network that are currently unassigned
- **Comment** - Indicates if the addresses displayed are a Range, Broadcast address, or Subnet address.

To view the Available IPs report:

On the main IP Address Manager menu, click **Reports**, then select **Available IPs**. The report is generated and displayed.

To filter the report by subnet:

Select the desired subnet from the list in the report toolbar. The report title displays the selected subnet instead of *All Subnets* and the report displays data applicable to the selected subnet.

About the Managed IPs report

The Managed IPs report provides a detailed view of IP addresses currently assigned to devices on the network. The report displays the following information:

- **Address** - Lists IP addresses currently leased to Mac addresses.
- **Status** - Displays the current status of the corresponding IP address.
- **Host Name** - Displays the name of a host associated with a specific IP address.
- **Mac** - Lists Mac addresses alongside their associated IP addresses.
- **Machine Type** - Describes the device on the network associated with a specific reserved IP address.
- **System Name** - Displays the name of the system associated with a specific reserved IP address.

To view the Managed IPs report:

On the main IP Address Manager menu, click **Reports**, then select **IPs In Use**. The report is generated and displayed.

To filter the report by subnet:

Select the desired subnet from the list in the report toolbar. The report title displays the selected subnet instead of *All Subnets* and the report displays data applicable to the selected subnet.

About the Leased IPs report

The Dynamic Host Configuration Protocol (DHCP) Lease Report provides a view of specific IP addresses on the network which are leased to corresponding Mac addresses and an indication of when each of those leases ends. The report presents the following information:

- **Address** - Lists IP addresses currently leased to Mac addresses.
- **Server** - Lists the servers for displayed IP addresses.
- **Host Name** - Lists the host name for displayed IP addresses.
- **Mac** - Lists Mac addresses alongside their associated IP addresses.
- **Machine** - Lists the hardware type for displayed devices.
- **Sys Name** - Lists the system names for displayed devices
- **Expiration** - Lists IP/Mac address lease expiration dates.

To view the Leased IPs report:

On the main IP Address Manager menu, click **Reports**, then select **Leased IPs**. The report is generated and displayed.

To filter the report by subnet, server, or scope:

Select the desired server, subnet, or scope from the list in the report toolbar. The report title displays the selected server, subnet, or scope instead of *All DHCP Servers* and the report displays data applicable to the selection.

About the Reserved IPs report

The Reserved IPs report provides a view of IP addresses which may or may not be in use but have been marked for future use by Mac devices on the network. The report presents the following information:

- **Address** - Displays the IP address that can only be leased by the specified Mac address.
- **Server** - Displays the Server associated with a specific reserved IP address.
- **Host name** - Displays the name of a host associated with a specific reserved IP address.
- **Mac** - Displays the Mac address associated with a specific reserved IP address.
- **Machine Type** - Describes the device on the network associated with a specific reserved IP address.
- **System Name** - Displays the name of the system associated with a specific reserved IP address.

To view the Reserved IPs report:

On the main IP Address Manager menu, click **Reports**, then select **Reserved IPs**. The report is generated and displayed.

To filter the report by subnet, server, or scope:

Select the desired subnet, server, or scope from the list in the report toolbar. The report title displays the selected subnet, server, or scope instead of *All Subnets* and the report displays data applicable to the selection.

About the Duplicate IPs report

The Duplicate IPs report provides a detailed view of IP addresses currently appearing more than once on the network. The report displays the following information:

- **Address** - Lists IP addresses currently appearing more than once.
- **Status** - Displays the current status of the corresponding IP address.
- **Host Name** - Displays the name of a host associated with a specific IP address.
- **Mac** - Displays the Mac address associated with a specific IP address.
- **Machine Type** - Describes the device on the network associated with a specific reserved IP address.
- **System Name** - Displays the name of the system associated with a specific reserved IP address.

To view the Duplicate IPs report:

On the main IP Address Manager menu, click **Reports**, then select **Duplicate IPs**. The report is generated and displayed.

To filter the report by subnet:

Select the desired subnet from the list in the report toolbar. The report title displays the selected subnet instead of *All Subnets* and the report displays data applicable to the selected subnet.

About the IP History report

The IP History report provides a detailed log of IP address activity on the network for a predetermined time interval of either 24 hours or 7 days. The report displays the following information:

- **Date/Time** - Displays the date and time of listed activity for a specific IP address.
- **IP** - Displays a specific IP address on the network.
- **Mac** - Displays the Mac address associated with a specific IP address.

