UVexplorer

User Guide

Copyright © 2022

Table of Contents

Getting Started 4
UVexplorer System Tray application 6
UVexplorer Installation 7
System Requirements 8
Installing UVexplorer 9
Updating UVexplorer 12
UVexplorer Activation 13
Activating UVexplorer 14
Updating UVexplorer License 16
Deactivating UVexplorer 18
License Execution Modes 20
Configuring UVexplorer 21
Application Skins 22
SMTP Email Server Settings 23
Discovering Networks 26
Starting Network Discoveries 27
Using the Discovery Wizard 31
Discovering a Single Device 36
Adding Device Notes 37
Saving Discovery Results 39
Selecting Discovery Results 41
Comparing Discovered Networks 43
Discovery Settings 46
Scheduling Network Discoveries 54
Scheduled Discovery Events 62
Opening Discovery Results 63
Discovery Tasks 65
Monitors 68
Monitored Devices 72
Configuring Monitors 75
Maintenance Policy 81
Monitor Device Picker 86
CPU/Processor Load 88
CPU History 91
Disk/Storage 92
Disk History 95
DNS Checks 96
HTTP Monitor 100
HTTP History 102
Ping/Latency Monitor 103
Ping History 106
Service (TCP) Port 108
SNMP IF Utilization 111
SNMP IF History 114
Custom SNMP Checks 116
SNMP History 119
WMI Counters 120
WMI History 123
Viewing Device Details 124
Selecting Devices 127

Selecting Monitor Devices ... 128
Network Connectivity ... 130
Manual Links ... 132
Device Filters ... 134
Selecting Device Filters ... 138
Device Preview ... 139
Network Topology Maps ... 140
Exporting Topology Maps ... 158
Map Draw Settings ... 160
Laying Out Map Node Children ... 162
UVexplorer Views ... 163
Startup Page ... 169
Backstage View ... 171
Ribbon Menu ... 174
Device Group/Category views ... 178
Device Groups ... 185
Device Group Editor ... 188
Device Group Folder Editor ... 192
Events ... 193
Reports ... 195
Help Desk ... 199
Using Network Tools ... 200
IP/MAC Address Finder ... 201
Layer 2 Trace ... 205
Startup vs. Running Configuration ... 208
Configuration Capture ... 213
DNS/Hostname Audit ... 215
Port Scanner ... 217
SNMP MIB Walker ... 220
Ping Response Poller ... 222
CPU Load Poller ... 224
Interface Status Poller ... 226
Managing Device Credentials ... 228
Configuring SNMP Communities ... 230
Configuring SNMP V3 Users ... 232
Configuring Windows (WMI) Credentials ... 234
Configuring Telnet Credentials ... 235
Configuring SSH Credentials ... 237
Configuring HTTP(s) / WEB Credentials ... 239
Configuring VMWare Credentials ... 241
Configuring PRTG Credentials ... 242
Capturing Device Configurations ... 243
Capturing Device Configurations ... 244
Selecting Configuration Capture Credentials ... 247
Saving Configuration Captures ... 248
Viewing Configuration Captures ... 249
Understanding Configuration Capture Scripts ... 250
Configuration Task Progress ... 252
Comparing Device Configurations ... 255
Supported Devices ... 260
PRTG Connector ... 261
Exporting to PRTG ... 262
PRTG Export Wizard ... 266
Scheduled Discovery PRTG Export ... 269

Topology Map PRTG Export 271
PRTG Export Templates 275
PRTG Devices 277
PRTG Sensors 278
PRTG Status Monitor 279
PRTG Status History 282
PRTG Server Settings 283
Support Tools 285
Master Network 286
Network Cleaner 288
Conclusion 291

Welcome to UVexplorer

UVexplorer is a network discovery and visualization application that can be used to quickly discover, and inventory devices attached to an IP network.
At the heart of UVexplorer is a discovery engine that utilizes detailed discovery data to build a comprehensive connectivity model of all devices connected to the IP network.

Discovery / Mapping

UVexplorer uses industry-standard protocols, such as ICMP, SNMP, and Windows (WMI), to find devices on your network. The information gathered during the discovery process can be seen through explorer-type views and detailed network topology maps. The detailed discovery results enable the use of advanced network management tools that simplify and automate common network management and troubleshooting tasks.

Use the Network Discovery Wizard to get started discovering your network.

See Discovering Networks to learn more about discovering your networks and managing your discovery results.

Documenting

UVexplorer allows network administrators to maintain a historical view of their network and network changes. In addition to the many tools and views available within UVexplorer, the discovered network information is also available in advanced reports which can be saved or printed in a variety of formats, including PDF, HTML, and CSV.

See Reports to learn more about available network discovery reports.

Discovering Differences

Whether network information is discovered on a regular basis using Scheduled Discoveries, or manually; the historical view of your network provides a powerful way to compare and discover changes to your network over time. Network Administrators can view network differences in reports generated by discovery tasks or by using the network comparison tool that provides a powerful way to compare network discovery snapshots.

See Comparing Discovered Networks to learn more about discovering network differences.

Monitoring

UVexplorer provides network administrators with customizable monitors to keep track of and be alerted of real-time device status. Using monitors such as Ping/Latency or CPU/Processor Load an administrator can be alerted of any unexpected changes in network performance or availability.

See Monitors to learn more about configuring and managing device and network monitors.

Assistance

UVexplorer has a lot of features and capabilities. If you'd like to schedule a 45-minute webinar with a Product Specialist to help you with your setup, please email UVadmin@UVnets.com, call (801) 801.871.5071 or schedule the webinar here: https://calendly.com/uvexplorer

UVexplorer System Tray application

To support Scheduled tasks UVexplorer is installed as a system tray application. When UVexplorer is opened it will run as a system tray service. Running as a system tray service allows the application to run scheduled tasks, such as network discovery, when the application is closed.

When exiting from the application you will be presented with the option to close the application entirely or minimize it to the system tray.

If the application is minimized to the system tray it will continue to run as a service and will run any enabled scheduled tasks during that time. The UVexplorer system tray icon is displayed with the running tray services using the UVexplorer logo. To re-open the application you can select the 'Show' menu item on the tray services context menu.

If the application is closed the entire application will be closed, including the service running in the system tray, and any scheduled discoveries will not run. If a discovery is running at the time the application close attempt is made you will be notified and given the option to allow the application to continue to run.

UVexplorer Installation

In this section:

System Requirements
Installing UVexplorer
Updating UVexplorer

System Requirements

UVexplorer is designed to be run as a long running process that will constantly discover and monitor your network. To this end it is recommended that UVexplorer be installed on a machine that remains running such as a server with the following specifications:

Operating System

UVexplorer will run on the following 32- and 64-bit windows operating systems

Windows Server 2003/2008/2012/2016/2019/2022
Windows 7 / 8 / 8.1 / 10 / 11

UVexplorer will run on virtual machines. If a virtual machine is used, a static MAC address is required for licensing to work correctly.

.NET Framework

UVexplorer is a .NET based application and requires Microsoft .NET Framework 4.5.2 or higher (Extended/Full versions). Microsoft .NET Framework 4.5.2 can be downloaded from the Microsoft website.

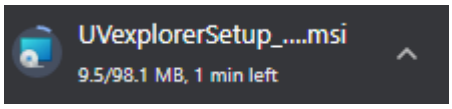
Hardware

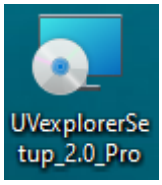
Component	Minimum Requirement
Processor	2 GHz
Memory	4 GB
Available Disk Space	4 GB
Network Interface card	100 Mbps
Display	1024 x 768

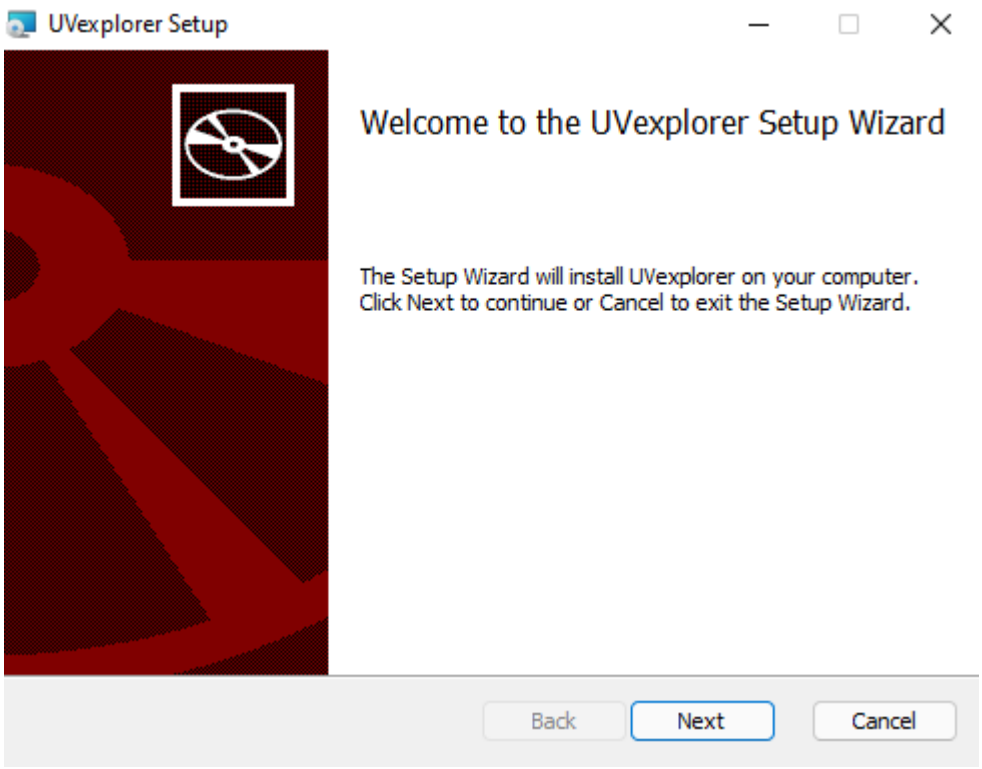
Installing UVexplorer

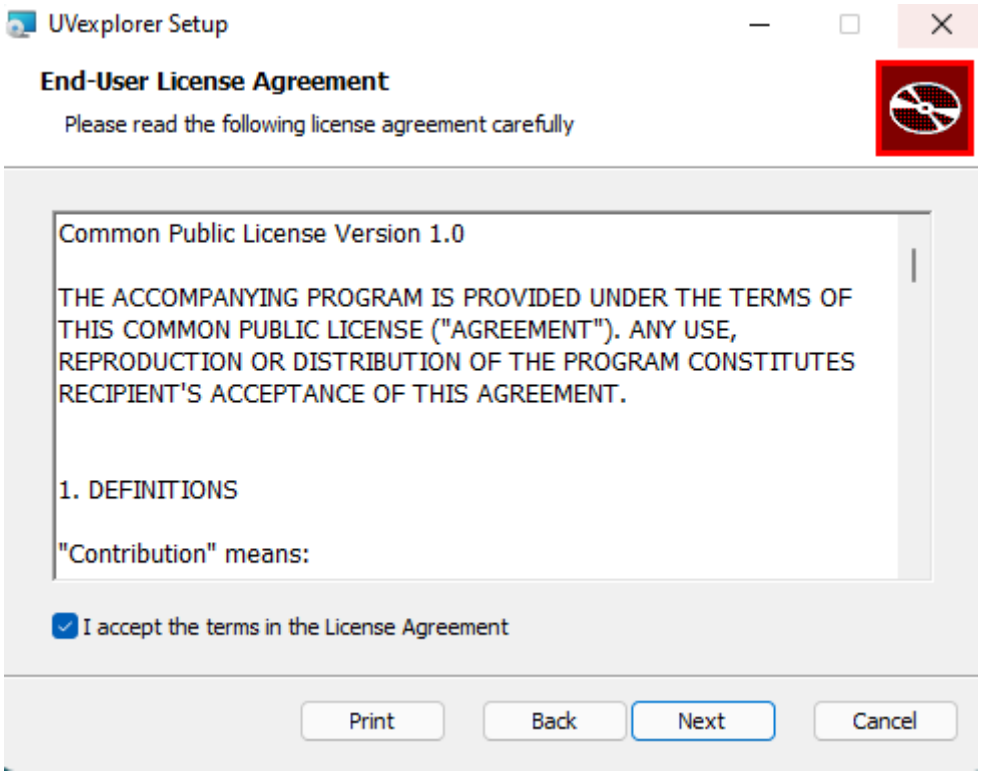
UVexplorer is installed using a Microsoft installer package. The installer package can be downloaded from the UVnetworks website. A link to download the file is provided when you register for a product license. If you received an installation package without registering for a product license you will be able to run UVexplorer with limited functionality. See License Execution Modes for more information.

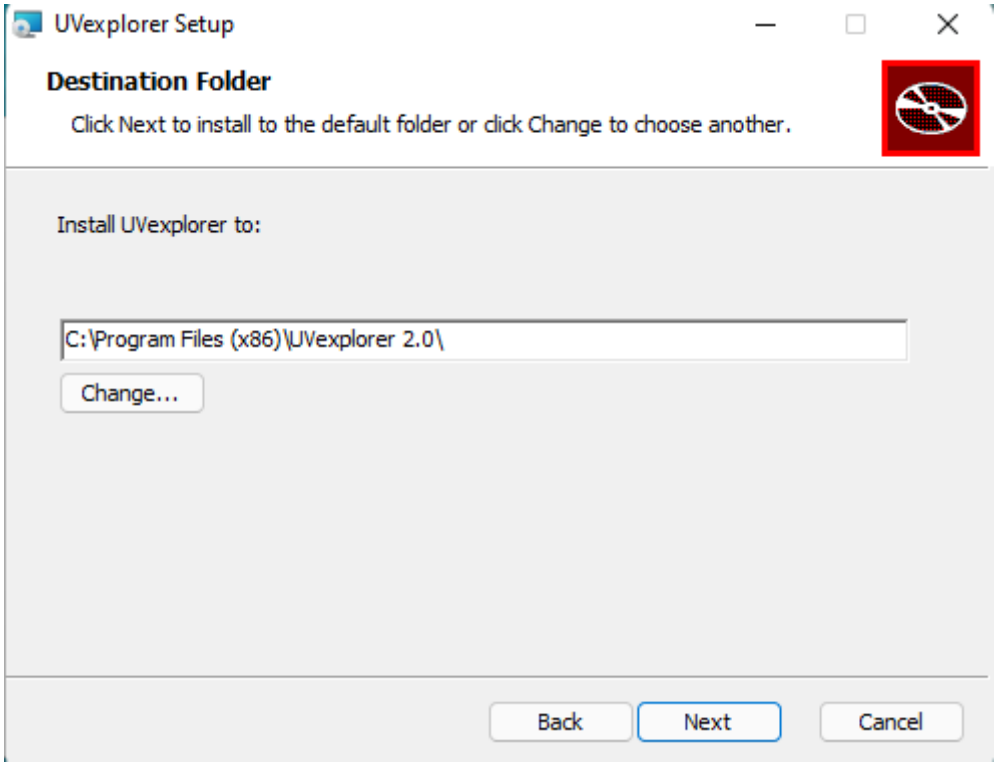
To install using the Microsoft installer package, launch the installer and follow the steps in the installation wizard.

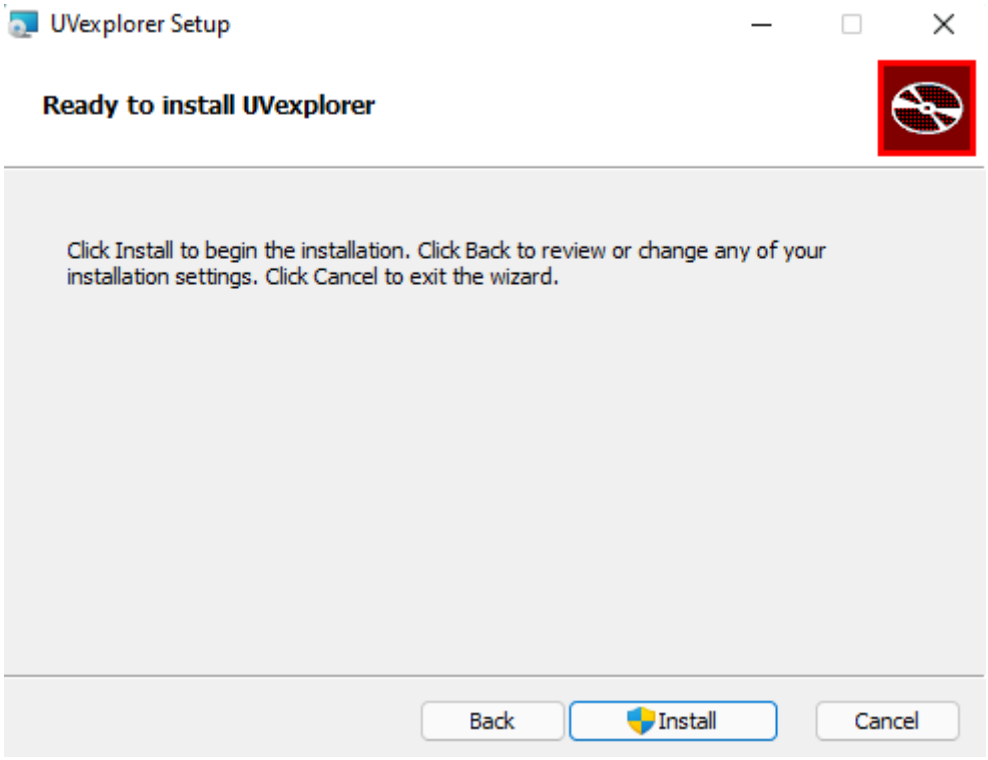






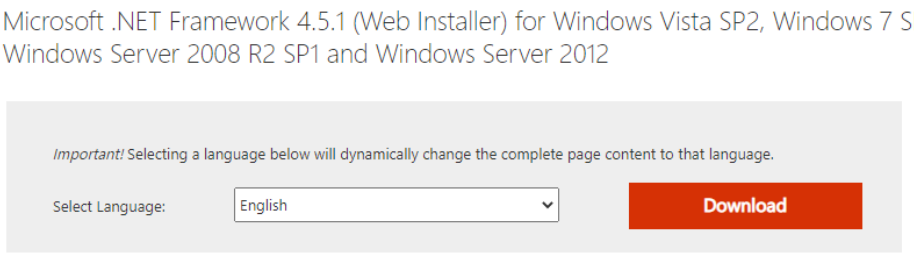

UVexplorer Setup
End-User License Agreement
Please read the following license agreement carefully
Common Public License Version 1.0
THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.
1. DEFINITIONS
"Contribution" means:
I accept the terms in the License Agreement
Print
Back
Next
Cancel


UVexplorer Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install UVexplorer to:
C:\Program Files (x86)\UVexplorer 2.0\
Change...
Back
Next
Cancel



.Net Framework

UVexplorer requires .NET Framework 4.5.1 (Extended/Full version) be installed before the application will run. .NET Framework 4.5.1 can be downloaded from the Microsoft website.

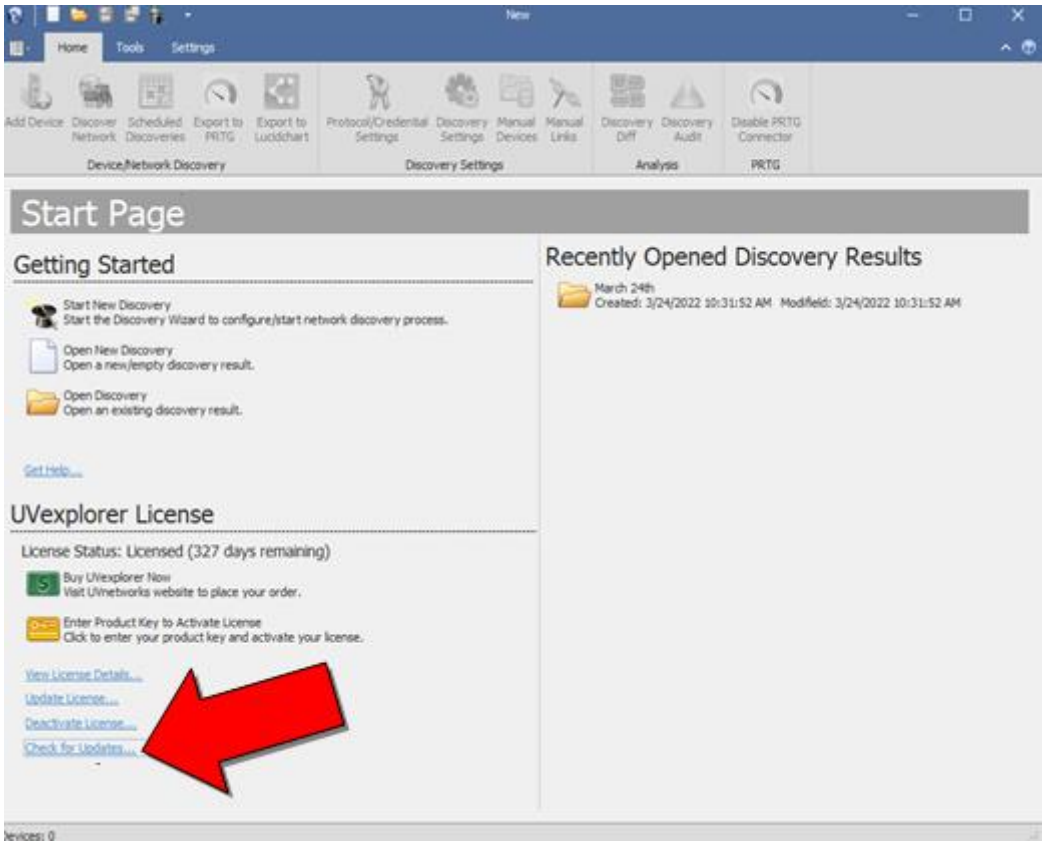


Updating UVexplorer

Updates to UVexplorer, including bug fixes and new features, may be made available from time to time. To update UVexplorer you may use the update utility.

Update Utility

The update utility allows you to check for and install any new updates to UVexplorer. The update utility is available on the Startup Screen of the application in the UVexplorer License section.



Check for Updates

To check for updates, select the 'Check for Updates...' link. UVexplorer will check for updates and display the results to the right of the link. If an update is available the update icon will appear. If the product is up to date a message indicating the application is current will appear.

Viewing Changes in the Update

The changes in the update can be viewed by selecting the update icon and choosing the 'View Changes in Version' option. A dialog containing the changes along with the option to update the application will appear.

Installing the Update

If an update is available it may be installed by selecting the update icon and choosing the 'Download and Update Now' option. Once selected the update will be downloaded. To complete the installation of the update the application must be restarted.

UVexplorer Activation

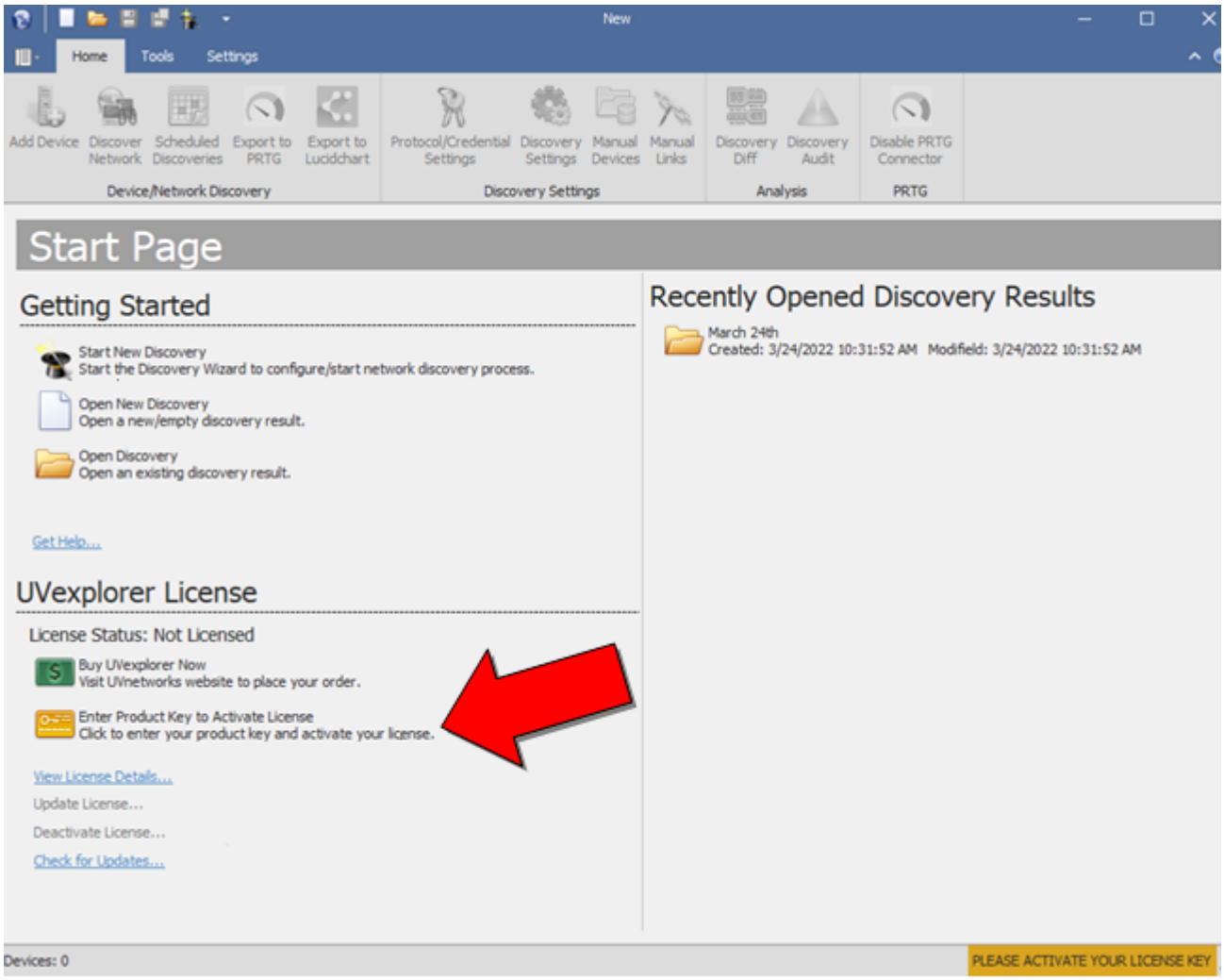
In this section:

Activating UVexplorer
Updating UVexplorer License
Deactivating UVexplorer
License Execution Modes

Activating Your UVexplorer License

After installing UVexplorer, you should register your installation with the UVnetworks licensing server. This process is called 'activating your license',and will give you access to UVexplorer 's features. To activate your license, click the 'Enter Product Key to Activate License' icon on the Start Page that appears when you run UVexplorer. Doing so will display the license activation wizard, which will step you through the process of license activation.

To activate your license, you will need the 'product key' that was emailed to you when you purchased the product or requested a free trial. Your product key will begin with 'P-' (for example, P-FR5V-IK7D-D3T3-YJCT-SZM3-6Q24-7HGV). If you did not go to the UVnetworks web site to purchase the product or request a free trial, you will need to do so in order to get a valid product key. The activation wizard provides a link you can click on to obtain a product key if you do not already have one.
NOTE: Your product key can only be activated on one computer at a time. If you want to use your product key on a different computer, you will need to first de-activate the key on the current computer.



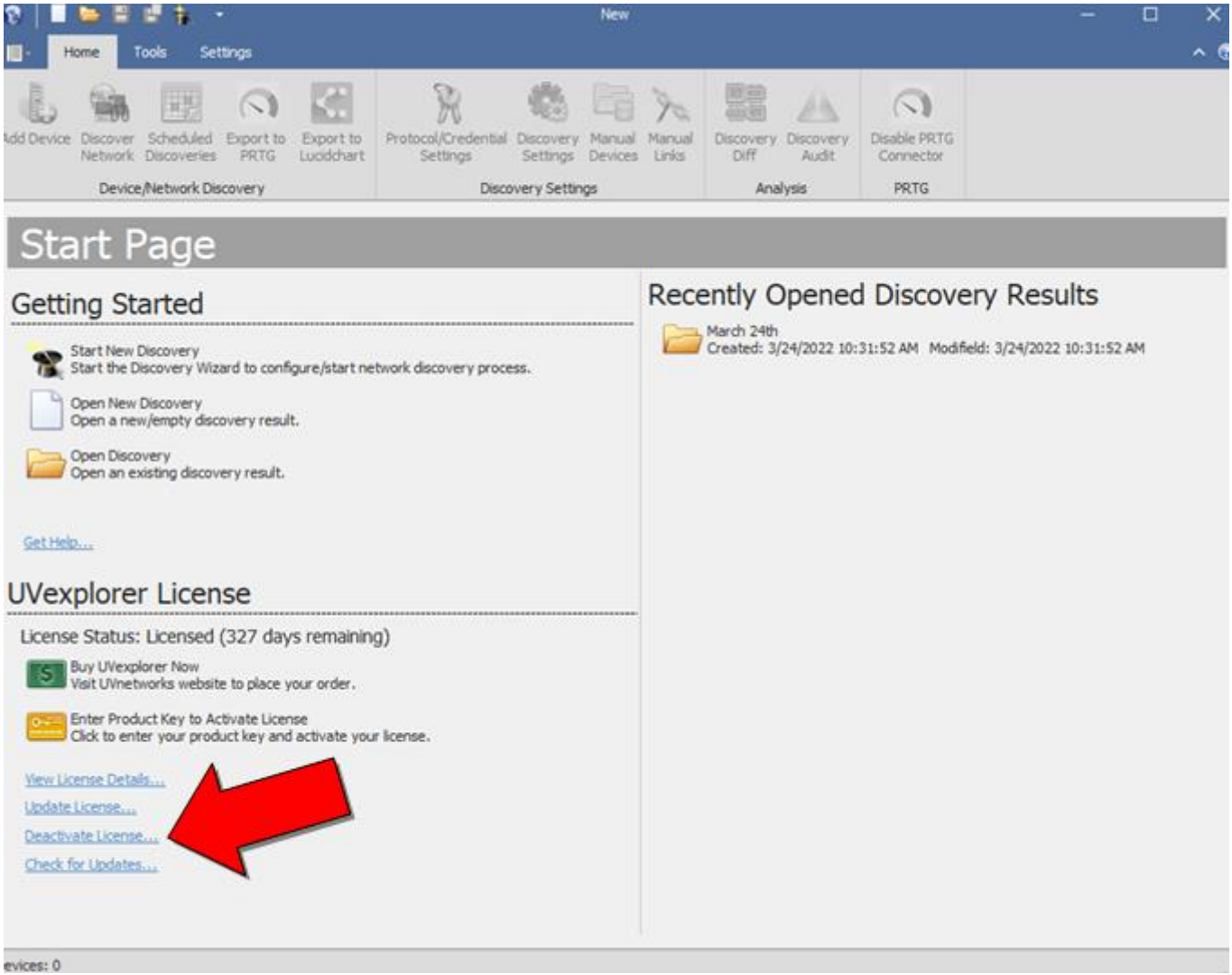
Activating your license will be easiest if your computer is connected to the Internet. This will allow the activation wizard to contact the UVnetworks licensing server and complete the activation process. You are highly encouraged to connect your computer to the Internet, at least long enough to complete the activation process. If for whatever reason you are unable to connect your computer to the Internet, offline activation is also available. If the activation wizard detects that your computer is not connected to the Internet, it will automatically step you through the offline activation process.

If you activate the product with a purchased product key, you will have access to UVexplorer's features up to the network interface level you purchased. If you activate the product with a free trial product key, you will have full access to UVexplorer's features up to 500 network interfaces. If you do not activate the product, all of the features, except discovery and device list will be disabled.

Re-activating Your UVexplorer License

Sometimes it is necessary to re-activate your UVexplorer license with a different product key than was used to originally activate it. For example, if after purchase you need to activate the product on your production server. After receiving the new, purchased product key, you will need to repeat the license activation process described in previous section, 'Activating Your UVexplorer License'. This process is initiated by clicking the 'Enter Product Key to Activate License' icon on the Start Page that appears when you run UVexplorer.

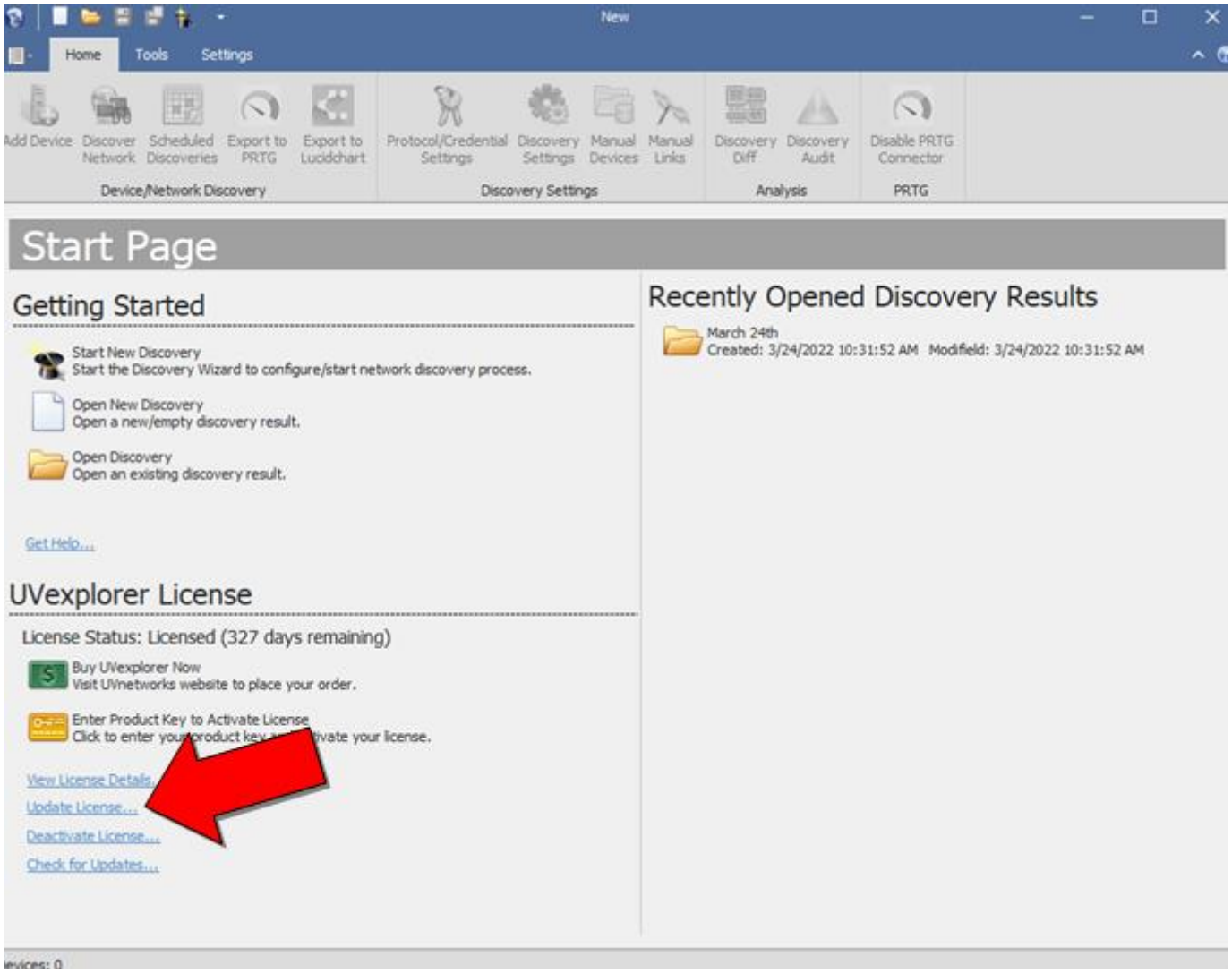
When re-activating with a new product key, you must first de-activate the old product key before activating with the new key. If the license activation wizard detects that the old product key is still activated, it will automatically launch the license de-activation wizard to step you through the process of de-activating the old key. After the old key has been de-activated, the wizard will step you through the license activation process. See the section titled 'De-Activating Your UVexplorer License' for more details on the de-activation process.



Updating Your UVexplorer License

When you activated your UVexplorer license, you entered a product key, and the license activation wizard downloaded the details of your license from the UVnetworks licensing server. The license details indicate the date on which your license will expire. If there are any limits on UVexplorer's features, such as maximum device counts, these will be displayed in the bottom bar of the product and when you click the 'Open Folder' icon on the Quick Access toolbar.

Periodically, the details of your license will change. For example, each time you purchase a UVexplorer subscription, the expiration date of your license will change. If the details of your license change on the UVnetworks licensing server, they will need to be re-downloaded before the changes will take effect on your computer. The process of re-downloading your license details is called 'updating your license'. UVexplorer will update your license automatically, as long as it can connect to the Internet.



Typically, UVexplorer will automatically update your license, so you don't need to worry about doing it yourself. However, if you want to update your license on-demand, you can click the 'Update License' link on the Start Page that appears when you run UVexplorer. This will ensure that your license details are up-to-date, and that you can view the purchased network interface level.

Offline Updating of Your UVexplorer License

Updating your license requires your computer to be connected to the Internet. If it is not, the update operation will fail. If your computer is not connected to the Internet, the 'Update License' operation will not work for you. Instead, you should do the following:

1. Go to the Start Page that appears when you run UVexplorer
2. Deactivate your license by clicking on the 'Deactivate License' link. This will run the license de-activation wizard which will step you through the offline deactivation process. (NOTE: Before deactivating, make sure you have a copy of your product key so you will be able to re-enter it in the next step. Click on the 'View License Details' link to find your product key.)
3. Re-activate your license by clicking on the 'Enter Product Key to Activate License' icon. This will run the license activation wizard which will step you through the offline activation process.

By deactivating and then re-activating your license, you will have effectively updated your license.

De-activating Your UVexplorer License

It is possible that you will need to de-activate your UVexplorer license. There are two common situations that require doing this.

1. You originally activated your license using a free trial product key so you could evaluate the product. After deciding to purchase the product, you completed the purchase process on the UVnetworks web site, and were emailed a new product key. If you want to use the new product key on the same computer on which you used the trial product key, you must first de-activate the old trial license before activating the new purchased license.
2. You activated your license on a computer, and now wish to move the license to a different computer. Since a given product key can be used on only one computer at a time, you must de-activate the license on the old computer first, and then activate the license on the new computer.

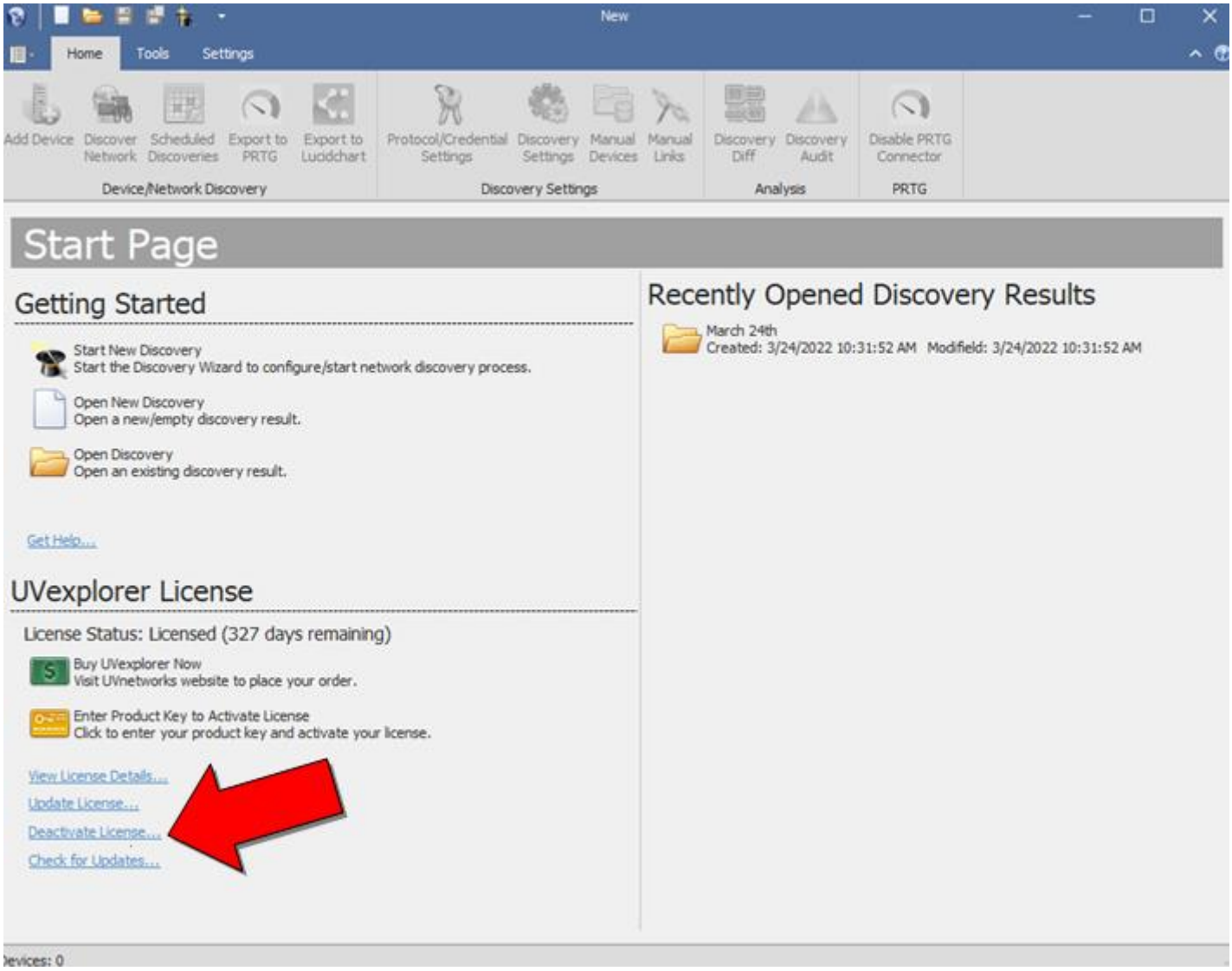
Backing Up Your Product Key

Before de-activating your UVexplorer license, make sure that you have a copy of the product key that was used to activate the license. This will be especially important if you want to re-use the product key in the future (e.g., on a different computer). Your product key was emailed to you by UVnetworks. If you still have that email message, you may find your product key there. Alternatively, if you previously activated the product with your key, you may also find your product key by going to the Start Page that appears when you run UVexplorer, and clicking on the 'View License Details' link. The product key will appear in the rightmost column in the 'License Information' section.

NOTE: The activation key begins with 'P-' (for example, P-FR5V-IK7D-D3T3-YJCT-SZM3-6Q24-7HGV).

Running the De-Activation Wizard

To de-activate your license, click the 'Deactivate License' link on the Start Page that appears when you run UVexplorer. Doing so will display the license de-activation wizard, which will step you through the process of deactivating your license. (The de-activation wizard will also automatically run if you try to enter a new product key without first de-activating the old product key.) De-activating your license will be easiest if your computer is connected to the Internet. This will allow the de-activation wizard to contact the UVnetworks licensing server and complete the de-activation process. You are highly encouraged to connect your computer to the Internet, at least long enough to complete the de-activation process. If for whatever reason you are unable to connect your computer to the Internet, offline de-activation is also available. If the de-activation wizard detects that your computer is not connected to the Internet, it will automatically step you through the offline de-activation process.


New
Home
Tools
Settings
Add Device
Discover Network
Scheduled Discoveries
Export to PRTG
Export to Lucidchart
Device/Network Discovery
Protocol/Credential Settings
Discovery Settings
Manual Devices
Manual Links
Discovery Settings
Discovery Diff
Discovery Audit
Analysis
Disable PRTG Connector
PRTG
Start Page
Getting Started
Start New Discovery
Start the Discovery Wizard to configure/start network discovery process.
Open New Discovery
Open a new/empty discovery result.
Open Discovery
Open an existing discovery result.
Get Help...
UVexplorer License
License Status: Licensed (327 days remaining)
Buy UVexplorer Now
Visit UVnetworks website to place your order.
Enter Product Key to Activate License
Click to enter your product key and activate your license.
View License Details...
Update License...
Deactivate License...
Check for Updates...
Recently Opened Discovery Results
March 24th
Created: 3/24/2022 10:31:52 AM Modifield: 3/24/2022 10:31:52 AM
evices: 0

License Execution Modes

When UVexplorer runs, it is in one of two "modes":

- NOT LICENSED
- LICENSED

NOT LICENSED Mode

UVexplorer runs in NOT LICENSED mode in the following situations:

1) You have never activated the product
2) You activated the product with a 1 year trial product key, but your trial period has expired
3) You purchased a UVexplorer subscription and activated the product with a purchased license key, but your subscription has since expired

You may continue to use the product in NOT LICENSED mode, but the following product features will be unavailable:

- Reports
- Network Maps
- Scheduled Discoveries (you can run discoveries manually, but they will not run automatically on a scheduled basis)
- Scheduled Monitor Execution (you can run monitors manually using 'Run Now', but they will not run automatically on a scheduled basis)

LICENSED Mode

UVexplorer runs in LICENSED mode when you have activated the product with either a trial or purchased product key. In LICENSED mode you have full access to all product features up to the network interface level purchased. The trial license provides up to 500 network interfaces at no cost.

Configuring UVexplorer

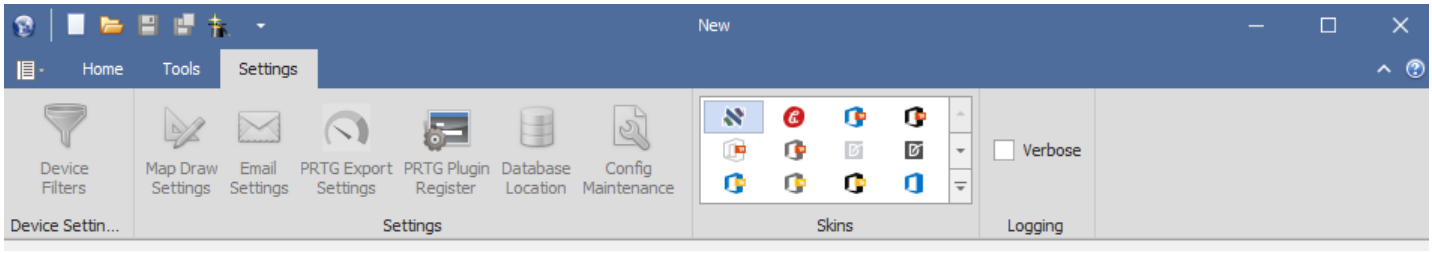
In this section:

Application Skins
SMTP Email Server Settings

Application Skins

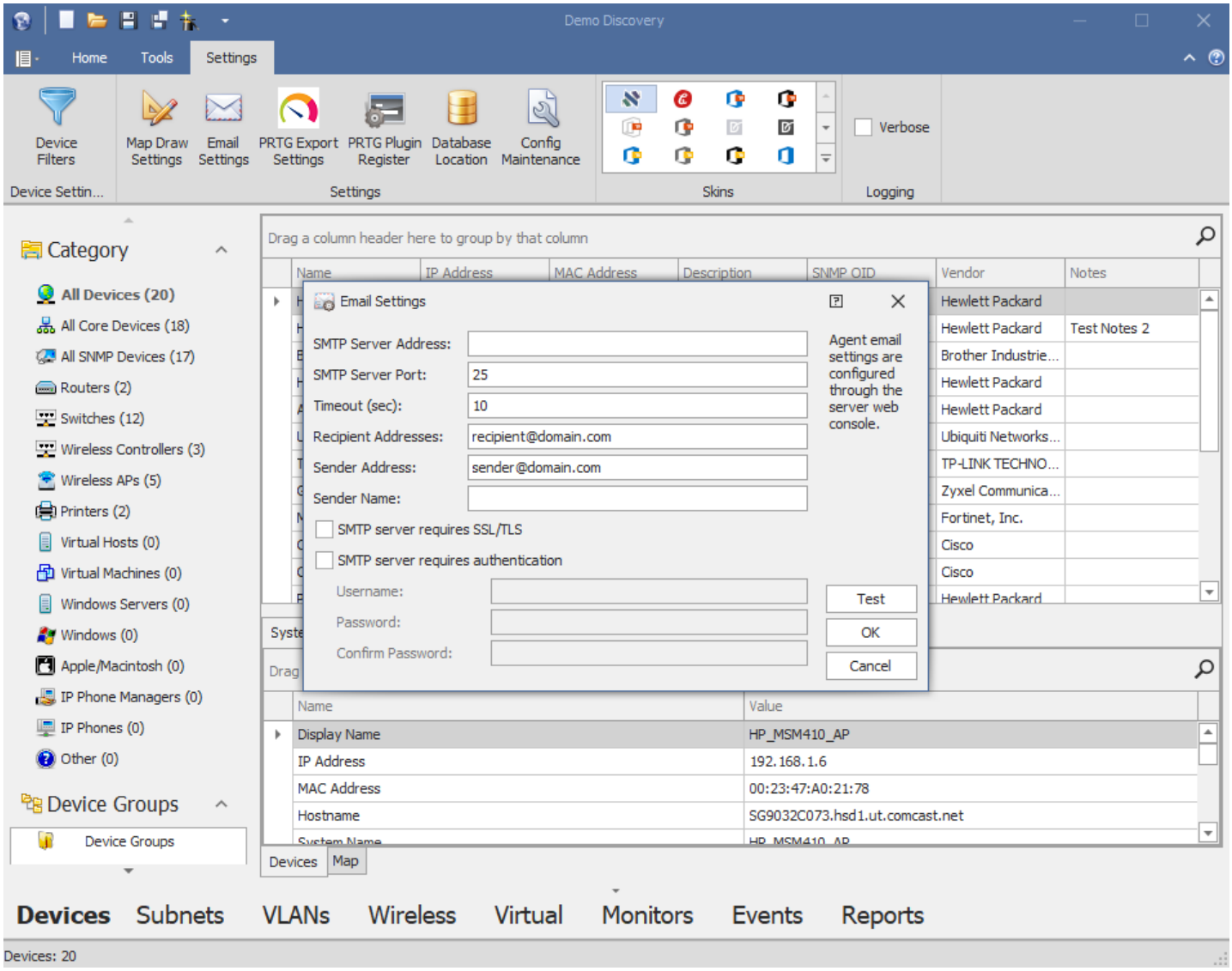
UVexplorer uses modern user interface widgets that support display theming. To change the theme of the application, select a new theme from the theme picker available in the settings menu tab.

While effort has been made to ensure all of the available themes behave appropriately within the application, the themes are provided and supported by a third-party supplier and full support of each theme cannot be guaranteed. If you experience any problems with the themes we would recommend returning to the default 'DevExpress' theme.



SMTP Email Settings

SMTP email settings are required to receive email notifications from UVexplorer features. The settings can be accessed from the 'Email Settings' item on the settings tab of the application menu.

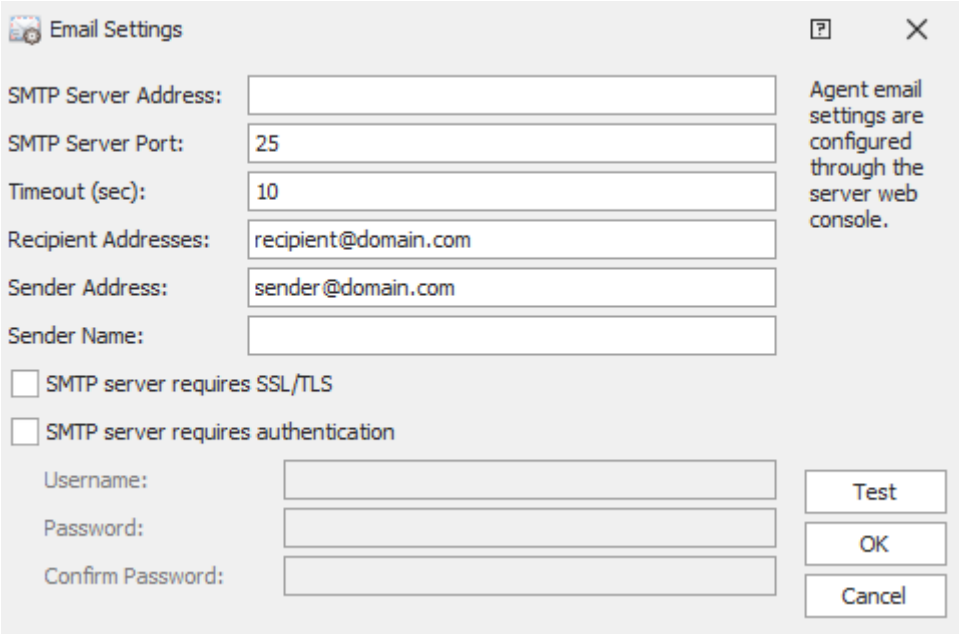


Configuring Email Settings

The email settings provide both email client and server settings. The server settings are required to provide UVexplorer with an email server to use to send the email notifications. The client settings are required to provide default recipients of the email notifications.

Server Settings

If you are using an email provider, the email server settings are readily available from the provider's documentations. If you are using a private server, the settings should be available from your network administrator.



SMTP Server Address
The SMTP server address is the name or IP address of the email server.

SMTP Server Port
The SMTP server port of the email server.

Timeout (sec)
The timeout in seconds to wait when attempting to send an email.

Recipient Addresses
Enter one or more email addresses to which UVexplorer should send email notifications. The addresses listed here will receive all email messages sent by UVexplorer. If you enter multiple email addresses, the addresses should be separated with either commas or semicolons.

Sender Address
When UVexplorer sends email messages, this is the Sender email address included in the message.

Sender Name
When UVexplorer sends email messages, this is the Sender Name included in the message.

SMTP Server requires SSL/TLS
Check this box if your email server requires secure communication using SSL/TLS.

SMTP Server requires authentication
Check this box if your email server requires you to log in when sending email messages. If so, provide the necessary Username and Password in the fields below.

Testing Your Email Configuration

After entering your email server configuration settings, you can send a test email message to ensure that everything is working properly. To send a test message, click the Test button.

Some email servers, like GMAIL will block the login from the app. To resolve this, go to your email and allow the login by selecting "Check activity".

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

Check activity

You can also see security activity at
https://myaccount.google.com/notifications

Discovering Networks

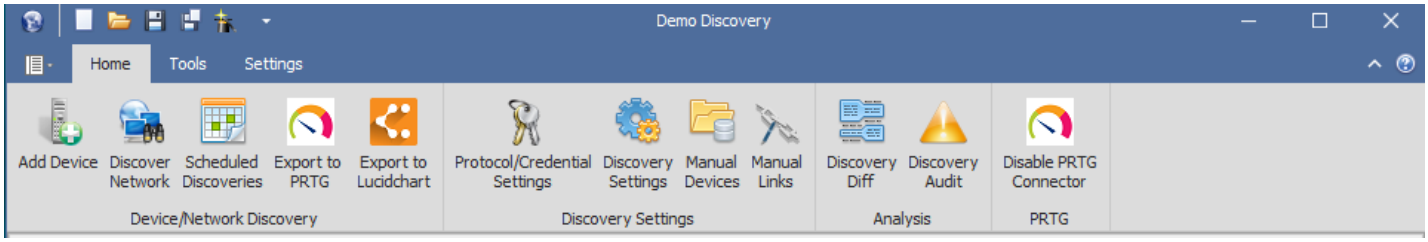
In this section:

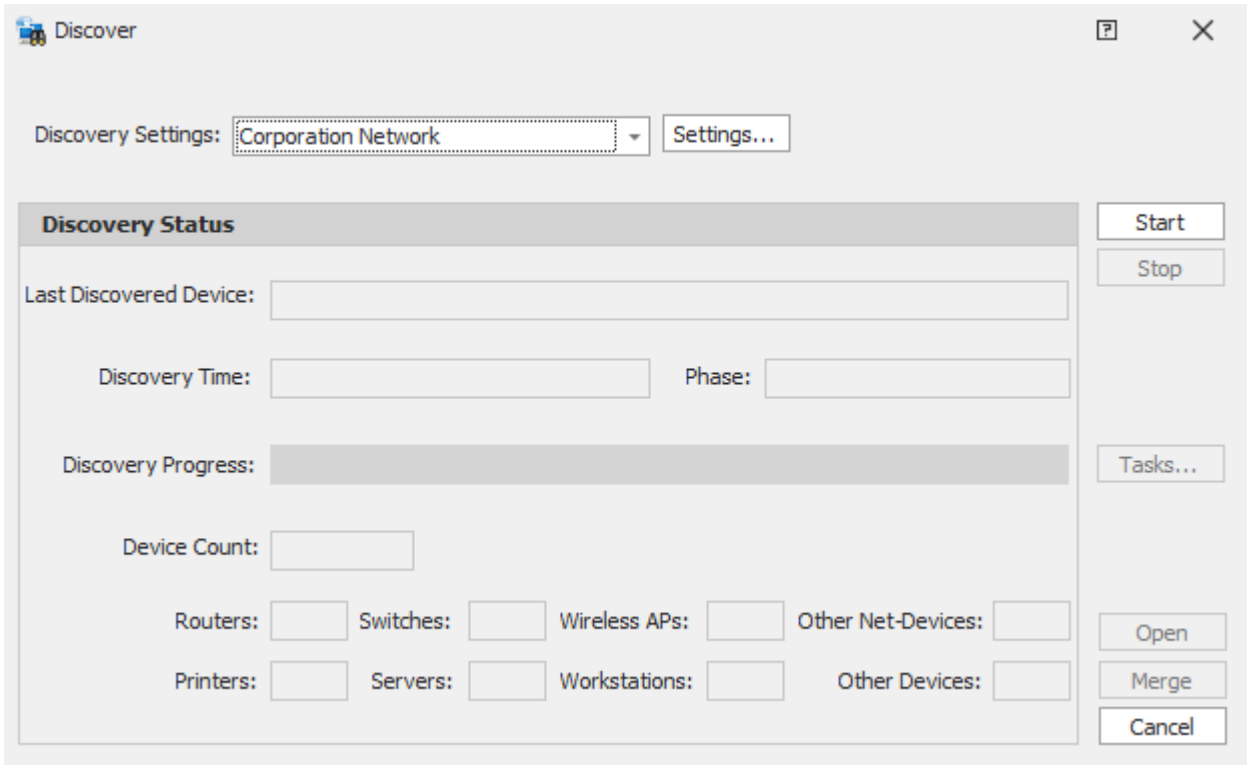
Starting Network Discoveries
Using the Discovery Wizard
Discovering a Single Device
Saving Discovery Results
Selecting Discovery Results
Comparing Discovered Networks
Discovery Settings
Scheduling Network Discoveries
Scheduled Discovery Events
Opening Discovery Results
Discovery Tasks

Running a Discovery

When you click the Discover Network icon on the Home toolbar, the Discovery Form is displayed. The Discovery Form lets you run a manual discovery of your network. Specifically, the form lets you do the following:

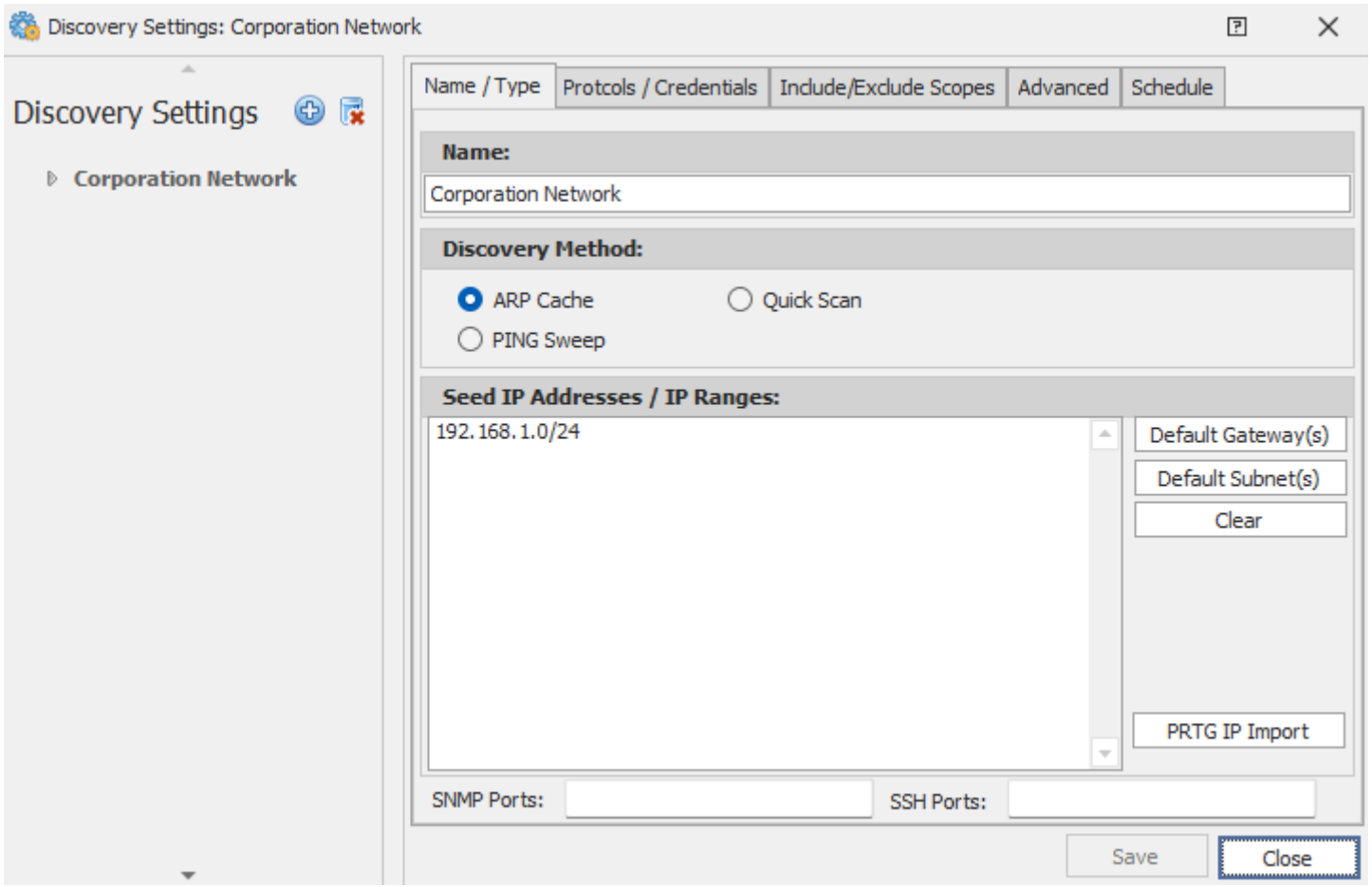
1. Select the discovery settings to be used during the discovery
2. Start and stop the discovery
3. Monitor discovery progress
4. Open or merge the result of the discovery





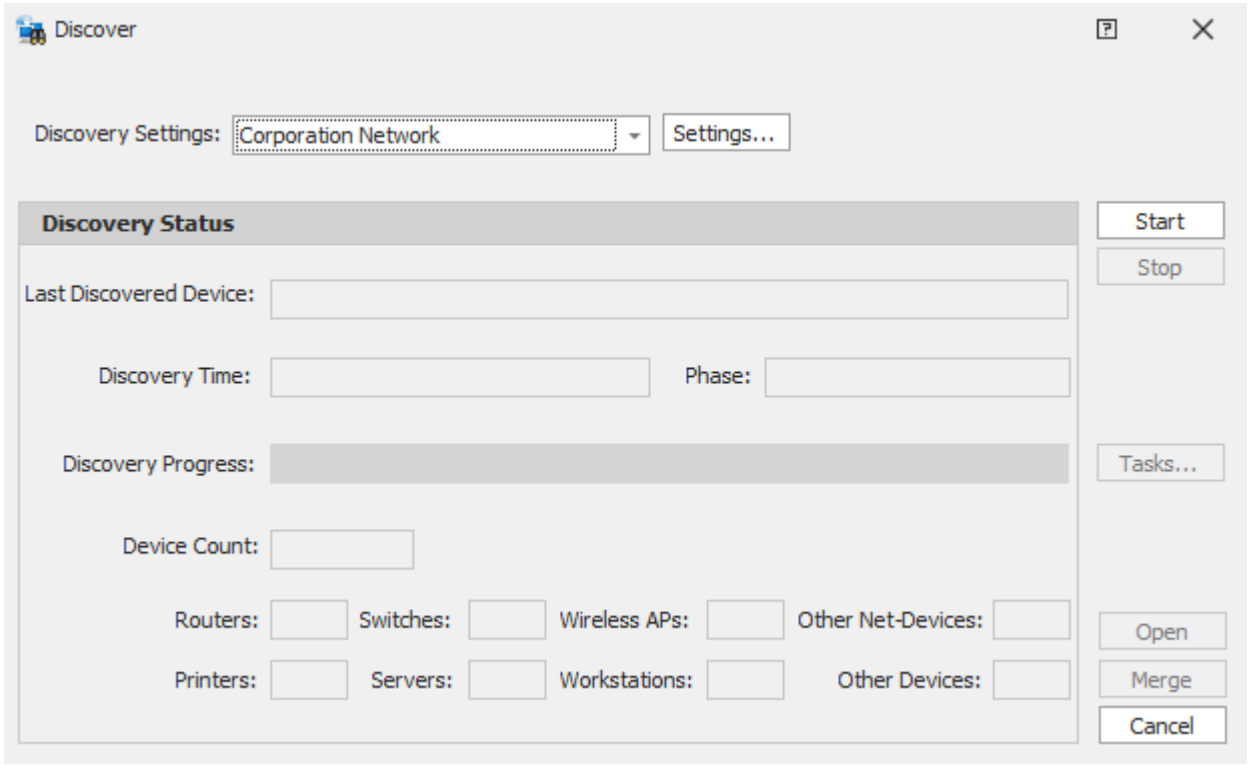
Selecting Discovery Settings

The Discovery Settings combo box lets you select the discovery settings to be used during the discovery. The drop-down list displays the names of all currently-defined discovery settings. By default, the most recently used discovery settings are selected. You may select any of the discovery settings in the list. If you would like to modify settings, or even define some new discovery settings, click the adjacent Settings button, which will display the Discovery Settings Form.