- **Host Name** - Displays the name of a host associated with a specific IP address.
- **Status** - Displays the current status of a specific IP address.
- **Message** - Describes the activity that occurred at the given time applicable to the specific IP address.

To view the IP History report:

On the main IP Address Manager menu, click **Reports > IP History for**. Then select either **Last 24 hours** or **Last 7 days**. The report for the selected time interval is generated and displayed.

To filter the report by subnet:

Select the desired subnet from the list in the report toolbar. The report title displays the selected subnet instead of *All Subnets* and the report displays data applicable to the selected subnet.

About the DHCP Scope report

The Dynamic Host Configuration Protocol (DHCP) Scope Report provides a detailed view of IP address ranges and quantities on the network organized by subnet. The report displays the following information:

- **Subnet** - Displays the subnet address.
- **Range** - Displays the range of IP addresses included in the subnet.
- **Excluded IP** - Displays the number of IP addresses currently excluded from the subnet.
- **Reserved IP** - Displays the number of IP addresses within the subnet currently marked for future association with Mac addresses.
- **Leased IP** - Displays the number of IP addresses within the subnet currently in use on the network.
- **Available IP** - Displays the number of IP addresses within the subnet currently available for use on the network.
- **Total IP** - Displays the total number of IP addresses within the subnet.

To view the DHCP Scope report:

On the main IP Address Manager menu, click **Reports**, then select **DHCP Scopes**. The report is generated and displayed.

To filter the report by DHCP Server:

Select the desired server from the list in the report toolbar. The report title displays the selected server instead of *All DHCP Servers* and the report displays data applicable to the selected server.

About the DNS Record report

The Domain Name System (DNS) Record report provides a detailed view of DNS record data currently stored on the network. The report presents the following information:

- **Record Name** - Lists the names of each DNS record on the network.
- **Domain Name** - Lists the domain name for each corresponding DNS record.
- **Zone Name** - Lists the zone name for each corresponding DNS record.
- **Data** - Lists the IP addresses associated with each corresponding DNS record.
- **TTL (Seconds)** - Time To Live. Lists in seconds how long the DNS record information is cached.
- **Type** - Currently the only DNS record type reported is 'Address'.

To view the DNS Record report:

On the main IP Address Manager menu, click **Reports**, then select **DNS Records**. The report is generated and displayed.

To filter the report by server or zone:

Select the desired server or zone from the list in the report toolbar. The report title displays the selected server or zone instead of *All DNS Servers* and the report displays data applicable to the selection.

About the DNS Zone report

The Domain Name System (DNS) Zone report provides an overview of DNS zones and associated records on the network. The report presents the following information:

- **Name** - Lists the name of the DNS zones on the network.
- **Records** - Lists the number of records associated with each corresponding DNS zone.

To view the DNS Zone report:

On the main IP Address Manager menu, click **Reports**, then select **DNS Zones**. The report is generated and displayed.

To filter the report by server :

Select the desired server from the list in the report toolbar. The report title displays the selected server instead of *All DNS Servers* and the report displays data applicable to the selection.

About the Subnet Report

The Subnet report provides an overview of each subnet established on the network. The report displays the following information:

- **Name** - Lists the subnet/mask addresses.
- **Address** - Lists the IP address associated with each corresponding subnet and mask.
- **Pct Used** - Displays the percentage of IP addresses used on the subnet.
- **IPs in Use** - Displays the percentage of IPs currently managed on the subnet.
- **Total IPs** - Displays the total number of IP addresses on the network.

To view the Subnet report:

On the main IP Address Manager menu, click **Reports**, then select **Subnets**. The report is generated and displayed.

To filter the report by subnet:

Select the desired subnet from the list in the report toolbar.

CHAPTER 9

Scheduling Reports

In This Chapter

About the Scheduled Reports Library.....	68
Configuring Scheduled Reports.....	68

About the Scheduled Reports Library

The IP Address Manager Scheduled Report Library displays all reports to be generated and distributed automatically by IP Address Manager.

To access the IP Address Manager Scheduled Report Library:

- Select **Reports > Scheduled Reports** from the IP Address Manager main menu.

Use the IP Address Manager Scheduled Report Library to configure new or existing tasks.

- Click **Add** to add a new scheduled report to the list.
- Select an existing report , then click **Edit** to modify its configuration.
- Select an existing report , then click **Copy** to create a new task based on the selected task.
- Select an existing report , then click **Delete** to remove it from the list.
- Select a report , then click **Run Now** to generate and display the report immediately.

See *Configuring Scheduled Reports* (on page 68) for more detail on adding and editing scheduled report configurations.

Configuring Scheduled Reports

Scheduled reporting tasks are configured in IP Address Manager to generate and distribute reports automatically. They are created using the New Scheduled Report dialog and managed using the Scheduled Report Library. You can schedule a reporting task to run daily, weekly, monthly, yearly or on some other defined time interval.

To add a new reporting task to the Scheduled Report Library:

- 1 Click **Reports > Scheduled Reports**. The Scheduled Report Library dialog appears.
- 2 Click **Add**. The New Scheduled Report dialog appears.
- 3 Enter a **Name** and **Description** for the reporting task.
- 4 From the **Discovery Filename** list, select the discovery file (.dis) you want to use with the task. This file is used to save the results of the scheduled discovery task. To add a

new discovery file, click **Browse**. Navigate and select the desired discovery file to add it to the list.



Note: If you select to use a discovery file (.dis) that is not the currently loaded discovery file, the selected discovery file must be loaded before you continue to configure the scheduled report.

- 5 From the **Report Recipients** list, select the default recipient for the scheduled reports. To add additional recipients, enter valid email addresses in **Report Recipients**, separated by semi-colons.



Note: This feature requires valid SMTP settings; if you have not already configured your IP Address Manager Email Settings, click Email Settings to configure SMTP Settings for this and other IP Address Manager features.

- 6 To select which reports will be generated, on the **Reports** tab, click the **Add** button. The Scheduled Task Report dialog appears displaying the Available IPs: All Subnets report by default.
- 7 Under Report Settings, select the report to be included in the reporting task using the **Report** list, select the desired Subnet or DHCP Server filter using the **Filter** list, and select the format in which the report will be generated using the **Format** list. The configured report is previewed as list selections are made. Click **OK** to add the report to the scheduled reporting task and close the dialog. Repeat this step as needed to add additional reports to the scheduled reporting task.
- 8 To enable the scheduled report task, on the **Schedule** tab, select **Enable this schedule**. Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the scheduled reporting to run.
- 9 Click **OK**. The New Scheduled Report dialog closes and the new task appears in the Scheduled Report Library dialog.

To edit an existing scheduled reporting task:

- 1 Select an existing scheduled reporting task, then click **Edit**. The Edit Scheduled Report dialog appears.
- 2 Modify the **Description** as needed.
- 3 Click the **Browse** button to navigate and select a new discovery file if desired.
- 4 Add or remove **Report Recipients** as needed.
- 5 To modify specific details of a report associated with the scheduled reporting task:
 - On the Reports tab, select the report and click **Edit**. The Scheduled Task Report dialog appears.
 - Modify the **Report**, **Filter**, and/or **Format** using the applicable lists as needed and click **OK**.
- 6 To edit a schedule for the task:
 - On the **Schedule** tab, ensure **Enable this schedule** is selected.
 - Select the **Repeat interval**, **Start Time**, and other schedule details to create the schedule on which you want the discovery scan to run and click **OK**.
- 7 To delete a report from the scheduled reporting task, select the report, then click **Remove > Selected**. The scheduled reporting task is removed from the library. To

delete all reports from the scheduled reporting task, click **Remove > All** and click **Yes** when prompted.

- 8** To view a specific report as configured within the scheduled reporting task, select the report and click **Preview**.
- 9** To create a copy of a specific report within the scheduled reporting task, select the report and click **Copy**.
- 10** Click **OK**. The Edit Scheduled Report dialog closes.

To preview an existing scheduled reporting task:

Select an existing scheduled reporting task, then click **Run Now**. The applicable reports are generated and displayed in the proper format.

To copy an existing scheduled reporting task:

Select an existing scheduled reporting task, then click **Copy**. The Scheduled Task Report dialog appears with information from the copied task in the dialog fields.

To delete a scheduled reporting task:

Select an existing scheduled reporting task, then click **Delete**. The scheduled reporting task is removed from the library.

To exit the Scheduled Report Library:

Click **Close**. The Scheduled Report Library dialog closes.

Copyright notice

©1991-2011 Ipswitch, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the expressed prior written consent of Ipswitch, Inc.

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc., also assumes no liability for damages resulting from the use of the information contained in this document.

IMail, the IMail logo, WhatsUp, the WhatsUp Gold logo, WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

This document was published on Tuesday, November 29, 2011 at 14:08.