Starting and Stopping the Discovery

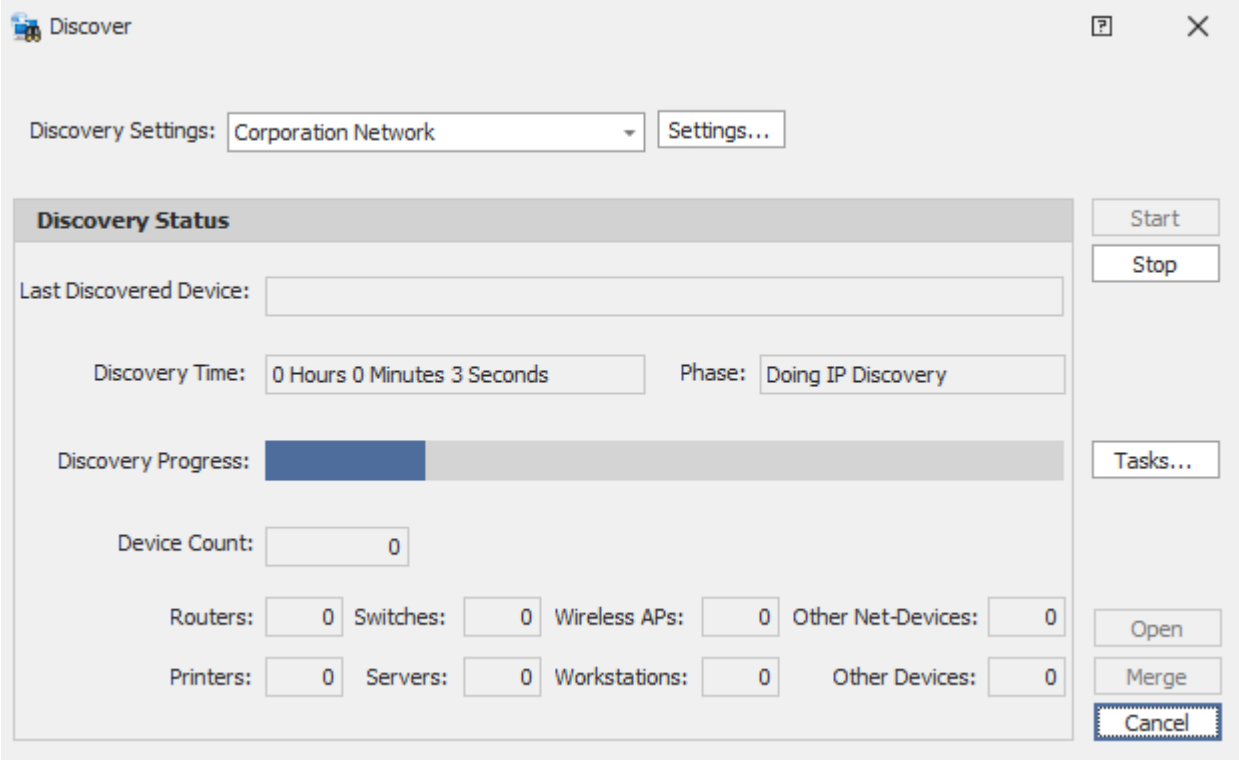
Click the Start button to start the discovery.
If you want to stop the discovery before it completes, click the Stop button. After clicking the Stop button, it might take several seconds for the discovery to terminate. Once the discovery has terminated, the partial discovery results can be viewed (i.e., opened or merged).
If you want to stop the discovery and discard the discovery results, click the Cancel button. This will immediately close the Discovery Form.



Monitoring Discovery Progress

While a discovery is running, the Discovery Status area displays the status of the discovery. Specifically, the following information is displayed:

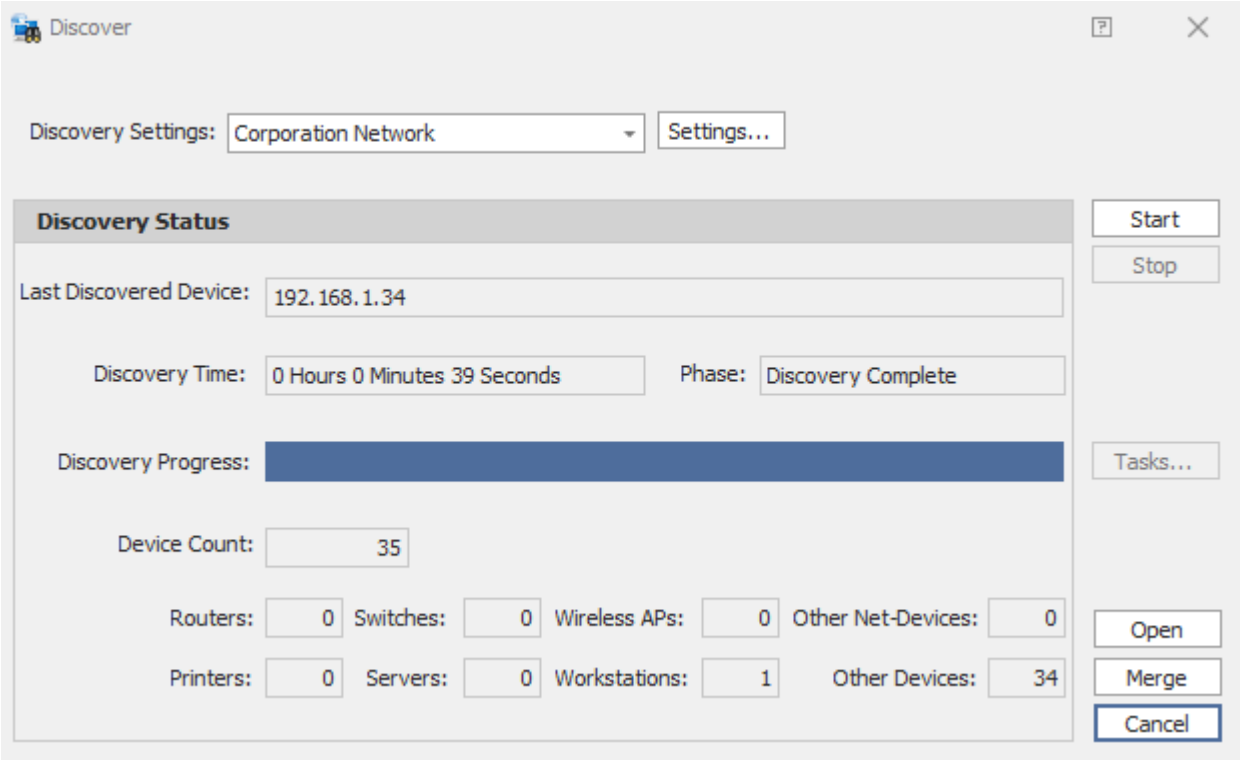
1. The name of the most recently discovered device
2. How long the discovery has been running
3. The discovery phase that is currently in progress (IP Discovery, Resolving Host Names, Detailed Discovery, Processing Connectivity, or Complete)
4. Progress bar indicating percentage complete
5. The total number of devices discovered so far
6. The number of devices found so far in several specific device categories (routers, switches, etc.)



In order to get specific details on what the discovery is currently working on, you can click the Tasks button. Clicking this button will display the Discovery Tasks form. This form shows what devices are currently being discovered, what information is being collected from those devices, and why the discovery has not yet completed. It also allows discovery tasks to be individually canceled, which can be useful if discovery gets stuck on a badly-behaving device.

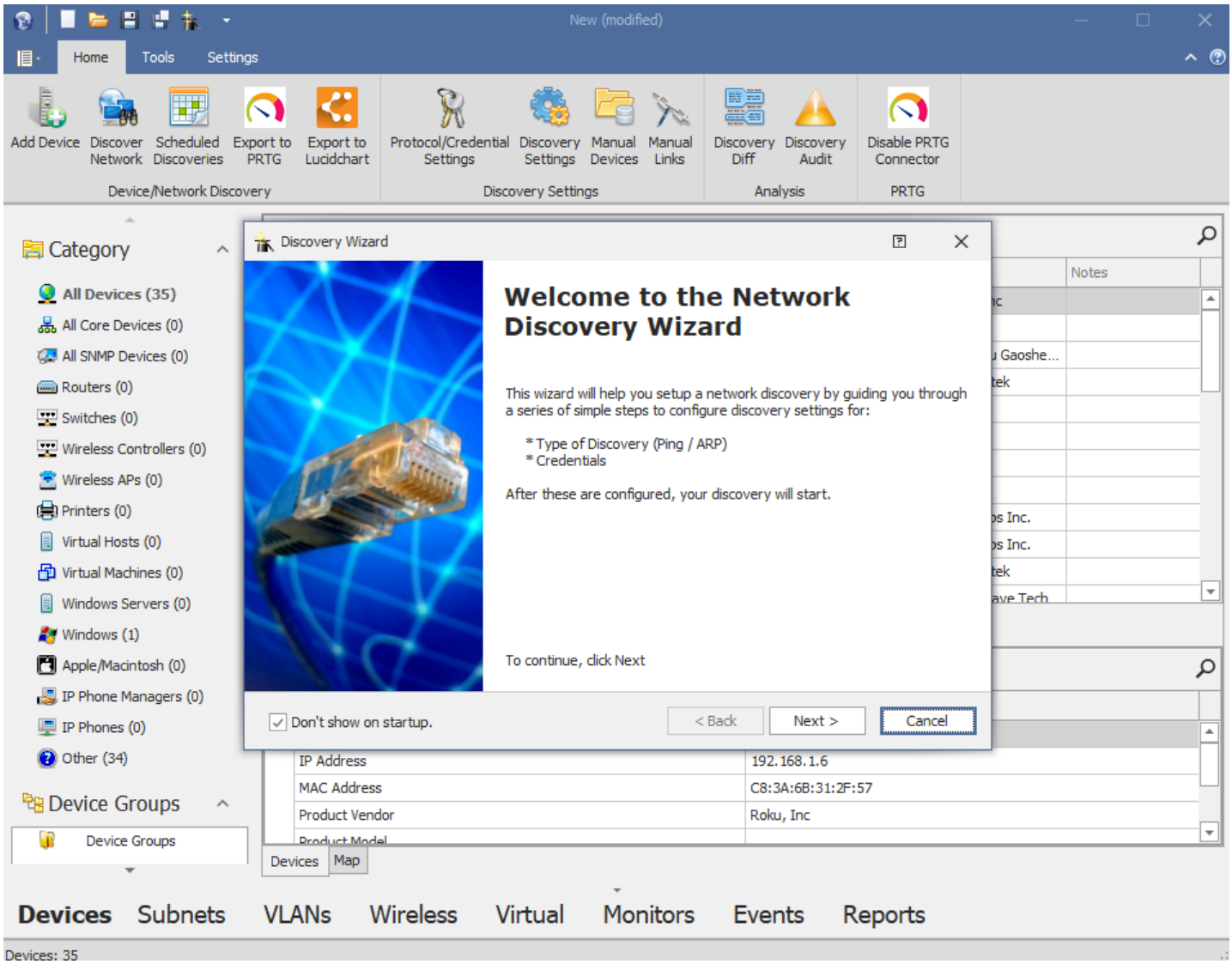
Opening and Merging Discovery Results

When the discovery is complete, you can view the results by clicking either the Open button or the Merge button. Clicking Open will unload the discovery result that is already open in UVexplorer, and then open the new discovery result. Clicking Merge will combine the new discovery result with the discovery result that is already open in UVexplorer. It is called a 'merge' because the devices in the two discovery results are merged to create a single discovery result. If you click Cancel, the new discovery result will be discarded, and the currently-open discovery result will be unaffected.


Discover
Discovery Settings:
Corporation Network
Settings...
Discovery Status
Start
Stop
Last Discovered Device:
192.168.1.34
Discovery Time:
0 Hours 0 Minutes 39 Seconds
Phase:
Discovery Complete
Discovery Progress:
Tasks...
Device Count:
35
Routers:
0
Switches:
0
Wireless APs:
0
Other Net-Devices:
0
Printers:
0
Servers:
0
Workstations:
1
Other Devices:
34
Open
Merge
Cancel

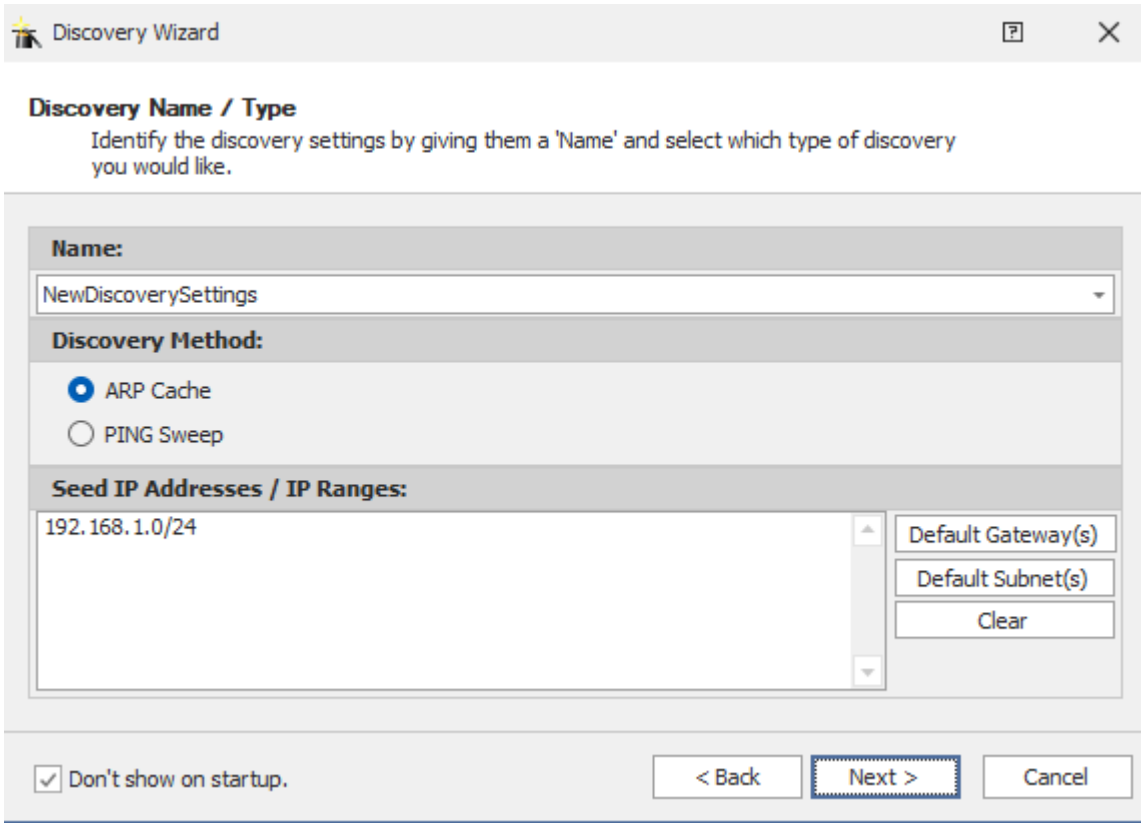
Using the Discovery Wizard

The Discovery Wizard steps you through the process of running a network discovery. First, it helps you enter a few necessary settings, and then it initiates the discovery.



The following settings must be specified:

Discovery Name / Type



Name

The discovery settings entered in the wizard will be saved under this name. It can be anything you want but cannot be empty. (See Network Discovery Settings for more information.)

Discovery Method

A discovery runs in two major phases: 1) Find devices on the network, and 2) Discover detailed information about each device. For the first phase, there are two major techniques for finding devices on a network: Ping Sweep and ARP Cache. The Discovery Method property specifies which of these two device discovery techniques you want to use. To help you select the one you want, both approaches are explained next.

Ping Sweep

Because you are familiar with your network's structure, you know what subnets you have, and what IP address ranges are in use on your network. Of course, not all IP addresses in these ranges are currently in use, but some of them are. For a Ping Sweep discovery, you simply specify ranges of IP addresses that should be searched for devices, and UVexplorer will ping every address in those ranges to determine which addresses correspond to actual devices. The IP address ranges to be searched are specified in the 'Seed IP Addresses / IP Ranges' section. For Ping Sweep discoveries there are two things to keep in mind: 1) Ping Sweep only works on devices that can be successfully pinged. If your network or devices are configured to disallow ping, Ping Sweep will not work, 2) The more IP addresses that need to be pinged, the longer discovery will take. Specifying large IP address ranges can cause discovery to take a long time. Therefore, you should specify the smallest IP address ranges possible.

ARP Cache

The alternative to Ping Sweep is ARP Cache. Rather than doing a brute-force, exhaustive search of your IP address space as Ping Sweep does, an ARP Cache discovery intelligently discovers active IP addresses (and therefore devices) by inspecting the ARP caches on your network devices. To run an ARP Cache discovery, you must specify the IP addresses of one or more "seed devices", which are the devices where the discovery will begin. The seed devices are typically your core network switches or other network devices that have large ARP caches containing IP addresses of other devices on your network. By interrogating the ARP caches on the seed devices, UVexplorer finds the

IP addresses of other devices on your network. UVexplorer then interrogates the ARP caches on these other devices to obtain even more device IP addresses, and so on. In this way, UVexplorer crawls your network, and eventually finds most of the devices on your network. The IP addresses of the seed devices are specified in the 'Seed IP Addresses / IP Ranges' section. ARP Cache discoveries are typically faster than Ping Sweep discoveries, but they do require that SNMP be enabled on your network devices so that their ARP caches are accessible to UVexplorer.

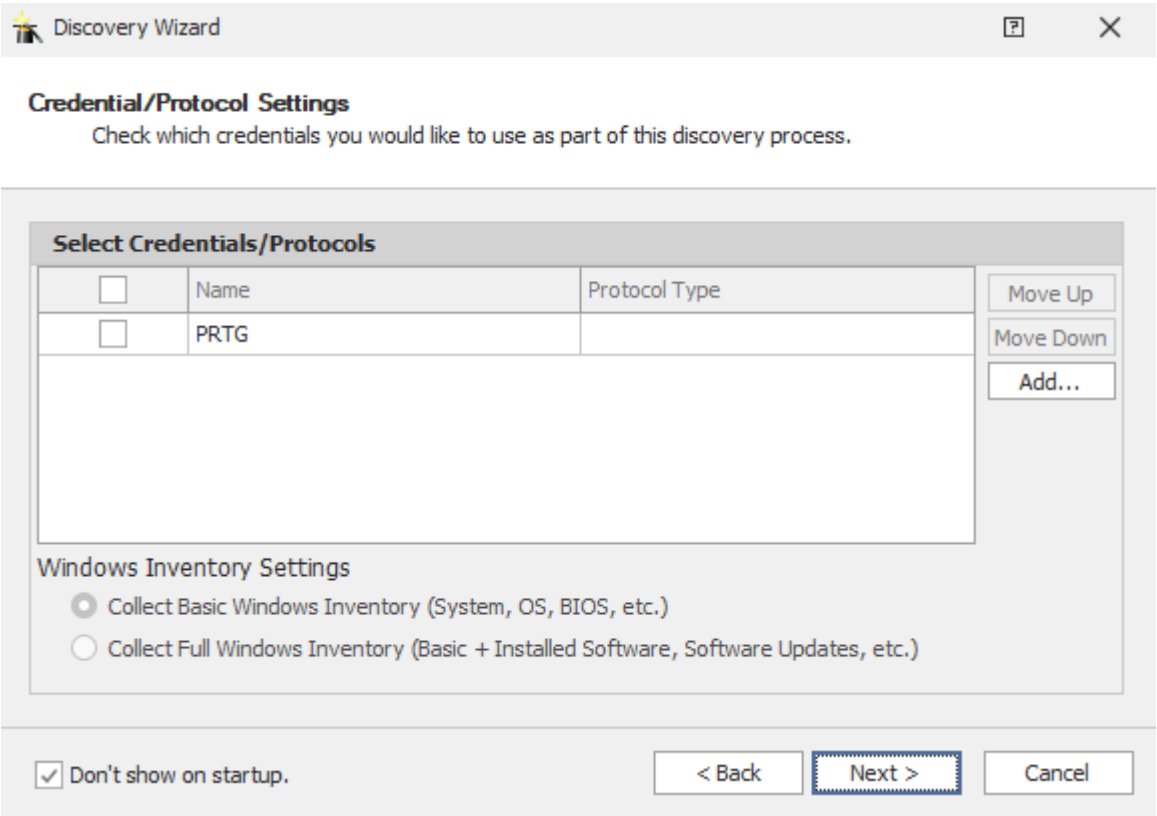
Seed IP Addresses / IP Ranges

For Ping Sweep discoveries, this field is used to enter the IP address ranges that should be pinged. For ARP Cache discoveries, this field is used to enter the IP addresses of the seed devices that are used to initiate the discovery (typically core network devices). To specify the desired IP addresses, enter one or more lines in the text field, each of which should contain one of the following:

- An individual IP address (e.g., 192.168.30.1)
- An IP subnet consisting of an IP address and subnet mask length (in bits) separated by a forward slash (e.g., 172.16.0.0/24)
- An IP address range consisting of minimum and maximum addresses separated by a dash (e.g., 10.0.0.32 – 10.0.0.96).

Pressing the 'Default Gateway(s)' button will automatically enter the IP addresses of the local computer's IP gateways. Pressing the 'Default Subnet(s)' button will automatically enter the subnets that the local computer is a member of. Pressing the 'Clear' button will clear the text field.

Credentials/Protocol Settings



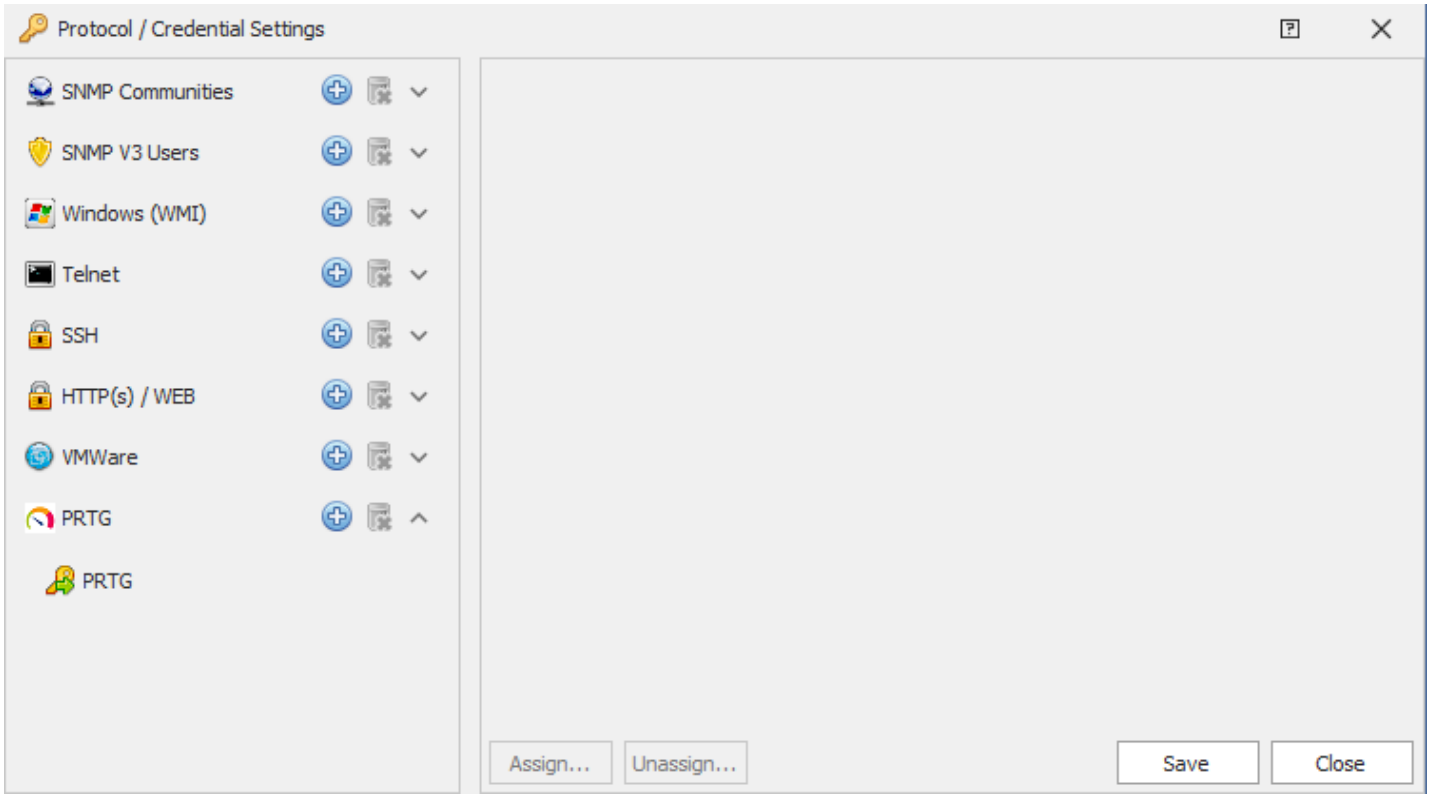
Credentials / Protocols

This section lets you select the network protocols and credentials that should be used during discovery. It displays a list of all credentials that have been previously defined (see Managing Device Credentials for more information). The row for each credential contains a checkbox that you can check to select the credential. The checkbox in the table header can be used to easily select ALL

credentials. When you select a credential, you are both telling UVexplorer to use that protocol during discovery, and which credential to use with that protocol. Only the selected protocols and credentials will be used during discovery.

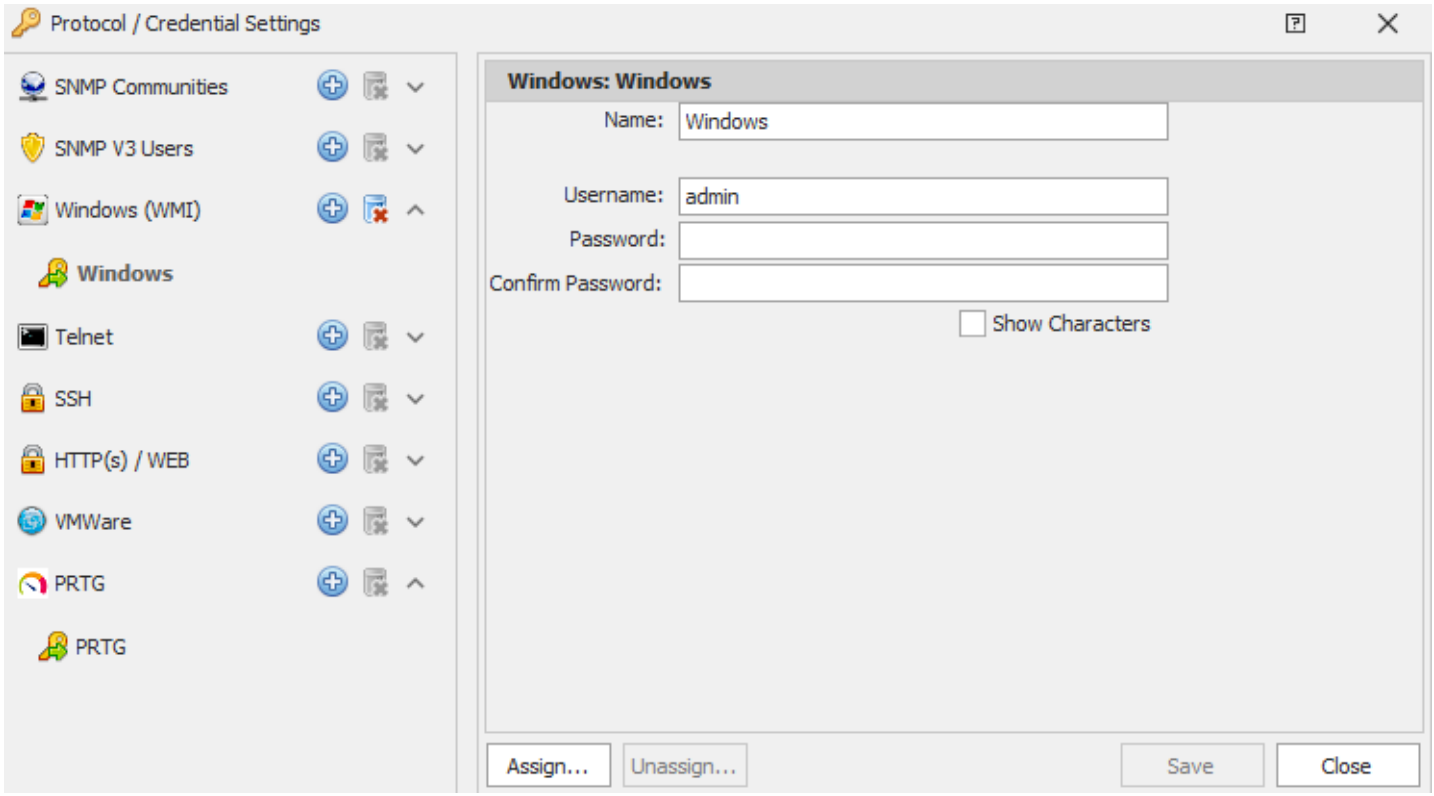
You may select multiple credentials for the same protocol, in which case UVexplorer will try them all on each device until it finds one that works. The order of the credentials in the table is significant, because it determines the order in which UVexplorer tries the credentials during discovery. You can use the 'Move Up' and 'Move Down' buttons to select a credential, and move it up or down in the table.

The 'Add' button can be used to create new credentials, or modify existing credentials.



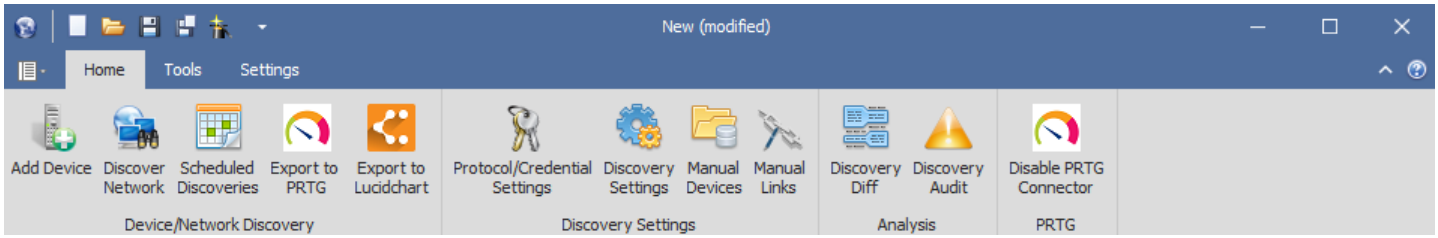
Windows Inventory Settings

UVexplorer uses the WMI protocol to collect inventory information from Windows devices. In order to collect WMI inventory, you must specify appropriate Windows(WMI) credentials. WMI data collection can be time-consuming, so this setting lets you specify how much WMI data to collect. If you select 'Collect Basic Windows Inventory', only basic WMI data will be collected. This will result in the fastest possible discovery. If you select 'Collect Full Windows Inventory', detailed WMI data will be collected. This will result in a slower discovery that produces much more detailed inventory information for Windows devices.


Protocol / Credential Settings
SNMP Communities
SNMP V3 Users
Windows (WMI)
Windows
Telnet
SSH
HTTP(s) / WEB
VMWare
PRTG
PRTG
Windows: Windows
Name:
Windows
Username:
admin
Password:
Confirm Password:
Show Characters
Assign...
Unassign...
Save
Close

Discovering a Single Device

You can discover a single device and add it to the currently-open discovery result by clicking the 'Add Device' icon on the Home toolbar. This will display the Add Device form.



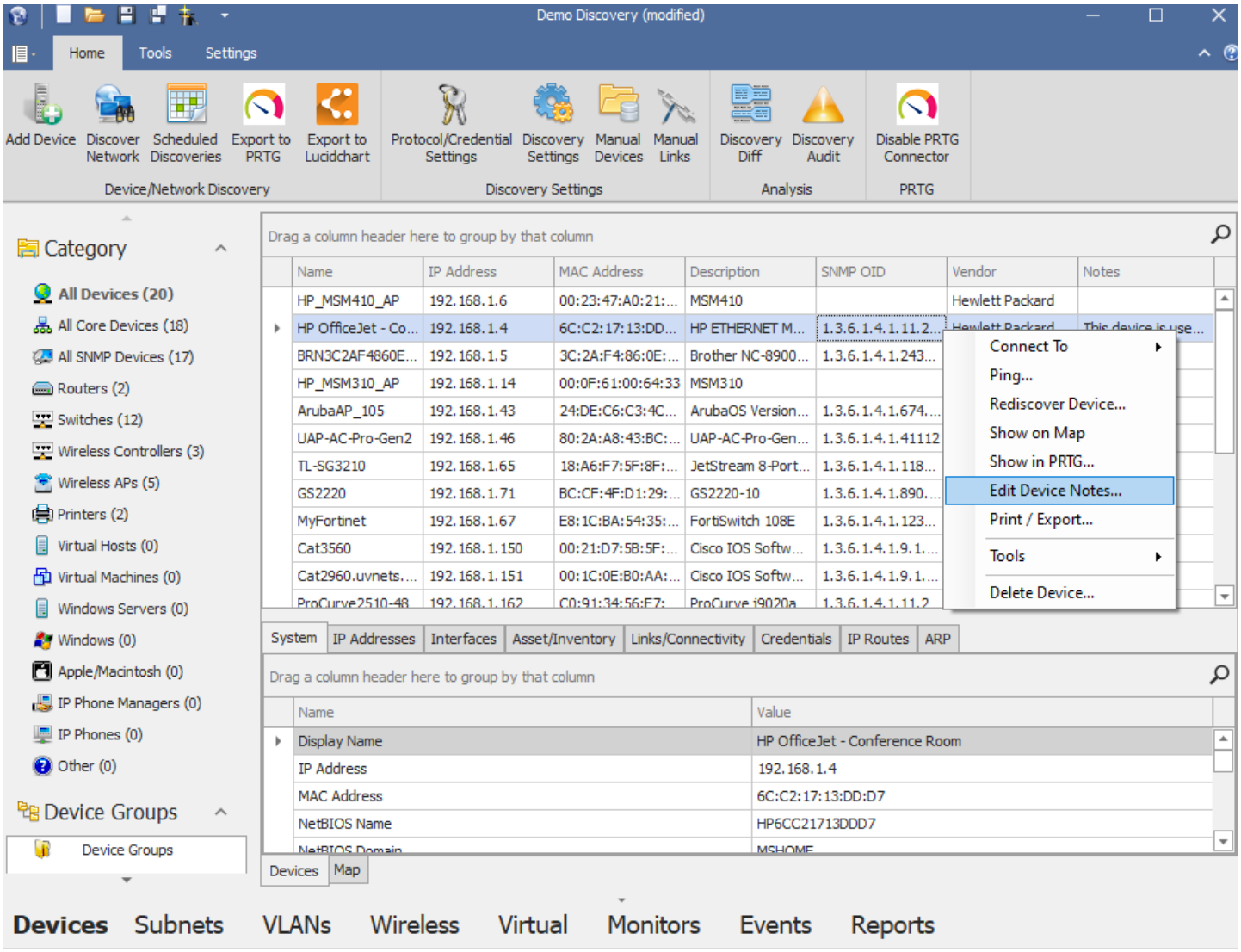
To discover a device, enter the following information:

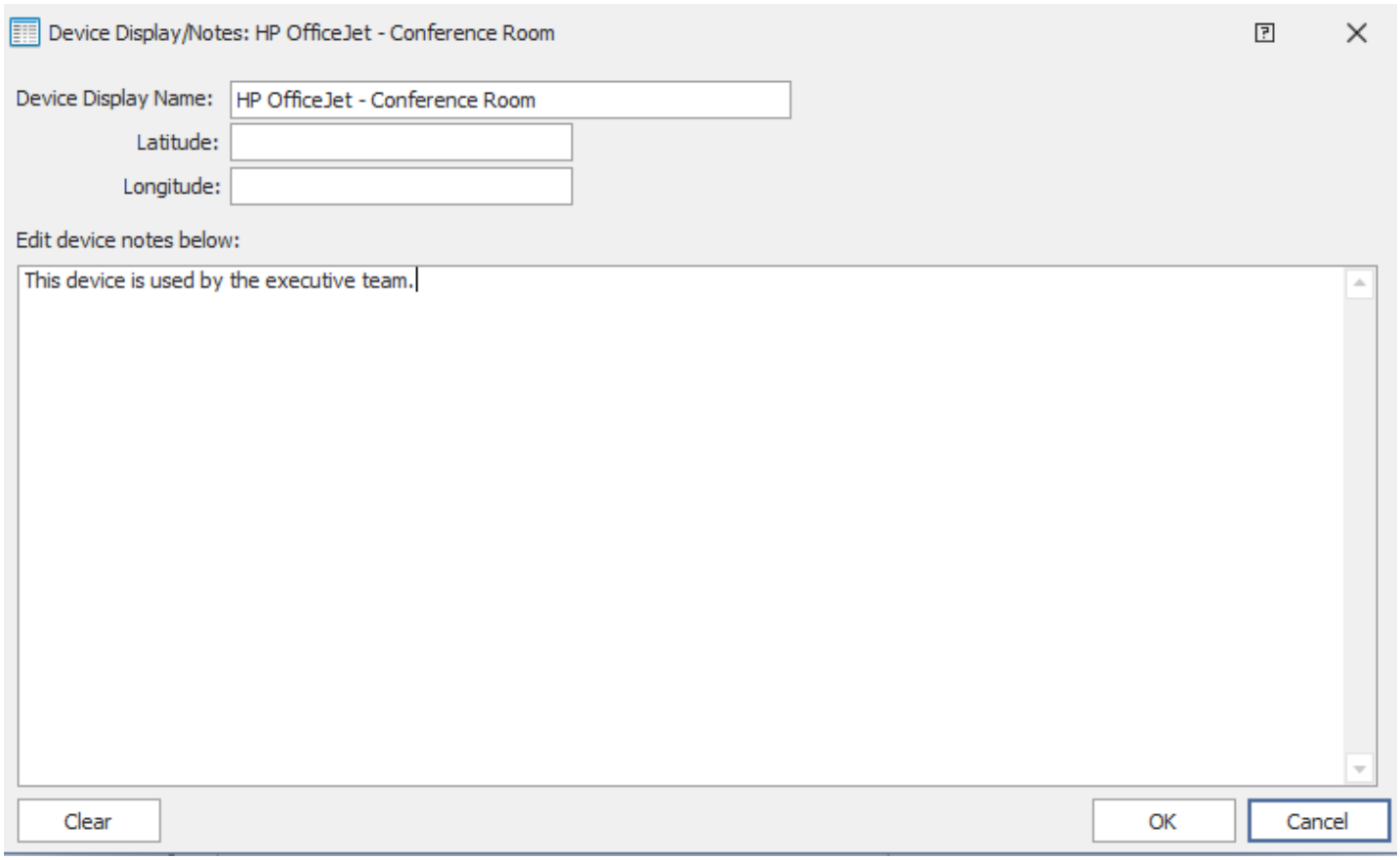
- IP Address / Hostname - Enter the IP address or DNS hostname of the device you want to discover. If you enter a hostname, UVexplorer will try to resolve it to an IP address before discovering the device.
- Credentials – From the drop-down list, select the protocol credentials you want to use when discovering the device.
- Ping Device First – Select this option if you want UVexplorer to ping the device before it tries to use other protocols to communicate with it. If the ping fails, the discovery will be aborted. If you unselect this option, UVexplorer will not ping the device before using other protocols, potentially resulting in a longer discovery. This is especially useful if your network or the device itself does not allow ping requests.

Clicking the 'Discover' button will start the discovery. You can cancel the discovery by clicking the 'Stop' button. When the discovery completes, you can click the 'Add' button to add the device to the current discovery result, or the 'Cancel' button to abort the operation.

Adding Device Notes

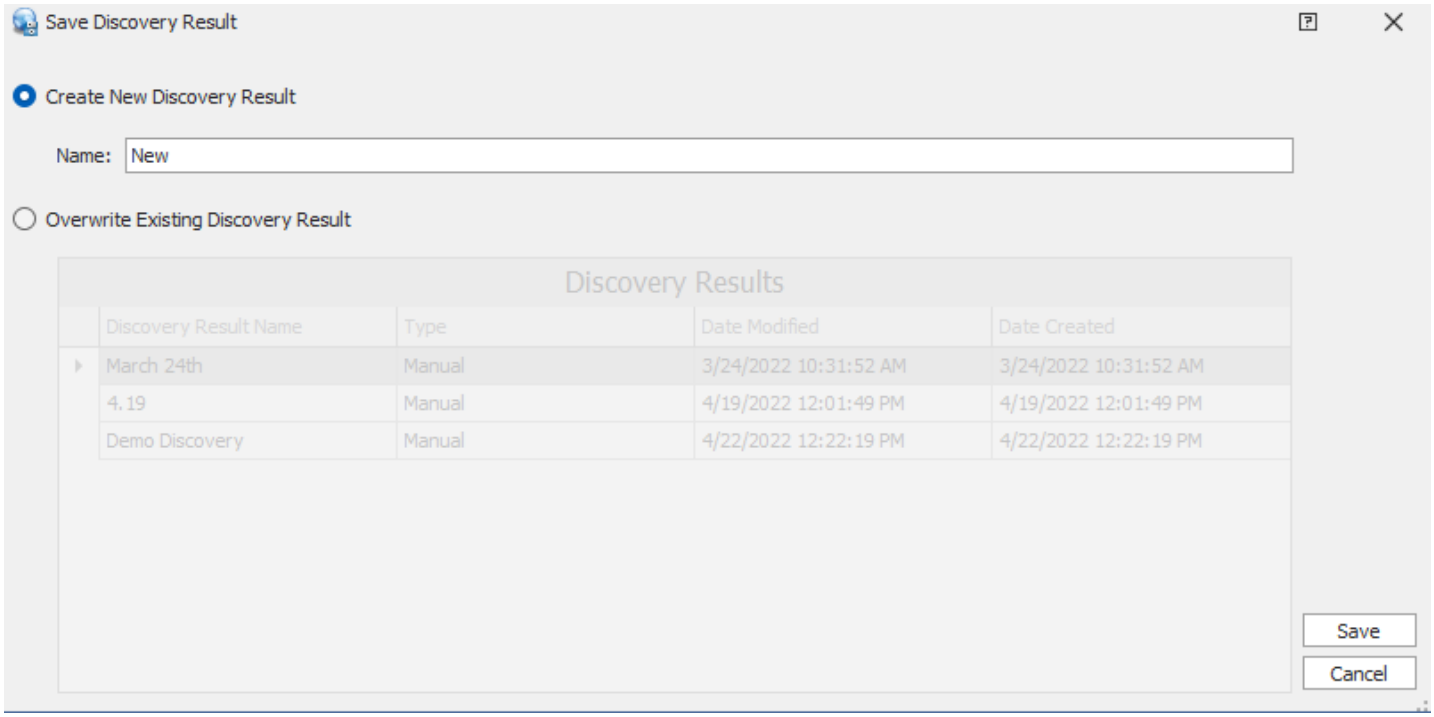
Once a device has been added to a discovery result, device notes can be added to provide information about the device that wouldn't be provided through normal device discovery. These notes are shown in the device list and be edited by simply double clicking on the device int the device list, or right-clicking and selecting "Edit Device Notes...".




Device Display/Notes: HP OfficeJet - Conference Room
Device Display Name:
HP OfficeJet - Conference Room
Latitude:
Longitude:
Edit device notes below:
This device is used by the executive team.
Clear
OK
Cancel

Saving Discovery Results

When a new discovery result is created or an existing discovery result is modified, you can save the new/modified result to the UVexplorer database. The Save Discover Result form makes this possible.



When a discovery result is saved, the following two options are available:

Create New Discovery Result

This option lets you create a new discovery result in the database. Type in a name, click the Save button, and the current discovery result will be saved in the database under the specified name.

Overwrite Existing Discovery Result

This option lets you replace an existing saved discovery result with the current one. That is, rather than creating a new discovery result in the database, this option will overwrite an existing result with the currently-loaded result. The result to be replaced is specified by selecting an existing discovery result from the displayed list. To assist in selecting a discovery result, the following properties are displayed for each result:

Discovery Result Name
This is the name assigned to the discovery result when it was saved.

Type
This is the discovery result's type, which describes the origin of the result. The possible values for this property are:

- Manual – The result was created by a manual (i.e., non-scheduled) discovery.
- Scheduled (Raw) – The result stores the raw result of a scheduled discovery execution. It stores a snapshot of what the network looked like during one particular execution of the

scheduled discovery. The Discovery Result Name property indicates which scheduled discovery created the result.

- Scheduled (Rollup) – The result stores the 'rollup' for a scheduled discovery. Unlike raw discovery results, of which there is one per execution of the scheduled discovery, there is only one rollup result for each scheduled discovery. The rollup discovery result contains the union of all devices that have been recently seen on the network by the scheduled discovery. The Discovery Result Name property indicates which scheduled discovery the 'rollup' result belongs to.

Date Modified

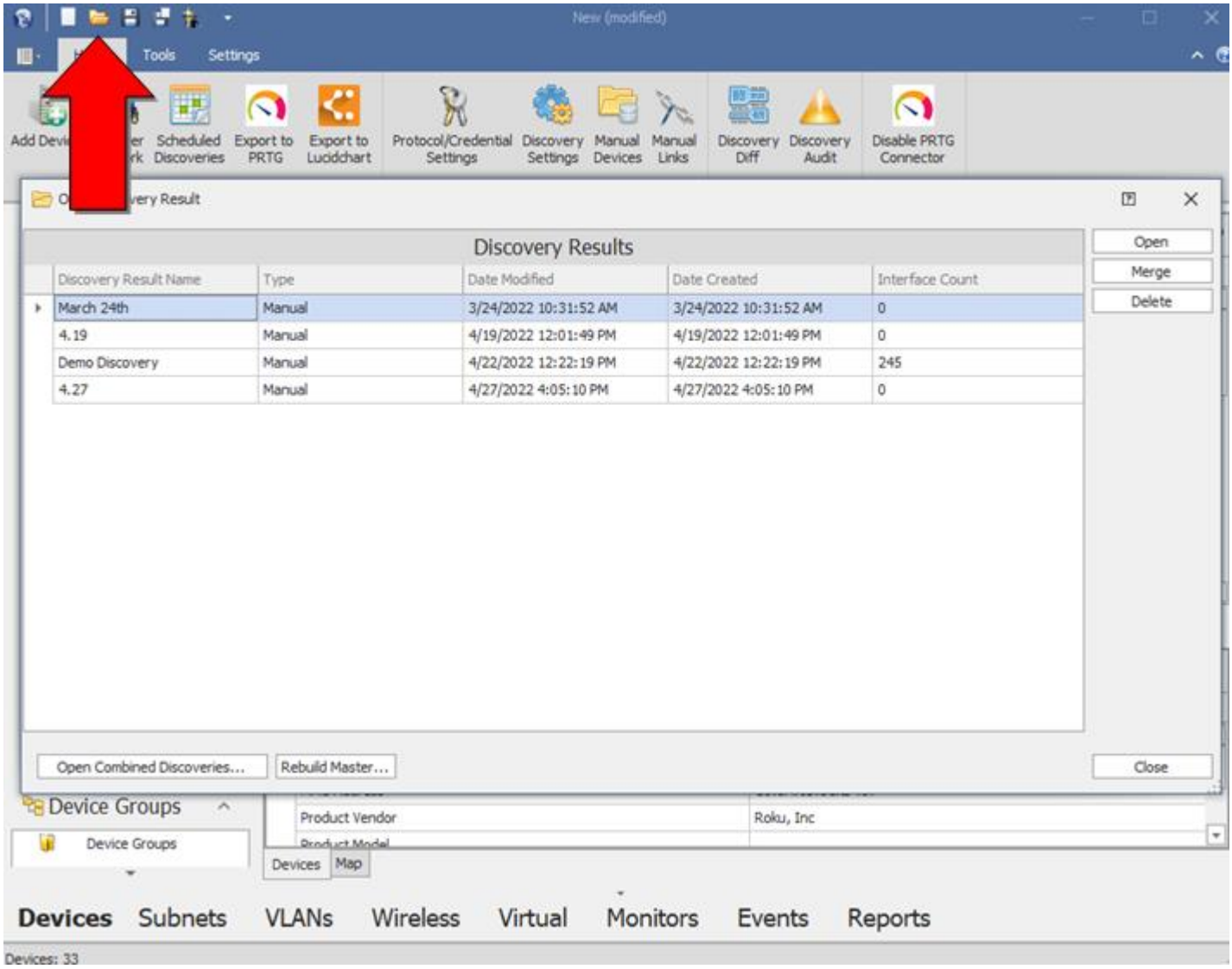
The date and time at which the most recent changes were made to the discovery result.

Date Created

The date and time at which the discovery result was originally created.

Selecting Discovery Results

The Select Discovery Result form lets you select a previously saved discovery result. It displays a list of all discovery results that are currently saved in the UVexplorer database. To select a discovery result, click on the desired discovery result in the list, and then click the Select button. (Alternatively, you can just double-click on the desired discovery result.)



Viewing available discovery results

To assist in selecting a discovery result, the following properties are displayed for each result:

Discovery Result Name

This is the name assigned to the discovery result when it was saved.

Type

This is the discovery result's type, which describes the origin of the result. The possible values for this property are:

- Manual – The result was created by a manual (i.e., non-scheduled) discovery.

- Scheduled (Raw) – The result stores the raw result of a scheduled discovery execution. It stores a snapshot of what the network looked like during one particular execution of the scheduled discovery. The Discovery Result Name property indicates which scheduled discovery created the result.
- Scheduled (Rollup) – The result stores the 'rollup' for a scheduled discovery. Unlike raw discovery results, of which there is one per execution of the scheduled discovery, there is only one rollup result for each scheduled discovery. The rollup discovery result contains the union of all devices that have been recently seen on the network by the scheduled discovery. The Discovery Result Name property indicates which scheduled discovery the 'rollup' result belongs to.

Date Modified

The date and time at which the most recent changes were made to the discovery result.

Date Created

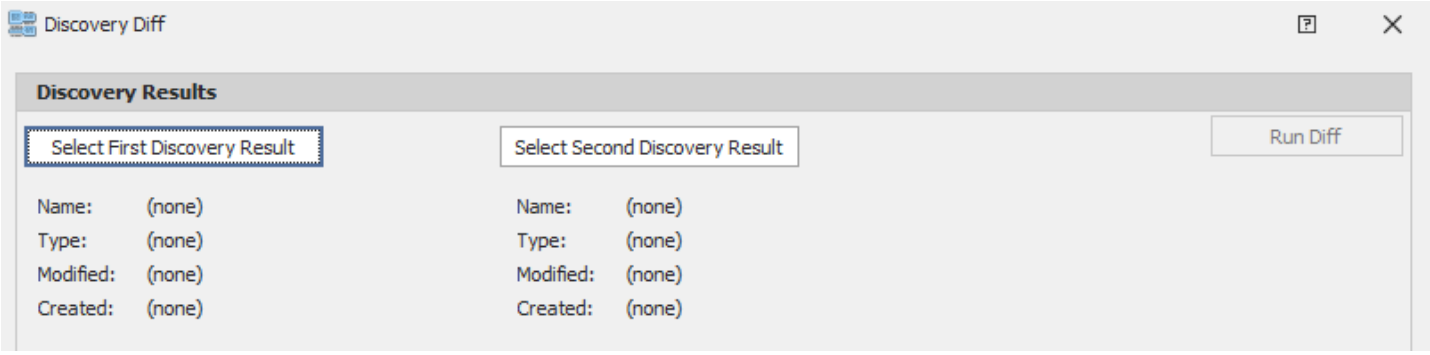
The date and time at which the discovery result was originally created.

Comparing Discovered Networks

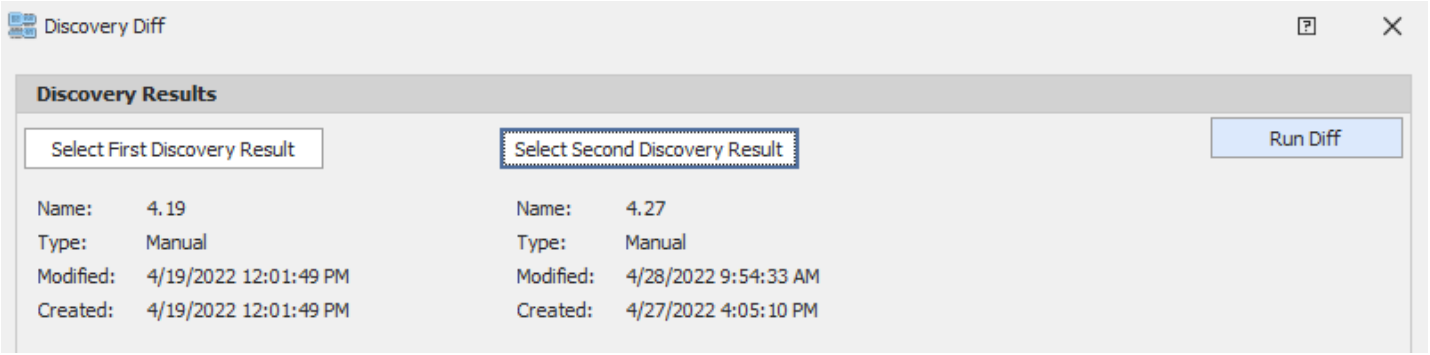
UVexplorer does detailed discoveries of your network and stores the results in its database. Each discovery result represents a snapshot of what your network looked like at a particular point in time. Over time your network will change: devices will come and go, the network links that comprise your network will change, the IP addresses of devices may change, etc. Because your network is always changing, it can be very useful to see exactly how your network changed between two specific points in time (i.e., between two different discovery results). Using the Discovery Diff command you can answer detailed questions about how your network changed, such as: What devices were added or removed from my network? What links were added or removed? Which devices changed their IP address? Etc.

To view the detailed differences between two discovery results, do the following:

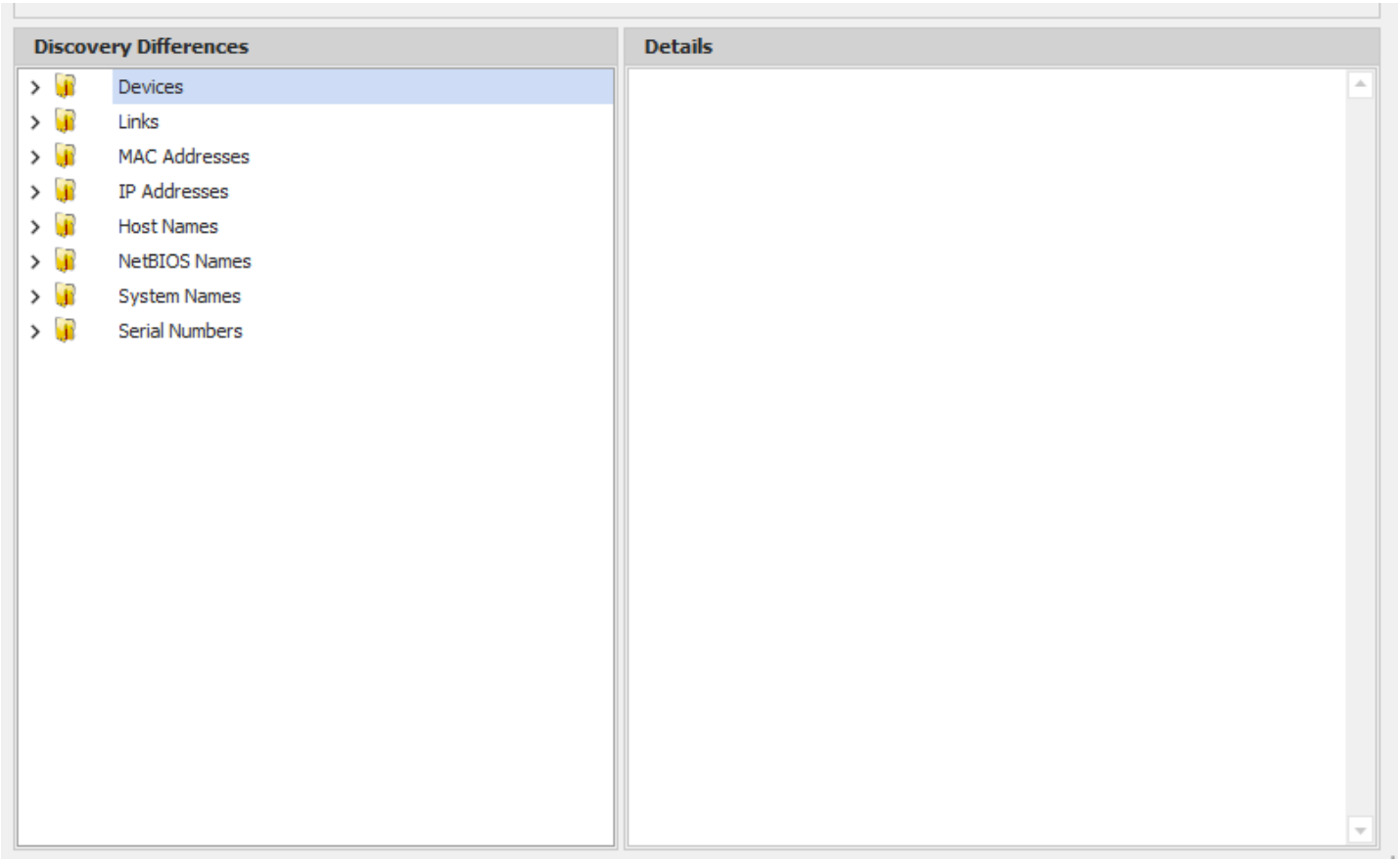
1) Click on the Discovery Diff icon on the Home toolbar. The Discovery Diff form will appear.
2) Select the two discovery results that you want to compare.
   a) To select the first discovery result, click the "Select First Discovery Result" button. This will cause the Select Discovery Result form to appear. After selecting the discovery result you want, click the "Select" button.
   b) To select the second discovery result, click the "Select Second Discovery Result" button and follow the same process.



1) Click the "Run Diff" button, and UVexplorer will compute and display the detailed differences between them.



The differences between the discovery results are displayed in two panels at the bottom of the form. The left panel displays the differences in a hierarchical tree format. By navigating the tree you can view the differences that exist between the two discovery results. When a difference is selected in the left panel, more details about the selected difference are displayed in the right panel.



The types of differences displayed include the following:

Device differences

- Removed Devices – A list of devices that appeared in the first discovery result, but not the second
- Added Devices – A list of devices that appeared in the second discovery result, but not the first
- Changed Devices – A list of devices that appeared in both discovery results, but for which some device details changed between the two discoveries. There are a number of device properties that could change between discoveries. For example, one of a device's IP or MAC addresses might change between discoveries.

Link differences

- Removed Links – A list of network links that appeared in the first discovery result, but not the second

- Added Links – A list of network links that appeared in the second discovery result, but not the first

MAC Address differences

- Removed MACs – A list of all MAC addresses that appeared in the first discovery result, but not the second.
- Added MACs – A list of all MAC addresses that appeared in the second discovery result, but not the first

IP Address differences

- Removed IPs – A list of all IP addresses that appeared in the first discovery result, but not the second.
- Added IPs – A list of all IP addresses that appeared in the second discovery result, but not the first
- Reassigned IPs – A list of all IP addresses that appeared in both discovery results, but were assigned to different devices in the two results (i.e., they were reassigned)

Host Name differences

- Removed Host Names – A list of all host names that appeared in the first discovery result, but not the second.
- Added Host Names – A list of all host names that appeared in the second discovery result, but not the first

NetBIOS Name differences

- Removed NetBIOS Names – A list of all NetBIOS names that appeared in the first discovery result, but not the second.
- Added NetBIOS Names – A list of all NetBIOS names that appeared in the second discovery result, but not the first

System Name differences

- Removed System Names – A list of all system names that appeared in the first discovery result, but not the second.
- Added System Names – A list of all system names that appeared in the second discovery result, but not the first

Serial Number differences

- Removed Serial Numbers – A list of all serial numbers that appeared in the first discovery result, but not the second.
- Added Serial Numbers – A list of all serial numbers that appeared in the second discovery result, but not the first

Discovery Settings

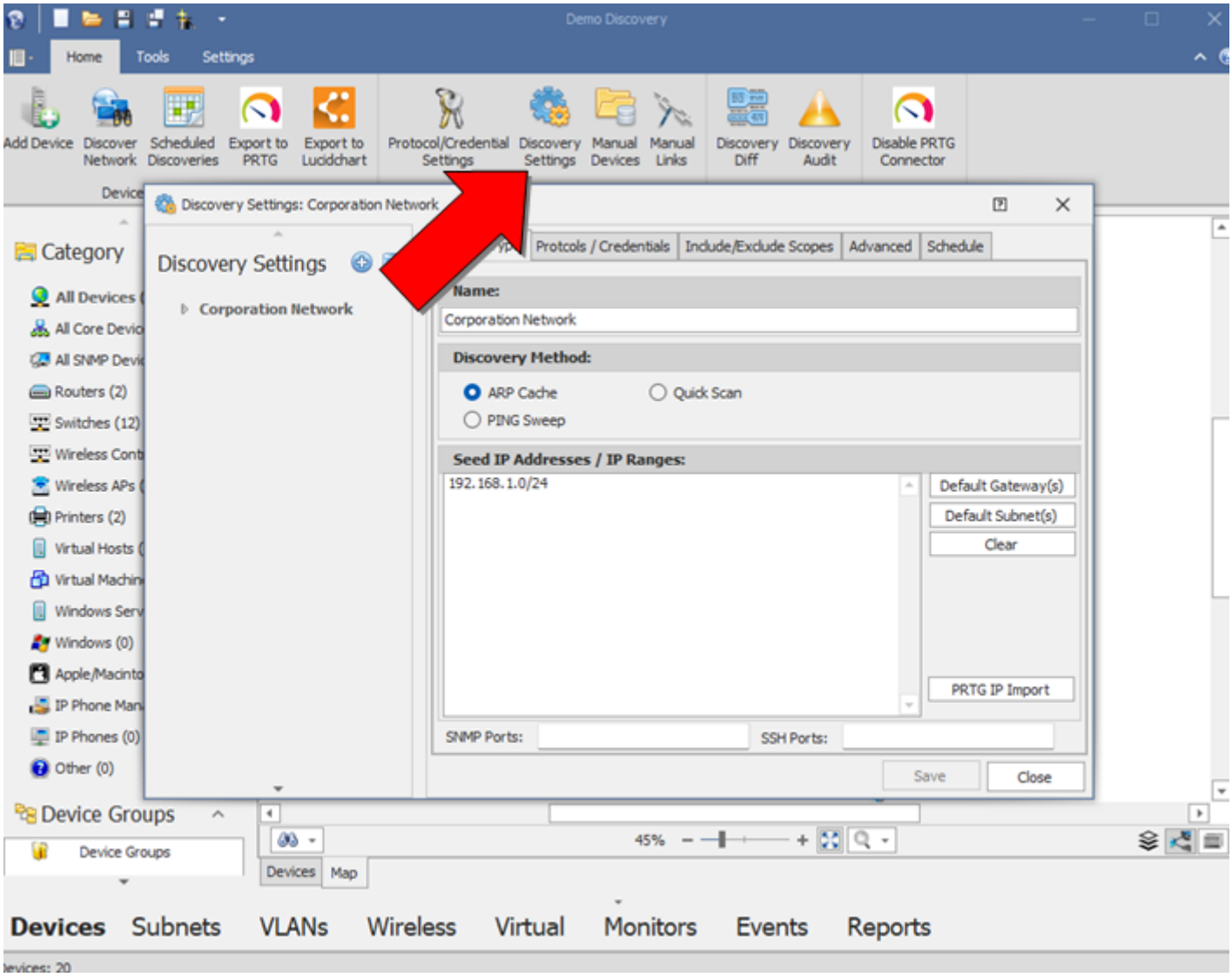
When running a network discovery, there are many parameters you can specify to control exactly how the discovery behaves. Collectively, these parameters are called 'discovery settings'. These settings let you control the following aspects of discovery:

- What type of discovery should be run (Ping sweep or ARP crawl)?
- What part of the network should be discovered?
- What network protocols and credentials should be used to discover and interrogate devices?
- What inventory information should be collected from Microsoft Windows devices?
- Should UVexplorer try to ping devices before proceeding to use additional protocols to interrogate them?
- Should IP addresses be resolved to their corresponding DNS host names?
- Should UVexplorer capture device configurations for those that support them?
- How many threads should be used to perform the discovery?
- Which types of devices should be included in the discovery result?

Any time you run a discovery, you must select the discovery settings to be used for that discovery run. Typically, you will have different sets of discovery settings for performing different types of discoveries on your network. For example, while it is possible to discover your entire network in a single discovery, you might prefer to instead discover subsets of your network individually (e.g., by site or subnet), thus allowing quicker, more targeted collection of the information you need. Because you are discovering different parts of your network separately, you would need to create different settings for each discovery you want to run. Similarly, you might use different credentials on different parts of your network, thus requiring the creation of different discovery settings for different parts of your network. UVexplorer makes it easy to create and manage the discovery settings needed to run different discoveries on your network.

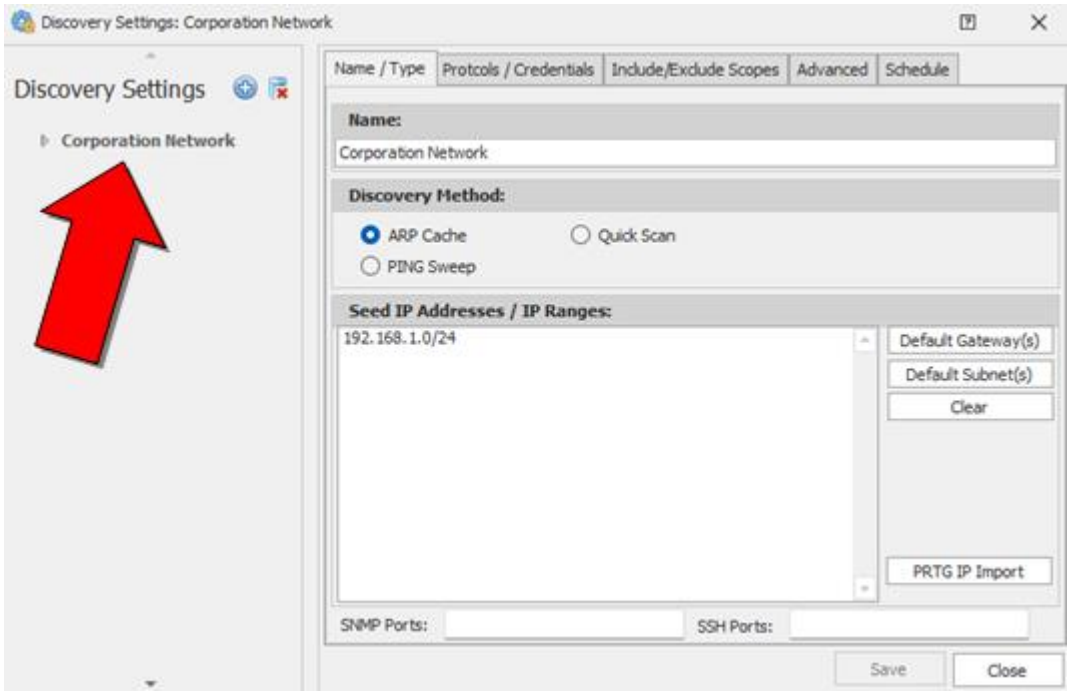
Managing Discovery Settings

To manage your discovery settings, click the Discovery Settings icon on the Home toolbar. This will display the Discovery Settings form. This form lets you add, configure, and delete discovery settings. A list of all existing discovery settings is displayed on the left side of the form. The right side of the form displays properties of the currently-selected discovery settings.



Adding Discovery Settings

To create new discovery settings, click on the Add icon (the plus sign) just above the discovery settings list on the left side of the form. Alternatively, you can right-click anywhere in the discovery settings list, and select Add from the context menu. This will cause new discovery settings with a default name to be created and selected. You can then edit the properties of the new discovery settings on the right side of the form.



Configuring Discovery Settings

The properties of a discovery settings object can be modified by first selecting it in the list of discovery settings. After it has been selected, the right side displays the various properties that can be edited. The following properties can be specified:

Name / Type

Name

Each discovery settings object must have a name, which can be anything you want, but cannot be empty.

Discovery Method

A discovery runs in two major phases: 1) Find devices on the network, and 2) Discover detailed information about each device. For the first phase, there are two major techniques for finding devices on a network: Ping Sweep and ARP Cache. The Discovery Method property specifies which of these two device discovery techniques you want to use. To help you select the one you want, both approaches are explained next.

- Ping Sweep – Because you are familiar with your network's structure, you know what subnets you have, and what IP address ranges are in use on your network. Of course, not all IP addresses in these ranges are currently in use, but some of them are. For a Ping Sweep discovery, you simply specify ranges of IP addresses that should be searched for devices, and UVexplorer will ping every address in those ranges to determine which addresses correspond to actual devices. The IP address ranges to be searched are specified in the 'Seed IP Addresses / IP Ranges' section. For Ping Sweep discoveries there are two things to keep in mind: 1) Ping Sweep only works on devices that can be successfully pinged. If your network or devices are configured to disallow ping, Ping Sweep will not work, 2) The more IP addresses that need to be pinged, the longer discovery will take. Specifying large IP address ranges can cause discovery to take a long time. Therefore, you should specify the smallest IP address ranges possible.
- ARP Cache – The alternative to Ping Sweep is ARP Cache. Rather than doing a brute-force, exhaustive search of your IP address space as Ping Sweep does, an ARP Cache discovery intelligently discovers active IP addresses (and therefore devices) by inspecting the ARP caches on your network devices. To run an ARP Cache discovery, you must specify the IP addresses of one or more "seed devices", which are the devices where the discovery will

begin. The seed devices are typically your core network switches or other network devices that have large ARP caches containing IP addresses of other devices on your network. By interrogating the ARP caches on the seed devices, UVexplorer finds the IP addresses of other devices on your network. UVexplorer then interrogates the ARP caches on these other devices to obtain even more device IP addresses, and so on. In this way, UVexplorer crawls your network, and eventually finds most of the devices on your network. The IP addresses of the seed devices are specified in the 'Seed IP Addresses / IP Ranges' section. ARP Cache discoveries are typically faster than Ping Sweep discoveries, but they do require that SNMP be enabled on your network devices so that their ARP caches are accessible to UVexplorer.

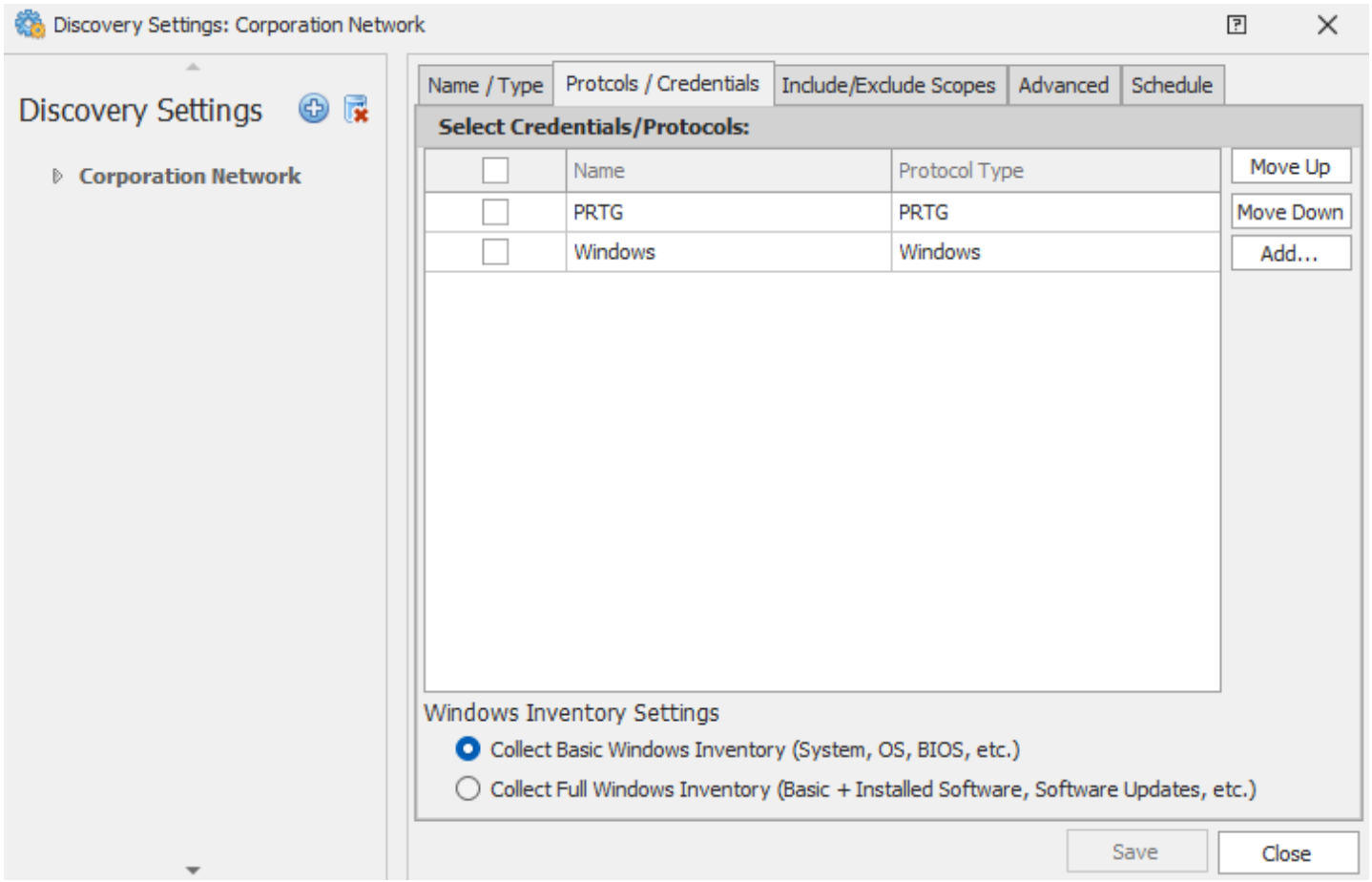
Seed IP Addresses / IP Ranges
For Ping Sweep discoveries, this field is used to enter the IP address ranges that should be pinged. For ARP Cache discoveries, this field is used to enter the IP addresses of the seed devices that are used to initiate the discovery (typically core network devices). To specify the desired IP addresses, enter one or more lines in the text field, each of which should contain one of the following:

- An individual IP address (e.g., 192.168.30.1)
- An IP subnet consisting of an IP address and subnet mask length (in bits) separated by a forward slash (e.g., 172.16.0.0/24)
- An IP address range consisting of minimum and maximum addresses separated by a dash (e.g., 10.0.0.32 – 10.0.0.96).

Pressing the 'Default Gateway(s)' button will automatically enter the IP addresses of the local computer's IP gateways. Pressing the 'Default Subnet(s)' button will automatically enter the subnets that the local computer is a member of. Pressing the 'Clear' button will clear the text field.

Protocols / Credentials

Protocols / Credentials
This section lets you select the network protocols and credentials that should be used during discovery. It displays a list of all credentials that have been previously defined (see Managing Device Credentials for more information). The row for each credential contains a checkbox that you can check to select the credential. The checkbox in the table header can be used to easily select ALL credentials. When you select a credential, you are both telling UVexplorer to use that protocol during discovery, and which credential to use with that protocol. Only the selected protocols and credentials will be used during discovery.



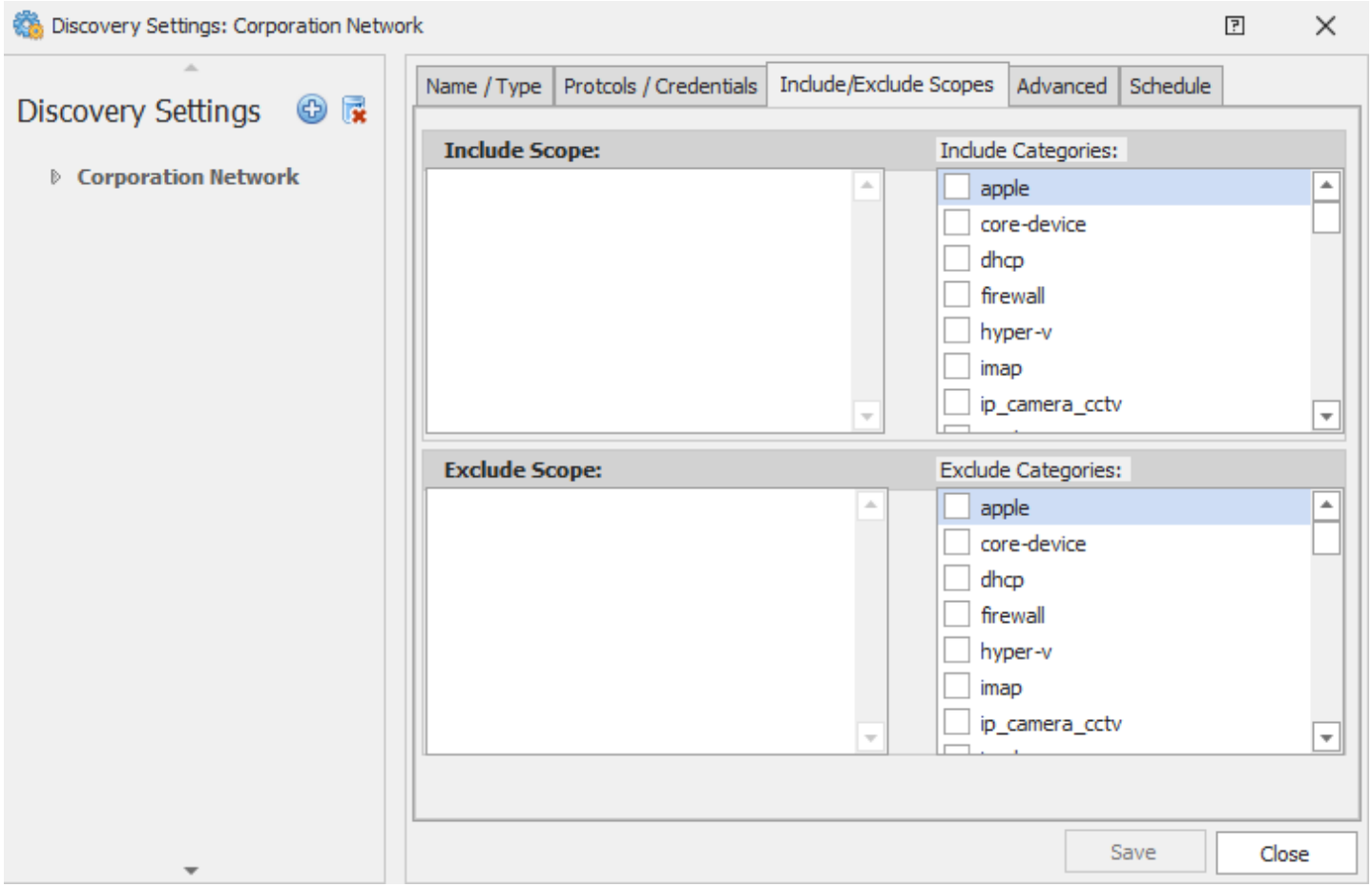
You may select multiple credentials for the same protocol, in which case UVexplorer will try them all on each device until it finds one that works. The order of the credentials in the table is significant, because it determines the order in which UVexplorer tries the credentials during discovery. You can use the 'Move Up' and 'Move Down' buttons to select a credential, and move it up or down in the table.

The 'Add' button can be used to create new credentials, or modify existing credentials.

Windows Inventory Settings
UVexplorer uses the WMI protocol to collect inventory information from Windows devices. In order to collect WMI inventory, you must specify appropriate Windows(WMI) credentials. WMI data collection can be time-consuming, so this setting lets you specify how much WMI data to collect. If you select 'Collect Basic Windows Inventory', only basic WMI data will be collected. This will result in the fastest possible discovery. If you select 'Collect Full Windows Inventory', detailed WMI data will be collected. This will result in a slower discovery that produces much more detailed inventory information for Windows devices.

Include/Exclude Scopes

UVexplorer makes every effort to find all of the devices on your network. By default, it probes all IP addresses that it comes across during the discovery process in order to find as many devices as possible. This is often exactly what you want. However, sometimes you might want to discover only a subset of your network rather than the whole thing. Additionally, there might be good technical or management reasons to keep the discovery process out of certain parts of your network. In scenarios where you want to carefully control which parts of your network are discovered, you can use the Include Scopes and Exclude Scopes settings.



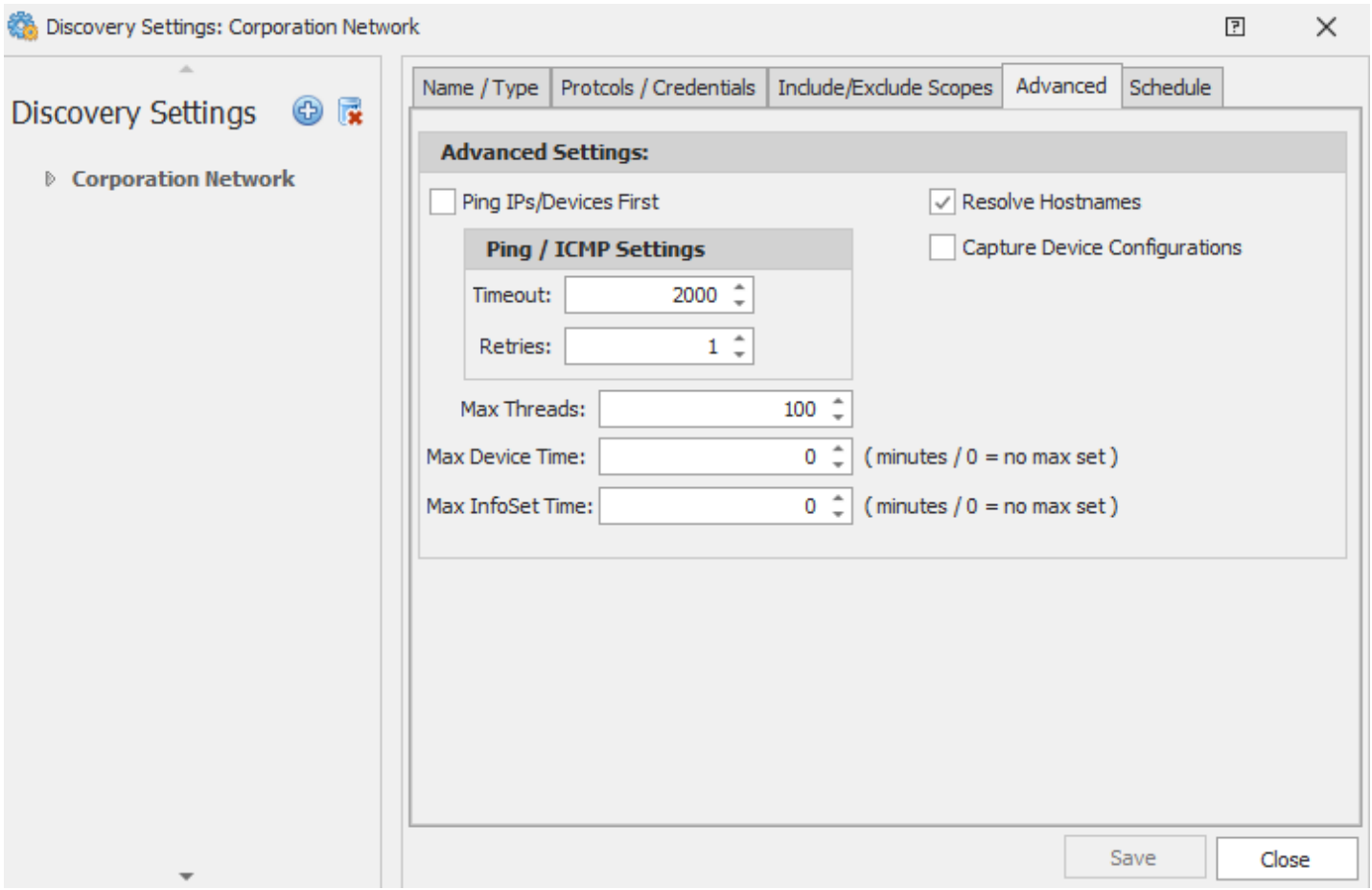
Include Scopes
The Include Scopes field can be used to specify precisely which IP addresses UVexplorer is allowed to discover. If specified, UVexplorer will discover ONLY IP addresses listed in this field.

Exclude Scopes
The Exclude Scopes field can be used to specify IP addresses that are off-limits during discovery. If specified, UVexplorer will discover all IP address EXCEPT the ones listed in this field.

Both of these fields may contain zero or more lines of text, each of which should contain one of the following:

- An individual IP address (e.g., 192.168.30.1)
- An IP subnet consisting of an IP address and subnet mask length (in bits) separated by a forward slash (e.g., 172.16.0.0/24)
- An IP address range consisting of minimum and maximum addresses separated by a dash (e.g., 10.0.0.32 – 10.0.0.96).

Advanced
This section contains a variety of advanced settings that you can specify. Each of them is described next.



Ping IPs/Devices First
For Ping Sweep discoveries, UVexplorer will always try to ping each device before trying to use other protocols to communicate with them. However, for ARP Cache discoveries you can use this setting to control whether or not UVexplorer will try to ping devices first. If your network and devices allow ping requests, enabling this option can result in faster discoveries (i.e., if UVexplorer can't ping a device, it won't bother trying other protocols on it, thus speeding things up). If your network and devices do not allow ping requests, disabling this option will allow UVexplorer to successfully discover your devices even though they can't be pinged.

Resolve Hostnames
If this option is enabled, UVexplorer will resolve IP addresses to their corresponding DNS hostnames. This is done using reverse-DNS lookup.

Capture Device Configurations
UVexplorer can capture device configurations for many types of network devices (switches, routers, wireless APs, etc.). If this option is enabled, UVexplorer will attempt to retrieve configurations for all devices it can. Configuration capture is done using the SSH protocol. In order for this feature to work, you must specify SSH credentials for any devices for which you want configuration captures.

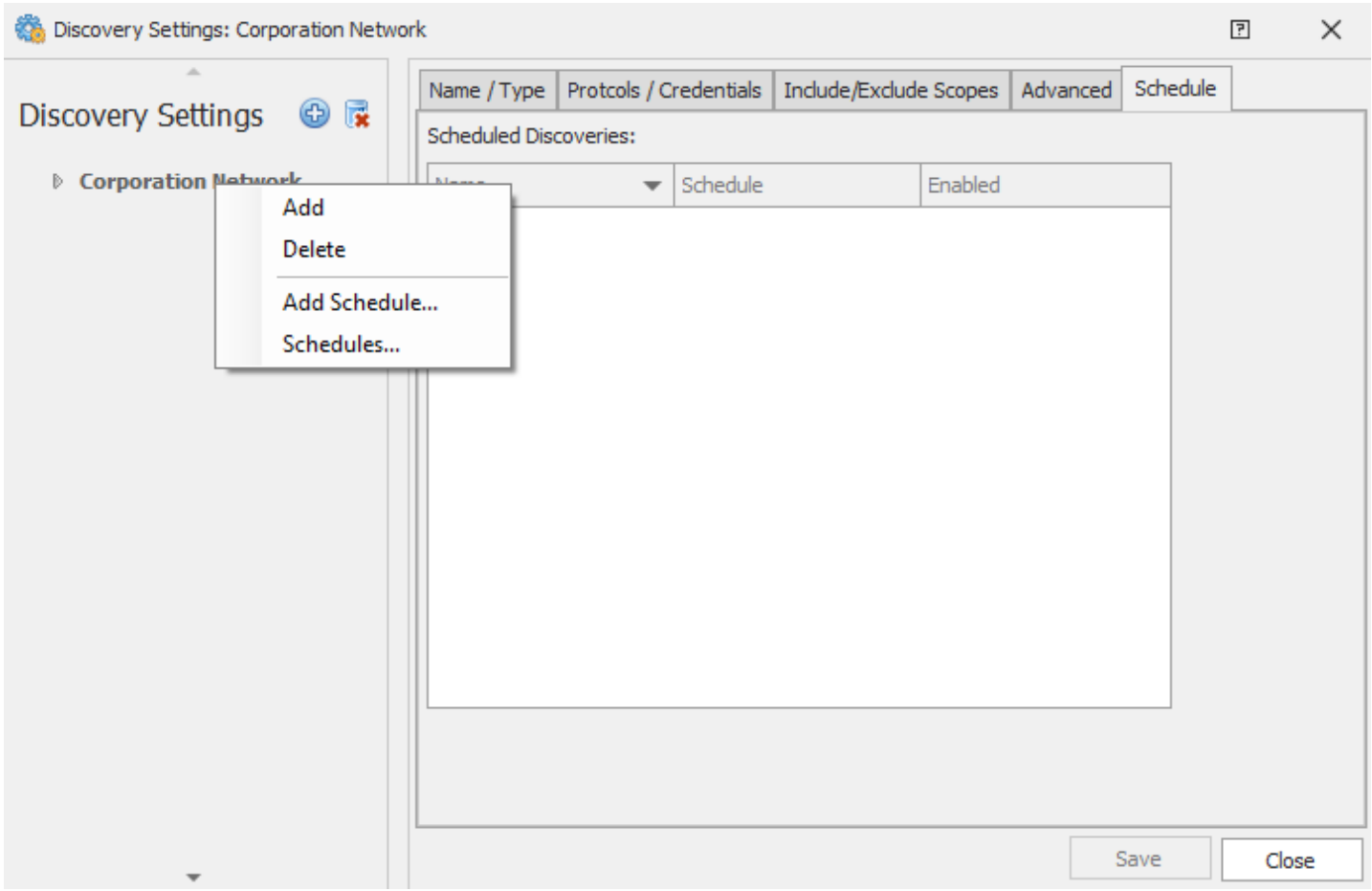
Max Threads
During a typical discovery, many devices need to be interrogated. To make discovery run as quickly as possible, UVexplorer works on many devices at the same time. However, discovering many devices at once can put more load on your network. Therefore, the 'Max Threads' setting can be used to precisely control the maximum number of devices that UVexplorer will communicate with concurrently. This lets you control the tradeoff between discovery speed and network load.

Exclude Categories
By default, UVexplorer will include all devices that it finds in the discovery result. Sometimes you might not be interested in certain kinds of devices, and prefer that they not be included in the

result. The 'Exclude Categories' setting lets you enumerate specific categories of devices to be omitted from the discovery result. Each type of device you select will be dropped from the discovery result.

Deleting Discovery Settings

To delete an existing discovery settings object, select it in the discovery settings list on the left side of the form, and then click the Delete icon (with the red X) just above the list. Alternatively, you can right-click on the discovery settings in the list, and select Delete from the context menu. The deleted discovery settings should disappear from the list.



Scheduling Network Discoveries

While you can always run network discoveries manually, it can also be convenient to have UVexplorer run discoveries for you automatically on a scheduled basis. For example, you could schedule a discovery to run every day at 2:00 PM. Scheduled discoveries allow you to capture the state of your network at regular intervals. Not only does this automatically keep your discovery results up to date, but it also allows you to have a record of how your network is changing over time, and to receive notifications of how things are changing. For example, you might want to be notified each time an unknown device attaches to your network. By running scheduled discoveries, UVexplorer can compare the latest discovery result with previous ones to detect when new devices come onto your network. In general, UVexplorer can notify you when devices enter or leave your network, as well as when network links between devices are added or removed. This information can be invaluable for helping you know what is happening on your network.

NOTE: UVexplorer must be running for scheduled discoveries to run. If you exit from the program, scheduled discoveries will no longer run. UVexplorer is a Windows tray application, and you can Hide the program while allowing it to still run. When it is hidden, UVexplorer will continue to run scheduled discoveries. However, if you exit entirely from the program, scheduled discoveries will not run.

Scheduled Discovery Results

UVexplorer stores two types of discovery results for each scheduled discovery.

Raw Discovery Result

Each time a scheduled discovery runs, UVexplorer stores the raw result of the discovery. The raw result stores a snapshot of what the network looked like at the time the scheduled discovery ran. There are multiple raw results for the scheduled discovery in the database, one for each execution of the discovery.

Rollup Discovery Result

UVexplorer also stores a 'rollup' discovery result for each scheduled discovery. Unlike raw discovery results, of which there is one for each execution of the scheduled discovery, there is only one rollup result for each scheduled discovery. The rollup discovery result is the union of all devices that have been seen recently on the network. This includes devices that were seen during the last several executions of the scheduled discovery. The rollup discovery result is useful because networks are dynamic with devices coming and going all the time. While a given scheduled discovery execution might miss some devices because they happened to be off the network when the discovery ran, combining all devices from several recent scheduled discovery runs gives a more accurate picture of the network.

Scheduled Discovery Events

One of the advantages of using scheduled discoveries is the ability it provides to determine how your network is changing over time. Each time a schedule discovery runs, it compares the current state of the network with the prior state of the network to determine what devices have been added and removed, as well as what network links have been added and removed. When changes in the network are detected, UVexplorer generates events to notify you of the changes. Specifically, the following types of events are generated:

Device Added

A new device was detected on the network. This type of event applies to all devices.

Device Removed

A previously known device disappeared from the network. This event is generated only for 'core' infrastructure devices such as routers, switches, wireless access points, servers, etc. It is not generated for 'dynamic' devices that come and go from the network on a regular basis.

Link Added

A new network link was added to the network.

Link Removed

A previously known network link disappeared from the network.

Events are displayed in the Events tab of the main UVexplorer window. Optionally, events are also emailed to one or more specified email addresses.

Managing Scheduled Discoveries

To manage your scheduled discoveries, click the Scheduled Discoveries icon on the Home toolbar. This will display the Scheduled Discoveries form. This form allows you to add, configure, delete, and view the status of scheduled discoveries. A list of all existing scheduled discoveries is displayed on the left side of the form. The right side of the form displays a tab view which can be used to view and edit the properties of the currently-selected scheduled discovery.

NOTE: Changes made in the Scheduled Discovery form do not take effect until the form is closed. For example, if you disable a scheduled discovery or change the scheduled on which it runs, these changes will not take effect until the Scheduled Discovery form is closed.

Adding a Scheduled Discovery

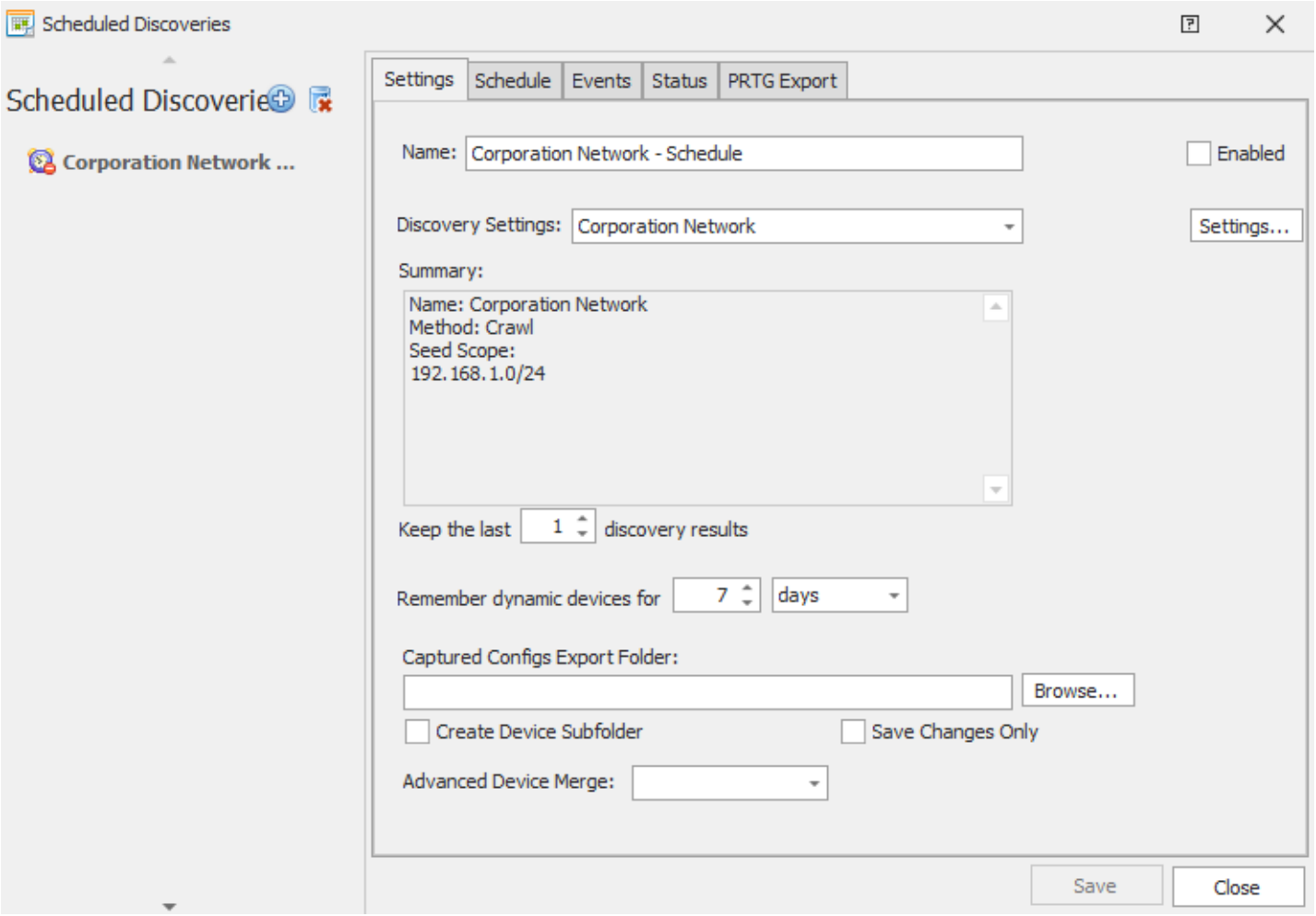
To create a new scheduled discovery, click on the Add icon (the plus sign) just above the scheduled discovery list on the left side of the form. Alternatively, you can right-click anywhere in the scheduled discovery list, and select Add from the context menu. This will cause a new scheduled discovery with the name 'ScheduledDiscovery' to be created and selected. You can then edit the properties of the new scheduled discovery in the tab view on the right side of the form.

Configuring a Scheduled Discovery

The properties of a scheduled discovery can be modified by first selecting it in the list of scheduled discoveries. After it has been selected, the tab view on the right side displays the various properties that can be edited.

Settings Tab

The Settings tab displays the following scheduled discovery properties:



Name

This is the scheduled discovery's name. This value must not be empty.

Enabled

This setting determines whether or not the scheduled discovery is enabled. If the scheduled discovery is enabled, it will run according to its specified schedule. When not enabled the scheduled discovery will not run automatically (but may still be run manually).

Discovery Settings

The Discovery Settings drop-down list is used to select the discovery settings that will be used when the scheduled discovery runs. If no discovery settings are selected, the scheduled discovery will not run. The Discovery Settings drop-down list displays all existing discovery settings from which you may choose. If the desired discovery settings do not already exist, you can click the Settings button to bring up the Discovery Settings form, which allows the creation of new discovery settings.

Keep the Last N Discovery Results

A scheduled discovery will run many times, and each execution will create an additional raw discovery result. Over time, many raw discovery results will accumulate. Typically, it is only useful to keep a relatively small number of the most recent discovery results. This setting lets you specify how many of the most recent raw discovery results to keep. All raw discovery results beyond the specified number will be automatically deleted.

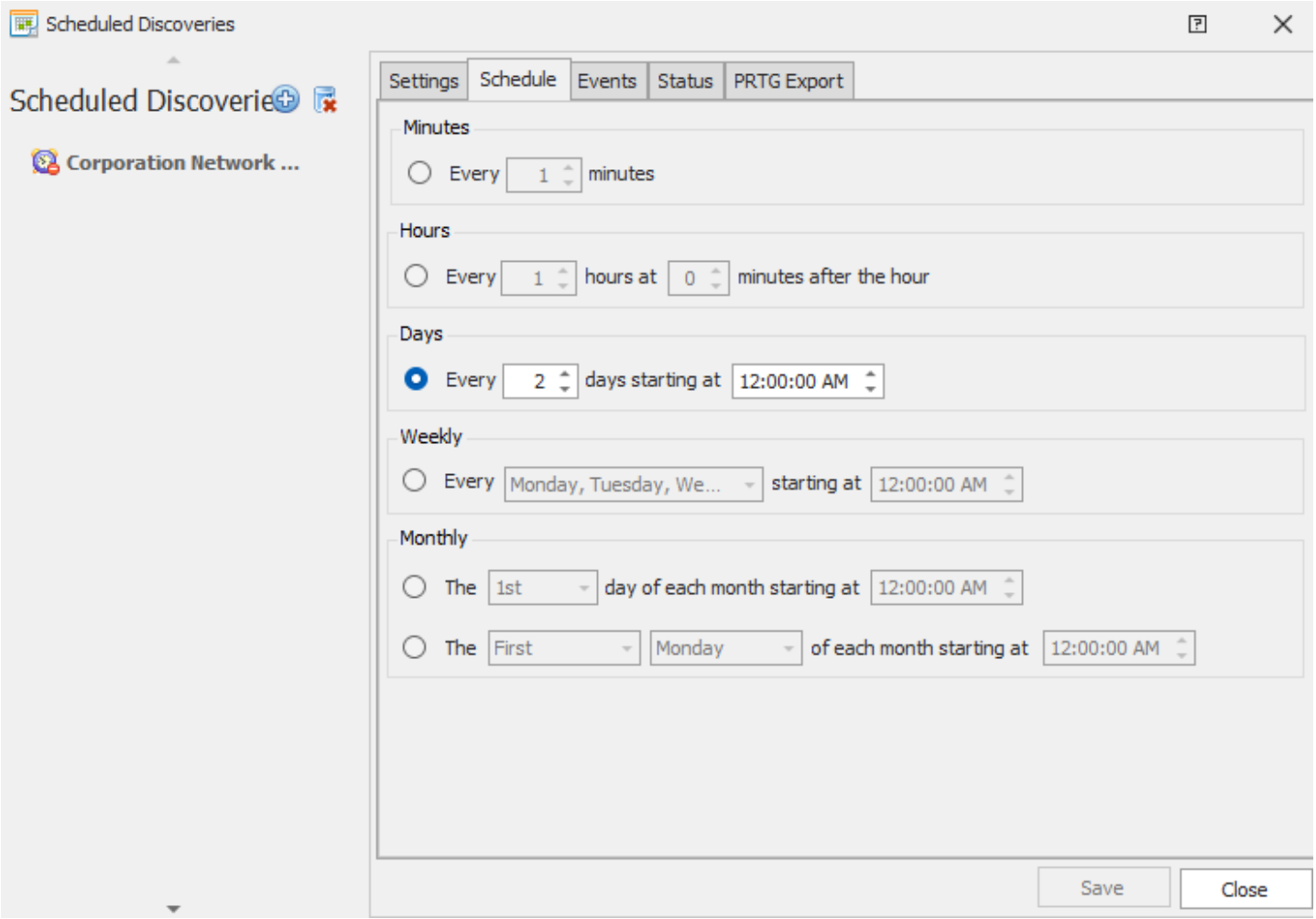
Remember Dynamic Devices for N (Days, Hours, Minutes)

A scheduled discovery's rollup discovery result contains all devices that have been seen in the several

most recent executions of the scheduled discovery. The rollup result contains the set of all 'known' devices on the network. When a device has not been seen for multiple consecutive discoveries, it is necessary to eventually drop the device from the rollup discovery result, at which point the device becomes 'unknown' again. This setting lets you specify how long to wait before dropping a device from the rollup discovery result. Once a device has been dropped, if it is ever seen again in a future discovery run, it will generate a 'device added' event.

Schedule Tab

The Schedule tab lets you specify the schedule on which the discovery should run.



The following schedule types are available:

Minutes
This schedule will run the discovery every N minutes. For example, 'Run every 30 minutes'.

Hours
This schedule will run the discovery every N hours at a specified minute during the hour. For example, 'Run every 6 hours'.

Days
This schedule will run the discovery every N days at a specified time of day. For example, 'Run every 3 days at 2:00 PM'.

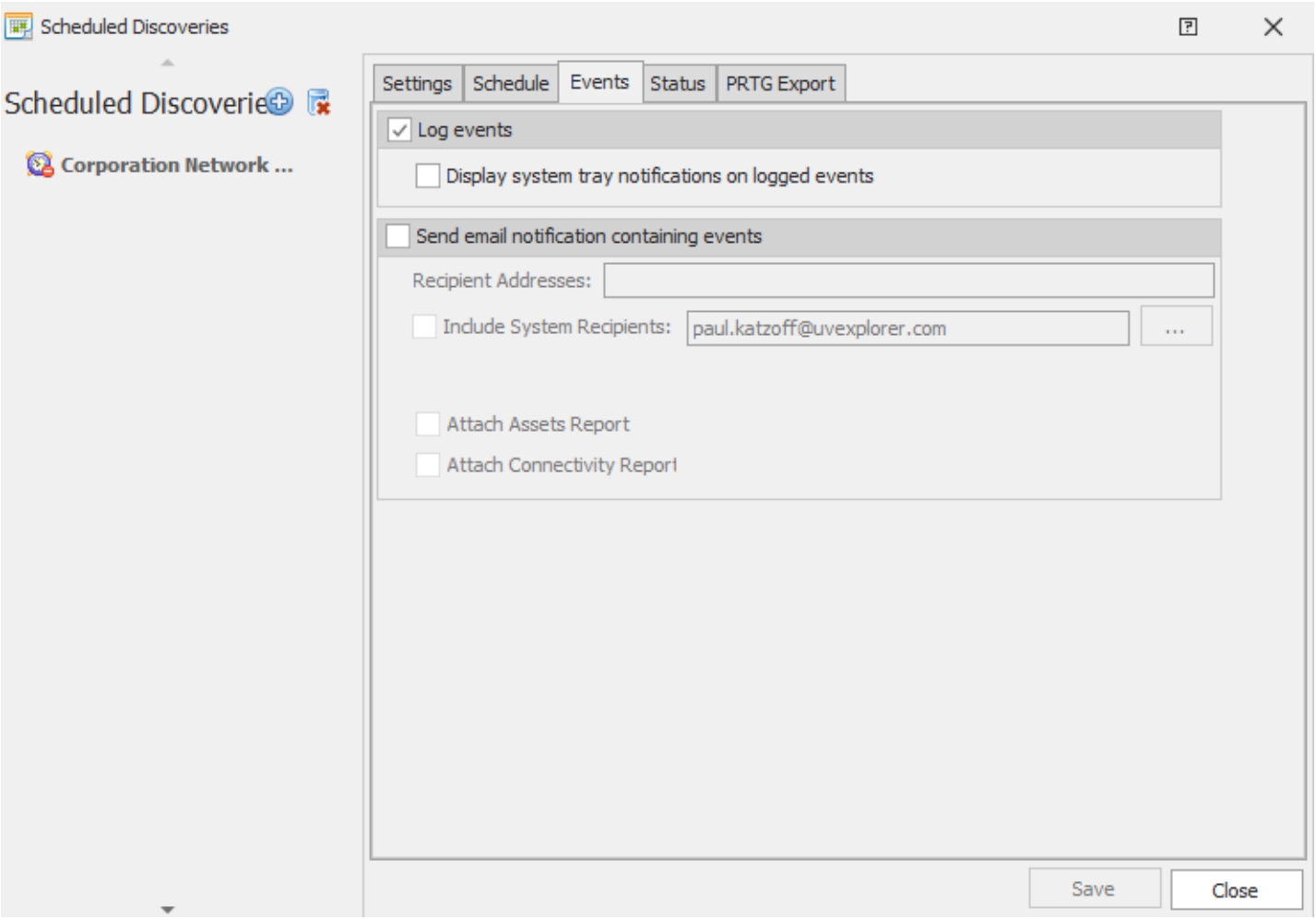
Weekly
This schedule will run the discovery weekly on specified days of the week at a specified time of day. For example, 'Run every Friday at 2:00 PM'.

Monthly (Nth day of month)
This schedule will run the discovery monthly on the Nth day of the month at a specified time of day. For example, 'Run on the 1st day of each month at 2:00 PM'.

Monthly (Ordinal day of week)
This schedule will run the discovery monthly on the first, second, third, fourth, or last occurrence of the specified week day. You can also specify the time of day at which the discovery will run. For example, 'Run the last Friday of each month at 2:00 PM'.

Events Tab

The Events tab lets you specify how scheduled discovery events will be reported.



Log Events
This setting controls whether scheduled discovery events are displayed in the UVexplorer Events tab.

Display System Tray Notifications on Logged Events
This setting controls whether a system tray (i.e., balloon) notification is displayed to alert you about new scheduled discovery events.

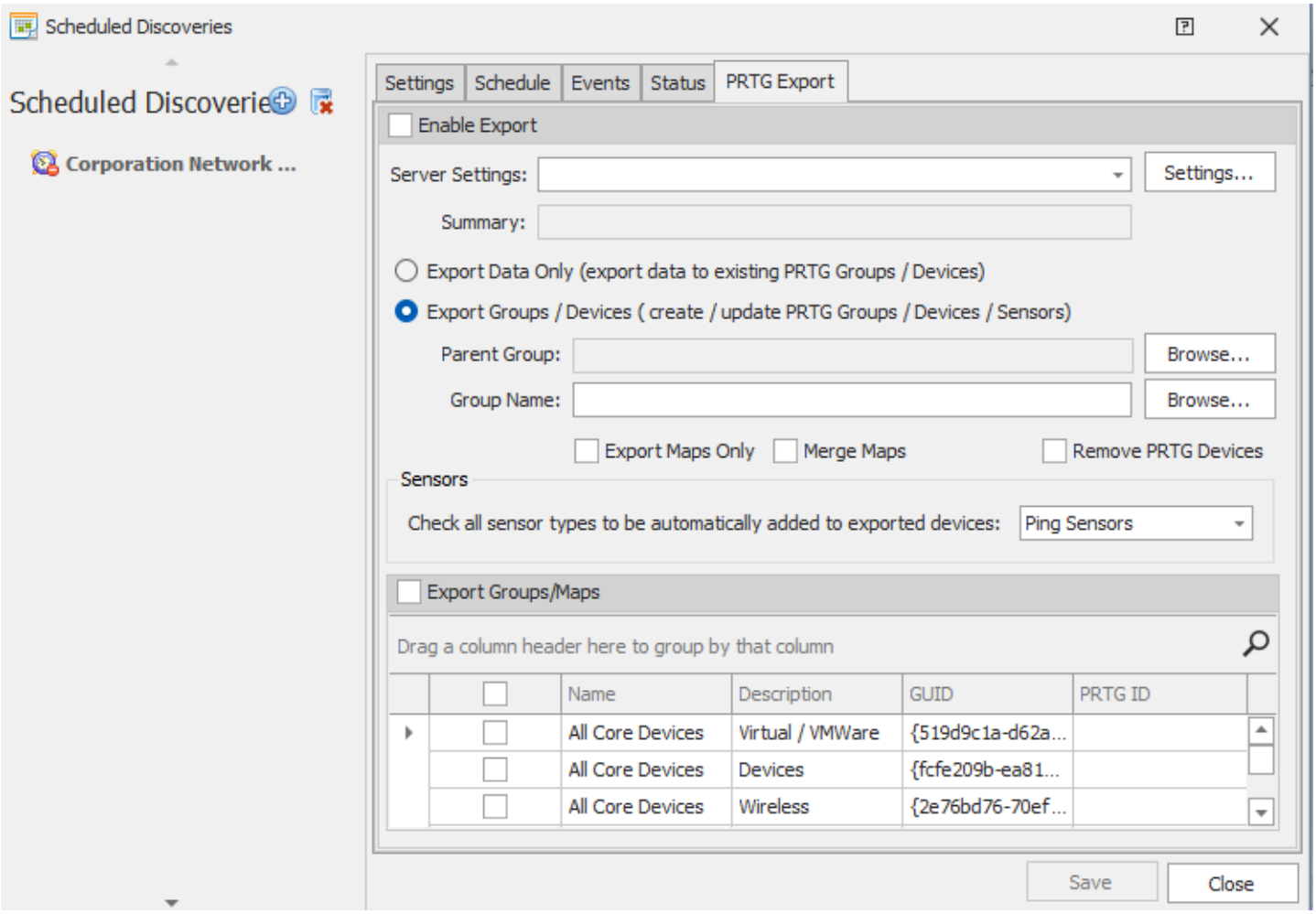
Send Email Notification Containing Events
This setting controls whether a notification email is sent each time the scheduled discovery completes. The email contains a summary of the scheduled discovery results, including all network changes that were detected. If this setting is checked, email notifications will be sent to all email addresses specified in the Recipient Addresses field.

Recipient Addresses
A list of email addresses to which scheduled discovery email notifications will be sent. If multiple addresses are specified, they should be separated with commas or semicolons.

Include System Recipients
If this option is checked, email notifications will also be sent to all email addresses specified in the Recipient Addresses field of the global email settings. (To view the global email settings, go to the main UVexplorer window, select the Settings toolbar, and click the Email Settings icon.)

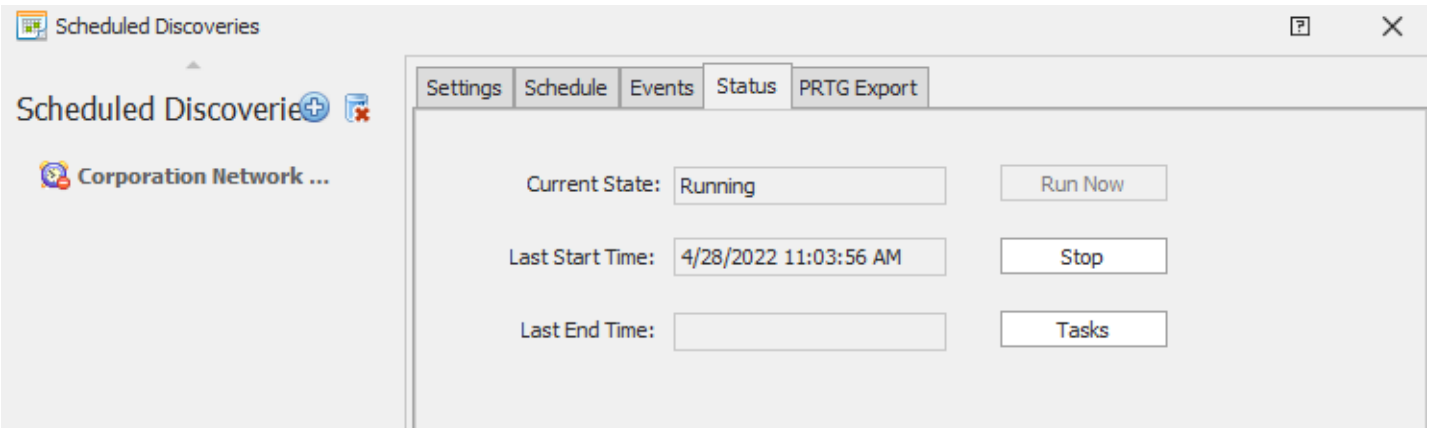
PRTG Export Tab

When the PRTG connector is available UVexplorer can export to PRTG at the conclusion of a scheduled discovery. See Export to PRTG for more information.



Viewing a Scheduled Discovery's Status

The status of a scheduled discovery can be viewed by first selecting it in the list of scheduled discoveries, and then selecting the Status tab on the right side.



The following information is displayed:

Current State
This field displays the current state of the scheduled discovery. The possible values for this field are as follows:

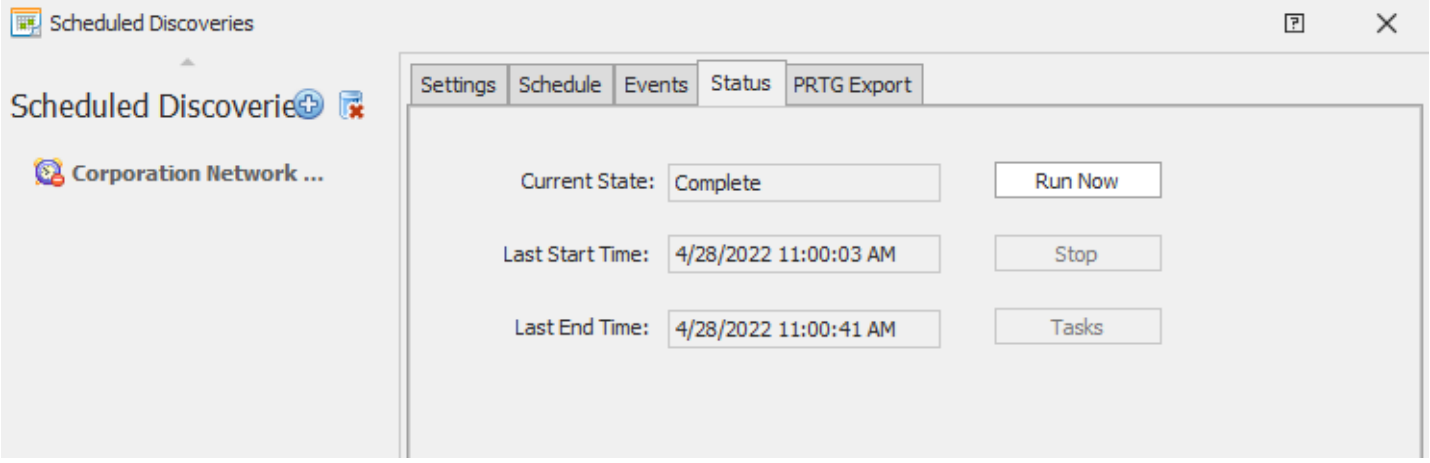
1. Created: The scheduled discovery was created, but has never run.
1. Running: The scheduled discovery is currently running.
2. Complete: The scheduled discovery is not currently running, and it successfully completed the last time it ran.
3. Canceled: The scheduled discovery is not currently running, and it was canceled the last time it ran.
4. TimedOut: The scheduled discovery is not currently running, and it timed out the last time it ran.
5. Faulted: The scheduled discovery is not currently running, and it encountered an error the last time it ran.

Last Start Time
This field displays the date and time at which the scheduled discovery last started. This will be empty if the scheduled discovery has never run.

Last End Time
This field displays the date and time at which the scheduled discovery last ended. This will be empty if the scheduled discovery has never run, or if it is currently running.

Manually Running a Scheduled Discovery

A scheduled discovery can be manually executed on demand by first selecting it in the list of scheduled discoveries, and then selecting the Status tab on the right side.



The following operations are available:

Run Now
This button is enabled only if the scheduled discovery is not already running. Clicking it will start the scheduled discovery. It might take several seconds for the discovery to begin.

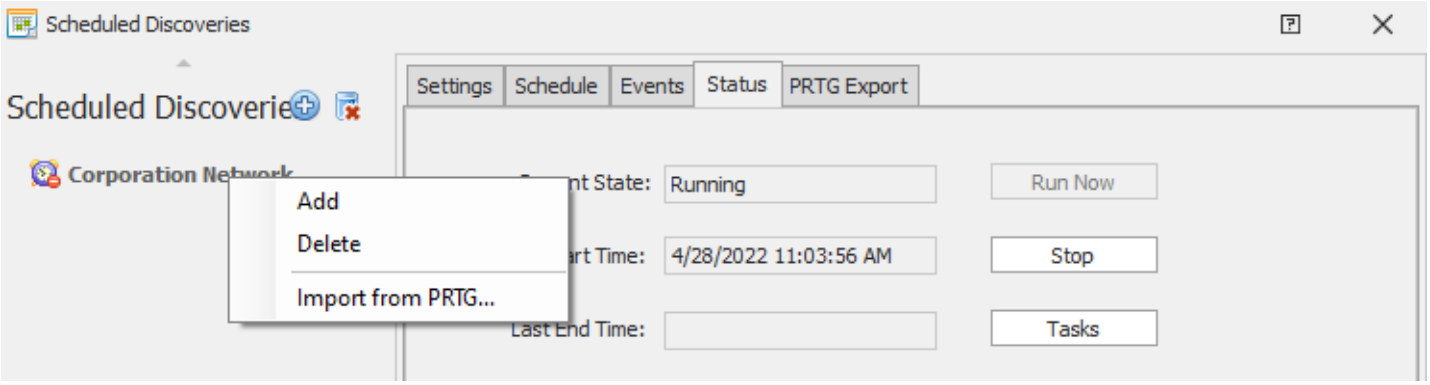
Stop
This button is enabled only if the scheduled discovery is currently running. Clicking it will cancel the scheduled discovery. It might take several seconds for the discovery to stop.

Tasks

This button is enabled only if the scheduled discovery is currently running. Clicking it will display the Discovery Tasks form. This form displays detailed information about what the scheduled discovery is currently doing. It is useful for determining what devices are currently being discovered, what information is being collected from these devices, and why the discovery has not yet completed. It also allows discovery sub-tasks to be individually canceled. This can be useful if for some reason discovery gets stuck on a badly-behaving device.

Deleting a Scheduled Discovery

To delete an existing scheduled discovery, select it in the scheduled discovery list on the left side of the form, and then click the Delete icon (with the red X) just above the list. Alternatively, you can right-click on the scheduled discovery in the list, and select Delete from the context menu. The deleted scheduled discovery should disappear from the list.



Scheduled Discovery Events

Scheduled discoveries run on a periodic basis. Each time a scheduled discovery runs, important events that occur during the discovery are added to the event log. These events are helpful in monitoring the activity and progress of your scheduled discoveries.
Each time a scheduled discovery runs, the following types of events are added to the log:

Completion Events

An event is generated each time a scheduled discovery ends execution.

Skip Events

An event is generated when a scheduled discovery does not run because it is already running. This happens when scheduled discovery runs are scheduled too close together, and one execution does not have time to complete before the next one begins. If this occurs, you should change your discovery schedule so that the discovery runs are farther apart.

Error Events

An event is generated each time an error occurs during a scheduled discovery run.

Device Added Events

An event is generated each time a new device appears on the network. For core devices (routers, switches, wireless access points, servers, etc.), events are generated every time one of these devices appears on the network. For dynamic devices that come and go on the network (cell phones, tablets, laptops, etc.), events are generated only when such a device appears on the network, and it has not been seen recently on the network. The settings of a scheduled discovery control how long a dynamic device must be gone from the network before it is considered new. (See the scheduled discovery setting named 'Remember dynamic devices for'.)

Device Removed Events

An event is generated each time a core device (router, switch, wireless access point, server, etc.) disappears from the network. These events are not generated for dynamic devices (cell phones, tablets, laptops, etc.), because it is entirely expected that these devices will frequently leave the network.

Link Added Events

An event is generated each time a new link appears on the network (i.e., each time a new connection between devices is detected).

Link Removed Events

An event is generated each time a link between core devices disappears from the network. Core devices are devices that form the core of your network, such as routers, switches, wireless access points, servers, etc. Each time a connection between such devices disappears, an event is generated. Events for removed links involving dynamic devices (cell phones, tablets, laptops, etc.) are not generated, because it is entirely expected that these devices will frequently leave the network.

Opening Discovery Results

The Open Discovery Result form lets you perform the following operations:

- Open a saved discovery result
- Merge a saved discovery result with the current discovery result
- Delete a saved discovery result

The form displays a list of all discovery results that are currently saved in the UVexplorer database. Before performing any of the operations listed above, you must first select one of the discovery results from the list.

The following properties are displayed for each discovery result:

Discovery Result Name
This is the name assigned to the discovery result when it was saved.

Type
This is the discovery result's type, which describes the origin of the result. The possible values for this property are:

- Manual – The result was created by a manual (i.e., non-scheduled) discovery.
- Scheduled (Raw) – The result stores the raw result of a scheduled discovery execution. It stores a snapshot of what the network looked like during one particular execution of the scheduled discovery. The Discovery Result Name property indicates which scheduled discovery created the result.
- Scheduled (Rollup) – The result stores the 'rollup' for a scheduled discovery. Unlike raw discovery results, of which there is one per execution of the scheduled discovery, there is only one rollup result for each scheduled discovery. The rollup discovery result contains the union of all devices that have been recently seen on the network by the scheduled discovery. The Discovery Result Name property indicates which scheduled discovery the 'rollup' result belongs to.

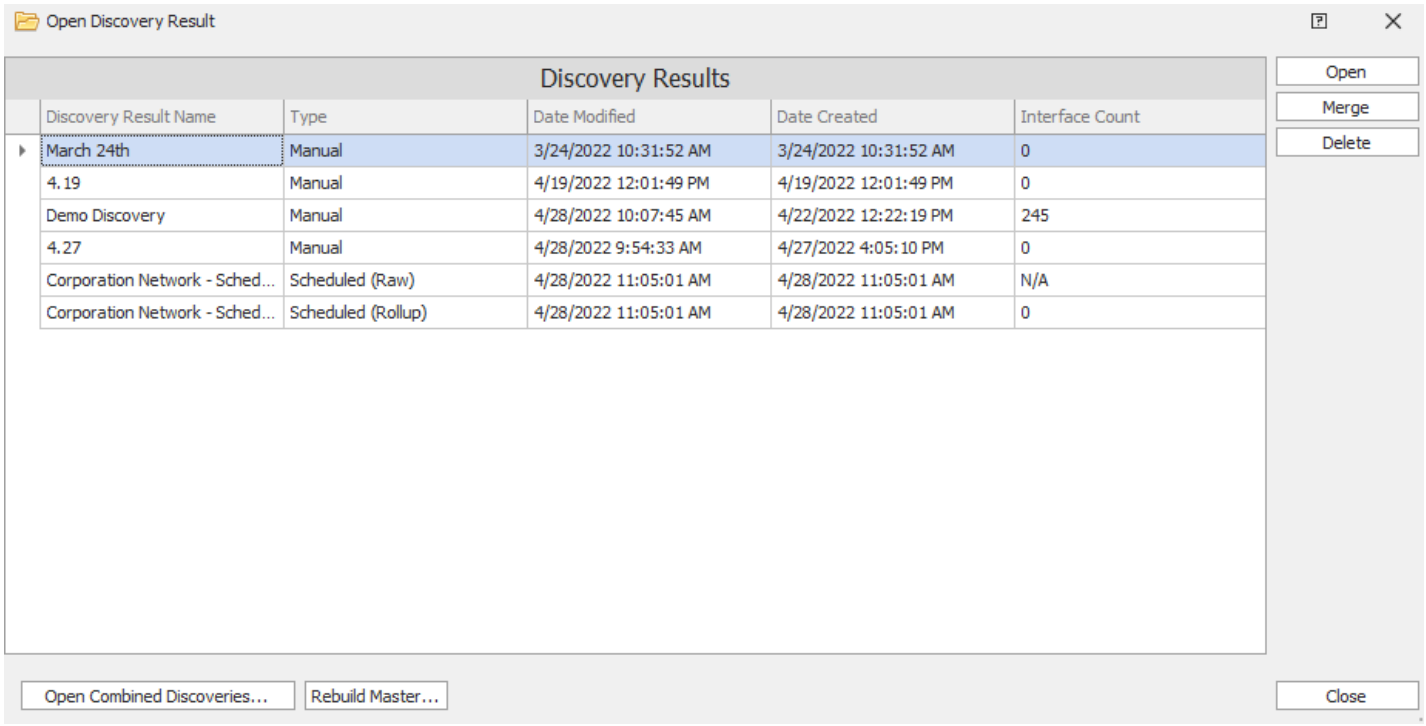
Date Modified
The date and time at which the most recent changes were made to the discovery result.

Date Created
The date and time at which the discovery result was originally created.

Opening Discovery Results

You will frequently want to open a saved discovery result from the database in order to view or modify it. This can be done in the Open Discovery Result form by selecting the desired discovery result in the displayed list, and clicking the Open button. (Alternatively, you can just double-click on the desired discovery result.) This will cause the selected discovery result to be loaded from the

database. The selected discovery result will replace whatever discovery result is already open in the program. If the current discovery result contains any unsaved changes, you will be prompted to save the changes before the new discovery result is loaded.



Merging Discovery Results

It is sometimes useful to merge separate discovery results into a single combined discovery result. To make this possible, at any time you can merge a saved discovery result with the currently-open discovery result. This can be done in the Open Discovery Result form by selecting the desired discovery result in the displayed list, and clicking the Merge button. This will cause all devices and network links from the selected discovery result to be merged (or combined) with the devices and network links in the current discovery result. You may then save the combined discovery result to the database, if you wish.

Deleting Discovery Results

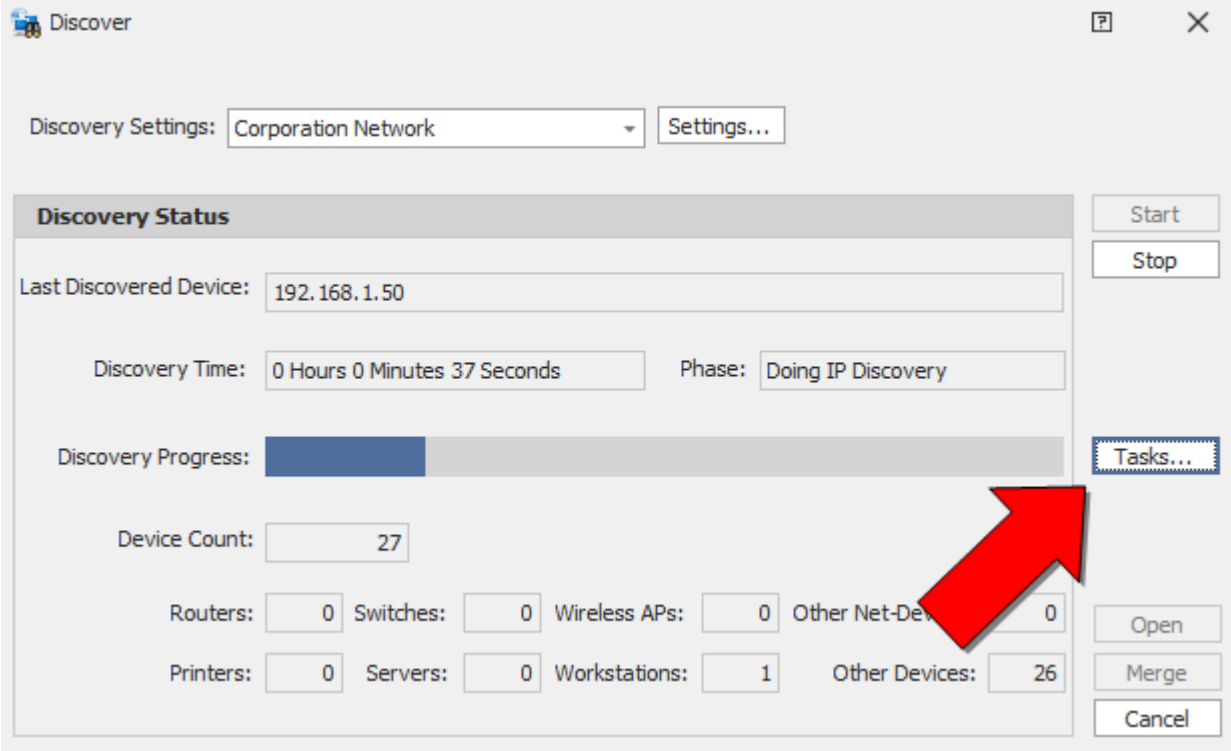
To delete a saved discovery result, select the result to be deleted in the displayed list, and click the Delete button. This will remove the selected result from the database.

Discovery Tasks

When a network discovery is running, UVexplorer performs many concurrent activities in order to find devices on the network and collect detailed information about them. Some devices are quite simple and can be discovered quickly. Other devices are complex, and more time is needed to discover everything about them. While discovery is going on, you might have questions such as:

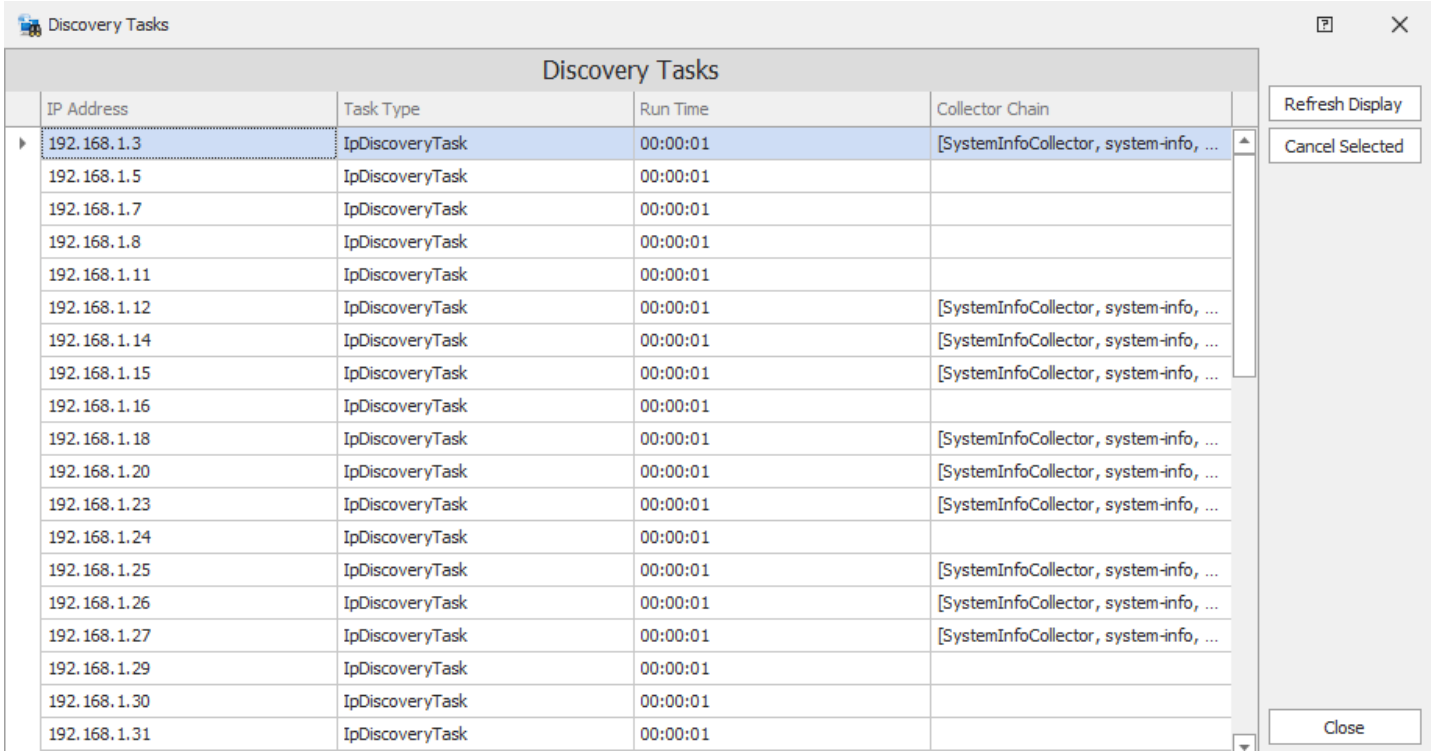
- How close is the discovery to being done?
- What devices are being discovered right now?
- What information about each device is currently being discovered?

These questions are even more relevant when a discovery is taking longer than you expect, and you want to know what is taking so long.
In order to help answer these questions, the Discovery Tasks form displays detailed information about exactly what tasks a discovery is currently working on. It is useful for determining what devices are currently being discovered, what information is being collected from those devices, and why the discovery has not yet completed. It also allows discovery tasks to be individually canceled, which can be useful if discovery gets stuck on a badly-behaving device.



Discovery Task Details

When the Discovery Task form is opened, it automatically populates the form with information about all discovery tasks that are currently in progress. Typically, each task listed represents a single IP address that UVexplorer is attempting to communicate with.



The following properties are displayed for each discovery task:

IP Address

This field displays the IP address that the discovery task is attempting to communicate with. If there is no device with the specified IP address, the communication will fail, and the discovery task will determine that no such device exists. If, however, there is a device with the specified IP address, the discovery task will collect all the information it can about the device before it completes.

Task Type

This field displays the discovery task's type. Discovery involves several different types of tasks that collect different types of data. Possible values for this field include:

- IpDiscoveryTask – This task determines whether there is a device with a specific IP address, and collects some basic information about the device.
- ResolveHostnamesTask – This task determines the host names for each device by doing a reverse DNS lookup for each discovered IP address.
- DetailedDiscoveryTask – This task collects in-depth, detailed information about the device with a specific IP address.

Run Time

This field displays the amount of time for which the discovery task has been running. The format is HH:MM:SS.

Collector Chain

This field displays detailed information about what the discovery task is currently doing. For some task types this field is empty.

Actions

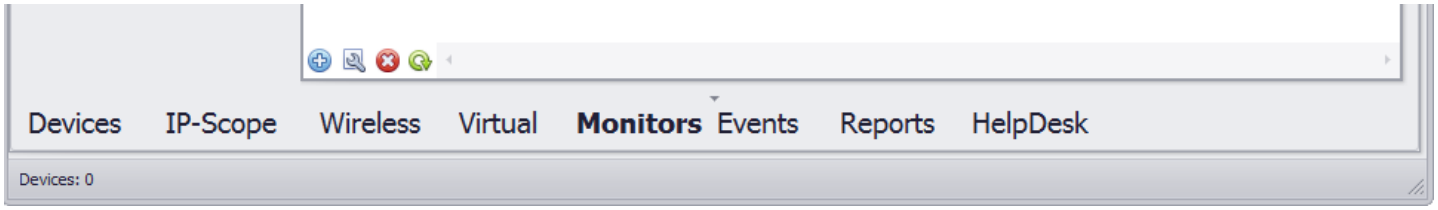
Clicking the Refresh Display button will update the discovery task information in the form.
Clicking the Cancel Selected button will cancel each discovery task that that is selected in the form. This allows you to selectively cancel the discovery of devices that are taking too long to finish. When a task is canceled, it can take several seconds before it actually terminates.

Clicking the Close button will close the Discovery Tasks form.

Monitors

UVexplorer monitors allow you to query specific information regarding device state and configuration from the monitored devices on a recurring interval. The Monitors view allows you to configure monitors and view their results.

To access the monitor view, select the 'Monitors' link at the bottom of the main application view. The Monitors view contains a navigation pane with the available monitors and monitor results and a main monitors view where the corresponding results and monitors can be viewed.

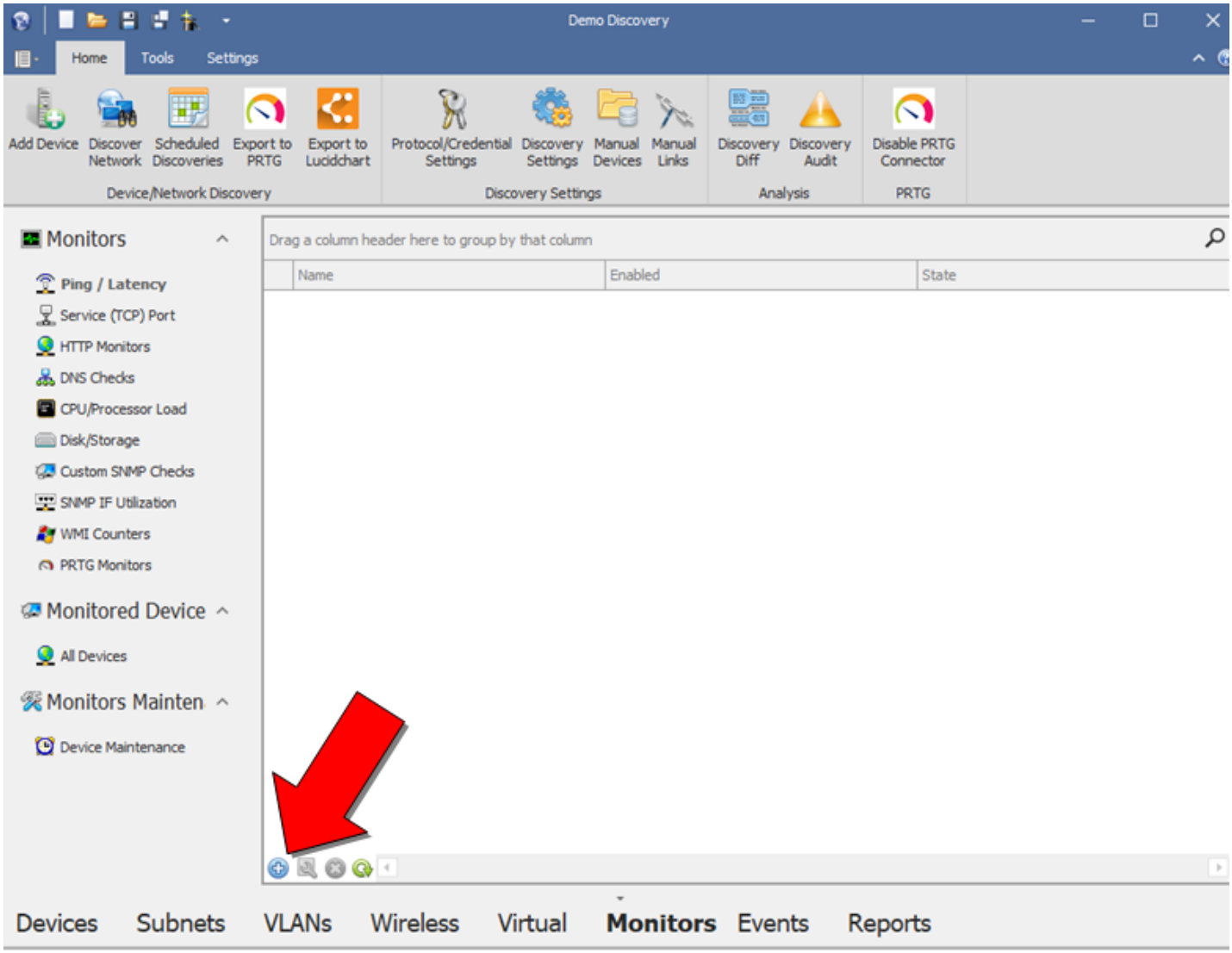


Monitored Devices

UVexplorer manages monitored devices separate from the devices stored in the Discovery Results. See Monitored Devices for more information on managing monitored devices.

Creating Monitors

To create a monitor of a specific type, start by selecting the desired monitor type in the left navigation pane. For example, to create a ping monitor you would select the 'Ping / Latency' item in the Monitors section of the navigation pane. Selecting a monitor type will change the context of the main view and all monitors of the corresponding monitor type will be showing in the main view. With the desired monitor selected, add a monitor by right clicking on the main grid and selecting 'Add...' in the context menu, or by pressing the add button in the lower left corner of the monitor view. A monitor configuration editor for the selected monitor will appear.



Editing Monitors

To edit a monitor, select the monitor in the list and right click and select 'Edit...' in the context menu, or press the edit button in the lower left corner of the monitor view. The monitor editor will be displayed.

Deleting Monitors

To delete a monitor, select the monitor and right click and select 'Delete' in the context menu, or press the delete button in the lower left corner of the monitor view. A confirmation dialog will be presented, and the monitor will be deleted upon confirmation.

NOTE: When a monitor is deleted all results associated with that monitor will be deleted.

Running a Monitor

Monitors will be run based on their schedule and if the monitor is enabled. A monitor can also be run on demand by selecting 'Run Now' in the monitors context menu. When a monitor is run on demand, it will be run quietly in the background, for most monitors depending on the number of devices included in the monitor this will happen very quickly. When the monitor completes the application will update automatically reflecting any changes to the monitor or related device states.

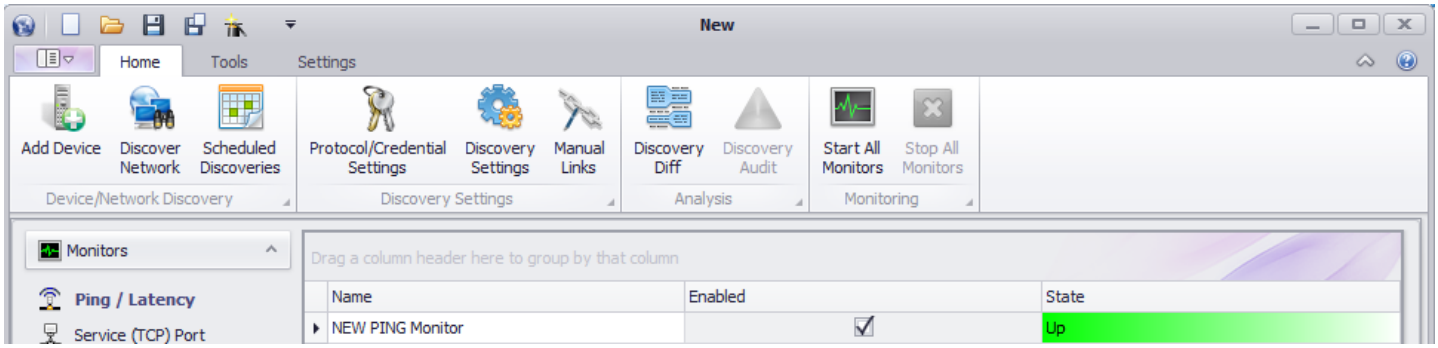
Enabling a Monitor

A monitor will only run on its schedule if it is enabled. A monitor can be enabled within the monitor editor by checking the enable check box. Monitors can also be enabled/disabled in the main monitor

view by selecting the check box for that monitor in the 'Enabled' column. When a monitor is disabled, it will not run on its schedule again until the enabled checkbox is re-selected.

Starting and Stopping All Monitors

At times it may be desirable to pause all monitors for time. This may be accomplished by selecting the 'Stop All Monitors' button in the "Home" tab of the main form ribbon header. Stopping all monitors will stop any new monitors from being scheduled to run. Any currently running monitors will run till completion. To restart the monitors so that they run on their schedules select the 'Start All Monitors' button. If a monitor missed its scheduled run time while the monitors were stopped, it will run shortly after restarting the monitors.



Monitors may still be run on demand when the scheduled monitors are stopped.

Monitor Maintenance Policies

Occasionally you may want to pause the monitors for a particular device on a one time or recurring basis. This can be accomplished using maintenance policies. See Maintenance Policy for more information.

Clearing Monitor History

When a monitor runs the results of the monitor queries will be stored and available for viewing and used to determine the monitor state. To manage the number of results stored each monitor can be configured to limit the number of stored results. If at any point you would like to clear all of the results collected by a particular monitor, you may select 'Clear History...' in the monitors context menu. This will delete all the data collected by that monitor to that point.

Viewing Monitor Results

When a monitor is run it will collect information for all of the devices or entries associated with that device. Each entry in the device will have its own state associated with its results. The monitor will also have an overall stated based on the state of the entries within the monitor. With a Ping/Latency monitor for example, if one of the devices failed to respond to the ping queries and received a state of 'Down'; the monitor would also be considered to have a state of 'Down'. This state would be reflected in the 'State' Column of the Monitors Grid.

Viewing Monitor State Details

To view the state of each device or entry in the monitor, select 'Monitor State Details...' in the monitors context menu. A dialog containing each entry in the monitor with their corresponding state will be displayed, along with any details associated with the state. This dialog can show you the state of the monitor when the dialog was opened, or it can show you the latest state of the monitor by refreshing the dialog as the monitor completes. To always display the latest state, select the 'Show Latest State' option at the bottom of the dialog.

Viewing Monitor History

Viewing the history of a monitor allows you to view the results of the monitor over time. To view

the history of a monitor, select the monitors history in the context menu. A dialog containing a grid, and for certain monitors a graph, with the results of the monitor will be displayed. See the help documentation for the following monitors that support monitor history.

Ping History
HTTP History
CPU History
Disk History
SNMP History
SNMP IF/Bandwidth History
WMI History

Viewing Results By Device

The state of a device is based on all the monitors it is associated with and can be viewed using the Monitored Devices view. To view all devices associated with a monitor select the 'All Devices' option in the Monitored Devices navigation pane. A list of all devices associated with a monitor is displayed along with their overall state. The overall state is based on the 'worst' state of any associated monitors.

To view detailed information about the state of the device in all its monitors select the 'Monitor State Details' context menu. A dialog containing a list of all the monitors the device is associated with, a monitor summary, notes, and the current state within the monitor is presented.

If the monitors associated with the device support viewing the monitor history then the monitor history for the device can be viewed by selecting the monitor history in the devices context menu. The history for that single device will be displayed in the monitors history dialog.

Available Monitors

UVexplorer supports the following monitors. For details about each monitor, follow the link to their corresponding help documentation.

Ping/Latency
Service (TCP) Port
HTTP Monitors
DNS Checks
CPU/Processor Load
Disk/Storage
Custom SNMP Checks
SNMP IF Utilization
WMI Counters

Monitored Devices

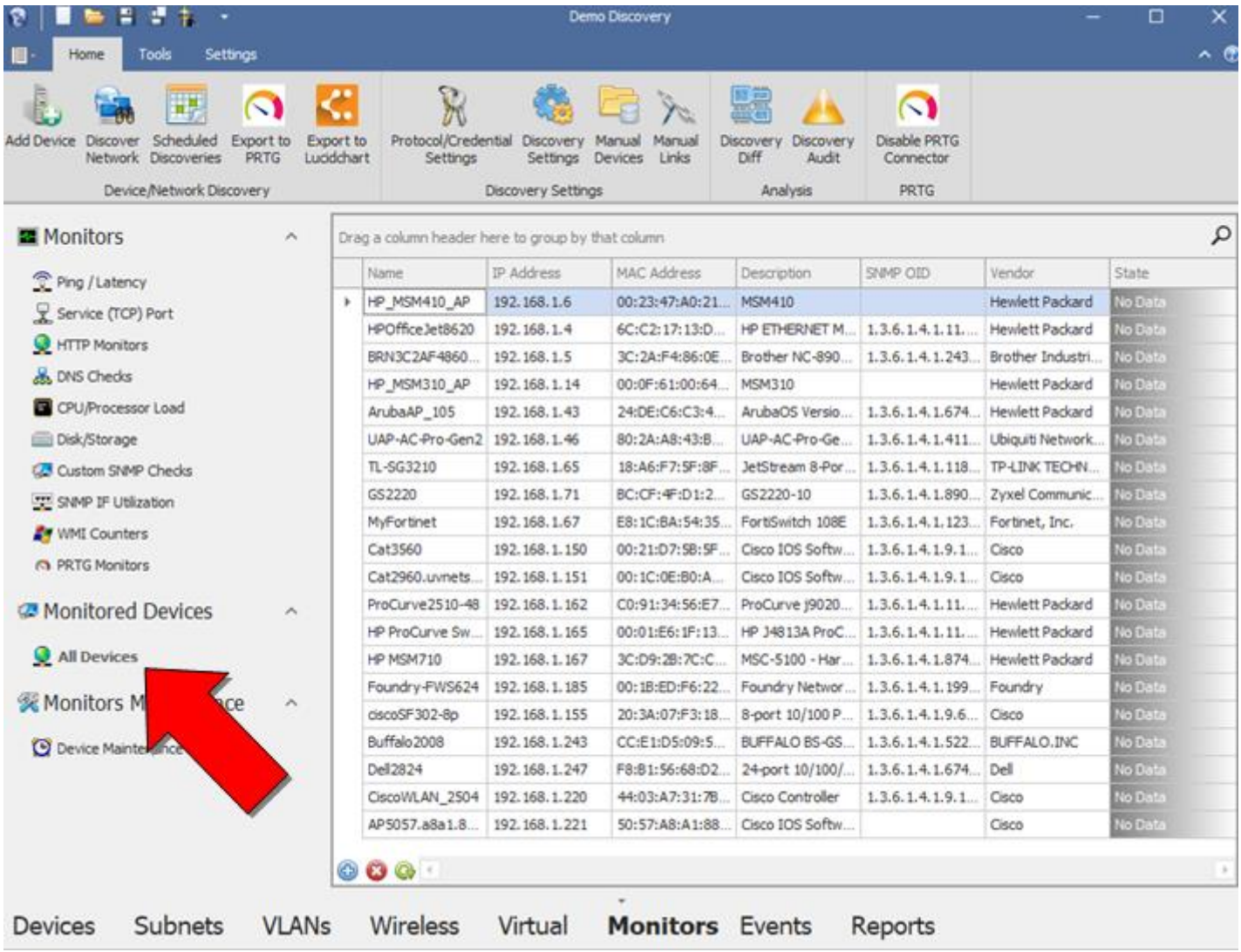
UVexplorer manages monitored device data separate from the device information stored in the discovery results. Several of the monitors require detailed information about the device and the relevant device assets in-order to effectively monitor the devices and store the monitored data. For example, the SNMP Interface monitor requires information about the device's interfaces in-order to collect and store the interface utilization statistics from the monitored interfaces.

Managing Monitored Devices

To facilitate configuring and running monitors, UVexplorer stores a snapshot of a discovered device as a monitored device in a data store separate from the discovery results. This creates a device that can be re-used by other monitors as well as storing/tracking collected monitoring data. Storing a snapshot of the device for monitoring purposes separate from the discovery results allows UVexplorer to maintain the historical view of the discovered networks free from changes made by the monitors. It also allows monitors to operate without the risk of losing data based on changes made by subsequent network discoveries.

Viewing Monitored devices

To view the monitored devices, select the 'All Devices' option in the monitor view navigation pane. A list of all devices monitored by UVexplorer is displayed in the main view pane. This list contains monitored devices taken from any discovery result regardless of which discovery result is currently open. Not all devices in this list must be part of monitor, rather it is a list of any devices that have been taken from a discovery result and added to the collection of monitored devices.



Adding Monitored devices

Discovery result devices can be added to the monitored devices when creating device monitors, or when viewing the monitored devices in the main monitors view.

When creating a monitor that monitors devices you must select the devices to monitor. The monitor device picker presents a list of devices currently in the monitored devices along with a list of devices in the currently opened discovery result that are not in the monitored devices. When choosing the devices to monitor, if you select a device from the unmonitored devices, it will be added to the monitored devices. **NOTE:** If you close the monitor device picker and confirm that you are OK adding the unmonitored devices to the monitored devices, the devices will be added to the monitored devices at that point. If you cancel creating the monitor at that time, the devices will have still been added to the monitored devices.

See Monitor Device Picker for more information about adding devices to the monitored devices in this way.

You can also add devices to the monitored devices from the list of monitored devices available in the main view of the monitor's page. First, select the 'All Devices' navigation item in the monitor view navigation pane. The list of all monitored devices is displayed. Press the add '+' button in the lower left corner of the monitored device list or select the 'Add Device...' option in the context menu. The device picker is presented containing any devices in the currently opened discovery result that are not in the monitored devices. Select the devices and hit OK, a snapshot of that device will be added to the monitored devices.

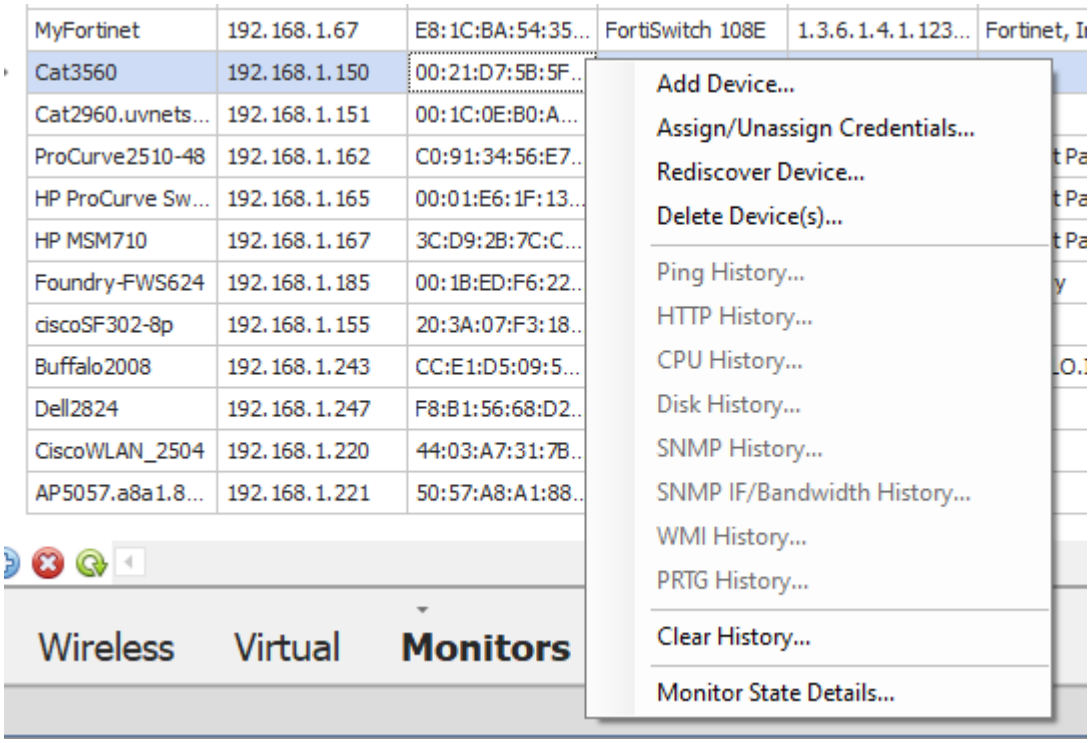
Deleting Monitored devices

To remove monitored devices select the 'All Devices' navigation item in the monitor view navigation pane. The list of all monitored devices is displayed. Press the delete 'x' button int he lower left corner of the monitored device list or select the 'Delete devices' option in the context menu. The device picker is presented containing all the monitored devices. Select the devices you want to delete from the monitored devices and press OK.

NOTE: Deleting a monitored device will remove it from the monitored devices and any monitors it is currently part of. It will also delete **ALL** monitor history associated with that device.

Managing Monitored Device Credentials

Once discovery result devices are added to the monitored devices, they must be managed separately from the discovery result devices. If the credential for a monitored device changes the UVexplorer associated credential must be reassigned to the monitored device. To reassign monitored devices credentials, select the 'Assign/Unassign Credentials...' context menu item in the monitored devices list. The protocol credential settings editor will be presented. The devices available to assign or unassign will be the Monitored devices. See Managing Device Credentials for more information on creating and assigning credentials.



Rediscover Monitored Devices

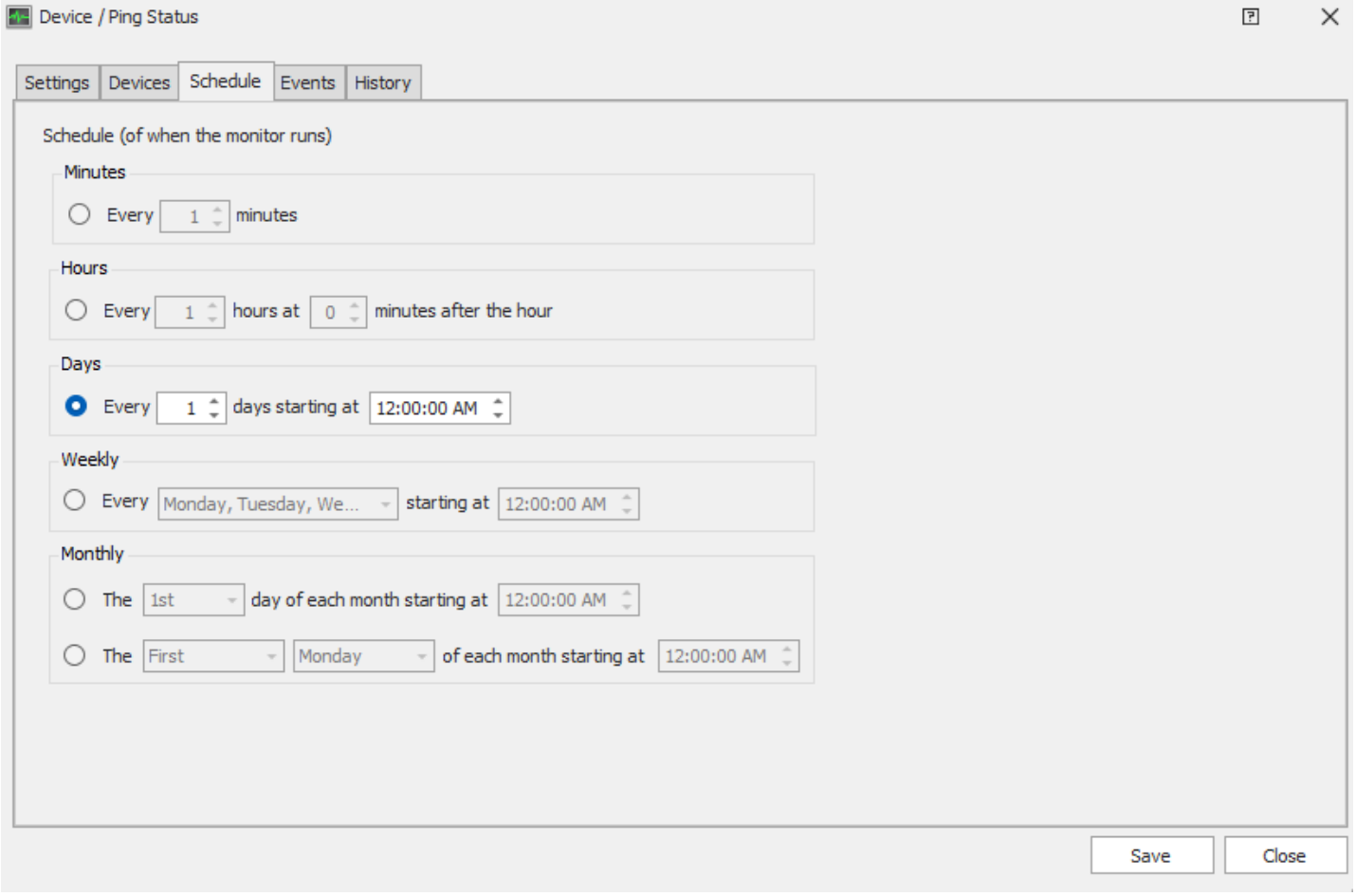
If a monitored device has changed significantly and needs to be updated, it can be rediscovered (for example: a valid protocol/credential set could have been enabled for a specific device). To rediscover a device select it in the monitored device list and then select the 'Rediscover device...' context menu. The rediscover device dialog will be presented allowing you to specify the credentials and run the device discovery. When the discovery completes press the 'Add' button and the device will be added/updated in the monitored devices list. This will update the device as used by any monitors it is associated with.

See Discovering a single device for more information on rediscovering a device.

Note: If the rediscovery loses important information used by monitors such as interfaces, disks, or processors, those monitors may fail.

Configuring Monitors

Each monitor consists of settings specific to that monitor along with schedule settings, event notification settings, and monitor result history settings. For details on configuring settings specific to a monitor see the monitors associated help page. For information on configuring the schedule, event, or history settings see below.



Configuring Monitor Schedules

Monitors can be scheduled to run on a specified interval allowing you to monitor the state of a device over time. The following schedule types are available:

Minutes
This schedule will run the monitor every N minutes. For example, 'Run every 30 minutes'.

Hours
This schedule will run the monitor every N hours at a specified minute during the hour. For example, 'Run every 6 hours'.

Days
This schedule will run the monitor every N days at a specified time of day. For example, 'Run every 3 days at 2:00 PM'.

Weekly
This schedule will run the monitor weekly on specified days of the week at a specified time of day. For example, 'Run every Friday at 2:00 PM'.

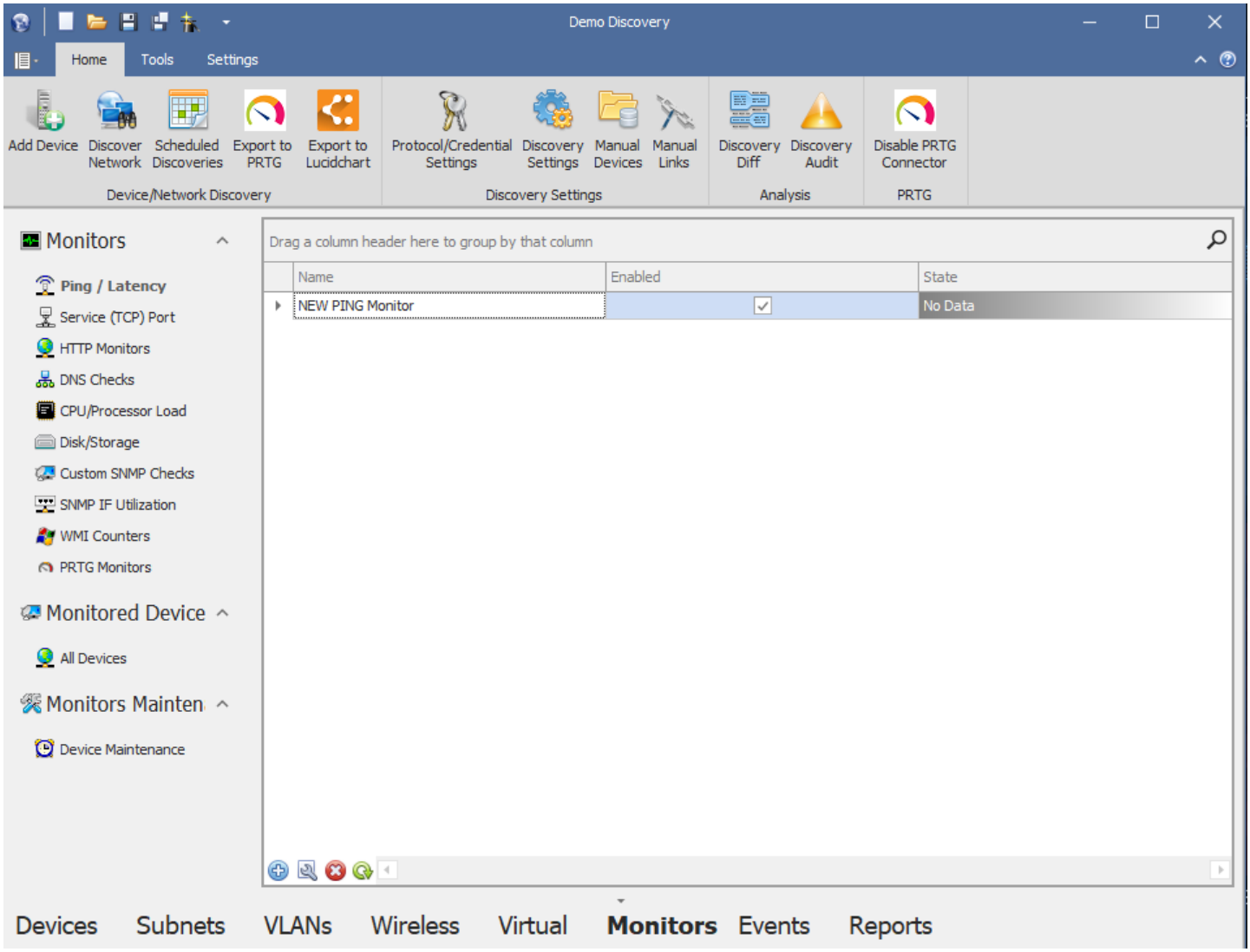
Monthly (Nth day of month)
This schedule will run the monitor monthly on the Nth day of the month at a specified time of

day. For example, 'Run on the 1st day of each month at 2:00 PM'.

Monthly (Ordinal day of week)
This schedule will run the monitor monthly on the first, second, third, fourth, or last occurrence of the specified week day. You can also specify the time of day at which the monitor will run. For example, 'Run the last Friday of each month at 2:00 PM'.

Configuring Monitor Events

Each monitor has a state associated with the monitor results. UVexplorer provides three ways to notify you of events that occur as a result of running the monitor. To select which events to be notified of select the states in the state drop down checklist.



Monitor States

The available states are:

UP
UP indicates that the results of the monitor queries are within the tolerances configured in the settings.

DOWN
Down indicates that the results of the monitor queries are completely outside of the configured tolerances.

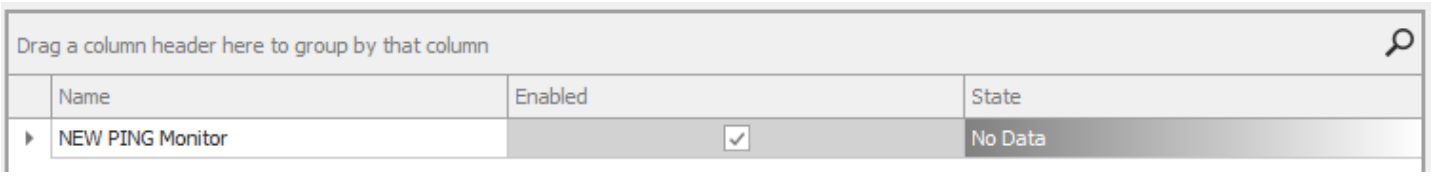
WARNING
Warning indicates that the results of the monitor queries are within the configured warning

tolerances.

UNKNOWN
An unknown state is a result of successfully running the monitor and not recognizing the response as one that can be compared to the monitors tolerances. Unknown should be treated as a DOWN monitor.

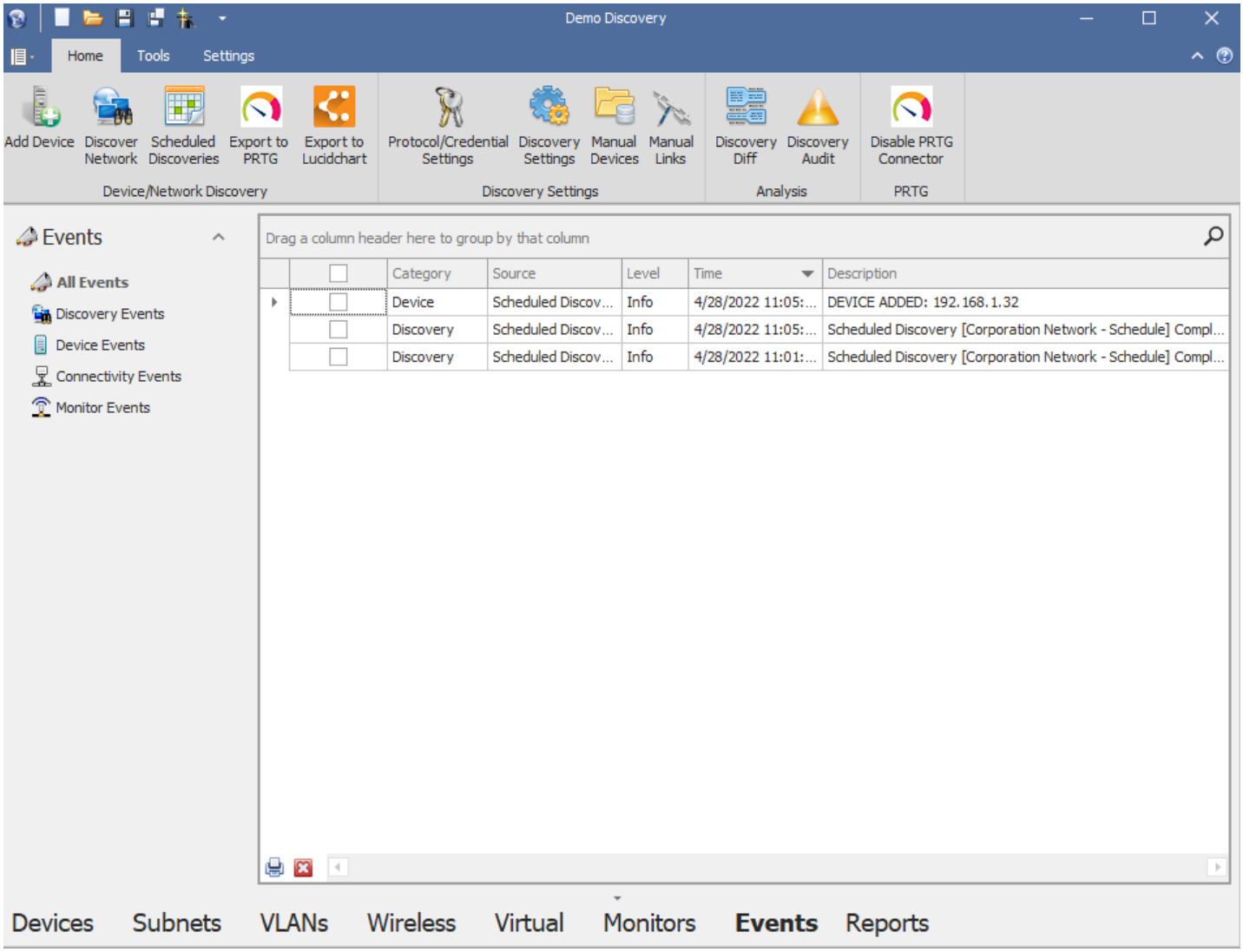
INFORMATION
The information state is only used for monitors whose queries could include additional information separate from the UP or DOWN state of the monitor. Ping monitors for example will provide an information state when it is recognized that the system up time has reset.

NO DATA
No data is a state used to indicate that the monitor has not yet been run and there is currently no available data.



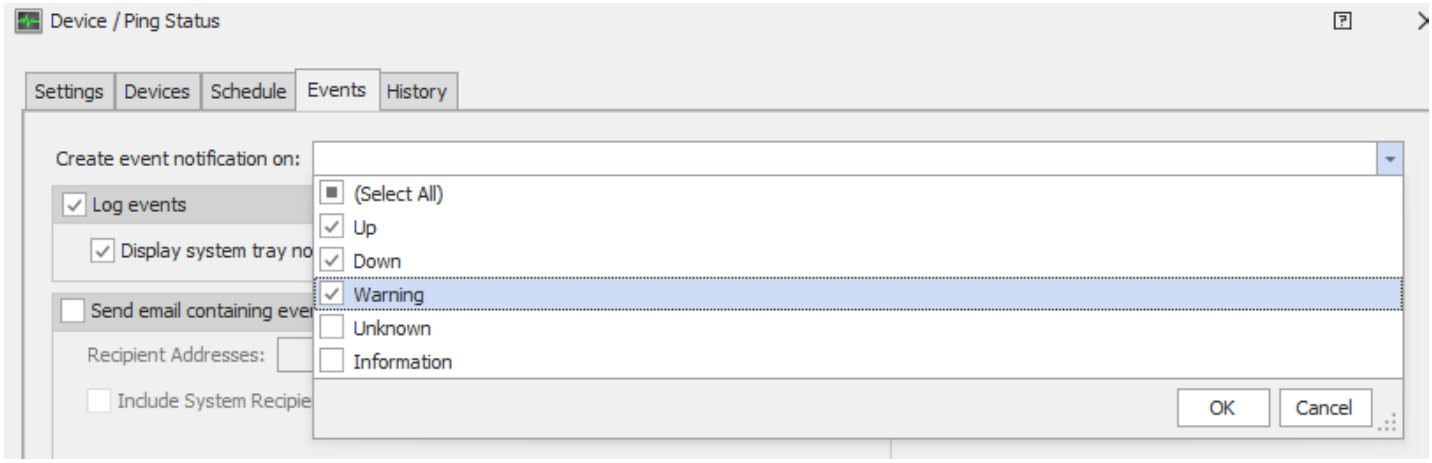
Monitor Event Notifications

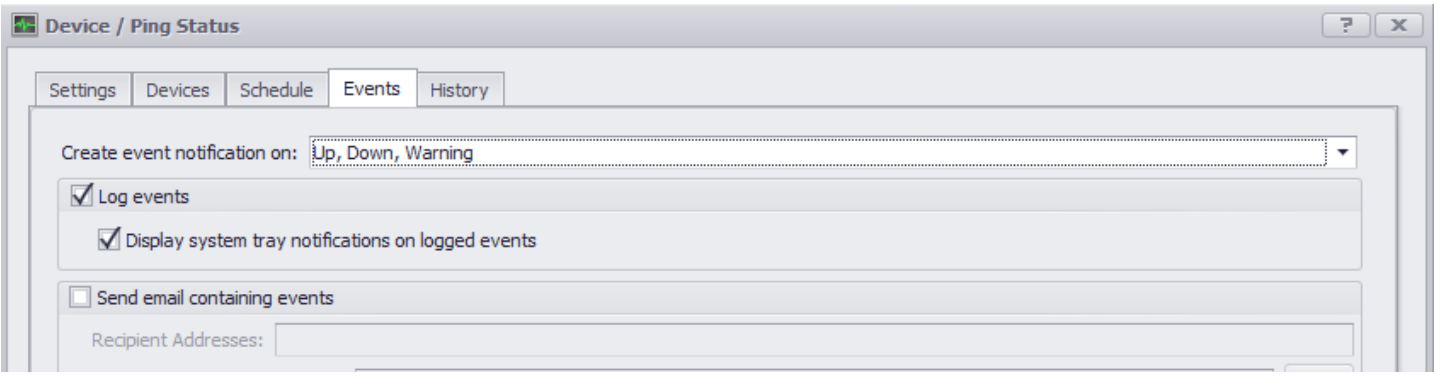
Log Events
UVexplorer provides an event log that contains all of the logged events. Monitor events will be included here if the log events option is selected. Details of the events will be available in the event view. See UVexplorer Events View for more information.



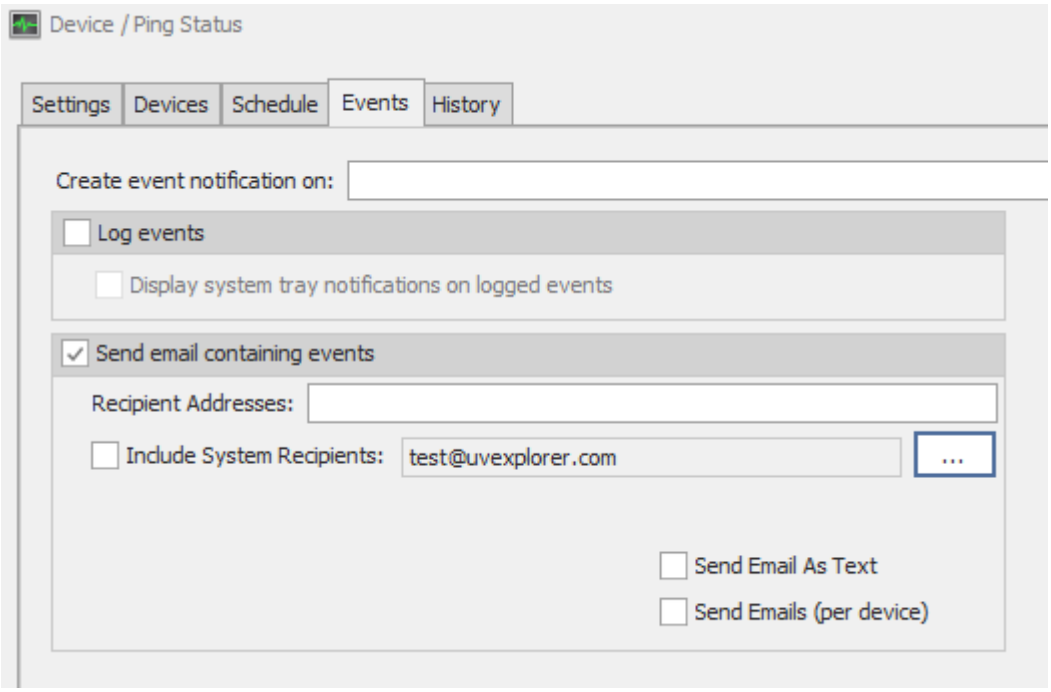
Desktop Notifications

Since UVexplorer runs as a System Tray application, event notifications can be displayed as a system tray 'balloon' message. This is a message appearing from the System Tray UVexplorer icon containing a message about the event that occurred. Details about the event can be seen by clicking on the balloon. Clicking on the balloon will display the UVexplorer applications Events View. Since the details of these notifications are the logged events, the 'Log Events' option must be enabled to enable the desktop notifications. To enable desktop notifications, check the 'Display System Tray Notifications' option within the Log Events group box.





Email Notifications
UVexplorer can be configured to send email notifications containing details about state changes within monitor results. To send emails on monitor state changes select the 'Send Email Containing Events' check box. Emails can be sent to the pre-configured system recipients, as well as to additional recipients specified for the monitor. When email notifications are enabled an email message containing information about the event will be sent to all of the specified recipients.



Email notifications will only work if the system email server settings are configured. The system settings can be accessed by pressing the browse '...' button to the right of the System Recipients check box. See SMTP Email Server Settings for more information.

Configuring Monitor History

Each time a monitor is run the results of the monitor queries are stored. Overtime, depending on the frequency of the monitor schedule, these results could become quite large and require a considerable amount of disk space and memory. The monitor history configuration allows you to dynamically limit the number of results to keep. As a convenience the time duration the monitor results will be stored is displayed based on the number of results and the current monitor schedule. This value will change as the number of results and or the schedule are changed. For example, if you choose to store 72 results and the monitor is scheduled to run every hour you will see that monitor results will be stored for 3 days.

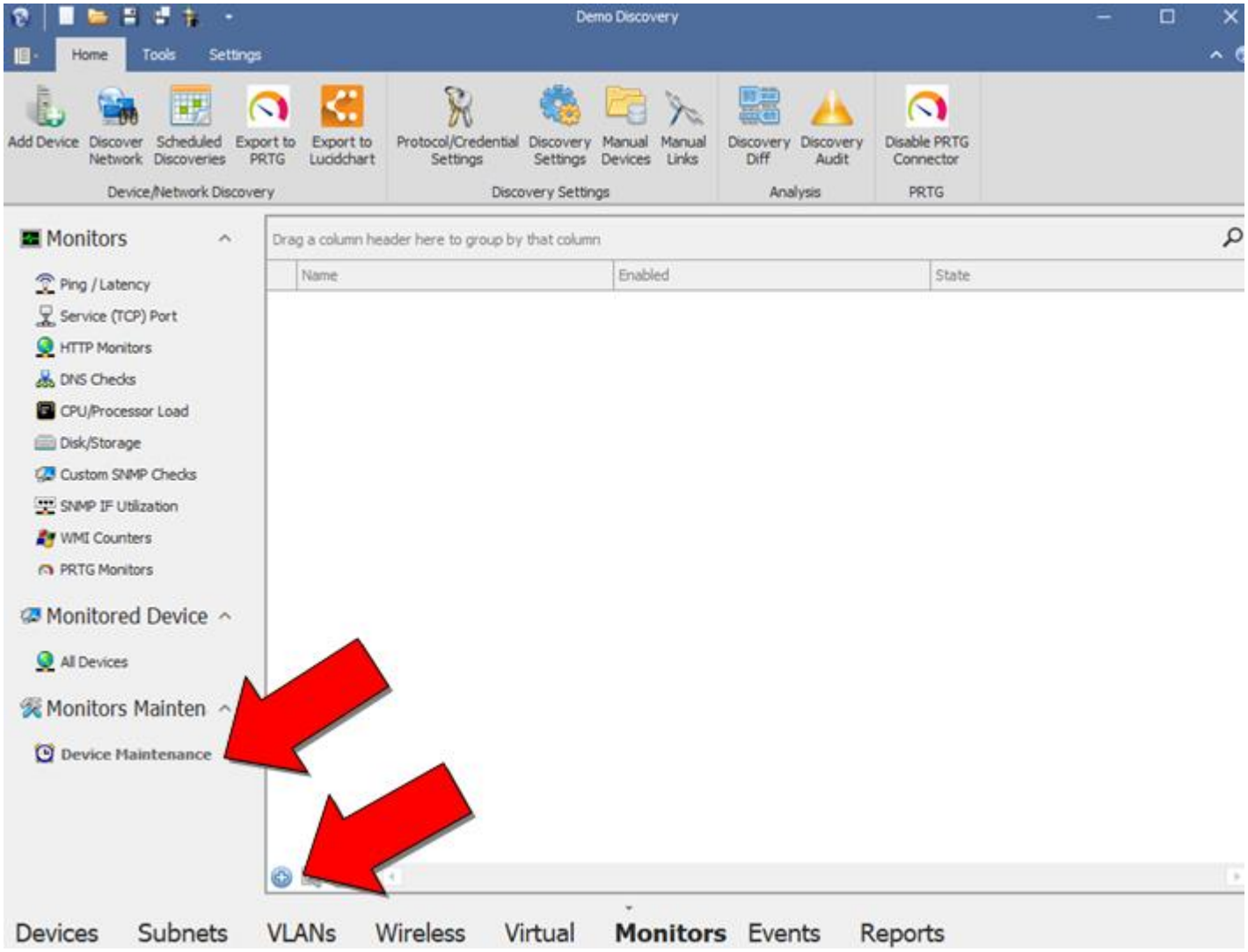
To maintain system stability, the maximum number of stored monitor results are limited to 1000.

Monitor Maintenance Policies

Maintenance policies allow you to pause all monitors on a particular device. Maintenance policies can be created for immediate suspension of a devices monitors, or on a recurring basis.

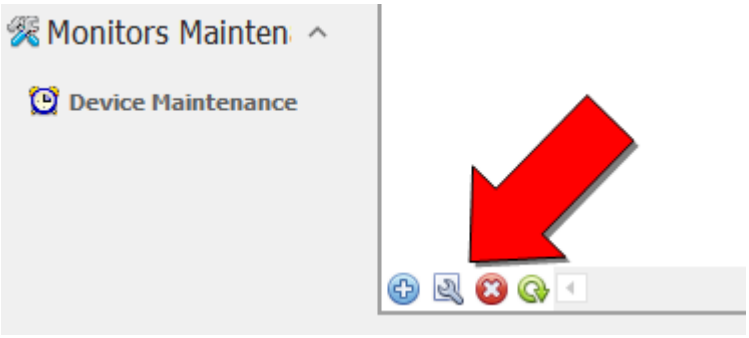
Creating Maintenance Policies

To create a maintenance policy, select 'Maintenance Policy' in the left pane of the monitor section and press the '+' button in the lower left corner of the center pane. A maintenance policy editor will be presented.



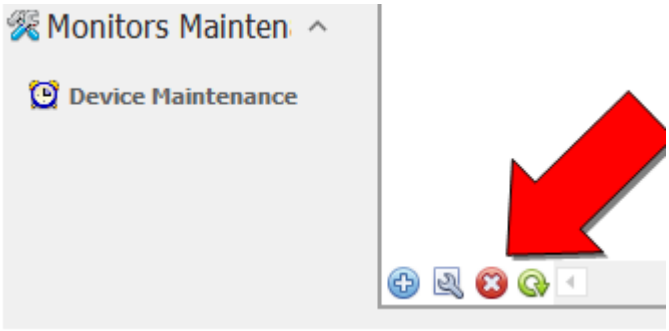
Editing Maintenance Policies

To edit a maintenance policy, select the policy in the list in the center pane and press the 'wrench' button. The editor will be presented.



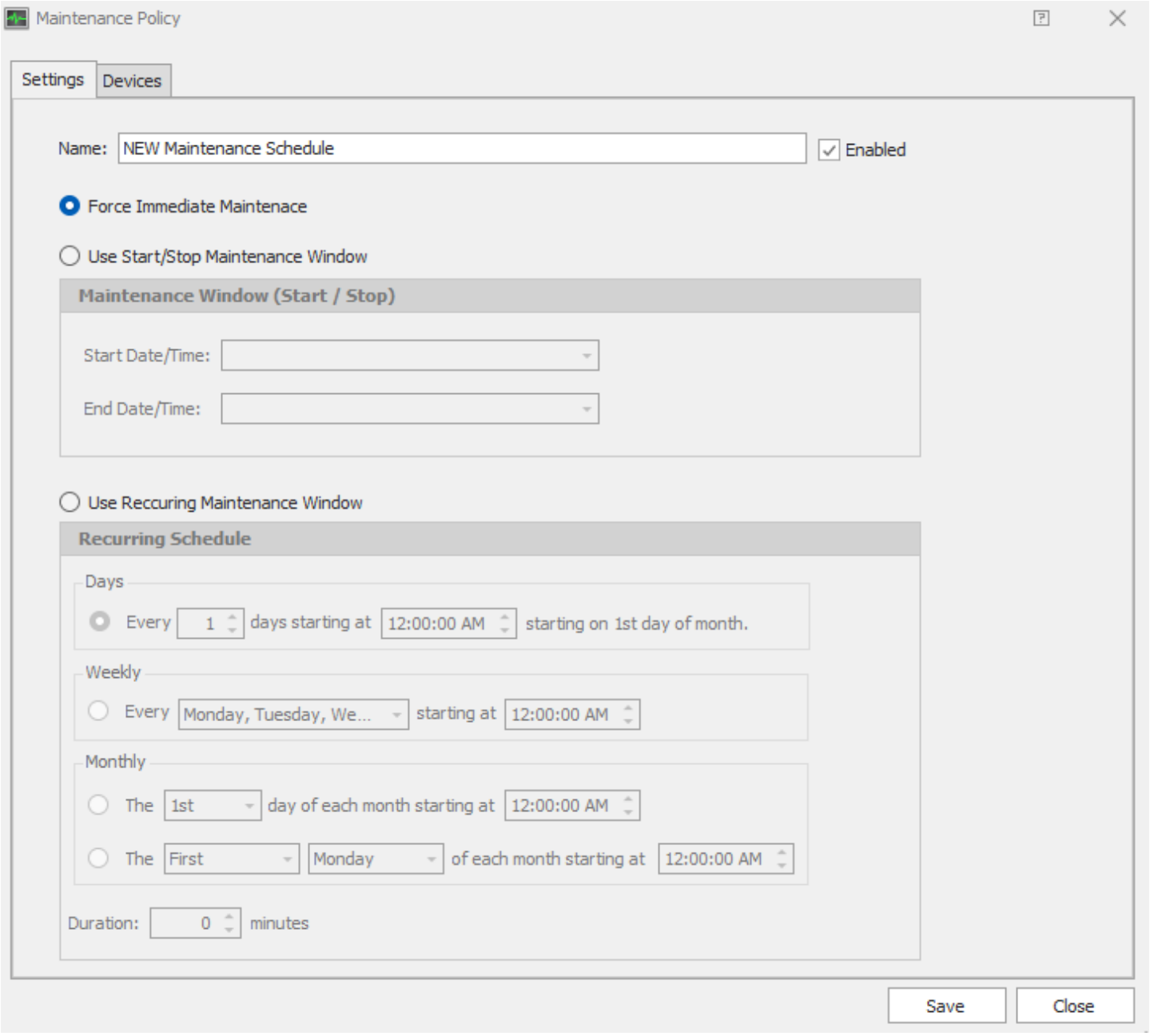
Deleting Maintenance Policies

To delete a maintenance policy, select the policy in the list in the center pan and press the 'X' button. The policy will be deleted.



Configuring Maintenance Policies

Maintenance policies can be configured in the ‘Maintenance Policy’ dialog box:



Settings

Name

The name of the policy used to identify it within UVexplorer

Force Immediate Maintenance

This will pause all monitors on the devices associated with the policy immediately upon policy creation. The devices monitors will remain in maintenance mode until this setting is changed or the policy is deleted.

Use Start Stop Maintenance Window

This will create a time frame the monitors on the devices associated with the policy will be paused. The devices will stop being monitored when the window starts and resume monitoring when the window ends.

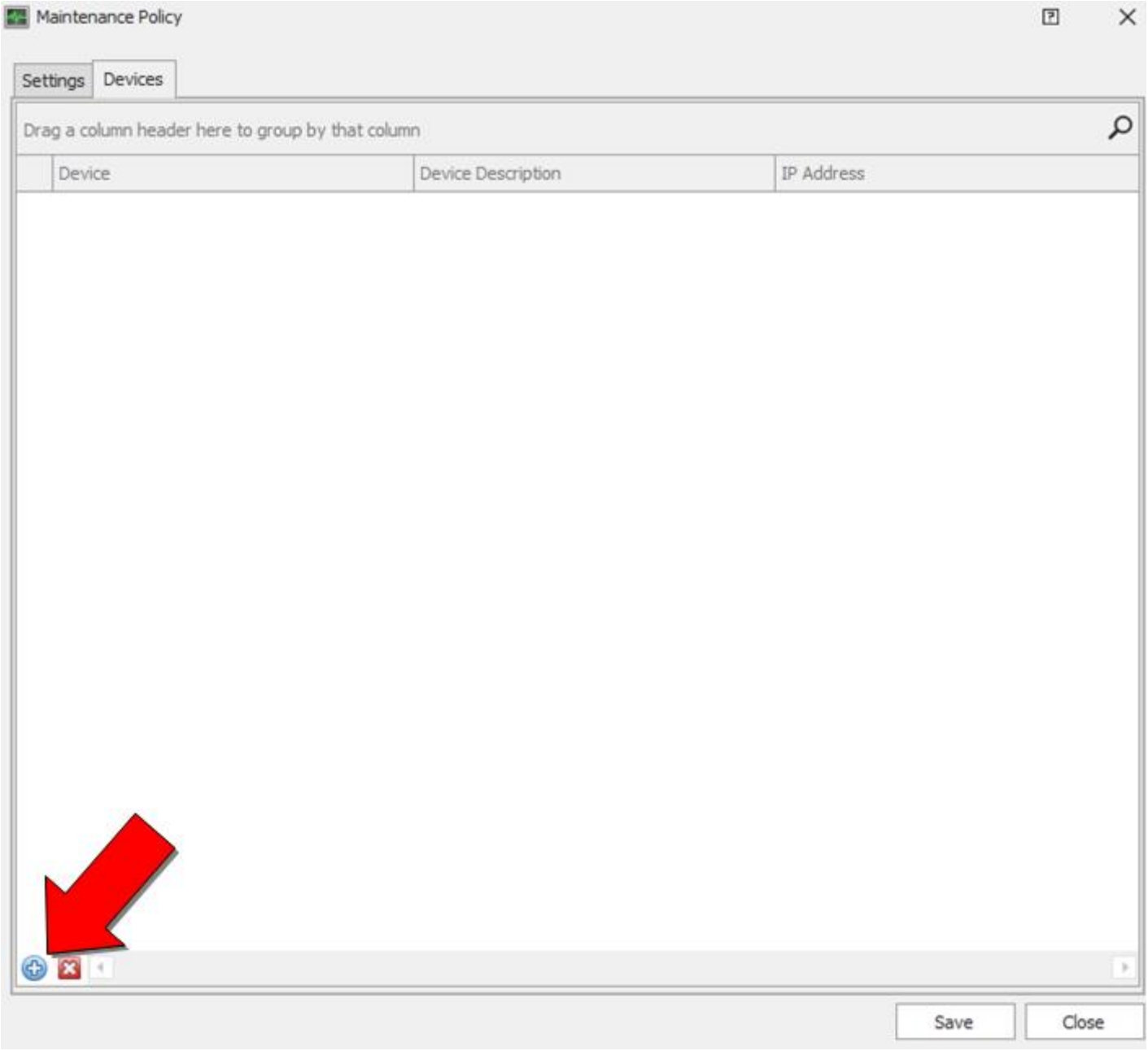
Use Recurring Maintenance Window

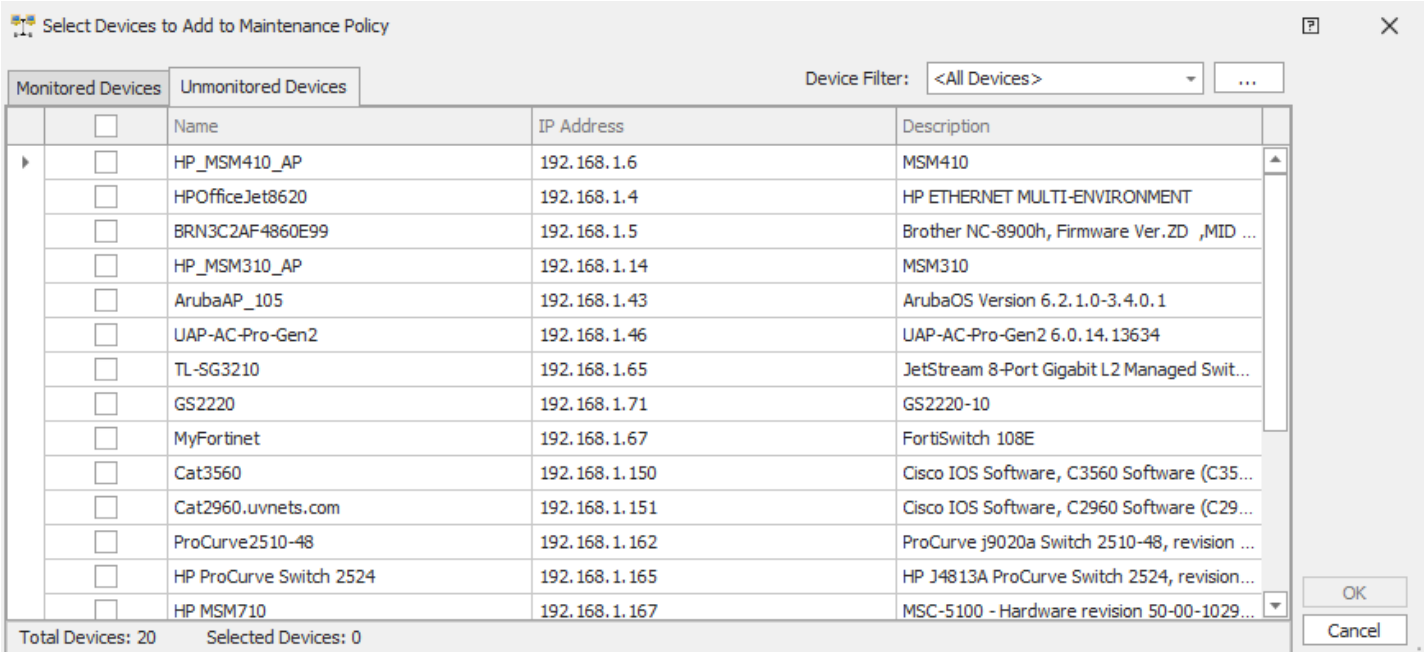
This allows you to create a maintenance window to pause the monitoring of a device on a scheduled

basis.

Devices

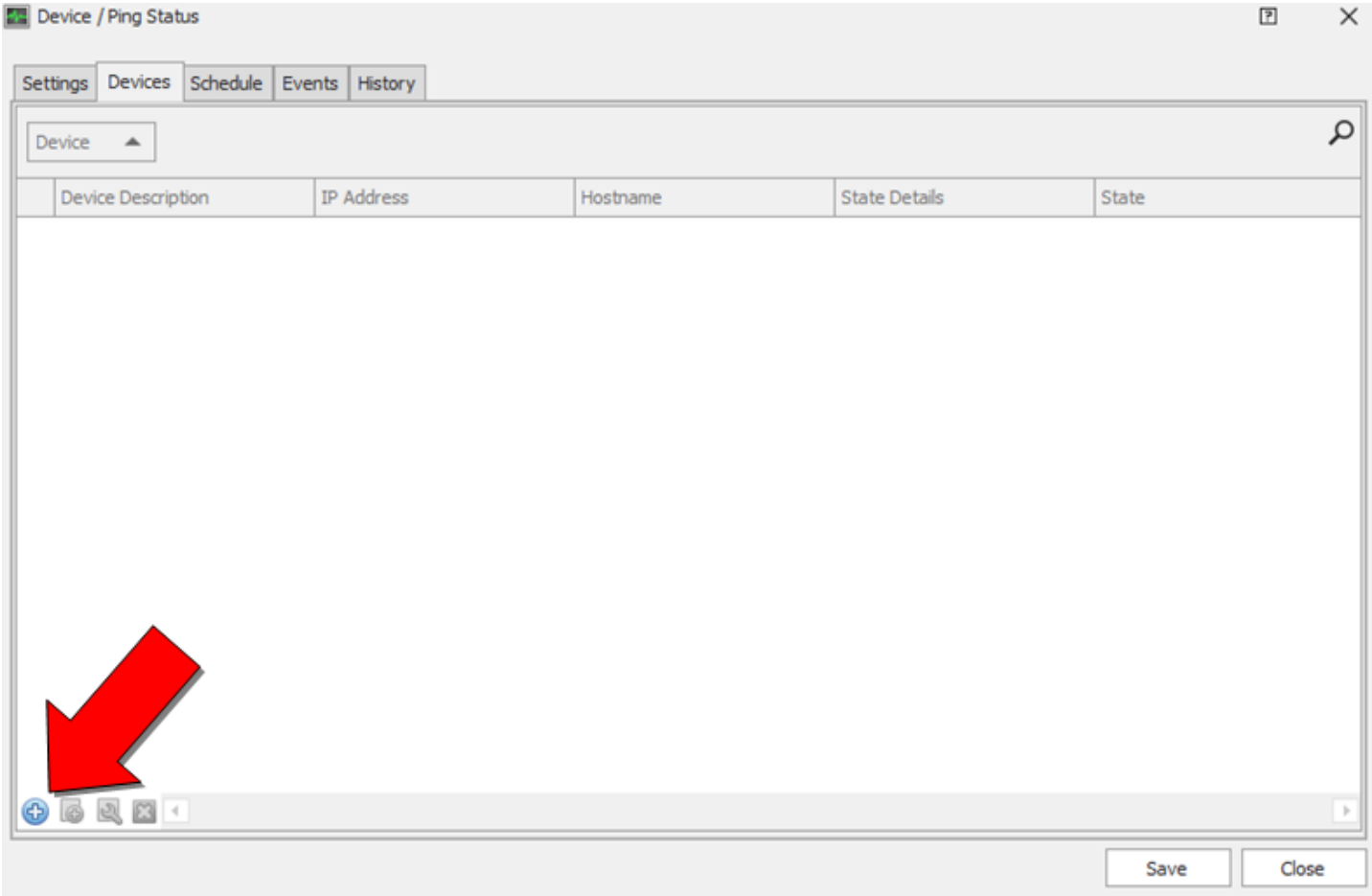
Devices can be added to the policy using the device picker in the devices tab. Any devices added to the policy will not be monitored when the policy is in its maintenance window. The monitors the devices participate in will still run for any devices not associated with an active maintenance policy.



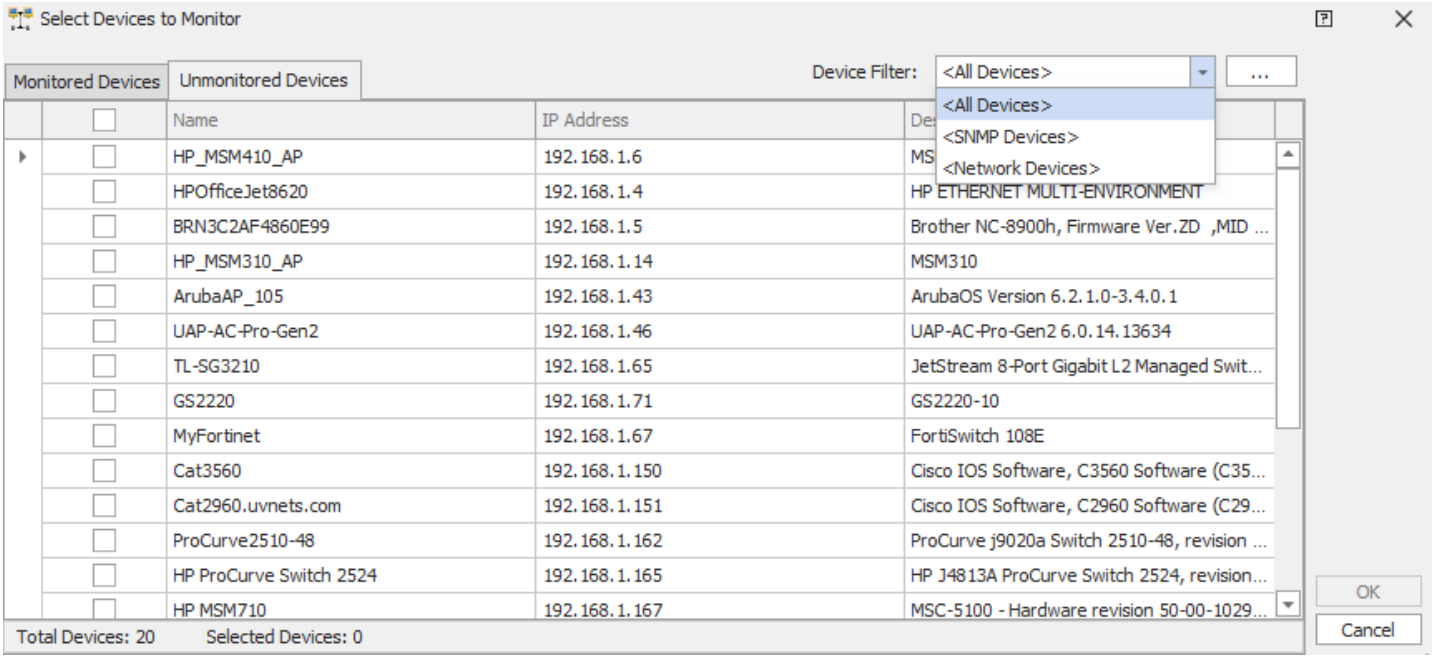

Select Devices to Add to Maintenance Policy
Monitored Devices
Unmonitored Devices
Device Filter:
<All Devices>
...
Name
IP Address
Description
HP_MSM410_AP 192.168.1.6 MSM410
HPOfficeJet8620 192.168.1.4 HP ETHERNET MULTI-ENVIRONMENT
BRN3C2AF4860E99 192.168.1.5 Brother NC-8900h, Firmware Ver.ZD ,MID ...
HP_MSM310_AP 192.168.1.14 MSM310
ArubaAP_105 192.168.1.43 ArubaOS Version 6.2.1.0-3.4.0.1
UAP-AC-Pro-Gen2 192.168.1.46 UAP-AC-Pro-Gen2 6.0.14.13634
TL-SG3210 192.168.1.65 JetStream 8-Port Gigabit L2 Managed Swit...
GS2220 192.168.1.71 GS2220-10
MyFortinet 192.168.1.67 FortiSwitch 108E
Cat3560 192.168.1.150 Cisco IOS Software, C3560 Software (C35...
Cat2960.uvnets.com 192.168.1.151 Cisco IOS Software, C2960 Software (C29...
ProCurve2510-48 192.168.1.162 ProCurve j9020a Switch 2510-48, revision ...
HP ProCurve Switch 2524 192.168.1.165 HP J4813A ProCurve Switch 2524, revision...
HP MSM710 192.168.1.167 MSC-5100 - Hardware revision 50-00-1029...
Total Devices: 20
Selected Devices: 0
OK
Cancel

Monitor Device Picker

The monitor device picker allows you to select devices from the monitored devices or from the currently opened discovery result. The monitor device picker is used when choosing devices to add to a monitor. The picker contains a device filter, a list of monitored devices and a list of unmonitored devices in the discovery network.



Then select the devices to monitor:



Use the device filter to change the type of available device in the list. Some monitors only work with

a monitor if they have certain credentials or device assets. In these cases, the list of available devices may already be filtered by these criteria.

Each device list (monitored/unmonitored) contains a list of devices with columns containing the device name, IP address, and device description.

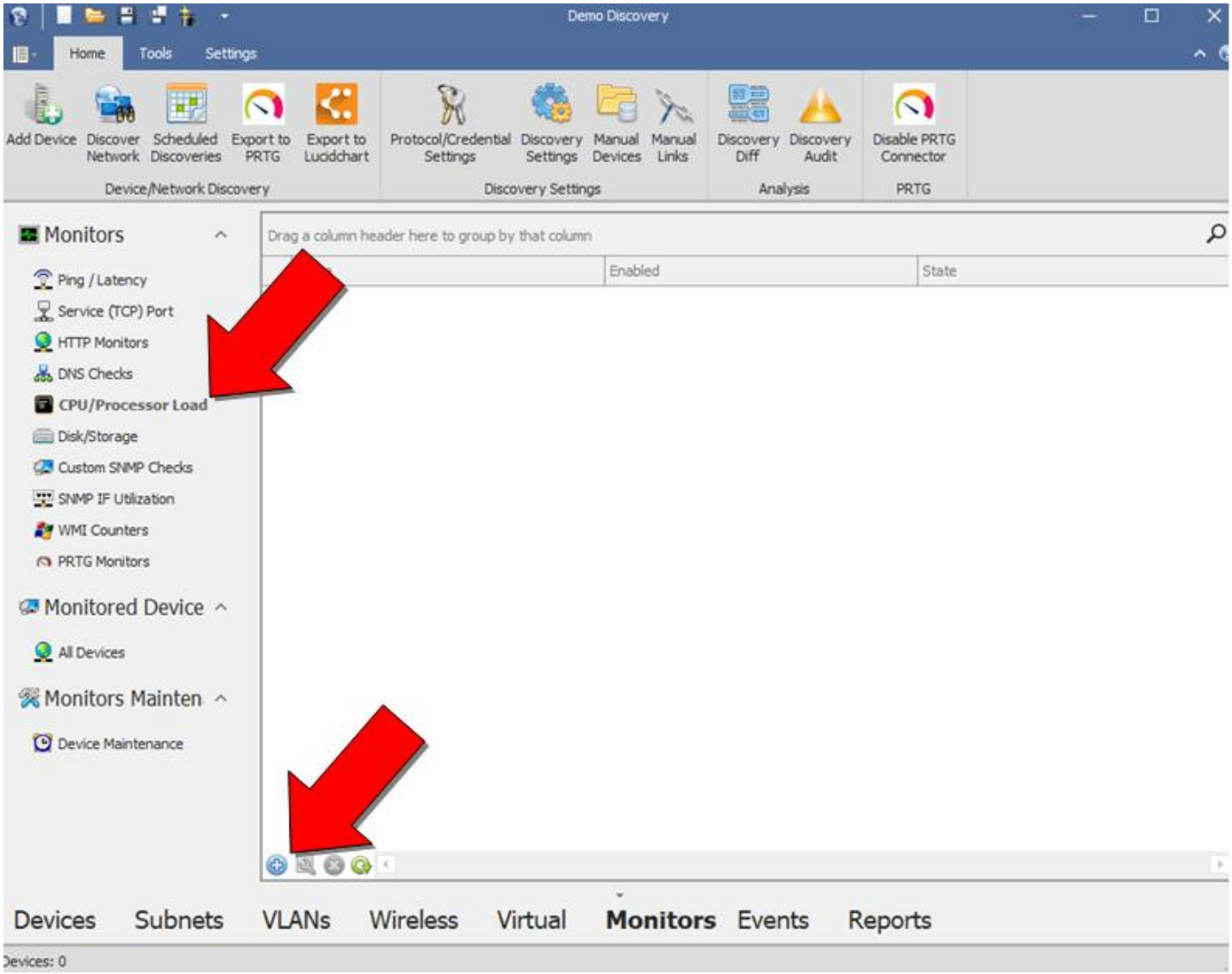
To select device in the list, use the checkbox in the far left column. To select all devices in a list, select the checkbox in the selection column header.

When devices in the unmonitored devices list are selected the devices will be added to the monitored devices at the time dialog is closed. This means the devices will be added to the monitored devices even if you do not complete creating the monitor.

See Monitored Devices to better understand the difference between monitored devices and discovery result devices.

CPU/Processor Load

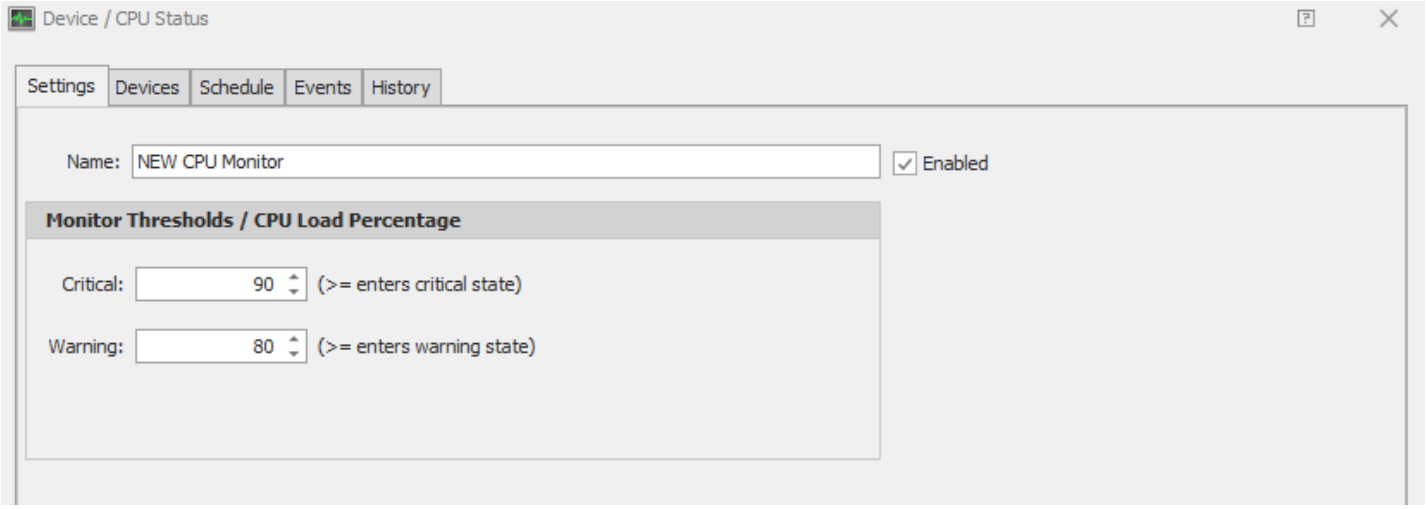
The CPU Load monitor allows you to monitor the CPU load of a devices CPU/Processor. When a CPU monitor runs it requests the CPU load from the monitored devices and compares the result with the monitors specified thresholds.



Configuring the Monitor

The CPU monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the other tabs see the information below.



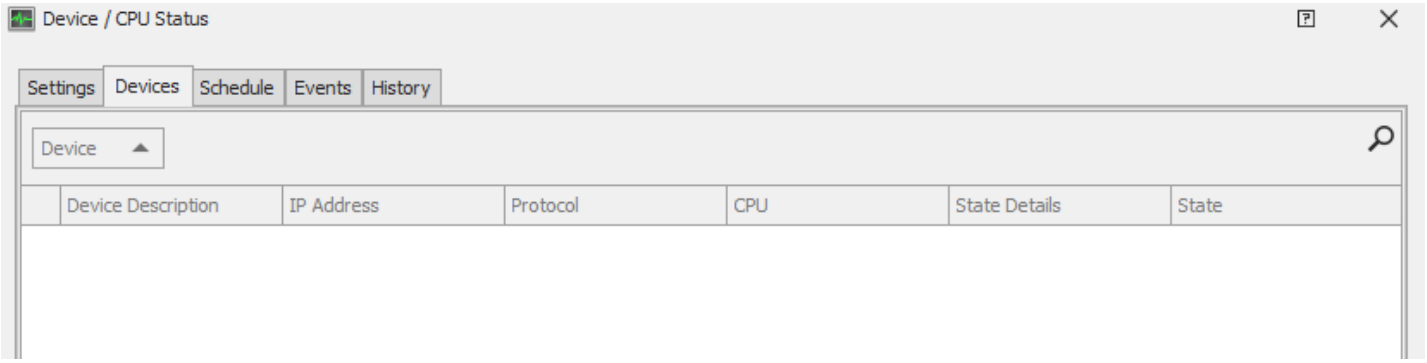
Settings

Name
The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique, but it is recommended you use unique names to differentiate them.

Threshold
The CPU monitor threshold specifies the CPU load level that would produce a down and warning state. The warning level must be less than or equal to the critical level. The warning and critical levels must be between 0 and 100.

Devices

The devices tab allows you to select which devices and their respective CPU/Processors to monitor. The CPU monitor can monitor 1 or more CPUs on a device depending on what CPU information is available on that device.



To add Devices/Processors to the monitor select the button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. When the device is selected each of the device's CPUs will be added to the monitor. **Note:** Only devices with an assigned SNMP or WMI credential will be available in the picker. If you do not see a device, ensure it has the appropriate credential assigned.

To edit which CPUs on a device to monitor. Select the device or one of its CPUs in the list and press the edit button . A list of all the devices available CPUs will be presented. Check the CPUs you would like to monitor and close the dialog. The monitored CPU list will be updated to reflect the changes. **Note:** If a CPU is not available it could be because it was not discovered during device discovery. To update the list ensure valid credentials are available and rediscover the device. See Monitored Devices for more information.

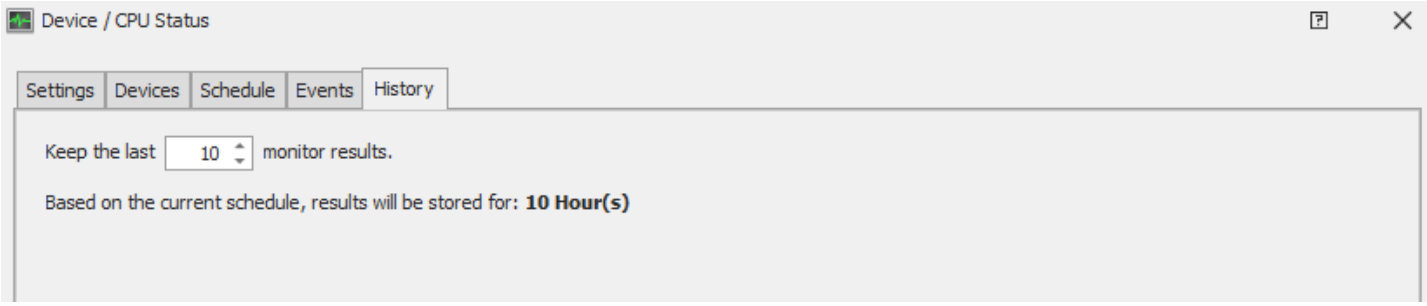
To remove a device or CPU from the monitor select the device or CPU in the list and press the delete button. The device/CPU will be removed from the monitor.

Note: UVexplorer can collect the CPU information using either the SNMP protocol or on windows machines using the WMI protocol. When selecting a CPU to monitor the entry in the list will indicate which protocol was used to collect that information. If a windows machine has both an SNMP and WMI agent enabled with valid credentials for each, then the CPU information could be collected using both protocols. If this occurs each CPU will have two entries in the monitor selection list, one for each protocol. This is done to allow you to specify which protocol you would like to use to collect the information. If the agents are written correctly the information should be the same for either. We recommend, and will choose by default, the SNMP protocol since it is usually quicker.

See Monitor Device Picker for more information on choosing devices.

CPU History

To open the CPU history view, select a CPU monitor in the CPU monitor list and open 'CPU History' in the monitors context menu.



The CPU history form contains a graph with the CPU utilization percentage based on the time the monitor was run.

Below the graph is a grid containing the devices with their collected monitor results. The grid is grouped by device name and CPU name

The following details are available for each entry in the grid

CPU Name

The name of the CPU/Processor.

Timestamp

The time the CPU utilization was queried.

Load

The CPU Load percentage at the time of the query.

Load (time)

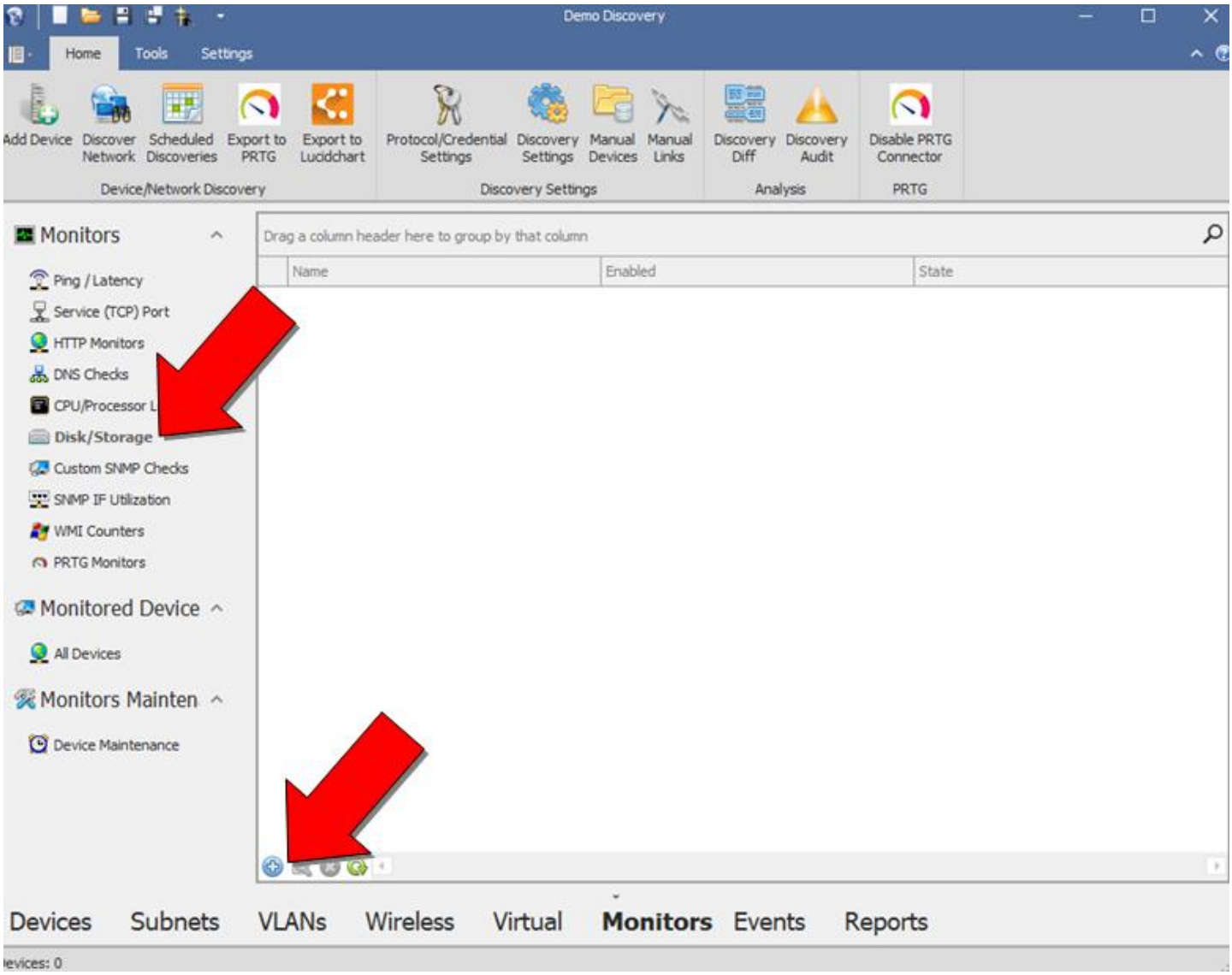
If the device stores results of the load within recent time intervals these values will be collected and presented here. Note not all devices support this query.

Show Latest State

By default, the history view will update as new monitor results are collected, providing a real-time view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

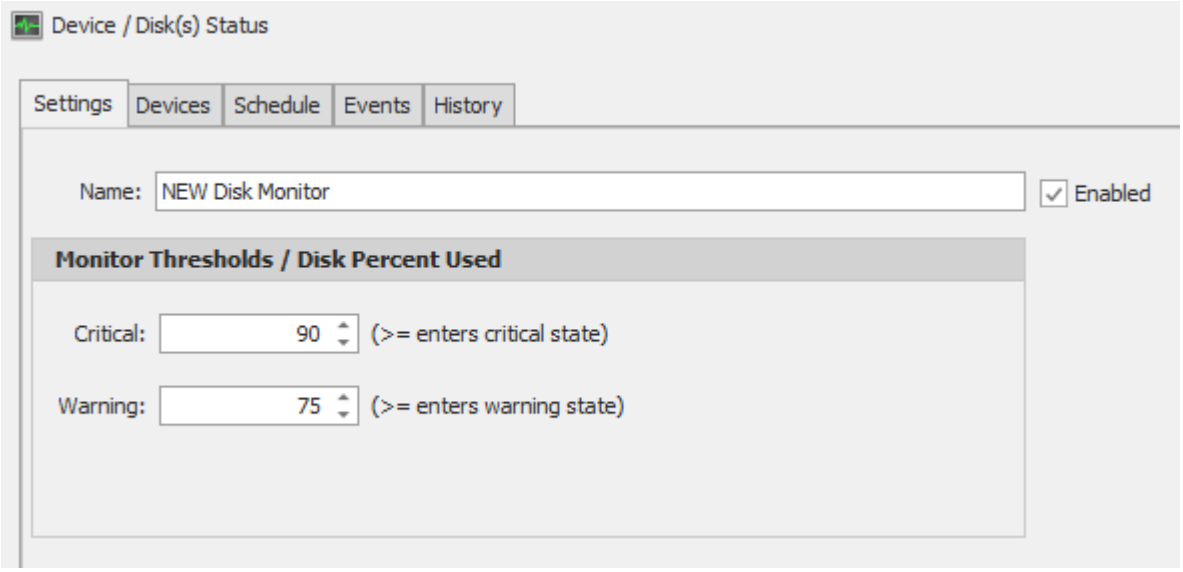
Disk/Storage

The Disk/Storage monitor allows you to monitor the used percentage of a device's available disk/storage space. When a disk monitor runs, the monitor requests the current percentage of disk space used from the monitored devices. These results are compared with the monitors specified thresholds.



Configuring the Monitor

The Disk monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.



The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the other tabs see the information below.

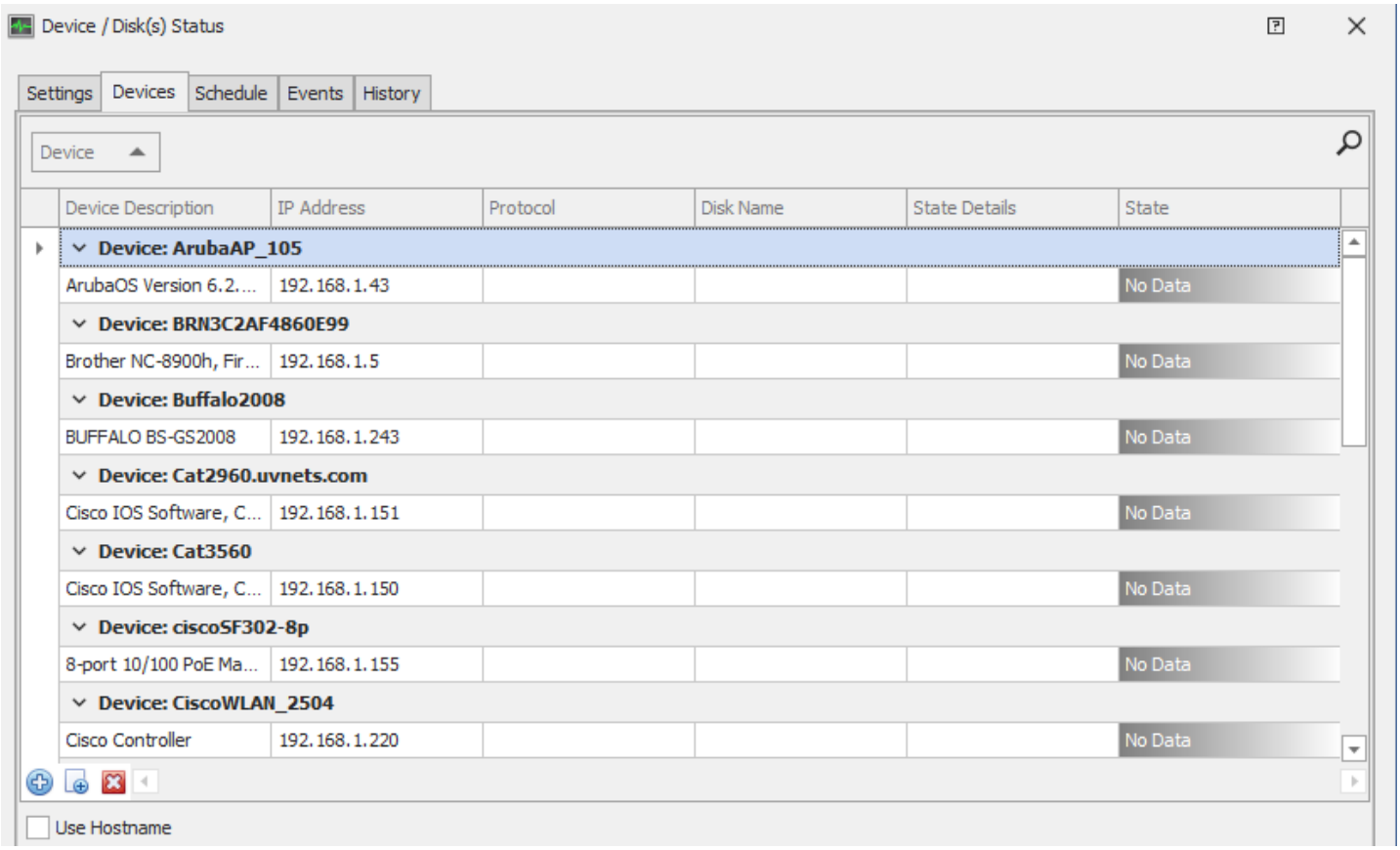
Settings

Name
The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique but it is recommended you use unique names to differentiate them.

Threshold
The Disk/Storage monitor threshold specifies the **Percentage of Used Disk Space** that would produce a down and warning state. The warning level must be less than or equal to the critical level. The warning and critical levels must be between 0 and 100.

Devices

The devices tab allows you to select which devices and their respective Disks to monitor. The Disk monitor can monitor 1 or more Disks on a device depending on what Disk information is available on that device.



To add devices/disks to the monitor select the button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. When the device is selected each of the devices physical Disks will be added to the monitor. **Note:** Only devices with an assigned SNMP or WMI credential will be available in the picker. If you do not see a device ensure it has the appropriate credential assigned.

To edit which Disks on a device to monitor. Select the device or one of its disks in the list and press the edit button . A list of all of the devices available disks will be presented. Check the disks you would like to monitor and close the dialog. The monitored disks list will be updated to reflect the changes. **Note:** If a disk is not available it could be because it was not discovered during device discovery. To update the list ensure valid credentials are available and rediscover the device. See Monitored Devices for more information.

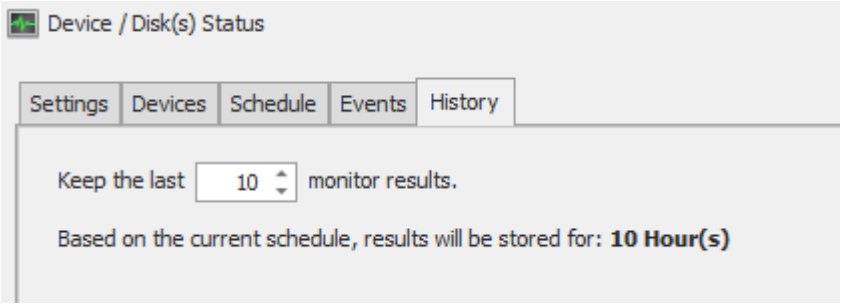
To remove a device or disk from the monitor select the device or disk in the list and press the delete button . The device/disk will be removed from the monitor.

Note: UVexplorer is able to collect the disk information using either the SNMP protocol or on windows machines using the WMI protocol. When selecting a disk to monitor the entry in the list will indicate which protocol was used to collect that information. If a windows machine has both an SNMP and WMI agent enabled with valid credentials for each, then the disk information could be collected using both protocols. If this occurs each disk will have two entries in the monitor selection list, one for each protocol. This is done to allow you to specify which protocol you would like to use to collect the information. If the agents are written correctly the information should be the same for either. We recommend, and will choose by default, the SNMP protocol since it is usually quicker.

See Monitor Device Picker for more information on choosing devices.

Disk History

To open the disk history view, select a disk monitor in the disk monitor list and open 'Disk History' in the monitors context menu.



The disk history form contains a graph with the disk utilization percentage based on the time the monitor was run.

Below the graph is a grid containing the devices with their collected monitor results. The grid is grouped by device name and device DISK

The following details are available for each entry in the grid

Disk

The name of the disk.

Timestamp

The time the disk utilization was queried.

Percent Used

The percentage of the disk space being used as calculated based on the size of the disk and disk used.

Disk Size

The size of the disk, usually in Gigabytes.

Disk Used

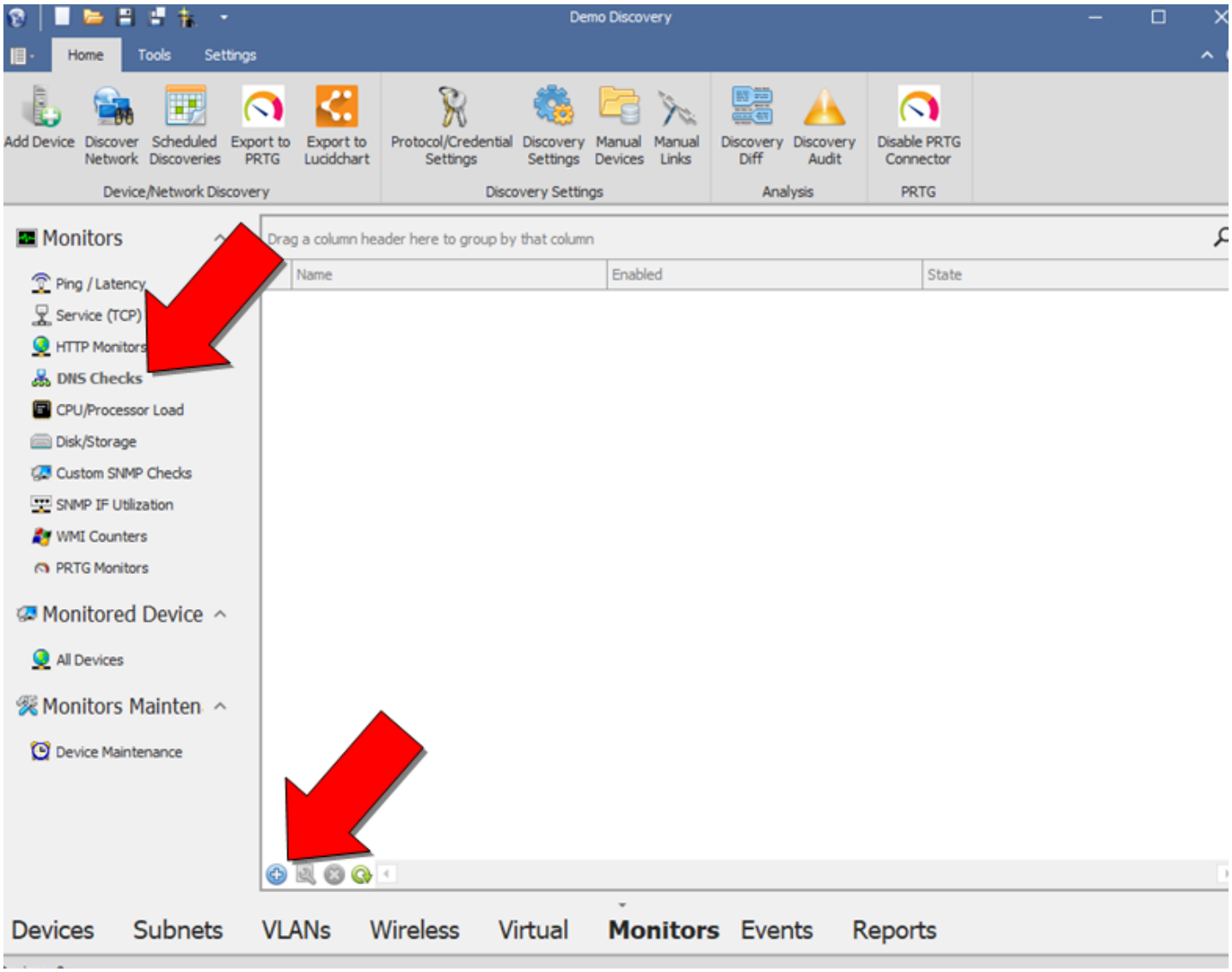
The amount of space used on the disk, usually in Gigabytes.

Show Latest State

By default, the history view will update as new monitor results are collected, providing a real-time view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

DNS Checks

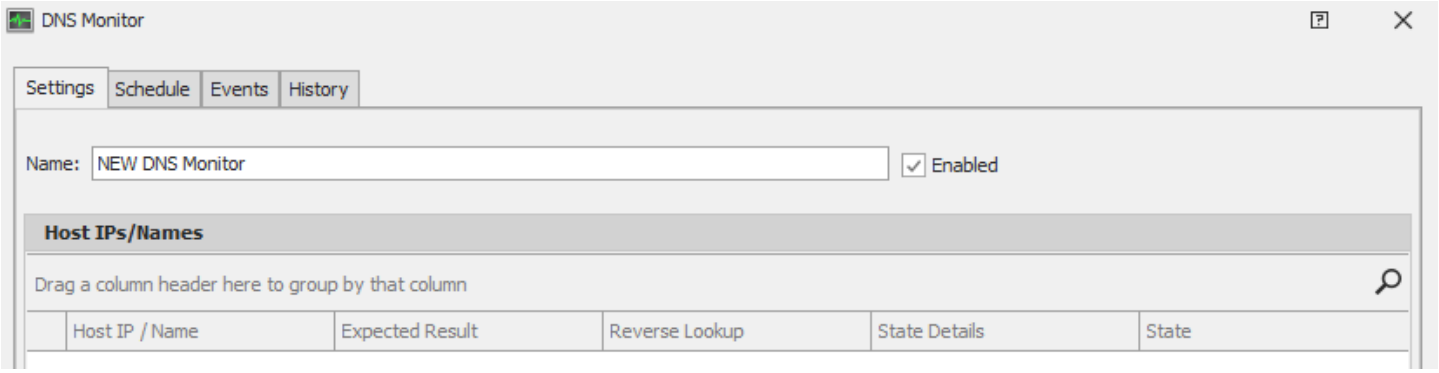
The DNS monitor allows you to monitor whether a hostname resolves to a valid or correct/desired IP address. Using reverse DNS lookup, it also allows you to monitor whether an IP address resolves to the correct hostname. When a DNS monitor runs it resolves the provided hostname and compares the resulting IP address to the expected result. Or, if an IP address is specified, it does a reverse DNS lookup on the IP address and compares the resulting hostname to the expected result.



Configuring the Monitor

The DNS monitor editor contains the following tabs that require configuration: Settings, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the settings tab see the information below.



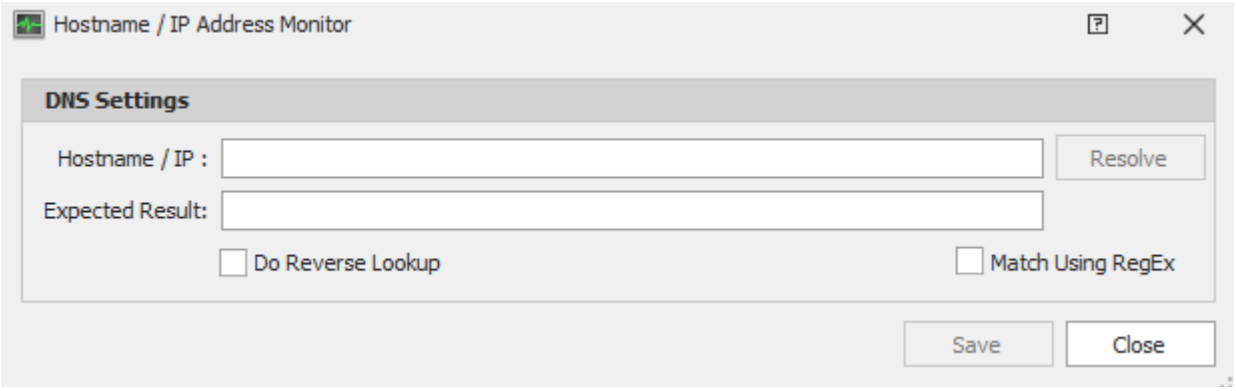
Settings

Name

The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique, but it is recommended you use unique names to differentiate them.

Host IPs/Names

The Host IPs/Names is a list of Hostnames and/or IP addresses to be resolved by the monitor.



Adding a Hostname / IP Entry

To add a new hostname or IP address to be monitored, press the add button . An editor allowing you to configure the new Hostname / IP entry is displayed. Once configured, press the save button and the new Hostname / IP entry is added to the list.

Editing a Hostname / IP Entry

To edit a Hostname / IP entry press the edit/configure button . The configuration editor is displayed. To save the changes press the save button and the Hostname / IP changes are applied.

Deleting a Hostname / IP Entry

To delete a Hostname / IP entry select the entry in the list and press the delete button . The Hostname / IP entry will be removed from the list.

Configuring a Hostname / IP Entry

In the Hostname / IP field, enter the hostname or IP address that you want to monitor. If you enter a hostname, the monitor will do a forward DNS lookup to resolve the hostname to an IP address. If you enter an IP address, the monitor will do a reverse DNS lookup to resolve the IP address to a hostname. If you enter a hostname and also check the Do Reverse Lookup checkbox, the monitor

will do both forward and reverse DNS lookups. (If you enter an IP address, the monitor will already do a reverse DNS lookup, so the Do Reverse Lookup checkbox has no effect.)

In the **Expected Result** field, you may optionally enter the expected result of the DNS lookup. (You may leave this field empty if you don't care what the result is, as long as the lookup succeeds.) If an Expected Result is specified, after resolving the hostname or IP address specified in the Hostname / IP field, the monitor will compare the lookup result with the value in the Expected Result field. If the lookup result and the expected result do not match, the monitor will report a Down status. If a hostname was specified in the Hostname / IP field, the Expected Result should specify the IP address that you expect the forward DNS lookup to return. Or, if an IP address was specified in the Hostname / IP field, the Expected Result should specify the hostname that you expect the reverse DNS lookup to return. If you want to specify the Expected Result as a regular expression, you may do so as long as you check the Match Using RegEx checkbox. (Regular expression checking is done using the .NET regular expression library.) Comparisons between DNS lookup results and Expected Results are done in a case-insensitive manner (i.e., case does not matter).

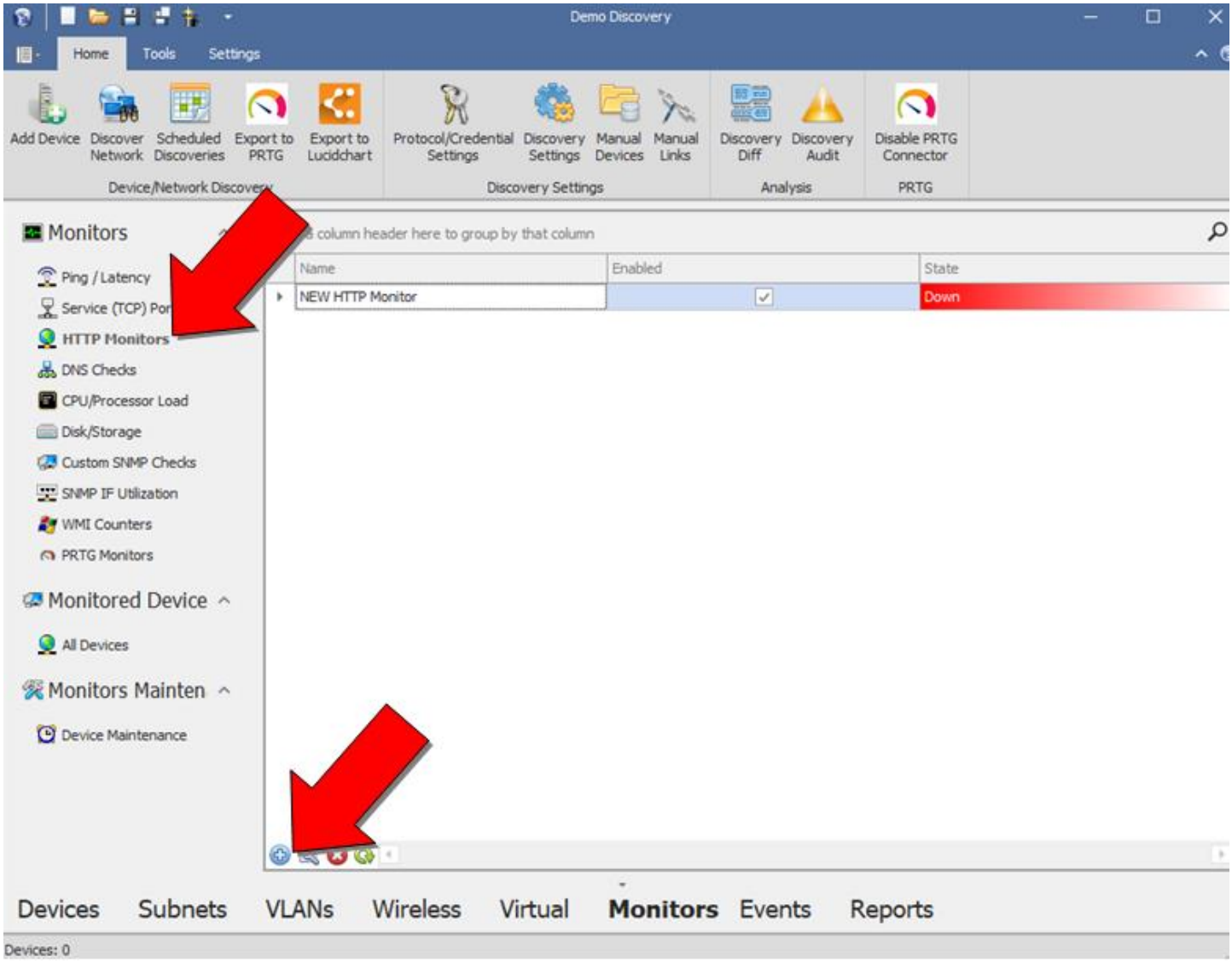
There are six different ways to configure a Hostname / IP entry, each of which is described in the following table.

Hostname / IP	Expected Result	Do Reverse Lookup	Meaning
Hostname	No	No	Do a forward DNS lookup to ensure that the specified hostname resolves to an IP address. Any IP address will do because no expected result is specified.
Hostname	No	Yes	Do a forward DNS lookup to ensure that the specified hostname resolves to an IP address. Any IP address will do because no expected result is specified. Also do a reverse DNS lookup on the resulting IP address to ensure that it resolves to the specified hostname.
Hostname	Yes	No	Do a forward DNS lookup to ensure that the specified hostname resolves to an IP address that matches the expected result.

Hostname	Yes	Yes	Do a forward DNS lookup to ensure that the specified hostname resolves to an IP address that matches the expected result. Also do a reverse DNS lookup on the resulting IP address to ensure that it resolves to the specified hostname.
IP Address	No	Not applicable	Do a reverse DNS lookup to ensure that the specified IP address resolves to a hostname. Any hostname will do, because no expected result is specified.
IP Address	Yes	Not applicable	Do a reverse DNS lookup to ensure that the specified IP address resolves to a hostname that matches the expected result.

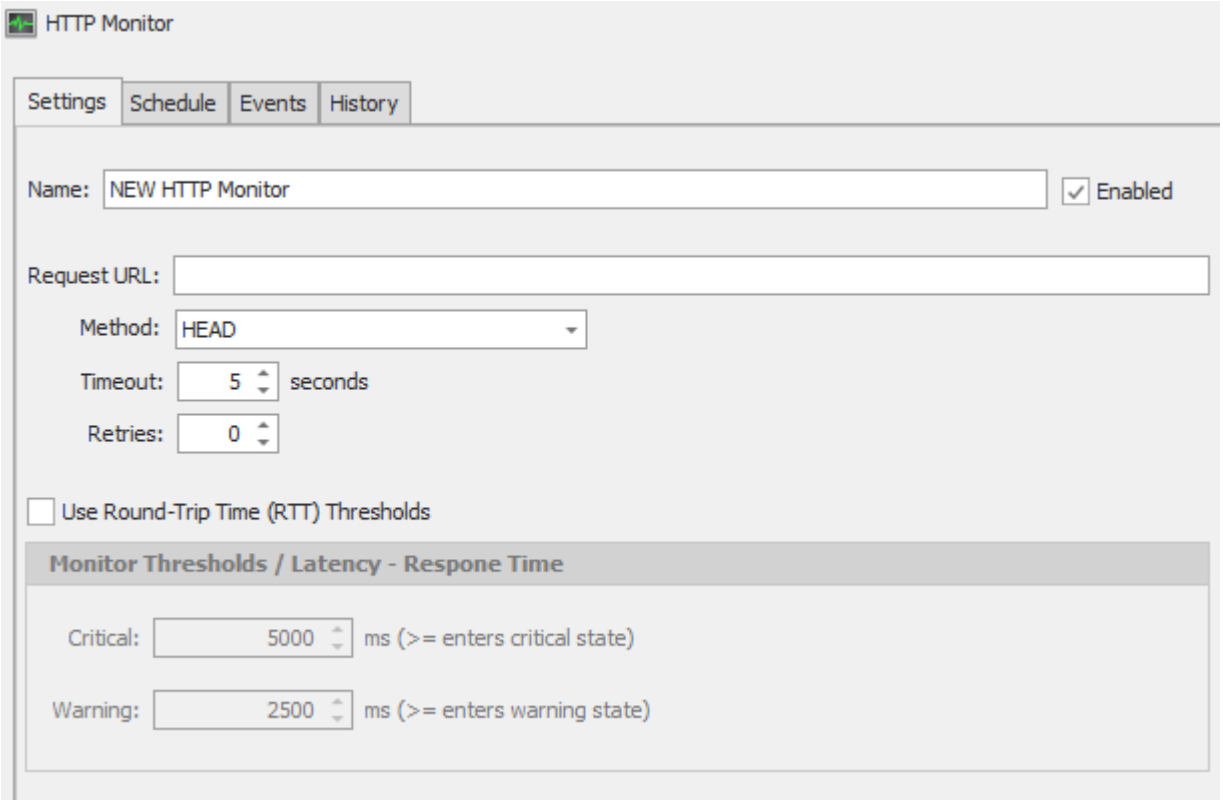
HTTP Monitor

The HTTP monitor allows you to monitor the response and response time of an HTTP request. When an HTTP monitor runs it performs an HTTP request and compares the result and result time with the expected result and result time.



Configuring the Monitor

The HTTP monitor editor contains the following tabs that require configuration: Settings, Schedule, Event, and History.



The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the settings tab see the information below.

Settings

Name
The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique, but it is recommended you use unique names to differentiate them.

Request URL
The request URL is the URL requested by the monitor.

Method
Method determines whether the request is and HTTP GET or HEAD request.

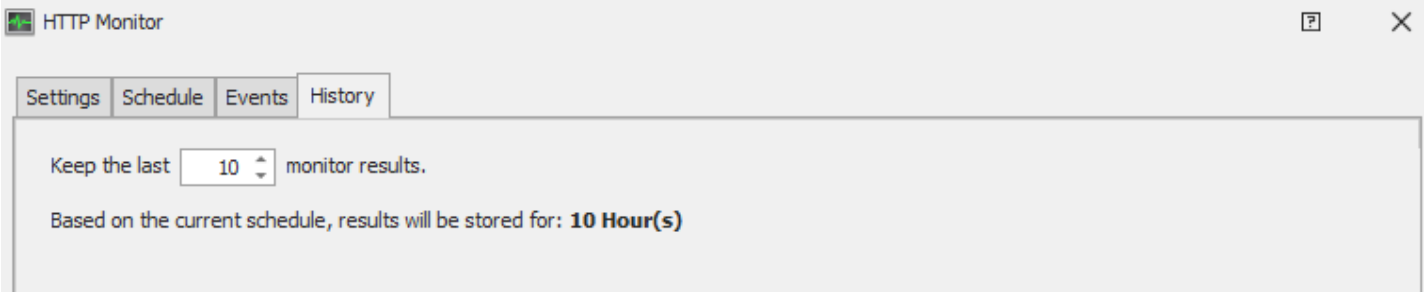
Timeout
Timeout is the maximum time to wait for a response.

Use Round-Trip Time
Use Round-Trip time specifies whether to use the response time as a threshold for determining the monitor state. If the response time exceeds the critical or warning response time a down or warning state occurs respectively.

HTTP History
To open the HTTP history view, select a HTTP monitor in the HTTP monitor list and open 'HTTP History' in the monitors context menu.

The HTTP history form contains a graph with the response time of the HTTP request in milliseconds based on the time the request was made.

Below the graph is a grid containing the HTTP requests with their collected monitor results. The grid is grouped by the request name.



The following details are available for each entry in the grid

Timestamp
The time the request was made.

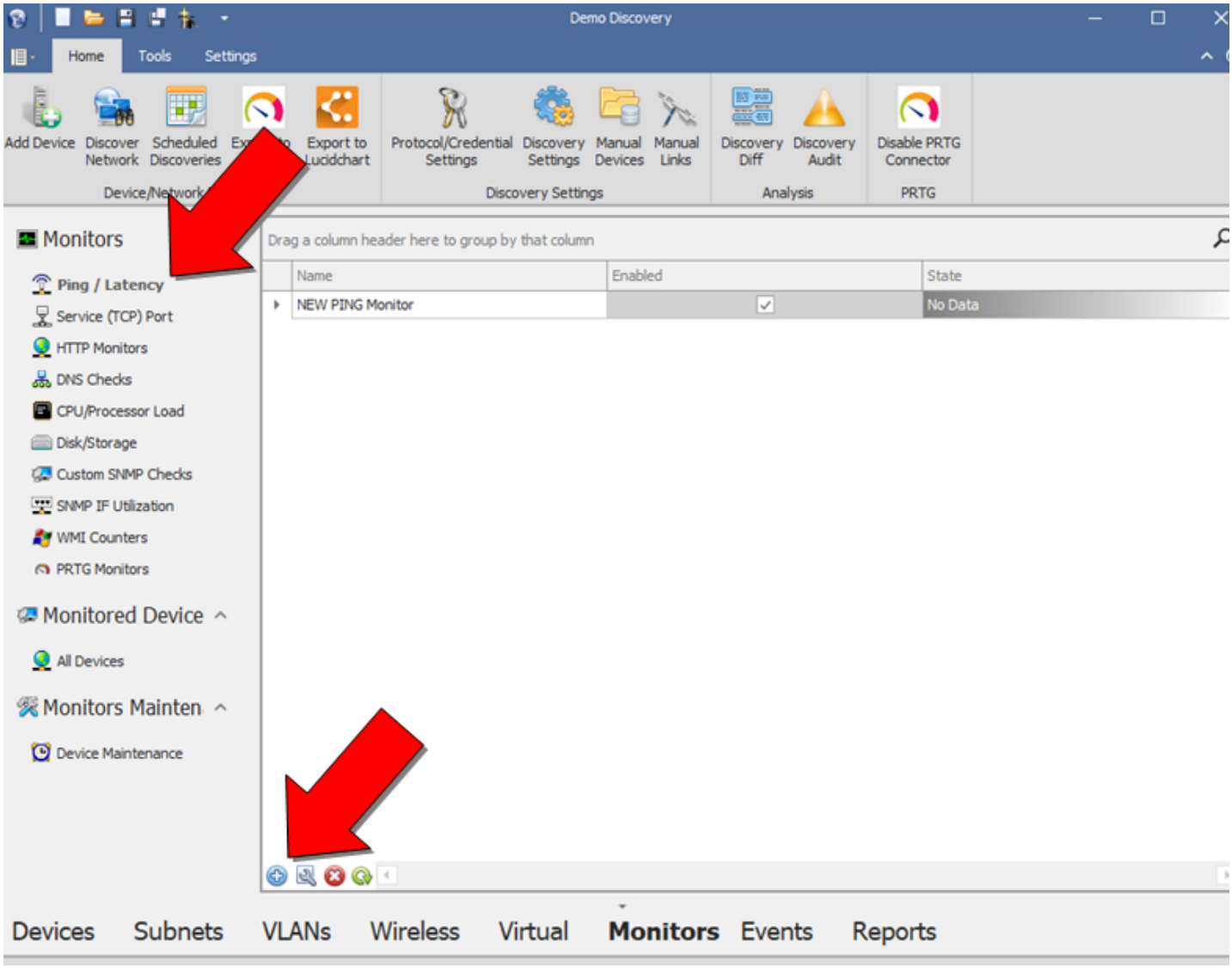
Connect
Indicates whether the HTTP request was successful.

Connect-Time (ms)
The round-trip time of the HTTP response in milliseconds.

Show Latest State
By default, the history view will update as new monitor results are collected, providing a real-time view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

Ping/Latency Monitor

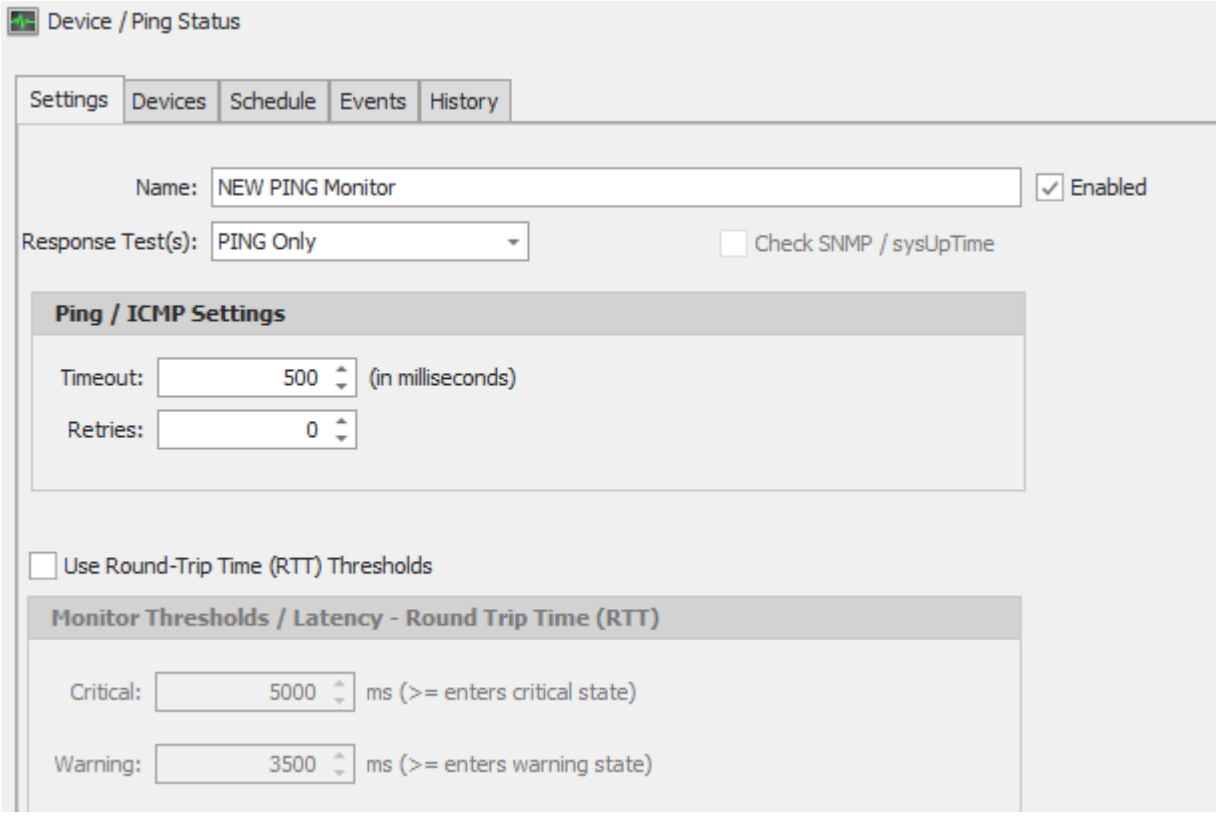
The Ping/Latency monitor allows you to monitor the Ping response time of a device. When a Ping monitor runs it sends a ping request to the device and compares the response time to the monitors specified thresholds.



Configuring the Monitor

The Ping monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the other tabs see the information below.



Settings

Name
The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique but it is recommended you use unique names to differentiate them.

Response Test(s)
The latency tests can be performed using either Ping, or SNMP responses or both. If both are selected the devices must respond to both Ping and SNMP requests for the monitor to remain in an up state. If SNMP is used, you can also specify whether to check the system up time of the device. If the System up time appears to have reset since the last query the state of that device will be considered in an "Information" state for the current request. (Meant not to alarm; but provide information that can be used for troubling shooting.)

Note: SNMP requests require the device have valid SNMP credentials associated with them. See Managing Device Credentials for more information.

Ping /ICMP Settings
The Ping/ICMP settings specifies the timeout in milliseconds and the number of retries to be performed for each ping request. If the device responds to the ping request within the specified timeout and retries the request will be considered valid.

Use Round-Trip Time
Use Round-Trip time specifies whether to use the response time as a threshold for determining the monitor state. If the response time exceeds the critical or warning response time a down or warning state occurs respectively. The warning time must be less than or equal to the critical time.

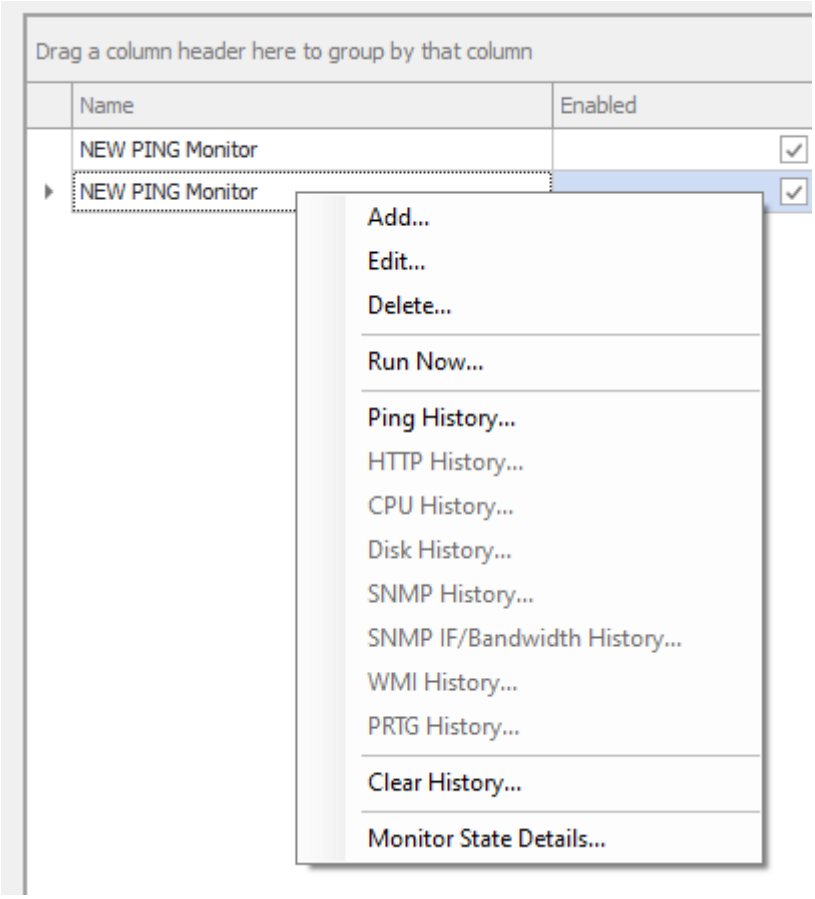
Devices

The devices tab allows you to select which devices will be monitored. To add devices to the monitor select the ⊕ button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. To remove a device from the monitor select it in the grid

and press the delete button .
By default, the main IP address of the device is selected as the IP address to Ping. Nevertheless, optional IP addresses can be added by selecting the device in the grid and selecting the edit button . Also, any Ping monitor can be configured to resolve a defined "Hostname" before sending the ping requests. To edit these settings, press the edit button .

Ping History

To open the ping history view, select a ping monitor in the ping monitor list and open 'Ping History' in the monitors context menu.



The ping history form contains a graph with the response time of the devices in milliseconds based on the time they were pinged.

Below the graph is a grid containing the devices with their collected monitor results. The grid is grouped by device name and device IP address.

The following details are available for each entry in the grid

Has Value

A Green up arrow if the device has a response and a red down arrow if the device did not respond.

Pings Replies

A ratio containing the ping responses over the ping tries (i.e., 4/5 is 4 responses of 5 tries).

Response Time

The ping response time in milliseconds.

SNMP/UP Time

The SNMP UP time of the device. This value will only be populated if the SNMP ping is requested, and the Check System Up Time option is selected.

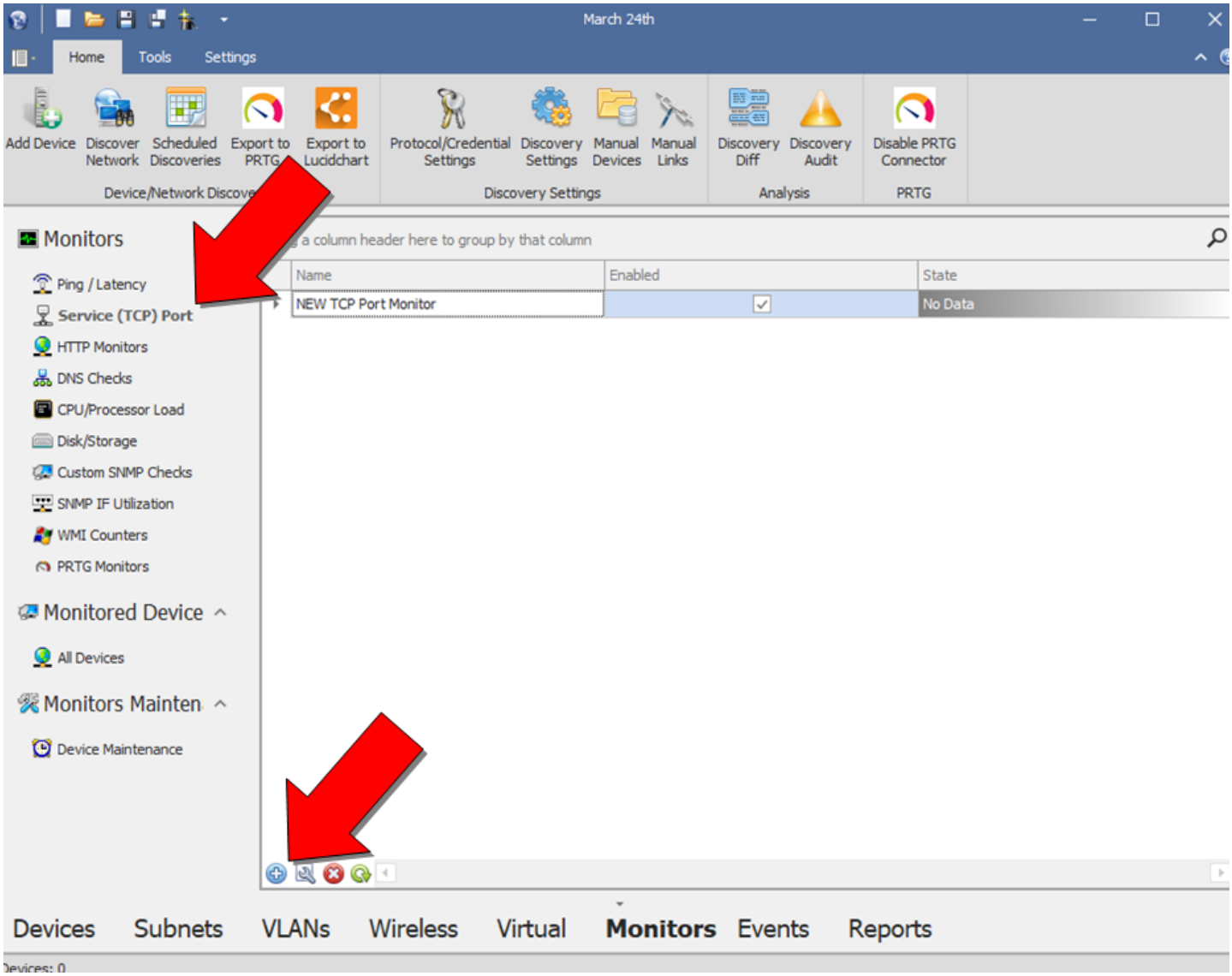
Show Latest State

By default, the history view will update as new monitor results are collected, providing a real-time

view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

Service (TCP) Port Monitor

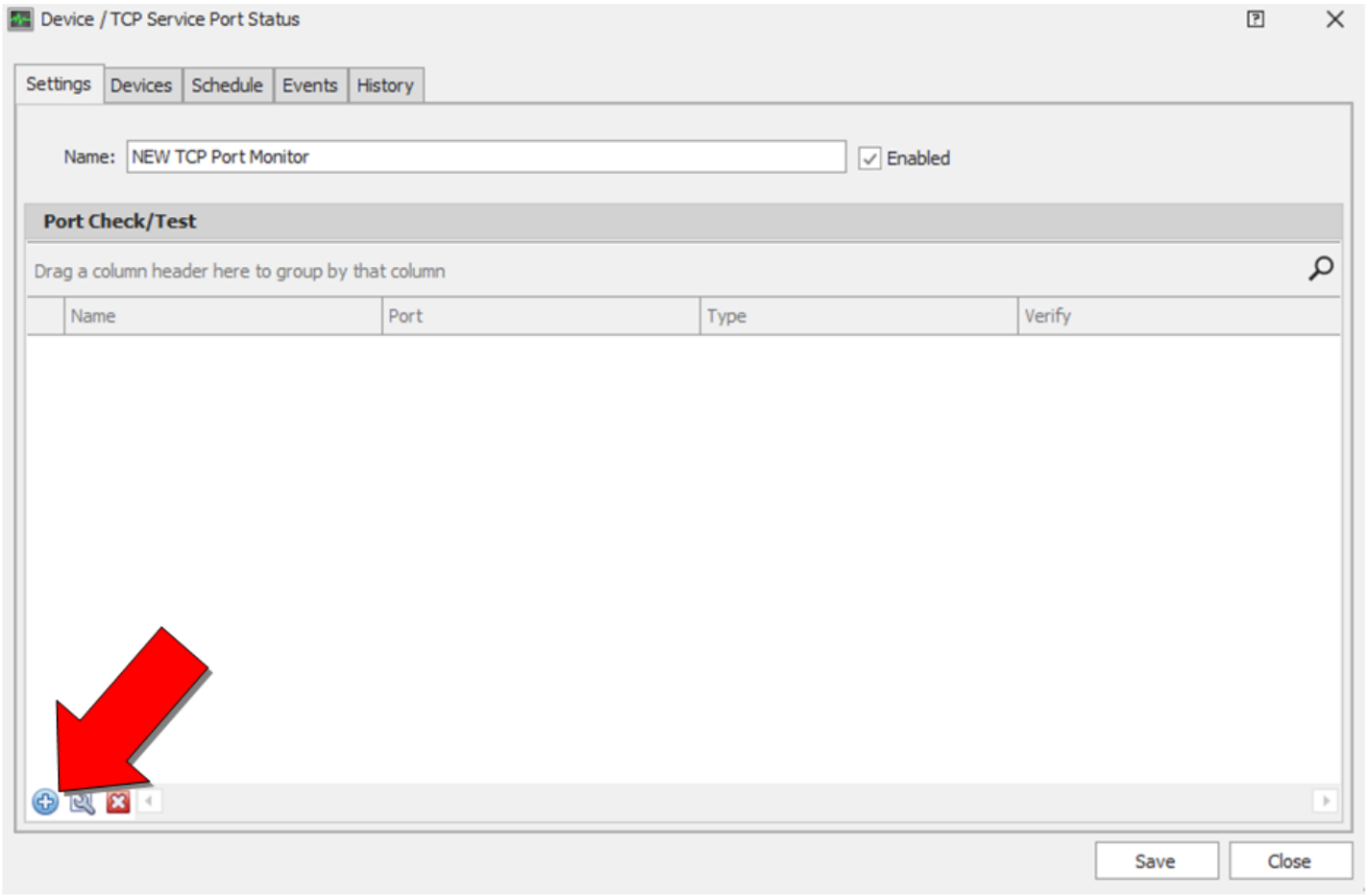
The Port monitor allows you to monitor whether a specified port is open or closed on a device. When a Port monitor runs it attempts to connect to monitored devices on the specified ports using the associated protocols and determines whether the port is open or closed.



Configuring the Monitor

The Port monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the settings tab see the information below.



Settings

Name

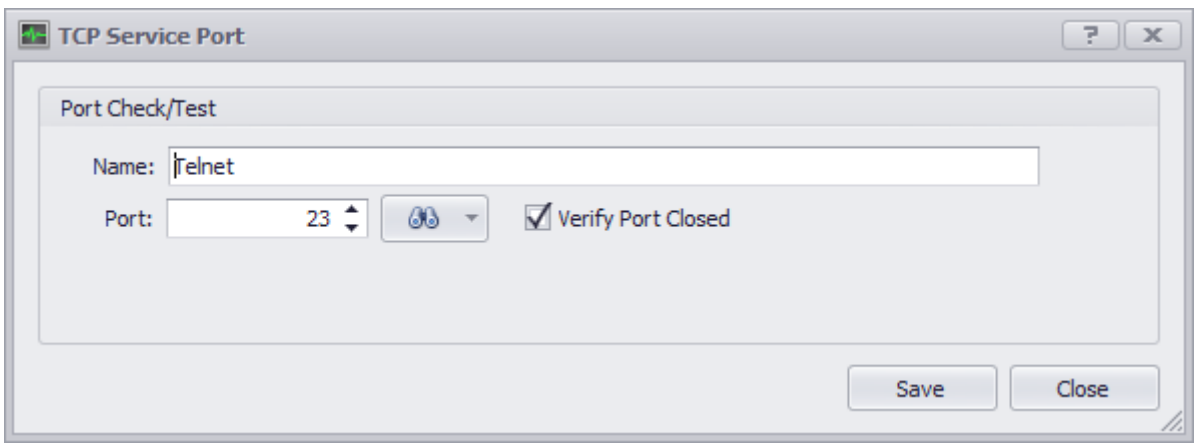
The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique, but it is recommended you use unique names to differentiate them.

Port Check/Test

The Port Check/Test section is a list of the ports to be checked by the monitor.

Adding a Port

To add a port test, press the add button . An editor allowing you to configure the port test entry is displayed. Once configured press the save button and the port test is added to the list.



Editing a Port

To edit a port test press the edit/configure button . The configuration editor is displayed. To

save the changes press the save button and the port test changes are applied.

Deleting a Port

To delete a port test, select the port test in the list and press the delete button . The port test entry will be removed from the list.

Configuring a Port Test entry

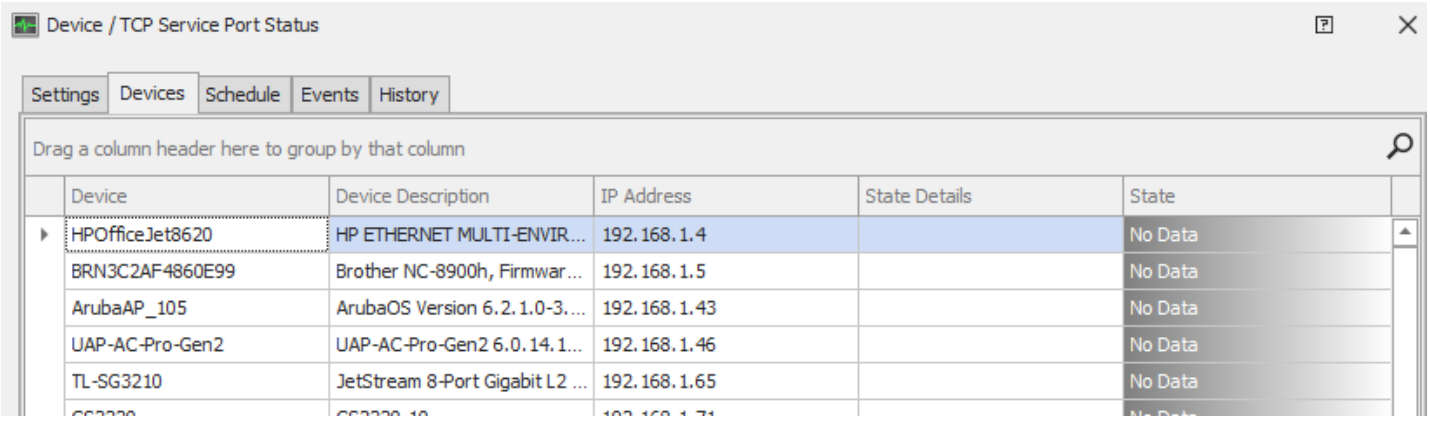
A port test entry contains the name of the test, the port, and whether the test is for open or closed.

The name is used to identify the test in the list. This name can be anything you choose but typically describes the service hosted on the port. If the port is chosen from the list of well-known ports the name is populated automatically.

The port is the port you would like to monitor. To see and search through a list of common ports select the search button to the right of the port editor. If the port, you want is in the list select the port in the list and the port editor will be populated with the result. You can also see common ports by using the spin editor arrows in the port editor. If the port, you want is not in the list of well-known ports you may manually enter the port and port name.

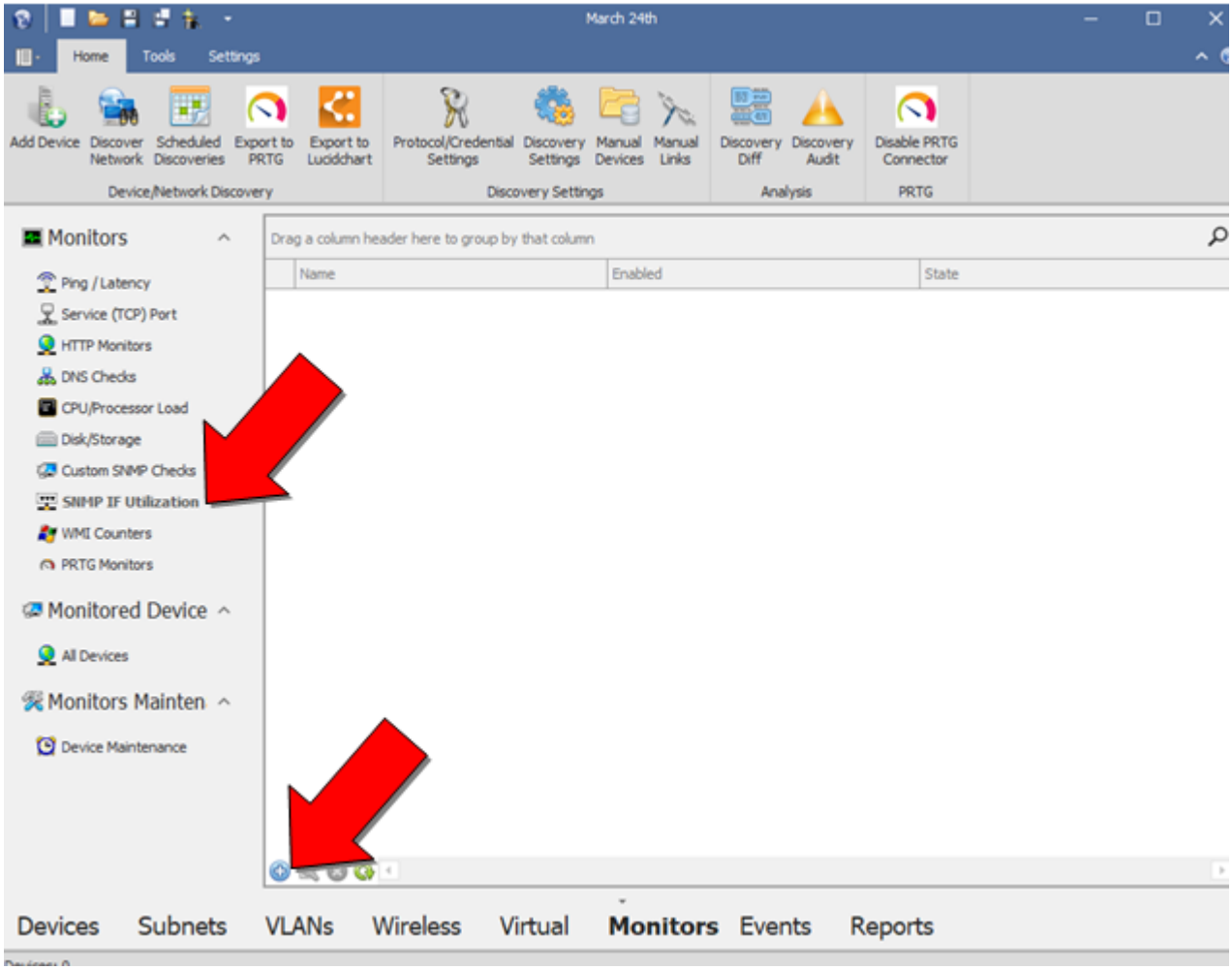
Devices

The devices tab allows you to select which devices will be monitored. To add devices to the monitor, select the button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. To remove a device from the monitor select it in the grid and press the delete button .



SNMP IF Utilization

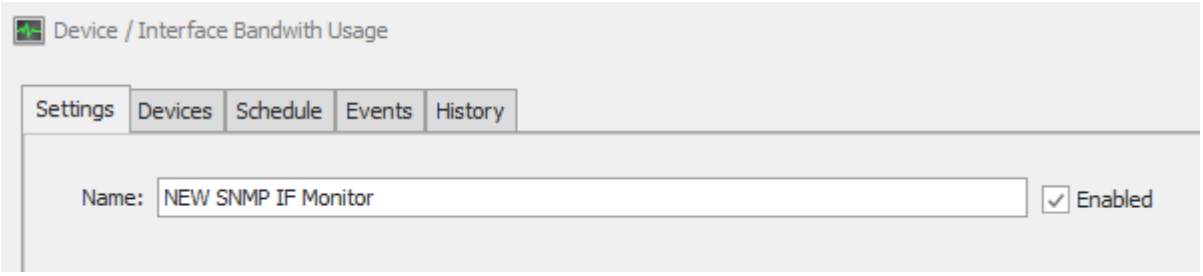
The SNMP IF Utilization monitor allows you to monitor the utilization of a device interface using the SNMP protocol. When a IF utilization monitor runs it requests the devices interface utilization from the monitored devices and compares the result with the monitors specified thresholds.



Configuring the Monitor

The Interface monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the other tabs see the information below.



Settings

Name

The Monitor name is the name of the monitor used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names must not be unique but it is recommended

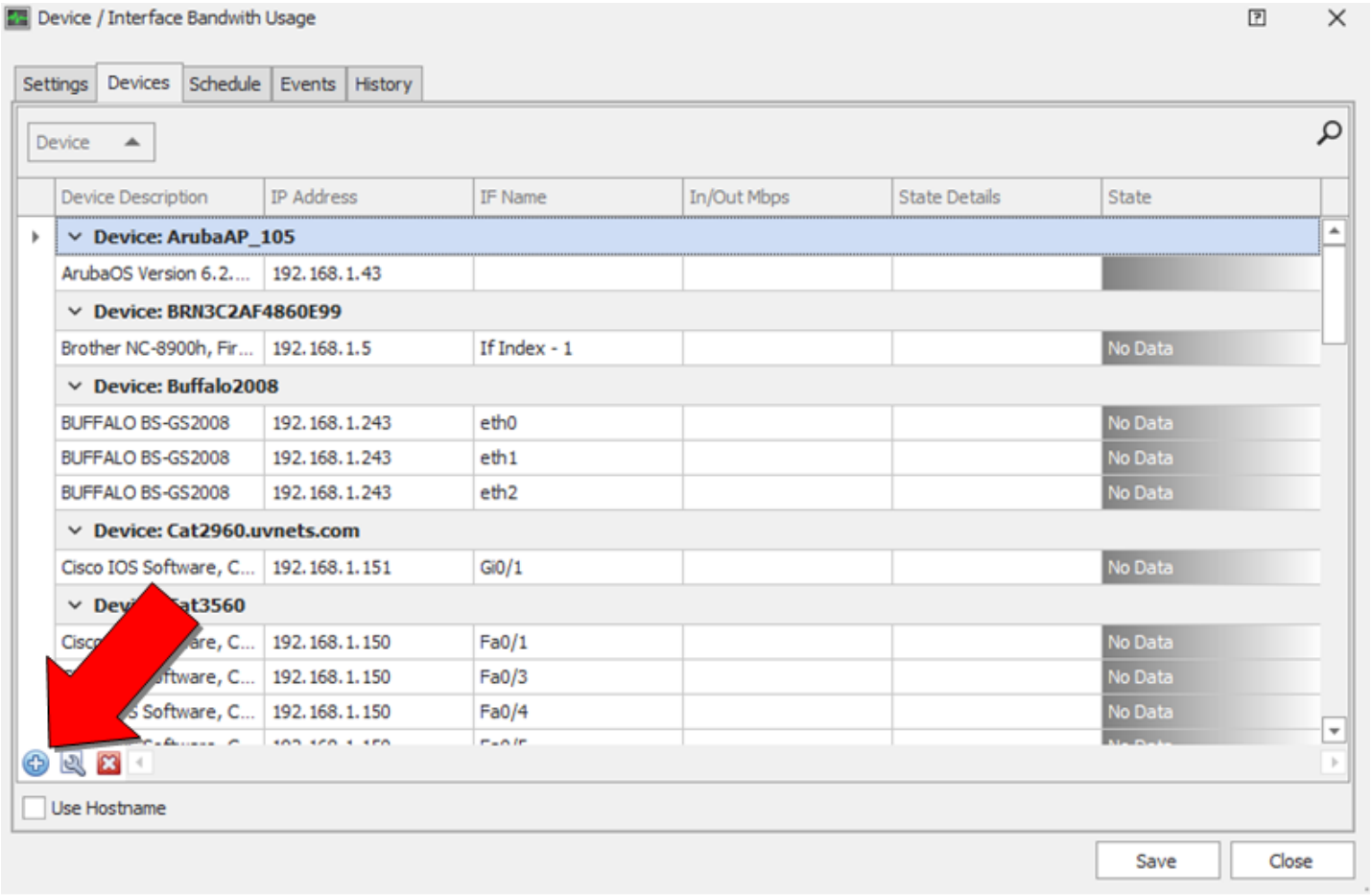
you use unique names to differentiate them.

Verify OperStatus = DOWN
The verify OperStatus down checkbox determines whether the monitor should test for the OperStatus to be up or down. If this option is not selected the monitor will fail if the OperStatus is down. If this option is selected the monitor will fail if the OperStatus is UP, this is used to monitor/ensure that a particular interface is down.

Use Usage Thresholds
The **Use Usage Thresholds** value specifies whether to compare the utilization response with the thresholds when determining the monitor state. If the utilization percentage exceeds the critical or warning percentages a down or warning state occurs respectively. The warning percentage must be less than or equal to the critical percentage.

Devices

The devices tab allows you to select which devices and its interfaces to monitor. The Interface monitor can monitor one or more interfaces on a device.



To add devices/interfaces to the monitor select the button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. When the device is selected each of the devices up interfaces that are passing traffic will be added to the monitor. **Note:** Only devices with an assigned SNMP credential will be available in the picker. If you do not see a device ensure it has the appropriate credential assigned.

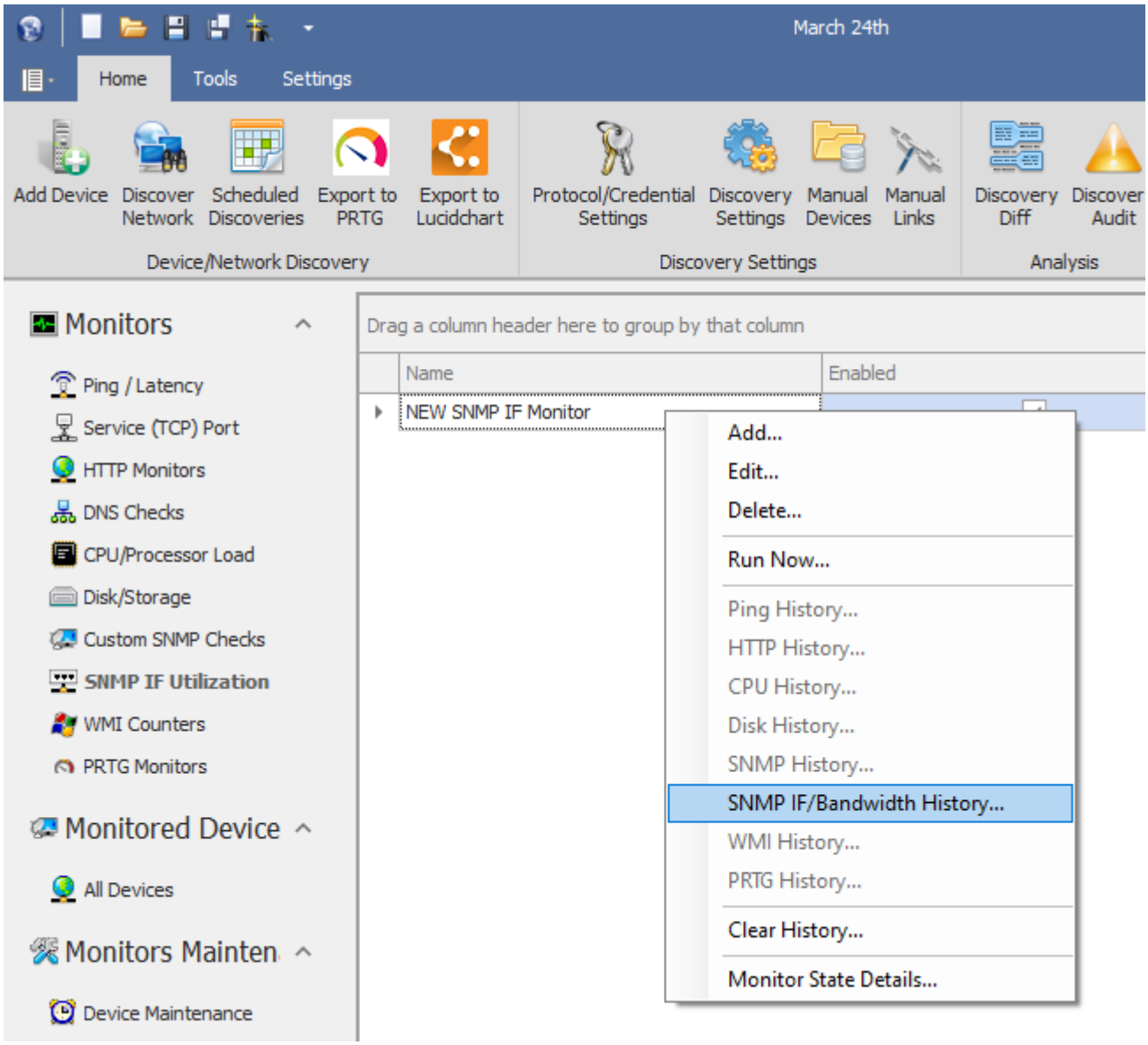
To edit which interfaces on a device to monitor. Select the device or one of its interfaces in the list and press the edit button . A list of all of the devices available interfaces will be presented. Check the interfaces you would like to monitor and close the dialog. The monitored interfaces list will be updated to reflect the changes. **Note:** If an interface is not available it could

be because it was not discovered during device discovery. To update the list ensure valid credentials are available and rediscover the device. See Monitored Devices for more information.

To remove a device or interface from the monitor select the device or interface in the list and press the delete button . The device/interface will be removed from the monitor.

SNMP IF History

To open the SNMP IF history view select the SNMP IF monitor in the SNMP IF monitor list and open 'SNMP IF/Bandwidth History' in the monitors context menu.



The SNMP IF history form contains a graph with the utilization of the interface as a percentage based on the time the monitor was run.

Below the graph is a grid containing the devices with their collected monitor results. The grid is grouped by device name and device IP address and interface name.

The following details are available for each entry in the grid

Timestamp
The time the interface utilization was queried.

In Octets (Mbps)
The number of incoming octets on the interface in Megabytes per second.

Out Octets (Mbps)
The number of outgoing octets on the interface in Megabytes per second.

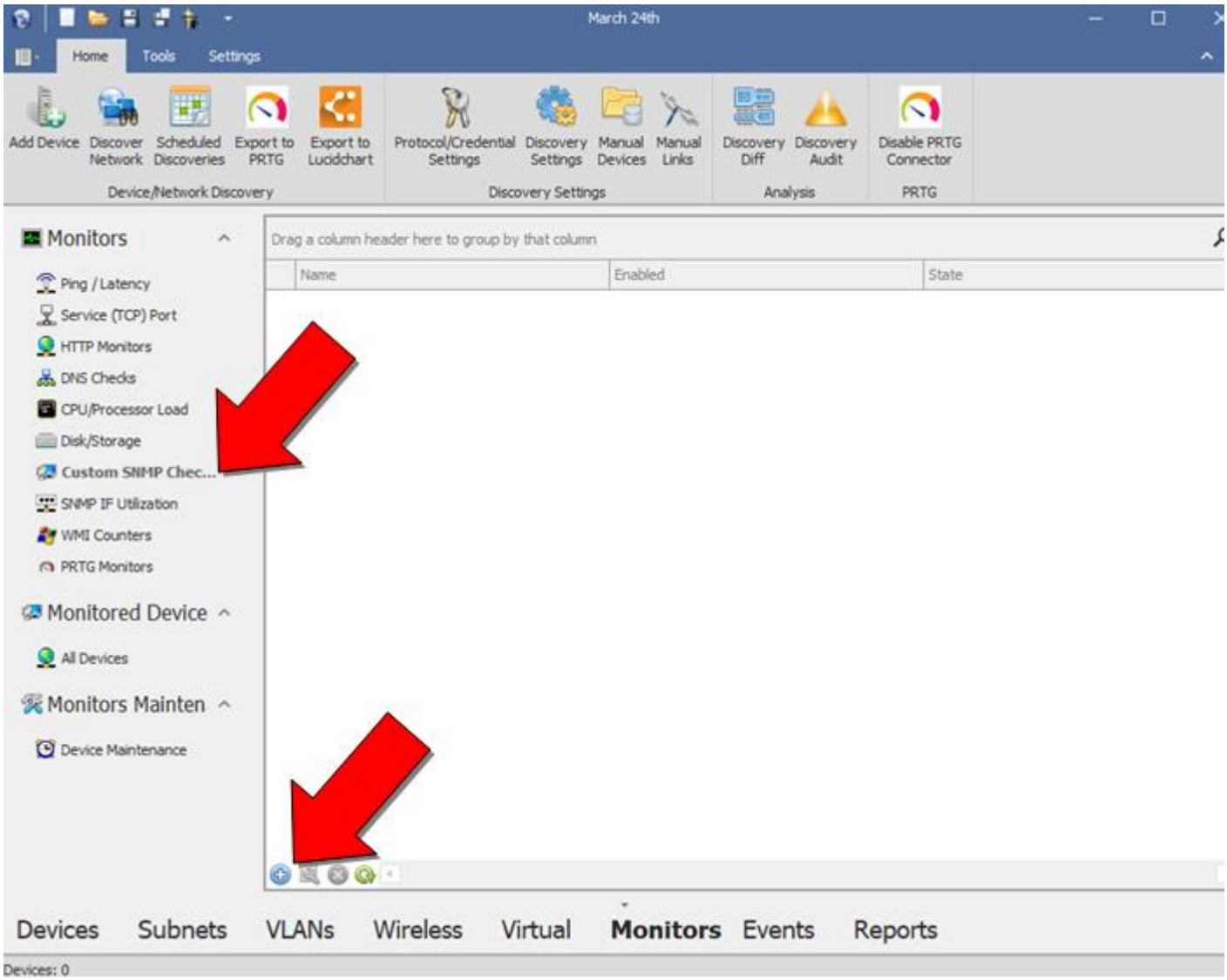
NOTE: In order to calculate In/Out Octets; the monitor must have ran at least twice.

Error
An error message if there was an error with an available message.

Show Latest State
By default, the history view will update as new monitor results are collected, providing a real-time view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

Custom SNMP Checks

The SNMP monitor allows you to query custom attributes from the device using SNMP and compare them to an expected result.



Configuring the Monitor

The Port monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the settings tab see the information below.

Settings

Name
The Monitor name is the name used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names need not be unique, but it is recommended that you use unique names to differentiate them.

SNMP OID Checks
The SNMP OID Checks section is a list of the OIDs that the monitor will query.

Adding an OID

To add an OID press the add button. An editor allowing you to configure the OID entry is displayed. Once configured press the save button and the OID is added to the list.

Editing a Port

To edit an OID double click the OID in the list (or press the edit button). The configuration editor is displayed. To save the changes press the save button and the changes are applied.

Deleting a Port

To delete an OID select the OID in the list and press the delete button . The OID entry will be removed from the list.

Configuring an OID entry

An OID entry contains the following settings

OID
The OID to request from the SNMP agent on the device. Within SNMP an OID is basically a unique identifier for a value stored on the device. To select an OID by browsing the device's OID structure, select the browse button to the right of the OID editor. The SNMP MIB walker will appear, and it will allow you to browse and select an OID from a selected device. Once selected the OID value will be placed in the OID editor. See SNMP MIB Walker for more information.

Name
Name is a description of the OID value.

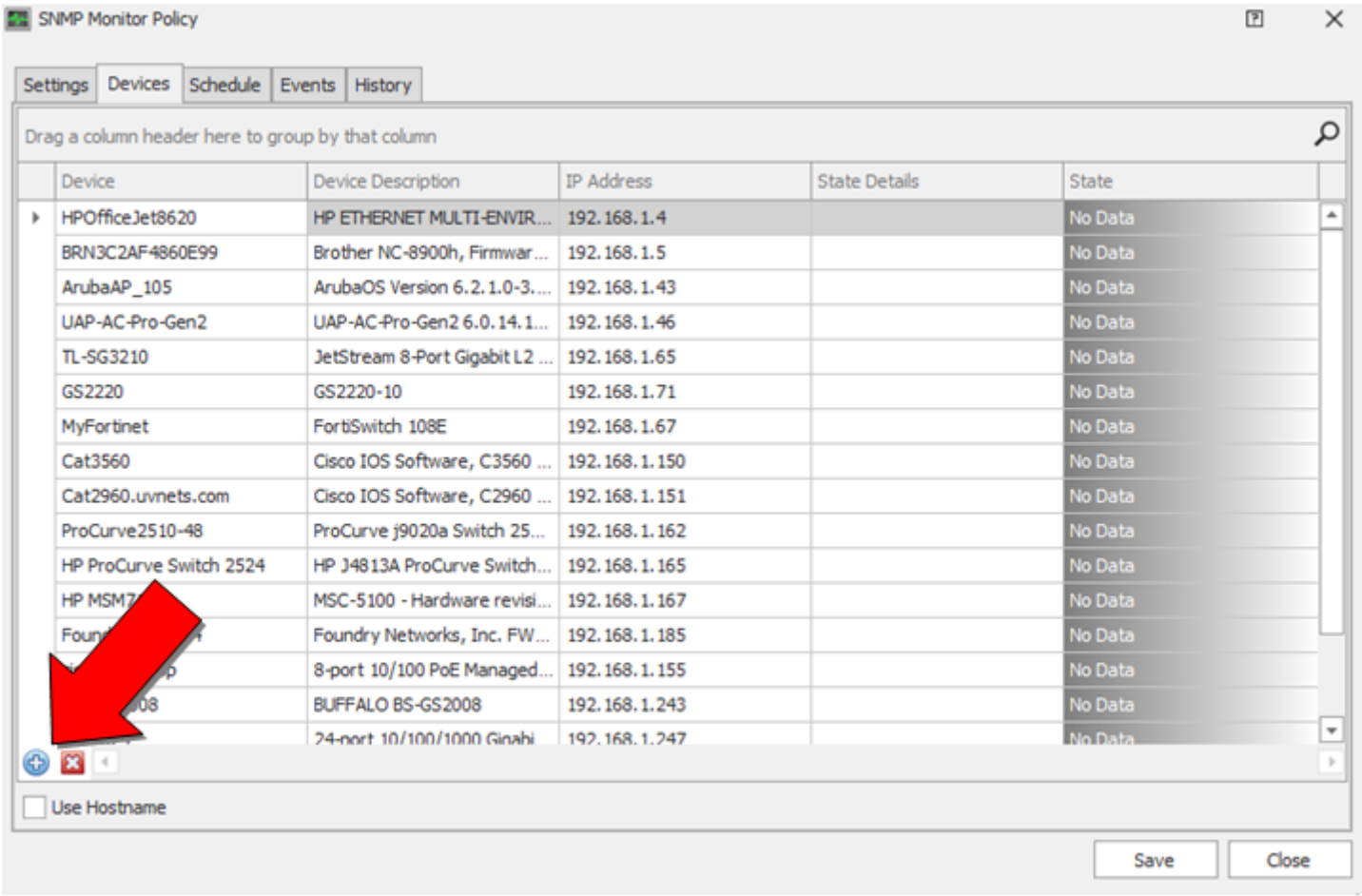
Use Expected Value
If you select Use Expected Value, the monitor will compare the SNMP response with the value you specify in the Expected Value field. By default, the monitor will check that the SNMP response value equals the expected value. However, if you check the Verify Not Equal box, the monitor will check that the SNMP response value does not equal the expected value.

Use Thresholds
Use Thresholds can be used with numeric OID responses to ensure that the value of the response does not exceed the specified Warning and Critical levels. If the value exceeds the Warning level, the monitor will report the Warning state. If the value exceeds the Critical level, the monitor will report the Down state. (The Critical value should be greater than or equal to the Warning value.)

If you check the Alert When Less Than box, the monitor will work in the opposite direction. That is, it will ensure that the value of the response does not go lower than the specified Warning and Critical levels. If the value goes below the Warning level, the monitor will report the Warning state. If the value goes below the Critical level, the monitor will report the Down state. (In this case, the Critical value should be less than or equal to the Warning value.)

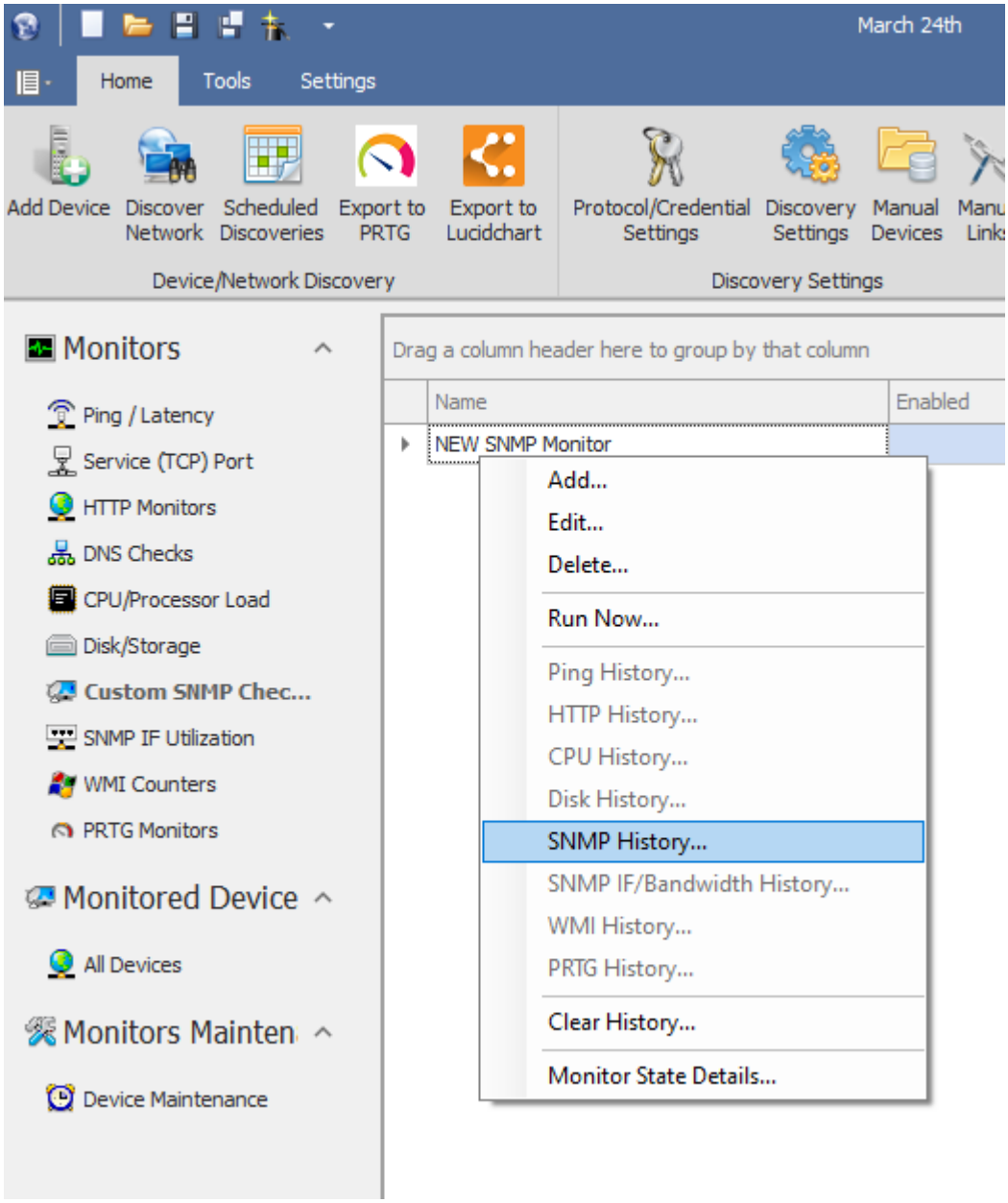
Devices

The devices tab allows you to select which devices will be monitored. To add devices to the monitor select the button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. To remove a device from the monitor select it in the grid and press the delete button .



SNMP History

To open the SNMP history view, select a SNMP monitor in the SNMP monitor list and open 'SNMP History' in the monitors context menu. The SNMP history view contains a grid with the following details about the collected results.



Name

The name of the SNMP query.

Timestamp

The time the query was run.

Value

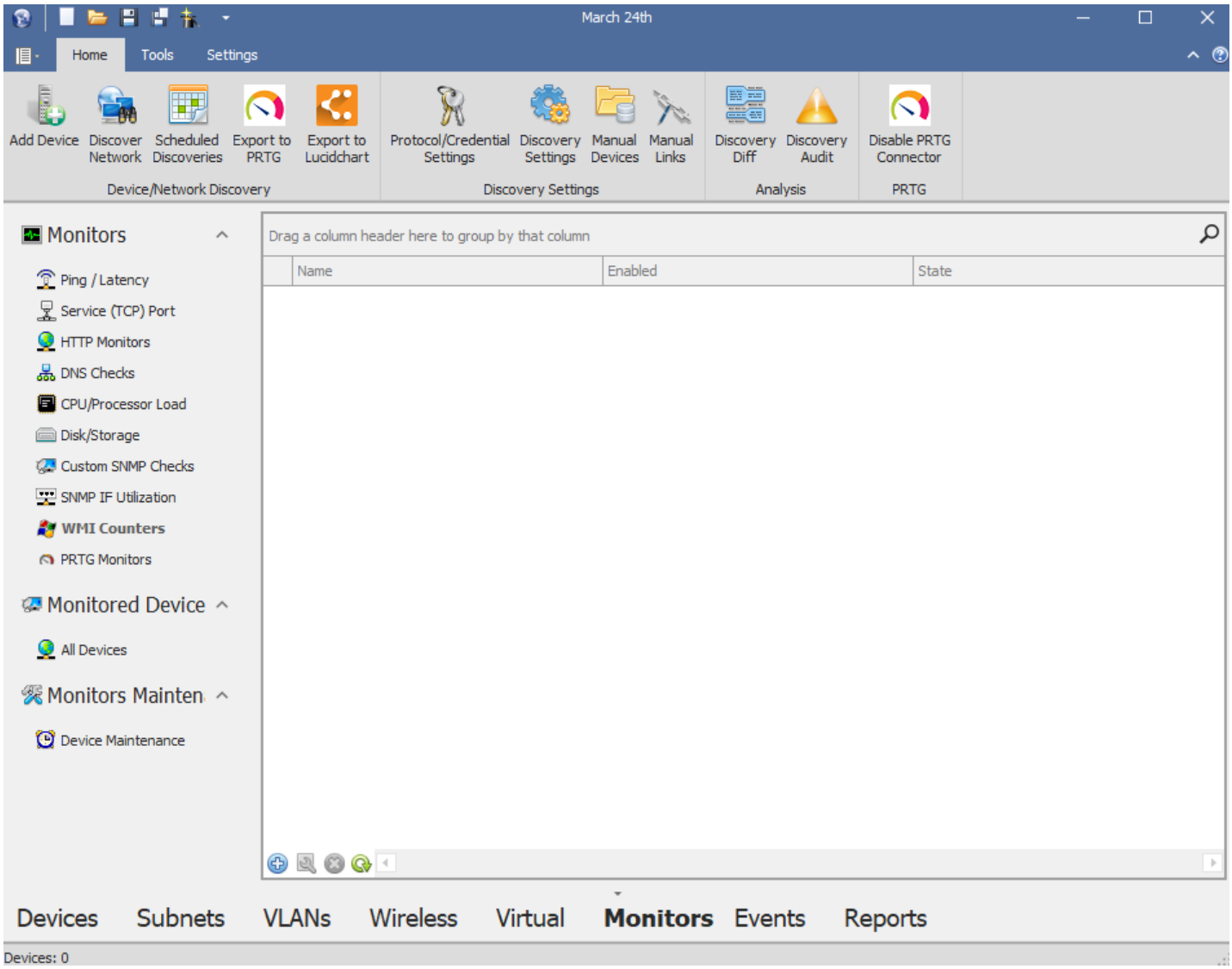
The response to the SNMP query from the SNMP agent.

Show Latest State

By default the history view will update as new monitor results are collected, providing a real-time view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

WMI Counters

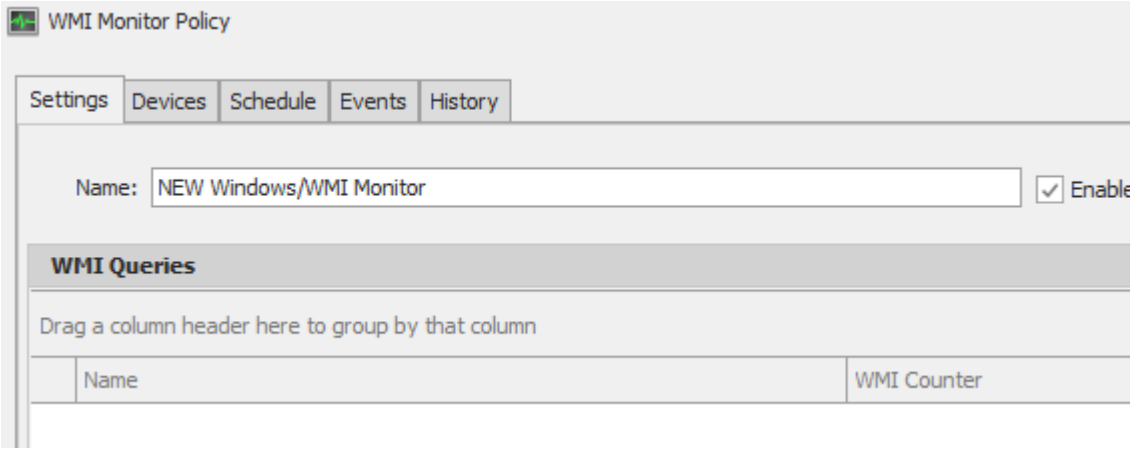
The WMI monitor allows you to query custom attributes from the device using WMI and compare them to expected results.



Configuring the Monitor

The WMI monitor editor contains the following tabs that require configuration: Settings, Devices, Schedule, Event, and History.

The Schedule, Events and History settings are the same for all monitor types. See Configuring Monitors for more information about configuring these settings. For the settings tab see the information below.



Settings

Name
The Monitor name is the name used to refer to the monitor in the monitors list view, and in monitor events and notifications. Monitor names need not be unique, but it is recommended that you use unique names to differentiate them.

WMI Queries
The WMI Queries section is a list of the WMI queries that the monitor will perform.

Adding a WMI Query

To add a WMI Query press the add button . An editor allowing you to configure the query is displayed. Once configured press the save button and the query is added to the list.

Editing a WMI Query

To edit a WMI Query double click the Query in the list or press the edit/configure button . The configuration editor is displayed. To save the changes press the save button and the changes are applied.

Deleting a WMI Query

To delete a WMI Query select the query in the list and press the delete button . The query will be removed from the list.

Configuring a WMI Query

A WMI Query contains the following settings.

WQL/Query
The WQL query to perform against the device. WQL is SQL for WMI and allows you to query information from Microsoft Windows devices on which WMI access is enabled. You can either enter your own WQL query, or click on the button next to the WQL / Query field (with the binoculars icon) to select from a list of pre-made queries. (See Microsoft's MSDN documentation for more information about WQL.)

The WQL query that you enter should return a single value that the monitor can check for validity (as opposed to a query that returns multiple values).

Name
Name is a description of the WQL query.

Use Expected Value
If you select Use Expected Value, the monitor will compare the WMI response with the value you

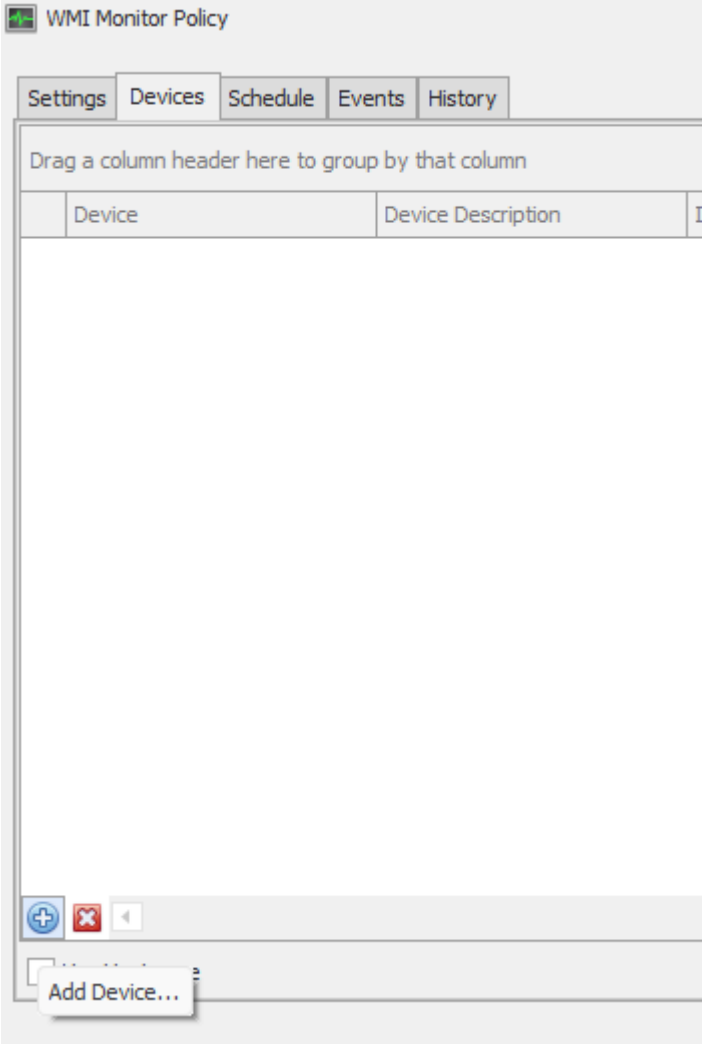
specify in the Expected Value field. By default, the monitor will check that the WMI response value equals the expected value. However, if you check the Verify Not Equal box, the monitor will check that the WMI response value does not equal the expected value.

Use Thresholds
Use Thresholds can be used with numeric WQL responses to ensure that the value of the response does not exceed the specified Warning and Critical levels. If the value exceeds the Warning level, the monitor will report the Warning state. If the value exceeds the Critical level, the monitor will report the Down state. (The Critical value should be greater than or equal to the Warning value.)

If you check the Alert When Less Than box, the monitor will work in the opposite direction. That is, it will ensure that the value of the response does not go lower than the specified Warning and Critical levels. If the value goes below the Warning level, the monitor will report the Warning state. If the value goes below the Critical level, the monitor will report the Down state. (In this case, the Critical value should be less than or equal to the Warning value.)

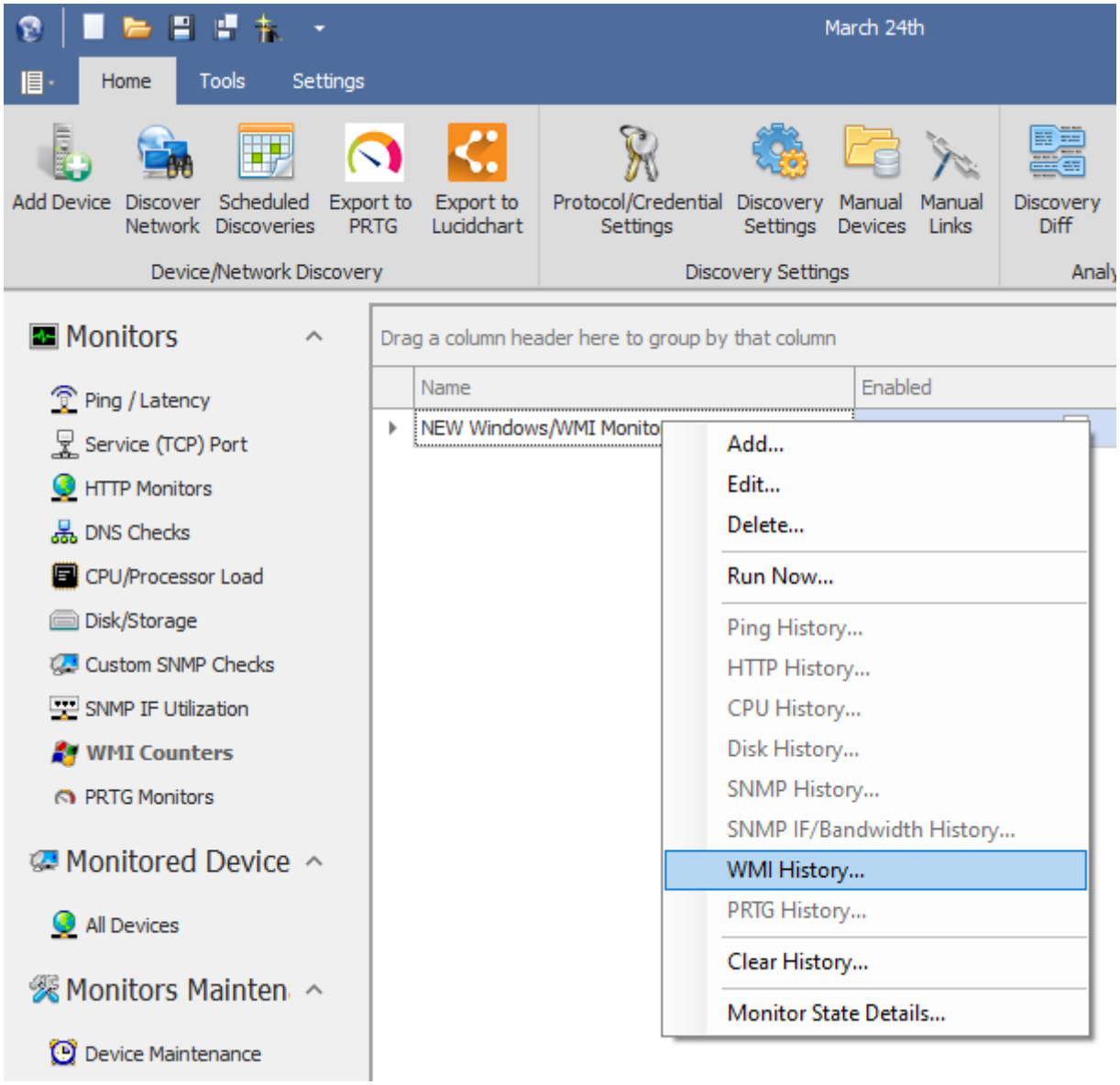
Devices

The devices tab allows you to select which devices will be monitored. To add devices to the monitor select the button in the lower left corner. A device selector will be presented allowing you to choose one or more devices to monitor. To remove a device from the monitor select it in the grid and press the delete button .



WMI History

To open the WMI history view select a WMI monitor in the WMI monitor list and open 'WMI History' in the monitors context menu. The WMI history view contains a grid with the following details about the collected results.



Name

The name of the WMI query.

Time stamp

The time the query was run.

Value

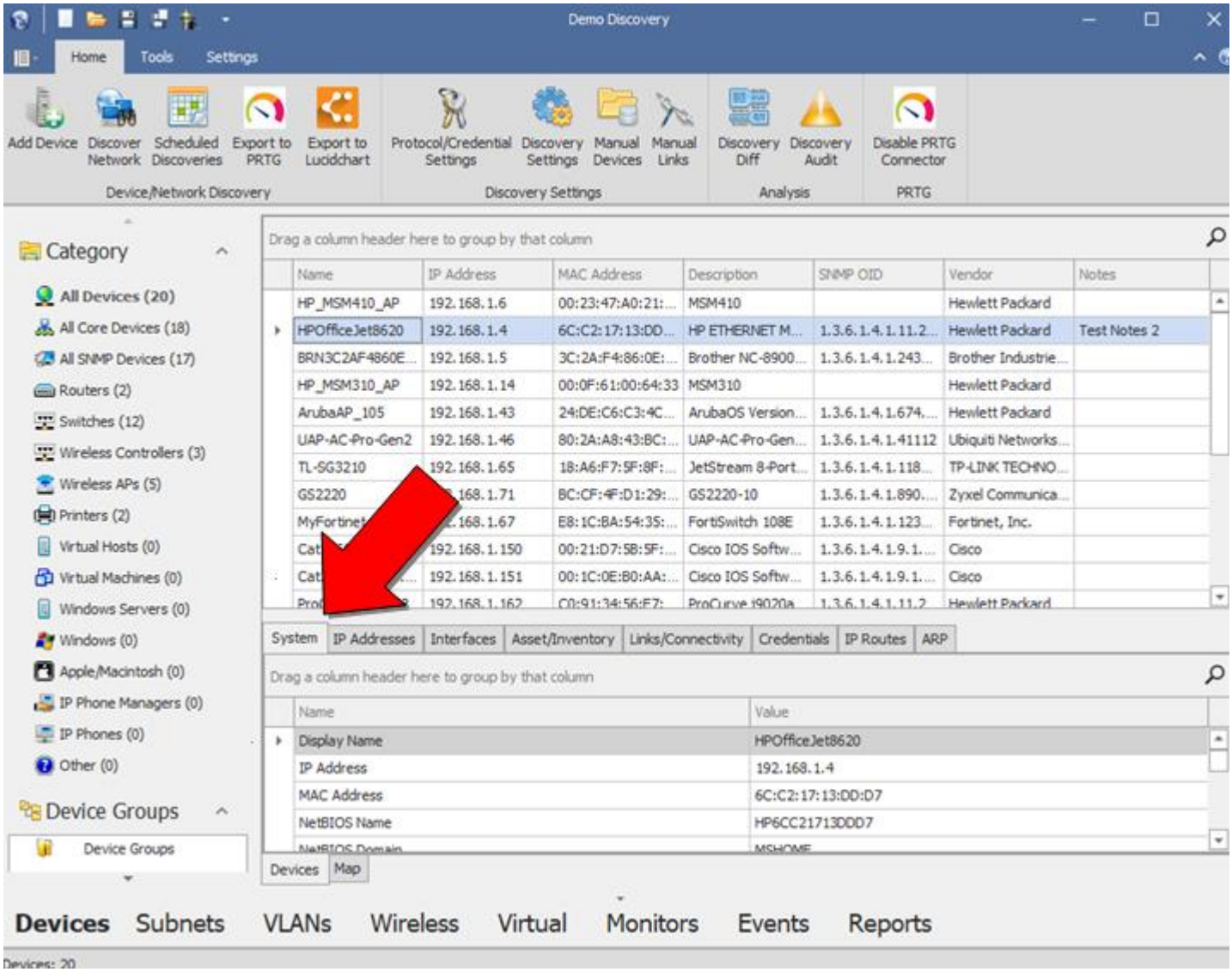
The response to the WMI query from the WMI agent.

Show Latest State

By default, the history view will update as new monitor results are collected, providing a real-time view of the monitor results. If you would like to stop the refresh of the view to inspect the current results, un-check the "Show Latest State" check box.

Viewing Device Details

Detailed device information collected during discovery is available to be viewed in the several device properties tabs. The device properties tab can be viewed as part of the tabular device details view available in both the Device Category and Device Groups views. The details can also be viewed from the map by double clicking the device or selecting device properties in the device context menu.



Each of the tabs represent data that has been discovered about the selected device. A tab is only displayed if the information was available through discovery. The following is a listing of available tabs.

System
Displays IP Address / MAC Address, MIB II information (such as System Name / System Contact), and Device Categories Labels.

IP Addresses
Displays IP Address configuration information.

Interfaces
Displays Interface (IF) information for each of the discovered interfaces.

Link Aggregation (LAG)

Displays LAG Trunk information.

Bridge Ports
Displays Bridge Port and VLAN mapping information.

Asset / Inventory
Displays details related to inventory components of the device (i.e. serial number)

Links / Connectivity
Displays details of how this device is connected to the network.

Credentials
Displays credentials that were used to discover information about this device.

VLANs
Displays Virtual LAN (VLAN) configuration information.

Address Resolution Protocol (ARP) Cache
Displays the latest collection of ARP information.

Forwarding
Displays the latest collection of forward tables from this device.

Virtual Routing Redundancy (VRRP)
Displays configuration information related to the VRRP protocol. This also includes information related to HSRP (Hot Standby Router Protocol) configuration.

IP Phone
Displays specific IP Phone data configured for this device.

IP Phone Manager
Displays data related to IP phones that are registered with this device (as its call manager)

IP Routes
Displays the configured IP routes for this device.

Spanning Tree (STP)
Displays spanning tree protocol entries discovered on this device.

Installed Software
Displays the software installed on this device.

Config
Displays the device configurations captured from the device.

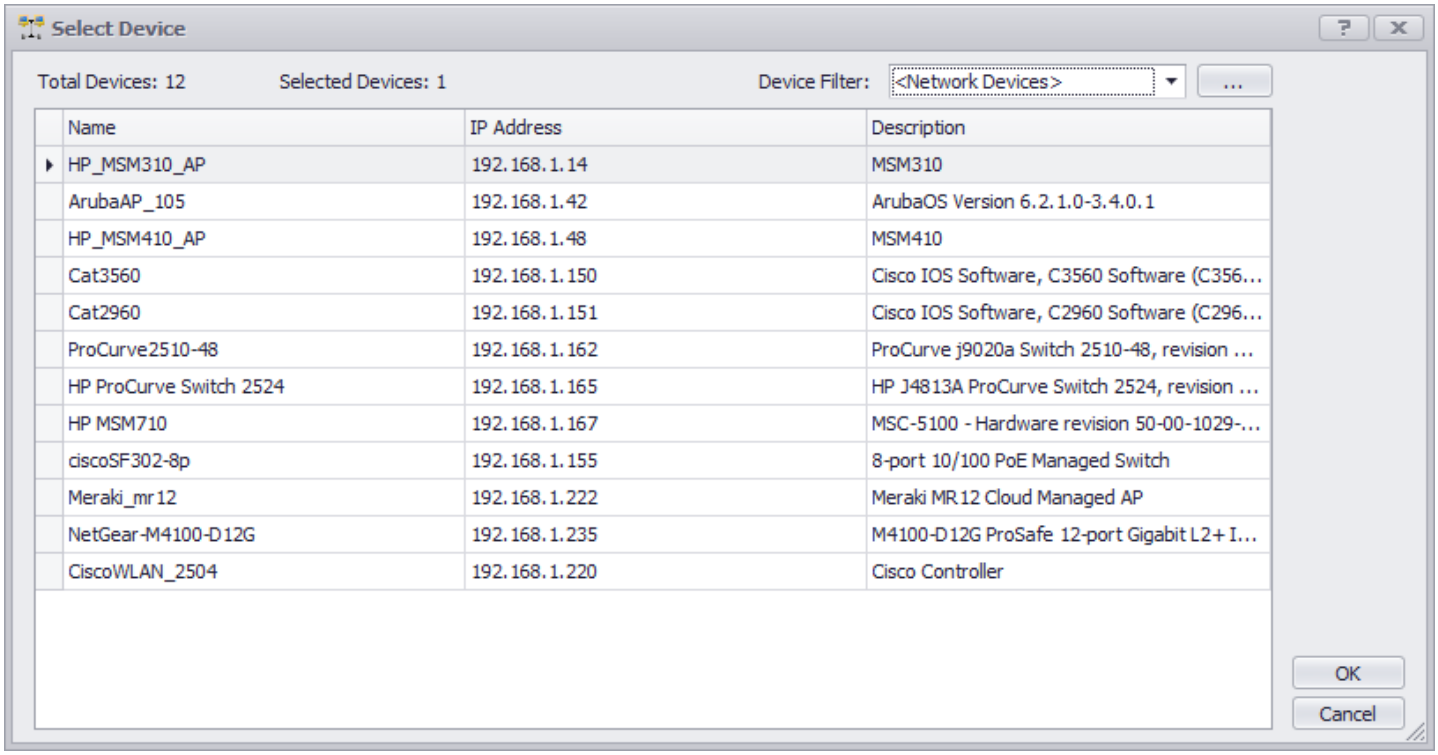
Windows
Displays the windows system information captured during discovery. Windows information includes BIOS, Computer System, Disk Drive, Installed Software, Logical disks, Network adapters, Operating System, Physical Memory, Processor, and running processes.

LLDP
Displays the information collected from the Link Layer Discovery Protocol data table.

CDP
Displays the information collected from the Cisco Discovery Protocol data table.

Device Selection Form

Many operations in UVexplorer require you to select one or more devices to be operated upon. The Device Selection form lets you select the devices that you want. This form displays a list of devices that can be selected. The row for each device displays the name, IP address, and description of the device. Each row also contains a check box that lets you select that device. The check box in the row headings can be used to select or de-select ALL devices in the list.



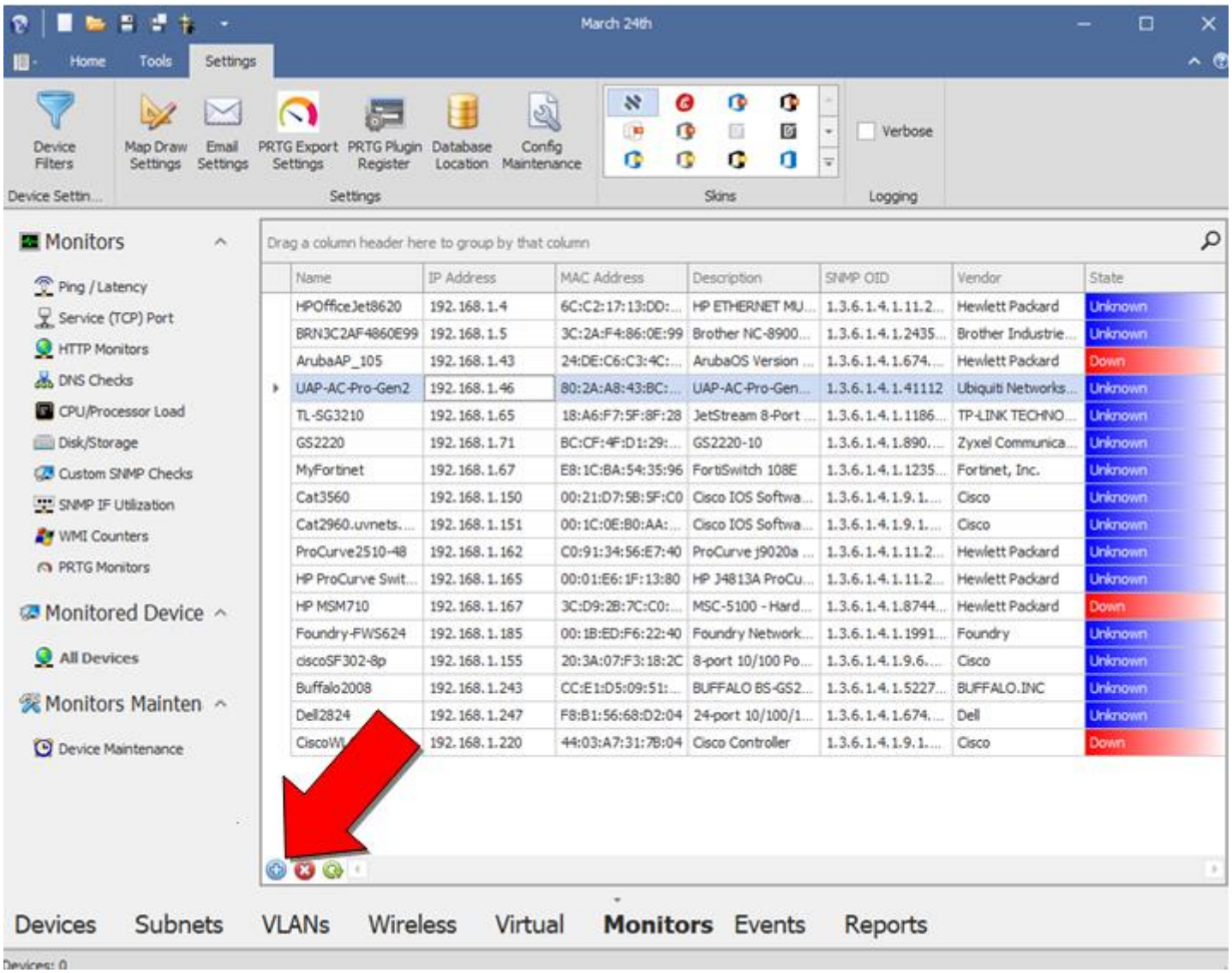
At the top of the form it displays the total number of devices in the list. Right next to that is displayed the number of devices that are currently selected.

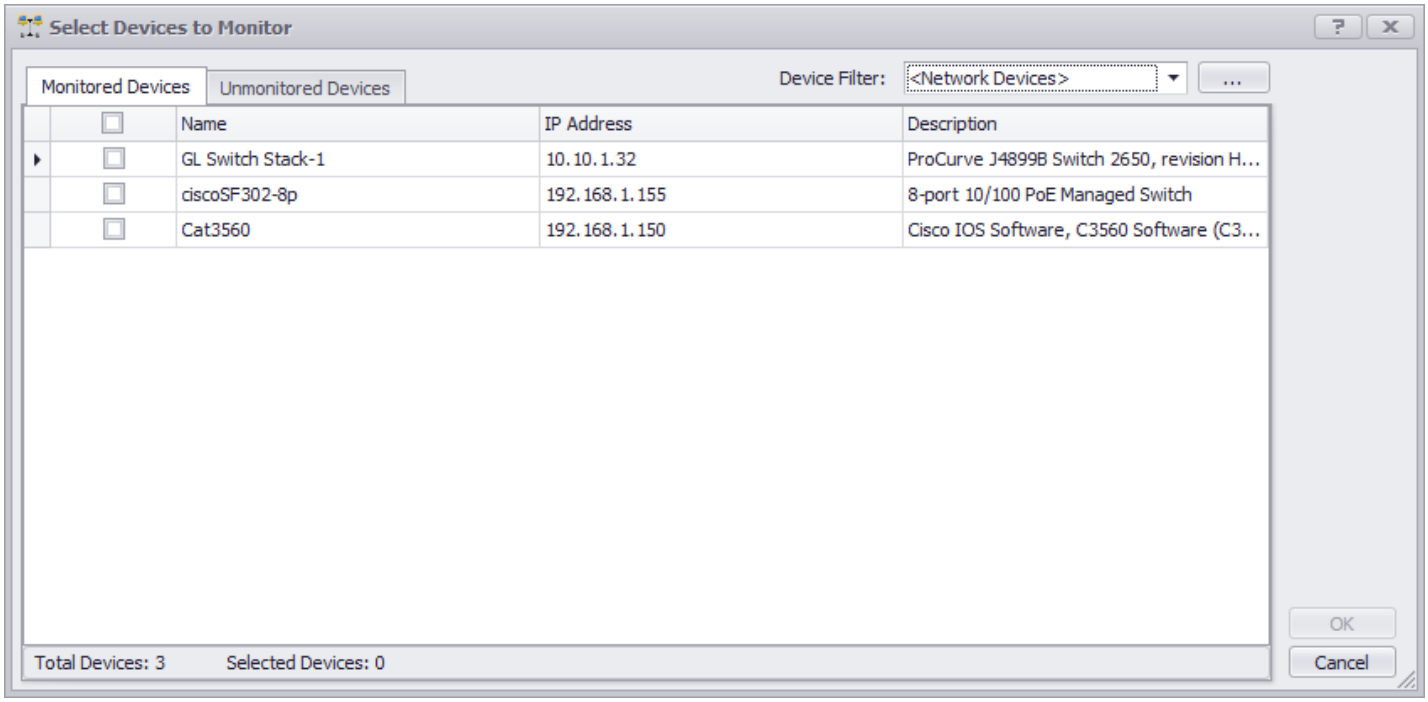
You can also filter the devices in the list using device filters that are currently defined in the system. The top-right corner displays a drop-down list of all the filters you can choose from. When you select a filter from the list, the filter will be applied so that only devices that match the filter will appear in the list. If you want to modify your filter definitions, or even create a new filter, you can click the "…" button, which will display the Device Filters form. This form lets you add, configure, and delete custom device filters.

The OK button will be enabled only when you have selected the required number of devices. If you have selected too many or too few devices for the current operation, the OK button will not be enabled.

Selecting Monitor Devices

Many operations in UVexplorer require you to select one or more devices to be operated upon. The "Select Devices to Monitor" form lets you select the devices that you want. This form displays a list of devices that can be selected. The row for each device displays the name, IP address, and description of the device. Each row also contains a check box that lets you select that device. The check box in the row headings can be used to select or de-select ALL devices in the list.





At the top of the form it displays the total number of devices in the list. Right next to that is displayed the number of devices that are currently selected.

You can also filter the devices in the list using device filters that are currently defined in the system. The top-right corner displays a drop-down list of all the filters you can choose from. When you select a filter from the list, the filter will be applied so that only devices that match the filter will appear in the list. If you want to modify your filter definitions, or even create a new filter, you can click the "…" button, which will display the Device Filters form. This form lets you add, configure, and delete custom device filters.

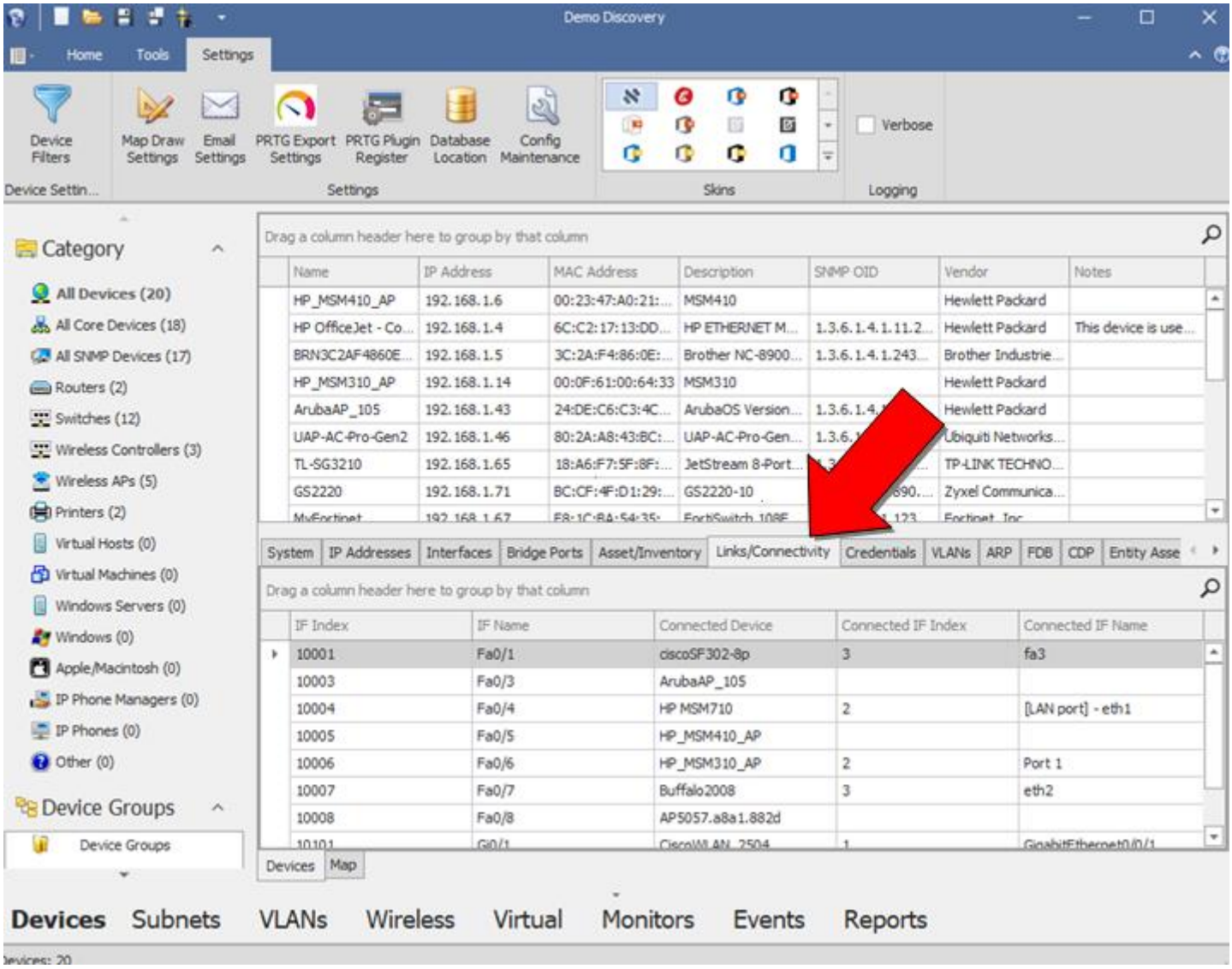
The OK button will be enabled only when you have selected the required number of devices. If you have selected too many or too few devices for the current operation, the OK button will not be enabled.

Network Connectivity

UVexplorer uses information collected from devices to calculate the network connectivity. The detailed knowledge of all the devices on the network allows it to create an extensive view of the network, the device interfaces and the ways they are connected.

Links

When connections between devices are calculated they are represented within the application as a link. The links can be seen on the device details 'Links/Connectivity' tab. Links can also be viewed as lines between devices on the topology maps. Each link contains information about the devices participating in the link and the interfaces they are connected on.



Unmanaged Links

Occasionally when calculating connectivity, connections between devices are seen, but there is enough information to indicate that an unseen device is between the connected devices. These unseen devices are actively participating in the network, and will often respond to simple requests, but for some reason UVexplorer was unable to capture the information from the device needed to complete the connectivity calculations. This is often a result of not having the correct SNMP credentials to communicate with the device, or the device being unsupported. Unseen devices are presented in the application as unmanaged, since there is enough information to know they exist but

the application is unable to manage them.

When unseen devices exist all device connections connecting through that device are included in one link. These links will include multiple devices, each indicating that it is connected to the same unmanaged device. These unmanaged devices are represented in the topology map as a single connection point with all connecting devices having lines attaching to it.

Link Properties

The details of a link can be viewed in the device details 'Links/Connectivity' tab or in a link properties view available by double clicking a link on the map or using the map links context menu.

Device
The 'Device' column displays the display name of the device participating in the link.

IF Index
The 'IF Index' column displays the interface index of the device interface participating in the link.

IF Name
The 'IF Name' column displays the interface name and description.

Connecting device
The second Device, IF Index, IF Name columns display the information for the device and interface on the other end of the link connection.

Wireless Links

Wireless clients are connected to the network on wireless radios that are usually part of a wireless access point. Typically multiple clients will connect to one wireless radio. A wireless link represents a wireless radio and all of the devices connected to it. Wireless links are displayed on the map as a single connection point representing the radio with all connecting clients having lines attaching to it.

Wireless link properties are displayed similar to other links displaying the Device, IF Index, and IF Name. The wireless properties also include the Radio name and SSID associated with the connection.

Manual Links

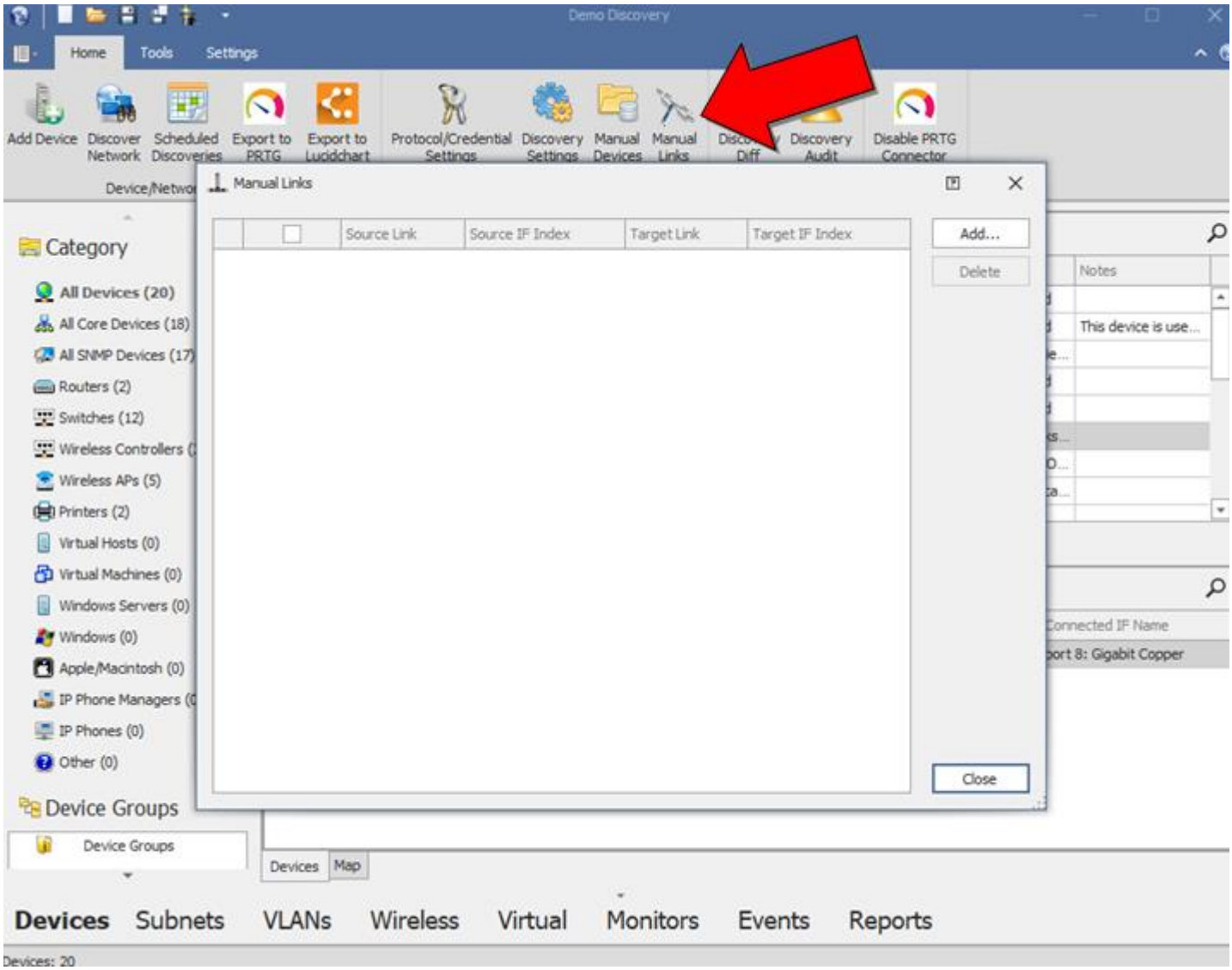
Occasionally you may want to manually link devices so that they are represented correctly on topology maps.

See Manual Links for more information.

Manual Links

Occasionally you may want to manually link devices so that they are represented correctly on topology maps. Manually linked devices will be treated like devices linked by the link calculator.

Manual links can be viewed on the topology maps or by using the manual links viewer launched from the "Home" tab of the main application view. The manual links viewer allows you to Add and Delete manual links.



Properties

Each manual link consists of a source device with interface and a target device with interface. Interfaces are not required when creating manual links. The order of the link is irrelevant. When manual links are presented the display name of the device and interface are included along with the interface index.

Adding Manual Links

To add a manual link in the manual link viewer, press the add button and configure the link using the manual link editor.

To add links from the map, select one or two devices and pressing the 'Link To...' or 'Link Selected...'

menu item available on the device context menu. The manual link editor will be displayed which allows the interfaces to be selected.

Deleting Manual Links

Manual links can be deleted in the manual link viewer by selecting the links in the list and pressing the delete button.

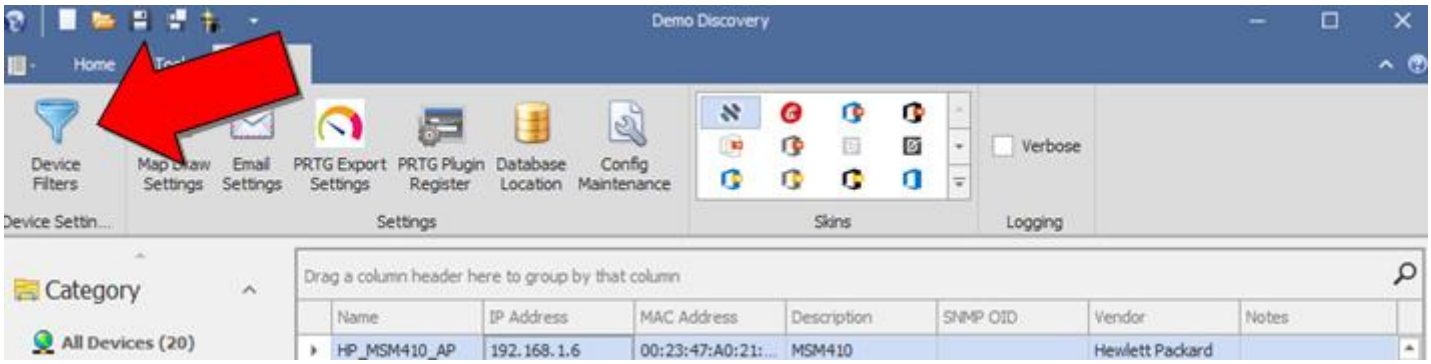
Manual links can also be deleted on the map by right clicking the link and using the 'Un-Link' context menu item.

Manual Links Editor

To edit/create a manual link in the manual link editor you must select both a source and target device using the device selectors. Optionally manual link interfaces can be selected using the interface drop down selectors when the devices have interfaces available. Interfaces are not required to create a manual link. When the devices and interfaces are selected the link can be created by pressing the OK button.

Device Filters

When using UVexplorer, it is often necessary for you to select the devices that you are interested in from a list. For example, when adding or removing devices to/from a device group, you must select the devices to be added or removed. Similarly, when creating a manual link between two devices, you must select the devices to be linked. In these and many other situations, you will be asked to select devices from a device list. Since networks can contain hundreds or thousands of devices, searching through a list of all devices in the network can be overwhelming. Therefore, UVexplorer uses the notion of a 'device filter' to let you trim down a device list to display only the devices you are interested in. By default, UVexplorer displays all devices. However, using device filters, you can say things like, "Only show printers" or "Only show routers and switches". This makes it much easier to find the devices you are looking for.



Default Device Filters

UVexplorer has a few built-in device filters that are always available. Here are the default device filters:

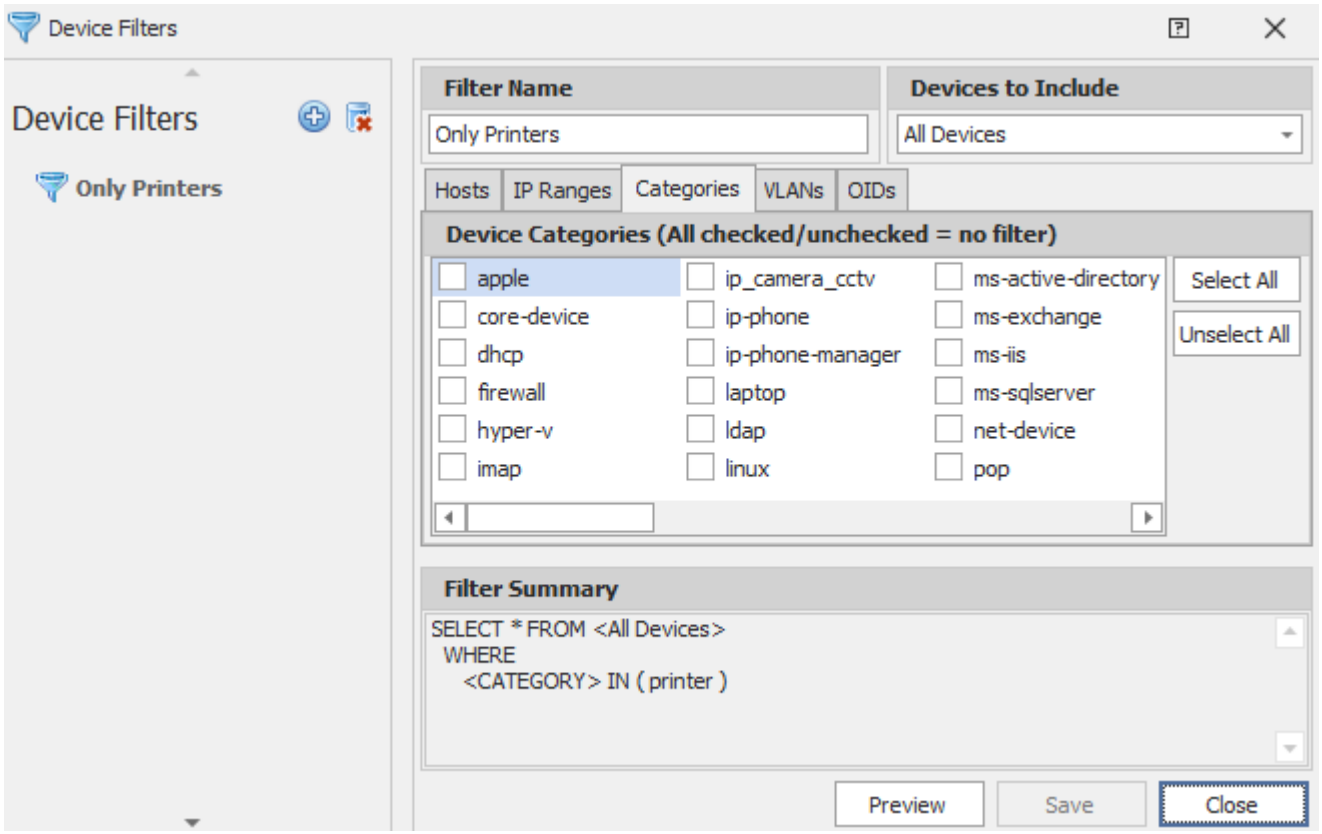
- 'All Devices' – This filter displays all devices. In effect, this filter can be used to turn off filtering.
- 'SNMP Devices' – This filter displays all devices that have SNMP enabled on them. This includes all devices that responded to SNMP queries when they were discovered.
- 'Network Devices' – This filter displays all network devices, which are devices that form the infrastructure of your network. This includes devices such as routers, switches, and wireless access points.

Custom Device Filters

You can also create custom device filters that represent subsets of devices that you frequently work with. For example, you could create device filters such as these:

- 'Only show servers in the 192.168.3.0/24 subnet'
- 'Only show wireless controllers and wireless access points'
- 'Only show devices in the Sales VLAN'

You can create as many custom device filters as you like, and they will always be available to you when you are asked to select devices from a list.



When you create a custom device filter, you must give it a name. For example, the custom device filters above might have these names:

- 'Core Servers'
- 'Wireless Infrastructure'
- 'Sales Devices'

Custom device filters let you filter devices based on the following criteria:

- Host/System/NetBIOS Name (including wildcards)
- IP Address (including address ranges and subnets)
- Device Categories (e.g., 'printer', 'router', 'server', 'wireless ap', 'virtual machine', etc.)
- VLAN Name (including wildcards)
- SNMP Enabled (or not)

Managing Device Filters

To manage your custom device filters, click the Device Filters icon on the Settings toolbar. This will display the Device Filters form. This form lets you add, configure, and delete custom device filters. A list of all existing device filters is displayed on the left side of the form. The right side of the form displays properties of the currently-selected device filter.

Adding a Device Filter

To create a new device filter, click on the Add icon (the plus sign) just above the device filter list on the left side of the form. Alternatively, you can right-click anywhere in the device filter list, and select Add from the context menu. This will cause a new device filter with a default name to be created and selected. You can then edit the properties of the new device filter on the right side of the form.

Configuring a Device Filter

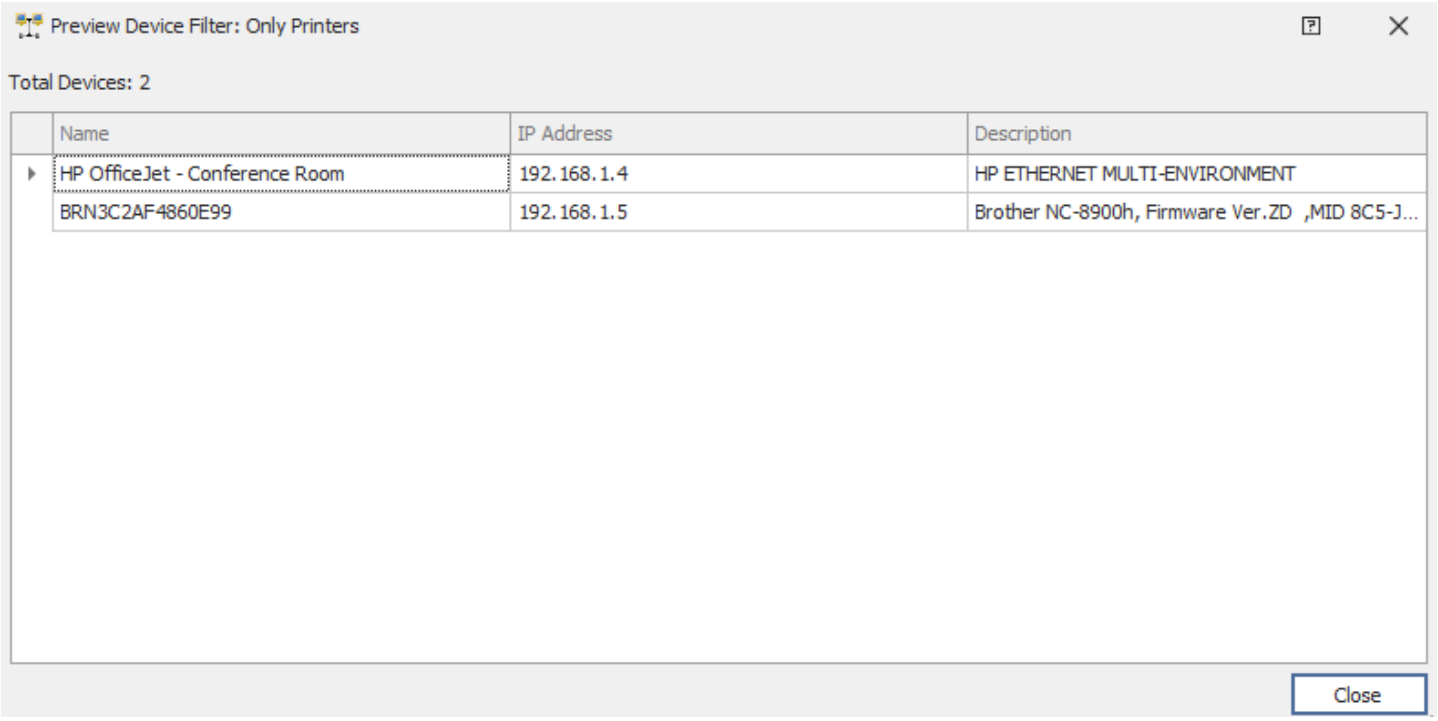
The properties of a device filter can be modified by first selecting it in the list of device filters. After it has been selected, the right side displays the various properties that can be edited. To help you

visualize the filter's properties, the Filter Summary field at the bottom of the form always displays a summary of the filter's current properties. This Filter Summary uses a SQL-like syntax to display all of the current filter properties in one place. It is updated any time the filter properties are modified. To create a device filter, you must first specify a name (which cannot be empty). Next, you must specify which devices match the filter. This is done in two steps:

1) Select a base set of devices that match the filter. The choices are: All Devices, SNMP Devices Only, and Network Devices Only. This selection defines which devices could potentially match the filter (i.e., devices outside the base set will not match the filter).
   a) All Devices – Any device can match the filter
   b) SNMP Devices Only – Only SNMP devices can match the filter
   c) Network Devices Only – Only network devices can match the filter (routers, switches, wireless access points, etc.)
1) Starting with the base device set selected in step 1, you may optionally specify additional criteria to narrow down the base set even further. The following additional filtering criteria may also be specified:
   a) Host/System/NetBIOS Name – You can specify one or more patterns to be matched against a device's names. For example, the pattern fileserver will match any device that has a DNS host name, SNMP system name, or NetBIOS name with the value fileserver. You can also include wildcard characters in a name pattern. For example, the pattern *.acme.com will match any device with a name ending in .acme.com. In general, an asterisk * will match zero or more adjacent characters, and a question mark ? will match exactly one character. If any device name patterns are specified, a device's names must match at least one of the name patterns in order to match the filter.
   b) IP Ranges – You can specify one or more IP addresses to be matched against a device's IP addresses. You can specify individual IP addresses, such as 172.16.3.25; ranges of IP addresses, such as 192.168.3.1 – 192.168.3.127; or IP subnets, such as 10.5.0.0/16. If any IP address constraints are specified, a device must have at least one IP address that matches at least one of the constraints.
   c) Categories – You can specify one or more device categories to be included in the filter. A list of all possible device categories is presented for you to choose from. Simply check the device categories that should match the filter. For example, if you select the 'printer' category, then printer devices will match the filter. If any device categories are specified, a device must be in at least one of the selected categories in order to match the filter.
   d) VLANs - You can specify that devices in particular VLANs should be included in the filter. This is done by listing one or more patterns to be matched against the names of a device's VLANs. For example, the pattern Sales will match any device that is in the VLAN named Sales. You can also include wildcard characters in a VLAN name pattern. For example, the pattern Marketing* will match any device that participates in a VLAN whose name begins with Marketing. In general, an asterisk * will match zero or more adjacent characters, and a question mark ? will match exactly one character. If any VLAN patterns are specified, a device's VLANs must match at least one of the patterns in order to match the filter.
   e) OIDS - You can specify that devices with an OID matching the provided OID pattern should be included in the filter. An OID is an unique object identifier provided by the manufacturer of a device or asset. The first portion of an OID is specific for a vendor and often a model. Multiple OID patterns can be provided, separated by a space or comma. Wild card's of '*' and '?' can be used when specifiying a match pattern. In general, an asterisk * will match zero or more adjacent characters, and a question mark ? will match exactly one character. If any OID patterns are specified, a device's OID must match at least one of the patterns in order to match the filter.

After modifying the properties of a device filter, there are two things you can do to make sure it is working correctly:

1) Review the Filter Summary
2) Click the Preview button, which will display a list of devices in the currently-open discovery result that match the filter



Deleting a Device Filter

To delete an existing device filter, select it in the device filter list on the left side of the form, and then click the Delete icon (with the red X) just above the list. Alternatively, you can right-click on the device filter in the list, and select Delete from the context menu. The deleted device filter should disappear from the list.

Selecting a Device Filter

The Device Filter Selection form lets you select a device filter from a list. This is helpful, for example, when creating a dynamic device group whose definition is similar to an existing device filter. Rather than entering the group's settings from scratch, it can be easier to copy the device filter's settings into the group. This requires you to select the device filter you wish to copy, which is the purpose of the Device Filter Selection form.

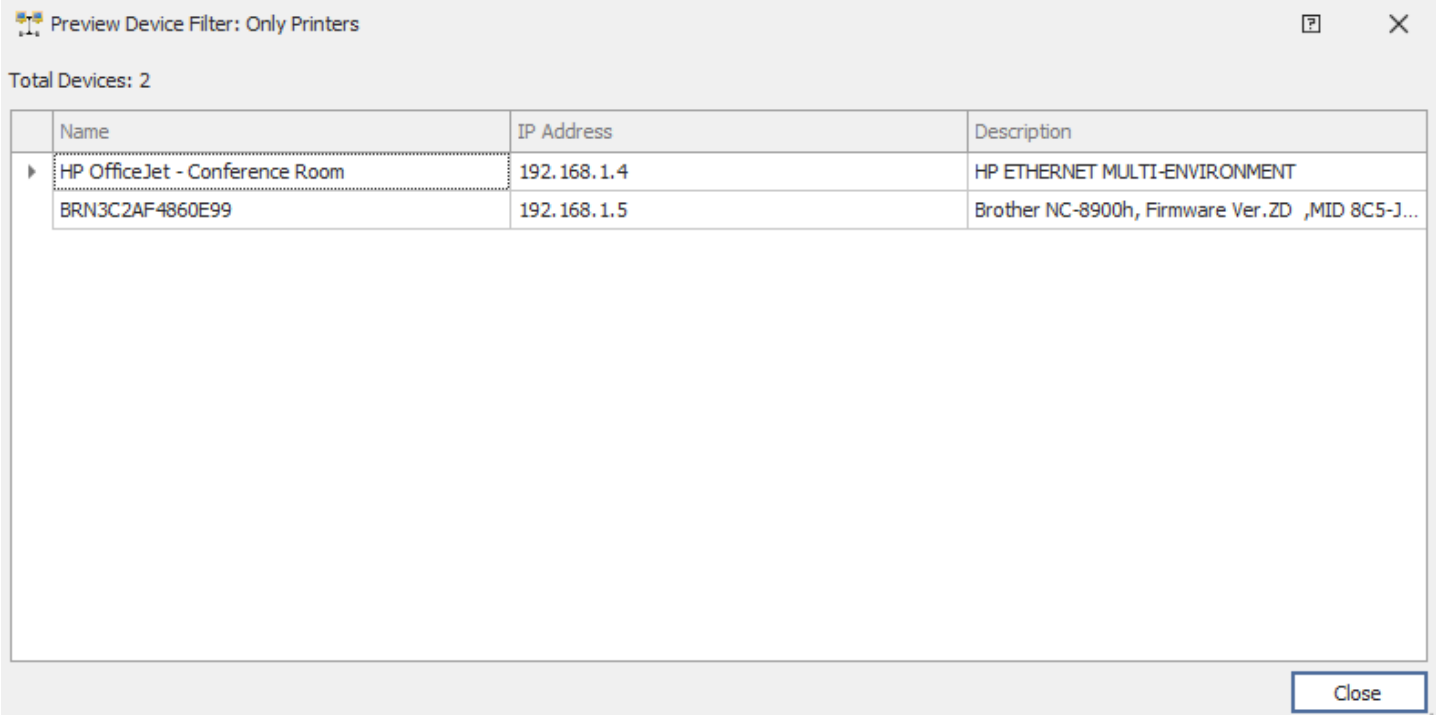
The Device Filter Selection form displays a list of all device filters that exist in the system, including both built-in and user-defined (i.e., custom) filters. The following properties are displayed for each device filter:

- Device Filter Name – the filter's name
- Date Modified – the date and time at which the filter was last modified
- Date Created – the date and time at which the filter was originally created

To select a device filter, first click on the desired filter in the list, and then click the Open button. Alternatively, you can just double-click on the desired filter.

Device Preview Form

The Device Preview form lets you view the devices that match a custom device filter you have created. This applies when you create or modify a custom device filter, or configure the settings on a dynamic device group. After modifying the settings on a filter, you can click the 'Preview' button to see which devices match the filter. The matching devices are displayed in the Device Preview form, which simply lists all of the matching devices, and displays the total number of matching devices at the top. For each matching device it displays the device's name, IP address, and description.



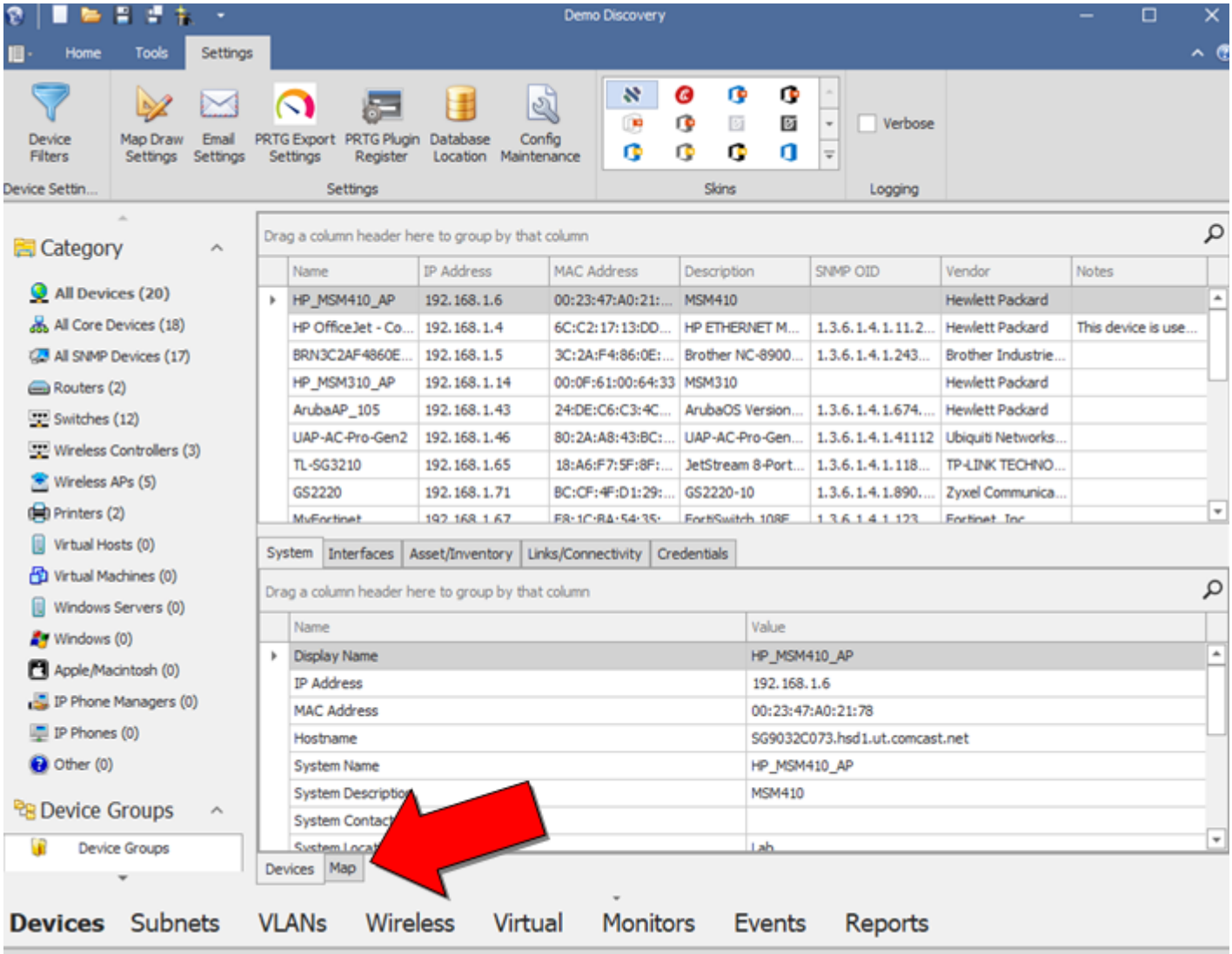
Network Topology Maps

Network topology maps provide a map view of the discovered network. Device groups and categories allow you to segment your network into logical groups. Each group and category have a topology map that gives you a map view of the group. The topology map provides a great way to visualize your network and the connections between your devices. Topology maps can be exported to Lucidchart, Visio, PDF, and SVG. The map also provides a way to interact with your devices, including easy access to UVexplorer tools and operations.

The topology map contains a node representing each device in the device group. Each node is positioned on the map either automatically using various layout algorithms or manually by moving the node to its location. The device connection links are displayed on the map as lines connecting the nodes.

In addition to the nodes and connectivity, the topology map provides a way to display custom images behind the topology.

To view the map, select a Device Group or Category and select the 'Map' tab at the bottom of the information pane.



Map Layers

Topology maps contain both a topology layer and a background image layer. To change layers, use the layer icons in the lower right corner of the map. The menus and interaction options change depending on which map layer is selected. When the topology layer is selected, you are interacting with the devices and links on the map. When the image layer is selected, you are interacting with the maps background images.

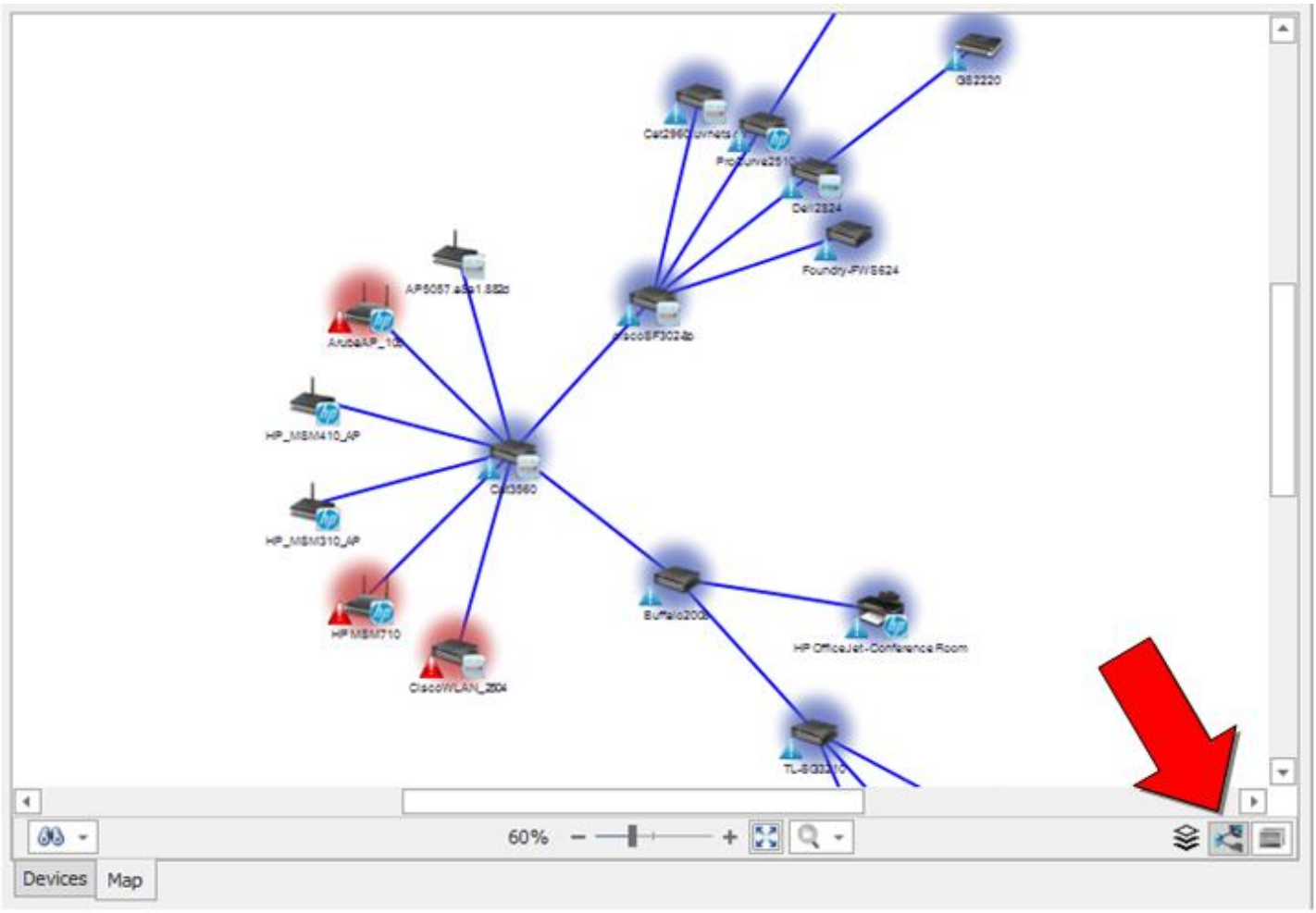
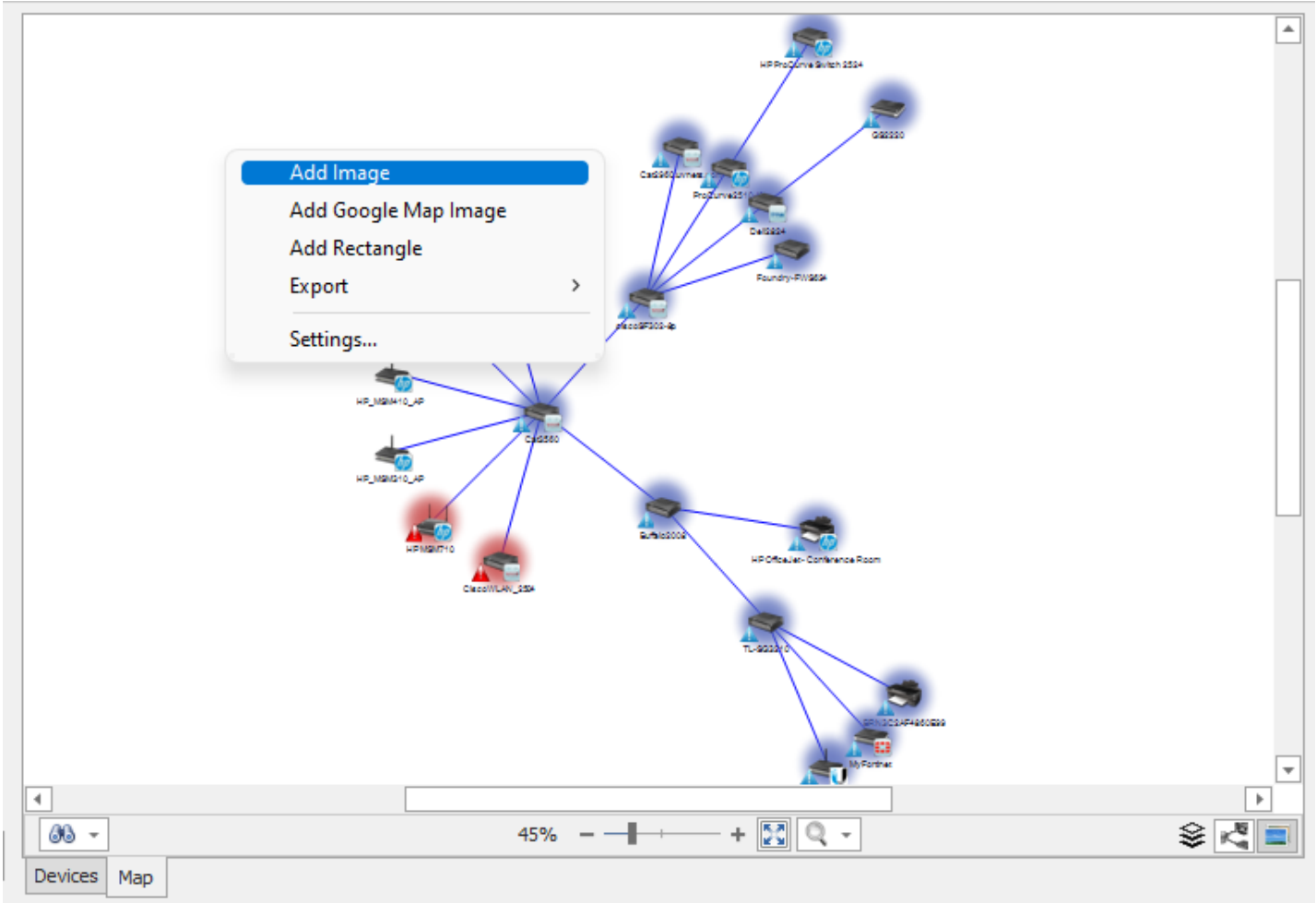


Image Layer

The image layer allows you to add background images to the map. Background images can be placed, dragged, and sized on the map. When multiple background images are on the map, they can be ordered as well.

Adding Images

To place an image on the map, right click on the map or an image and use the context menu's 'Add' option. An image chooser will be presented. When an image is selected the image will be placed on the map at the mouse location used to open the context menu.



Removing Images
To remove an image select it and press the delete key or use the context menu 'Remove' item.

Dragging Images
To drag an image simply click on it and drag it to the new location.

Sizing Images
To size an image, click on it and the node size handles will be shown. Then select the handle in the corner you want to size and drag the handle to the new size.

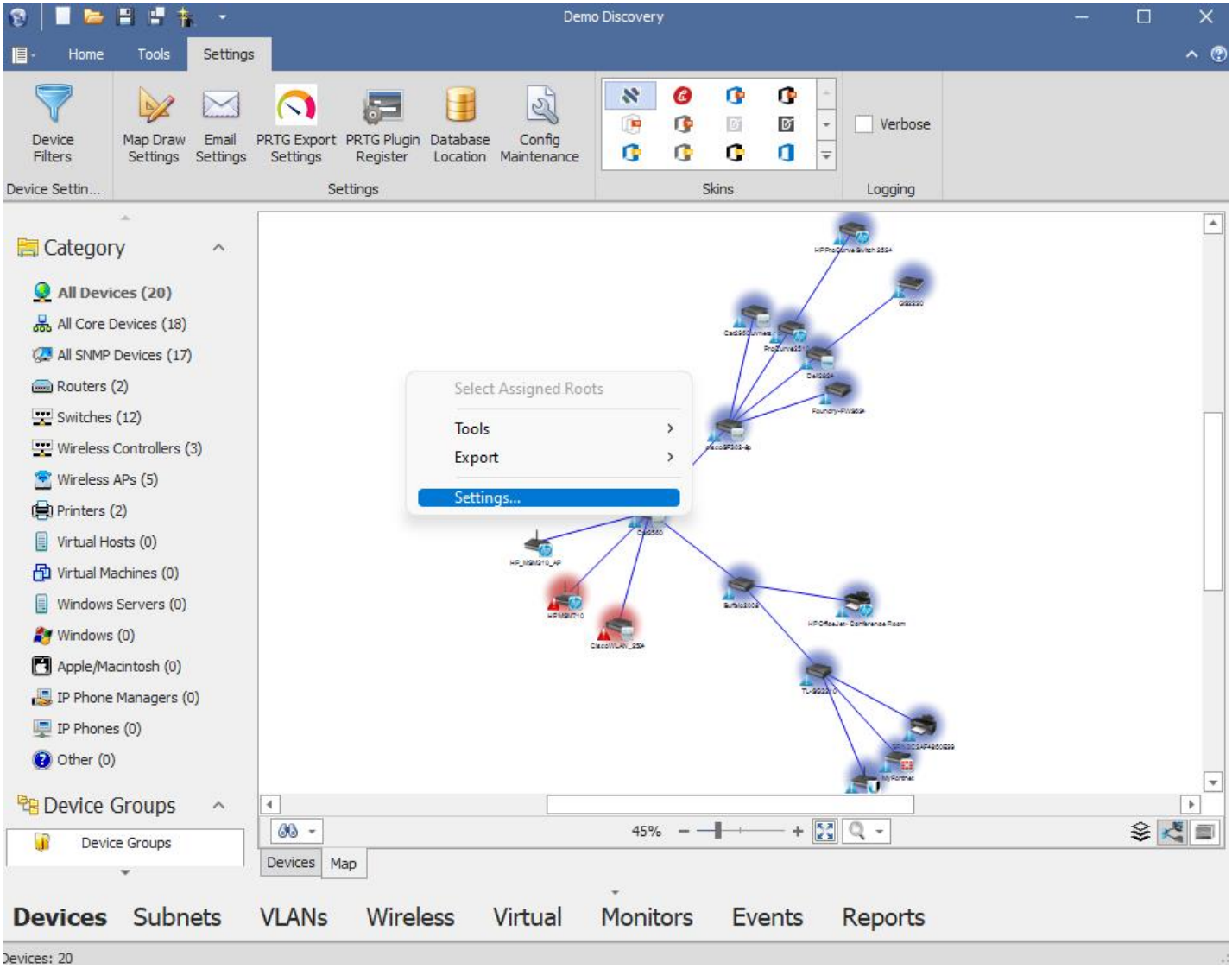
Ordering Images
Images on the image layer can be ordered. To order images use the images context menu and use the send forward or back options. If multiple images overlap, you can use the Send To Back or Bring To Front options to bring the image all the way to the front or send it all the way to the back.

Topology Layer

When the Topology layer is selected, you are working with the devices in the topology map. The operations available in the topology layer are outlined below.

Map Settings

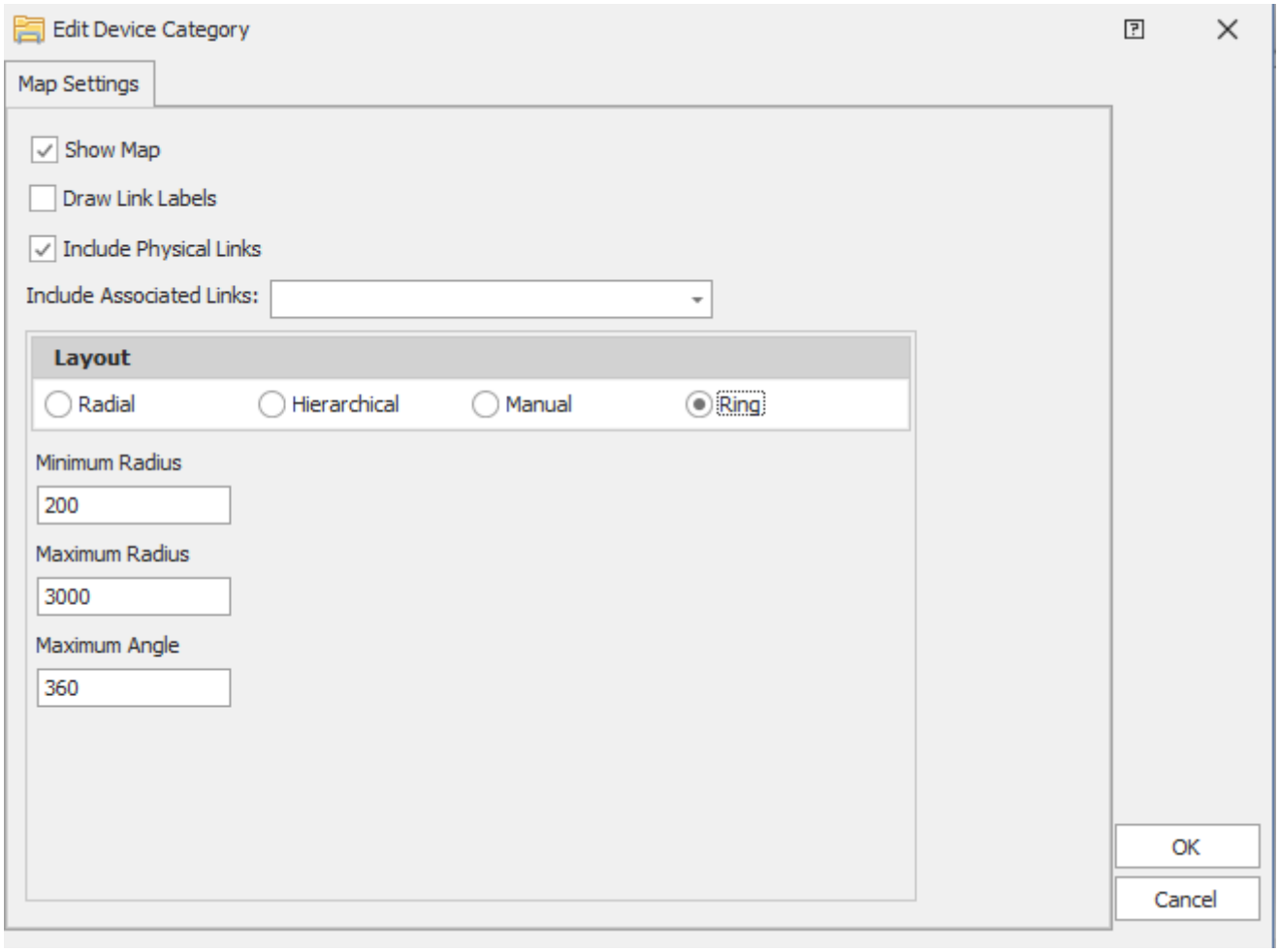
Map settings are part of the device groups or category settings. The settings can be accessed by selecting the 'Settings...' menu item from the map's context menu, or other places where the group or category settings are available.



The map settings provide an option of whether to display the map. For larger groups the topology map may not be useful and drawing the map can slow the time required to load and work with the groups. If you have a large group that makes the application slow to respond, and you don't need the map for that group, disabling drawing the map could speed up the application.

Map Layout

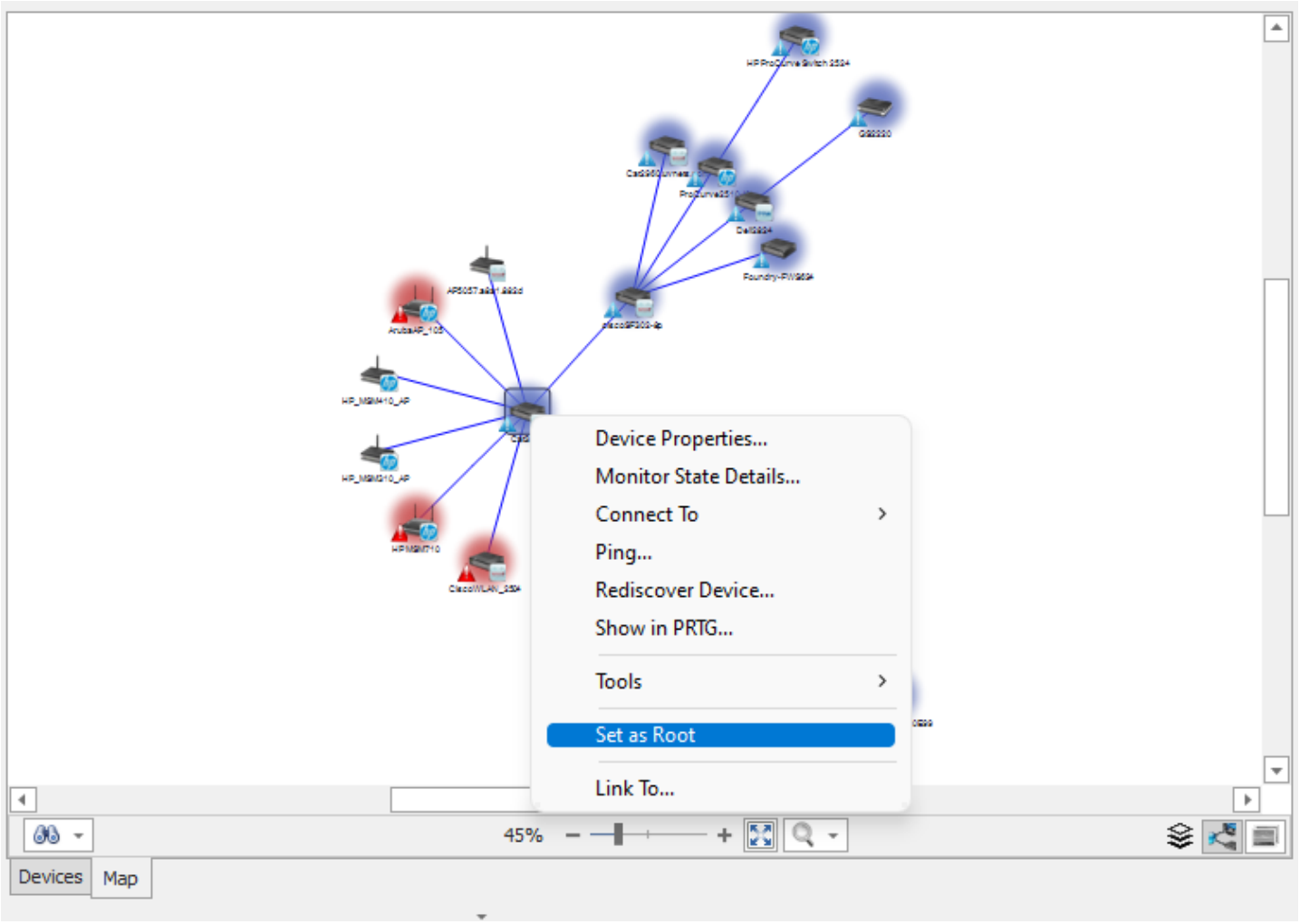
Topology maps can be laid out automatically using layout algorithms or manually. When maps are laid out automatically, the layout of each cluster of connected devices is placed on the map from left to right until all the clusters are placed. Any unconnected devices are laid out in a grid above the clusters.



Selecting Roots

When automatic layouts are used, the clusters of connected devices require a root before the layout algorithm can begin. A topology map can have a root for each cluster of connected devices. The root can be selected automatically by calculating the paths between the devices and choosing the device in the middle of the paths. This approach creates the smallest cluster.

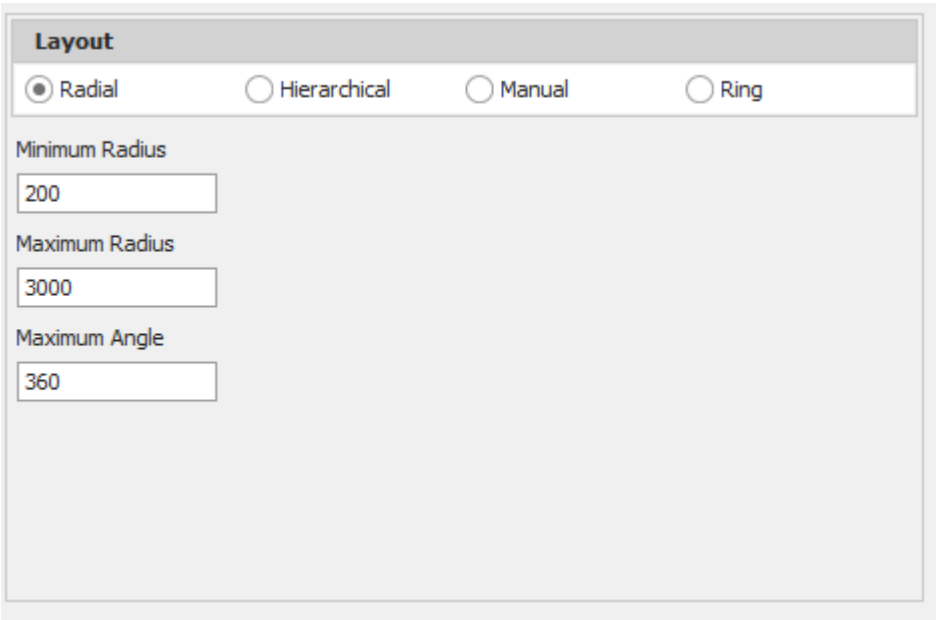
The root can also be specified manually by selecting the 'Set as Root' menu item on the node context menu item. To find manually selected roots on the map, use the maps 'Select assigned roots' context menu item. To return a cluster to using an automatically selected root, use the node 'Auto-Select Root' context menu item.



Radial Layout

The Radial Layout algorithm is applied to each cluster of connected devices on the map. The algorithm starts with the root and lays out each child node in a wheel spanning out from the root. Each layer of connected child devices is laid out recursively from there in a similar manner with the device nearest the root behaving as a root.

When using radial layout, the following settings are available:



Minimum Radius
Minimum radius is the minimum length in pixels between a node and its children. Child nodes won't be placed closer to the parent than the minimum radius

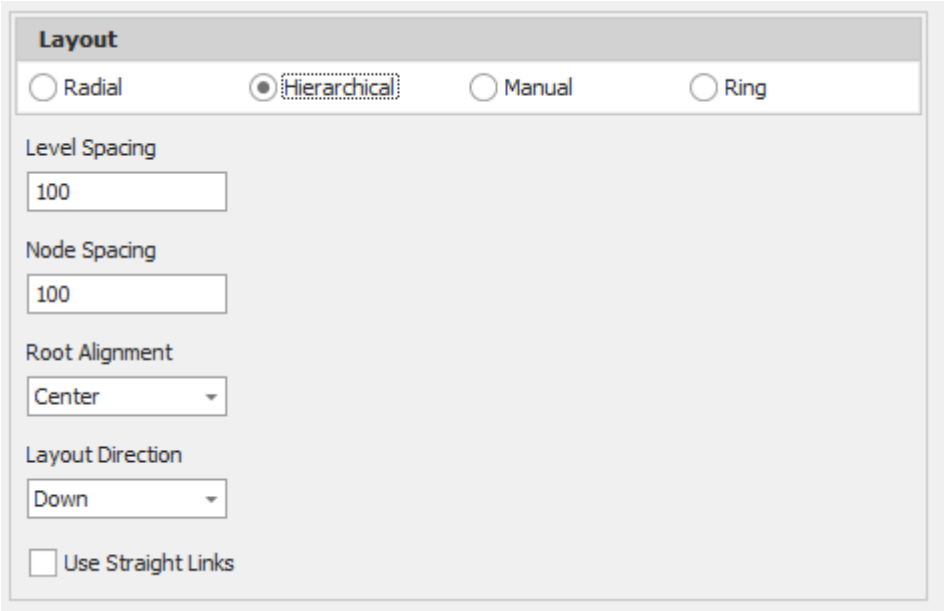
Maximum Radius
Maximum radius is the maximum length in pixels between a node and its children. When the nodes are laid out, they must stay within an angle. If the nodes won't fit within the angle at the radius distance, then the distance is expanded util the nodes will fit. If the maximum radius is reached before the nodes fit within the angle, then the layout will attempt to lay the nodes out in layers from the parent to reduce the needed angle. If the nodes can't be layered in a way that honors the maximum radius, the radius will be extended until the nodes fit the angle.

Maximum Angle
When child nodes are laid out from a parent, they are laid out within an available angle depending on neighboring nodes. The Maximum angle setting will artificially restrict the available layout angle to the specified value. The maximum angle value does not apply to the root node, it will be laid out in a full circle regardless.

Hierarchical Layout

The Hierarchical Layout algorithm is applied to each cluster of connected devices on the map. The algorithm starts at the root and lays out each child node in a straight layer extended away from it. Each layer of connected child devices is laid out recursively from there in a similar manner with the device nearest the root behaving as a root.

When using hierarchical layout, the following settings are available:



Level Spacing
Level spacing is the distance in pixels between a node and it children laid out in the level below it.

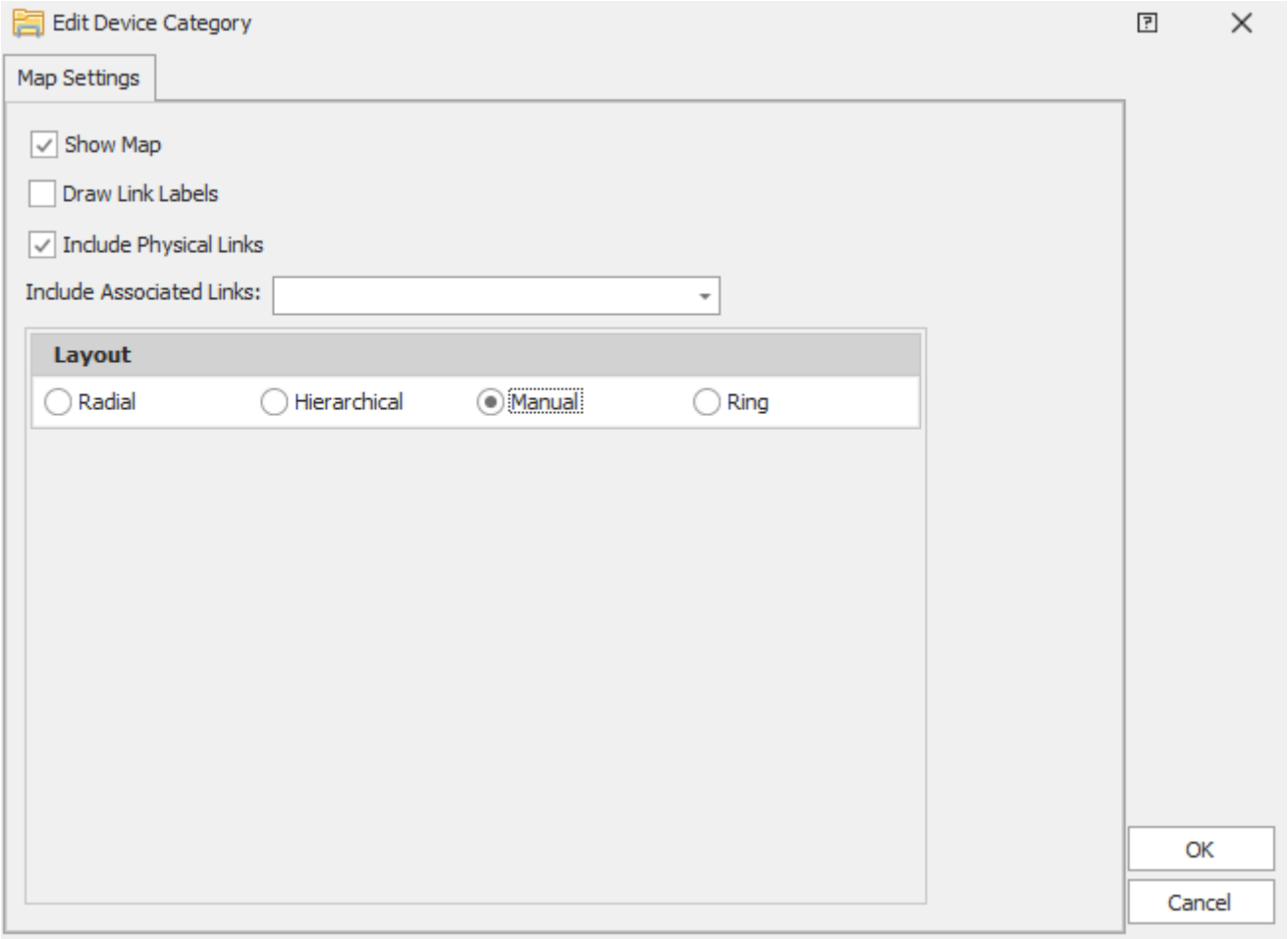
Node Spacing
Node spacing is the distance in pixels between neighbor nodes on the same level.

Root Alignment
When child nodes are placed on a level below a node, the node can be aligned centered above the nodes, or to the right or left of the nodes.

Layout Direction
When a node's children are placed, they can be placed either above(up), below(down), or left or right of the node. When placed to the left or right of a node, the level orientation changes from horizontal to vertical.

Manual Layout

When topology maps are laid out manually, nodes can be moved and placed as needed. When manual maps begin, all nodes are placed in a grid with no order. To manually place a node simply click and drag the node to its new location. Multiple nodes can be dragged at the same time by multi-selecting the nodes and dragging one of the selected nodes.



Automatic layouts can be used in conjunction with manual layouts. A great way to start a manual map is with an automatic layout. To accomplish this, start with an automatic layout and change the layout to manual. When this is done, the current position of the devices will be retained.

NOTE: Changing a map from manual layout to automatic layout will lose the manual positions of all devices on the map.

As new devices are added to the group or large changes are needed, you can layout the children of a device by selecting the 'Layout Children' menu item on the device node context menu. The 'Layout Children' dialog allows you to specify the layout settings. Once the settings are selected the algorithm will lay out all the children of the node as an independent cluster. The cluster will then be placed on the map oriented from the initiating node with no consideration to any other devices not in the newly laid out cluster.

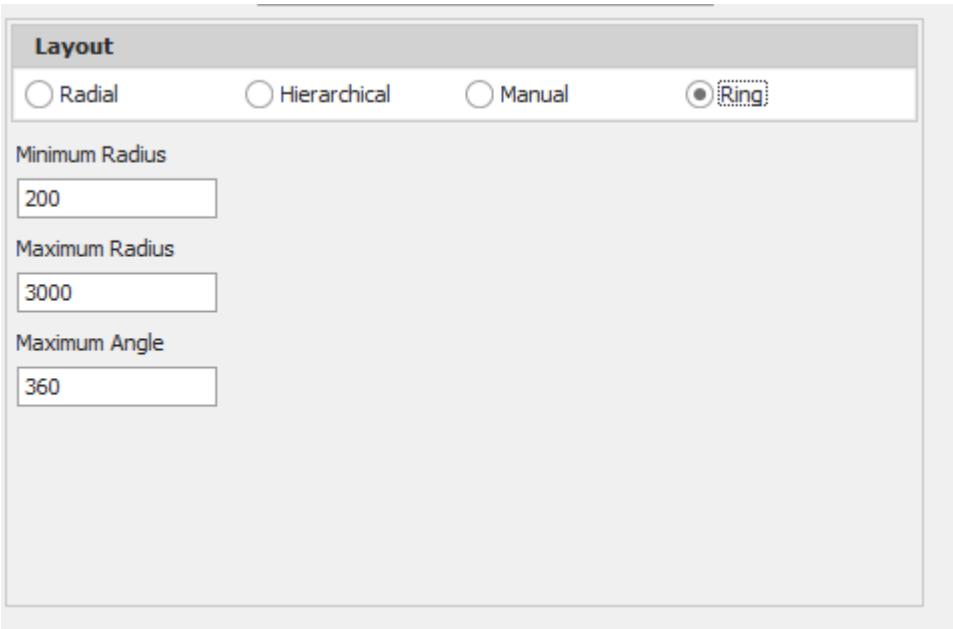
A final way to take advantage of automatic layouts in manual maps is to select the 'Layout Map...' option in the map context menu. The layout map option will allow you to select the automatic map

layout settings and layout all the nodes on the map with those settings as if it were an automatic map.

Ring Layout

The Ring Layout algorithm is applied to each cluster of connected devices on the map. The algorithm starts with the root and lays out each child node in a ring spanning out from the root. Each layer of connected child devices is laid out recursively from there in a similar manner with the device nearest the root behaving as a root.

When using ring layout, the following settings are available:



Minimum Radius
Minimum radius is the minimum length in pixels between a node and its children. Child nodes won't be placed closer to the parent than the minimum radius

Maximum Radius
Maximum radius is the maximum length in pixels between a node and its children. When the nodes are laid out, they must stay within an angle. If the nodes won't fit within the angle at the radius distance, then the distance is expanded util the nodes will fit. If the maximum radius is reached before the nodes fit within the angle, then the layout will attempt to lay the nodes out in layers from the parent to reduce the needed angle. If the nodes can't be layered in a way that honors the maximum radius, the radius will be extended until the nodes fit the angle.

Maximum Angle
When child nodes are laid out from a parent, they are laid out within an available angle depending on neighboring nodes. The Maximum angle setting will artificially restrict the available layout angle to the specified value. The maximum angle value does not apply to the root node, it will be laid out in a full circle regardless.

Topology Nodes

Topology nodes represent devices in the group and certain device links. The image representing the node is selected depending on the type of device such as switch, server, wireless access point etc. In addition to displaying the device type, an image for the vendor will also be included when

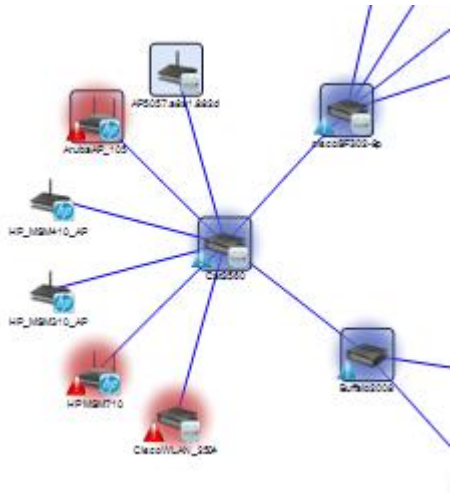
the vendor is known, and an image is available.

Device multi links and wireless links are also represented as nodes on the map. Each has an image and can be interacted with like devices. (A multi-link is a link with more than two participating devices.)

Selecting Devices

The topology map allows you to select a single device or multiple devices. To select a single device, simply click on the device. Selecting multiple devices can be done as follows

- Select multiple individual devices by holding down Ctrl while clicking on the devices. Any previously selected devices will remain selected when a new device is clicked while holding down Ctrl.
- Select all devices on the map by pressing Ctrl-A.
- Select all descendants of a device node by holding Shift-Ctrl while clicking on the device
- Select all devices within a selection rectangle. While holding down Ctrl, click and drag the mouse to draw a rectangle around the devices you want to select. All devices within the rectangle will be selected.



To unselect a selected device, click away from it on the map. To unselect a device when multiple devices are selected click on the device while holding the Ctrl button.

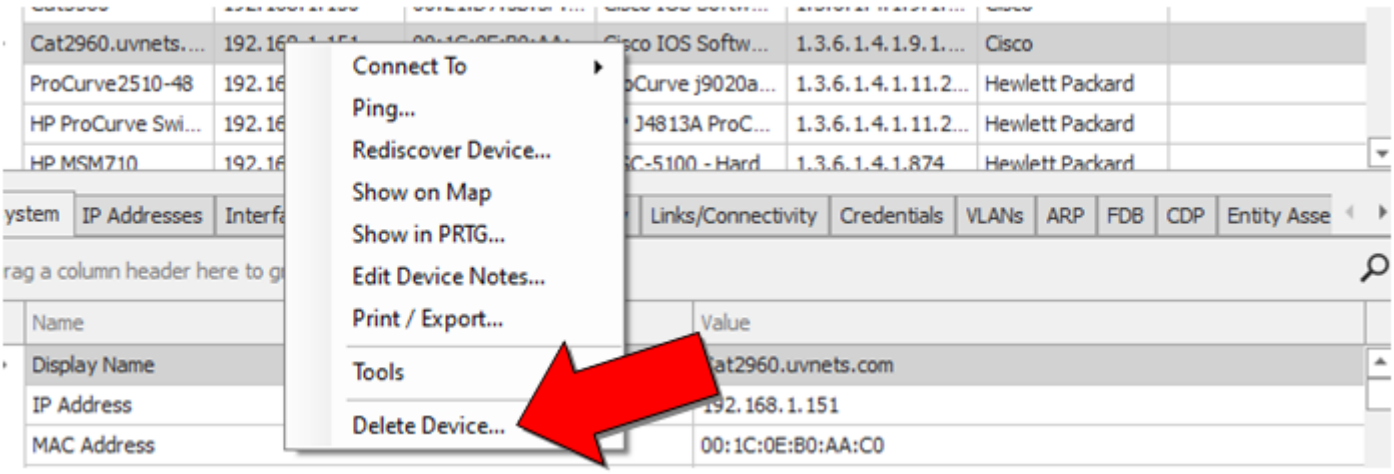
Dragging Devices

To drag an individual device, press and hold the Left mouse button and drag the device to a new location. To drag multiple devices, select the devices and press and drag any of the selected devices. All selected devices will be dragged.

Removing Devices

The devices presented on a map are determined based on the device membership of the group. They can be changed by changing the group membership settings. On static membership maps, there are several ways that you can remove devices from a map. Maps with dynamic membership do not support the below mentioned features. Removing the devices from the map will remove the devices from the group. A confirmation dialog will be presented for any remove operations.

Note: Removing devices from the map will not remove them from the discovery results. To permanently delete a device from the discovery result, use the device list view.



Note: Removing a Link Node will remove the link and all attached descendant device nodes as well.

The following options are available for removing devices from a static membership map:

Delete Key
To delete devices with the delete key, select the devices and press the delete key.

Remove Selected
The context menu on any device provides the 'Remove Selected' option. When selected, all currently selected devices will be removed.

Remove Devices
The topology map provides a context menu option 'Remove Devices'. The 'Remove Devices' context menu allows you to remove devices by selecting them from a device picker containing all devices currently on the map.

Remove Connected
The context menu on device and link nodes provides the ability to remove connected descendant devices of a certain type. The menu items will display counts of how many devices of each type are currently connected to the device. When selected, all connected descendant devices of that type will be removed from the map. The remove connected 'Select' option will display a device picker containing all the connected descendant devices.

You can also remove all connected devices by category type from the map using the map context menu.

Remove Associated
The context menu on device and link nodes provides the ability to remove associated descendant devices of a certain type. The menu items will display counts of how many devices of each type are currently associated with the device. When selected, all associated descendant devices of that type will be removed from the map. The remove associated 'Select' option will display a device picker containing all the associated descendant devices.

Associated devices are devices that have a relationship to the device without having an actual physical connection, such as Wireless Access Points and Virtual Hosts.

You can also remove all associated devices by category type from the map using the map context

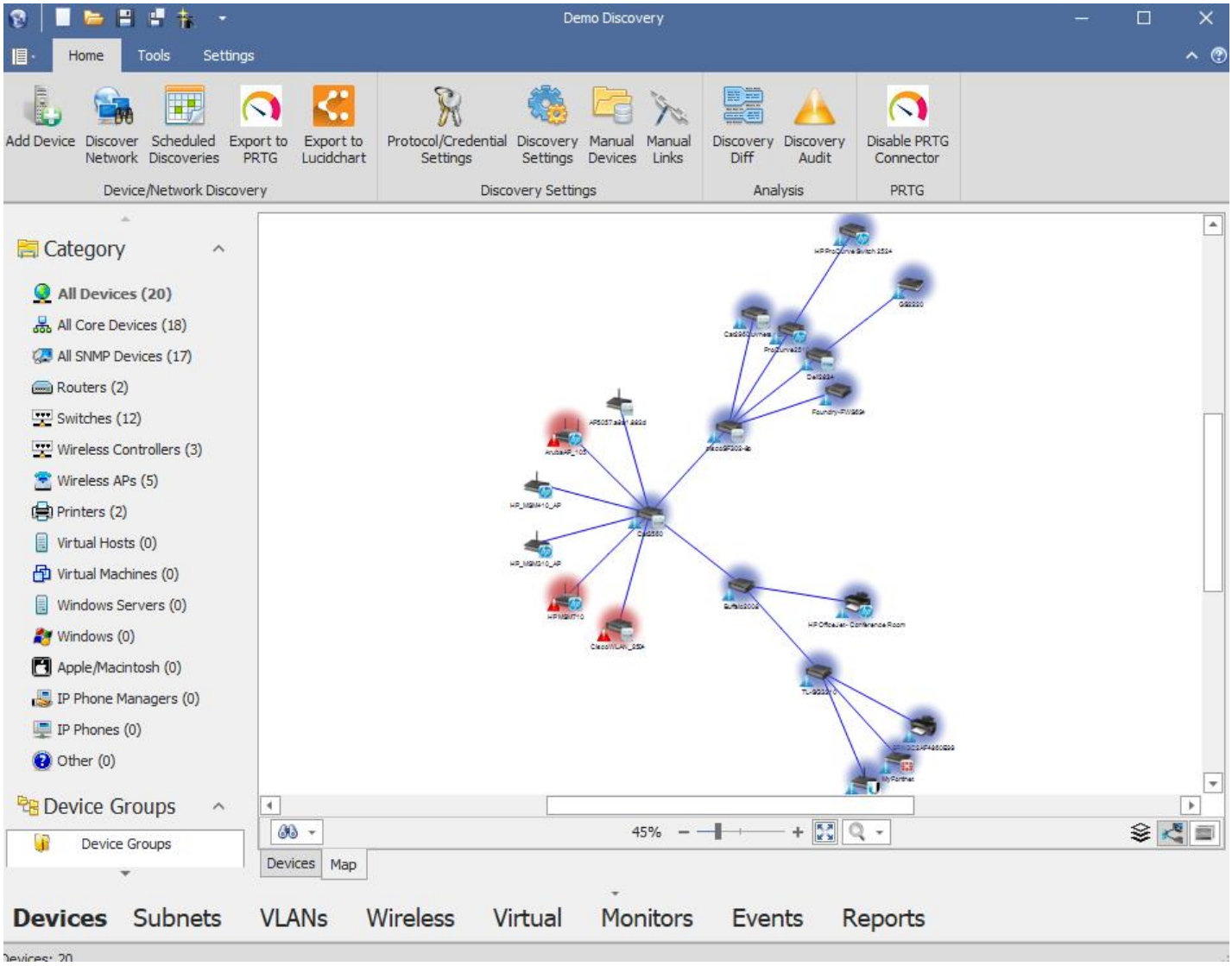
menu.

Changing Group Membership
The nodes on a map will also change as the group membership is changed based on the group membership settings.

Adding Devices

The devices presented on a map are determined based on the device membership of the group. They can be changed by changing the group membership settings. On static membership maps the devices can also be added in various ways while interacting with the map. Maps with dynamic membership do not support the below mentioned features. Adding the devices to the map will also add the devices to the group.

Note: Only devices that have been discovered and are part of the currently open discovery result can be added to the map using these methods. To Add/Discover a new device, use the 'Add Device' option in the main view's home menu.



Add Devices
The topology map provides a context menu option named 'Add Devices'. The 'Add Devices' context menu option allows you to add devices by selecting them from a device picker containing all devices not currently on the map.

Add Connected

The context menu on device and link nodes provides the ability to add connected devices of a certain type. The menu items will display counts of how many devices of each type are currently connected to the device and currently on the map. When selected, all connected devices of that type will be added to the map. The Add Connected 'Select' option will display a device picker containing all of the connected devices not currently on the map.

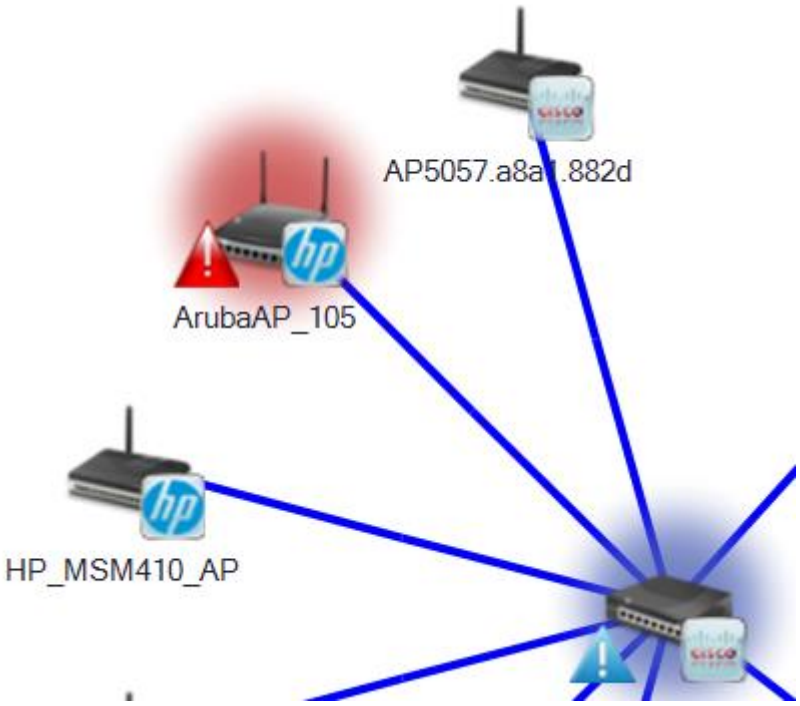
You can also add all connected devices by category type to the map using the map context menu.

Add Associated
The context menu on device and link nodes provides the ability to add associated devices of a certain type. The menu items will display counts of how many devices of each type are currently associated with the device and currently on the map. When selected, all associated devices of that type will be added to the map. The Add Associated 'Select' option will display a device picker containing all of the associated devices not currently on the map.

Associated devices are devices that have a relationship to the device without having an actual physical connection, such as Wireless Access Points and Virtual Hosts.

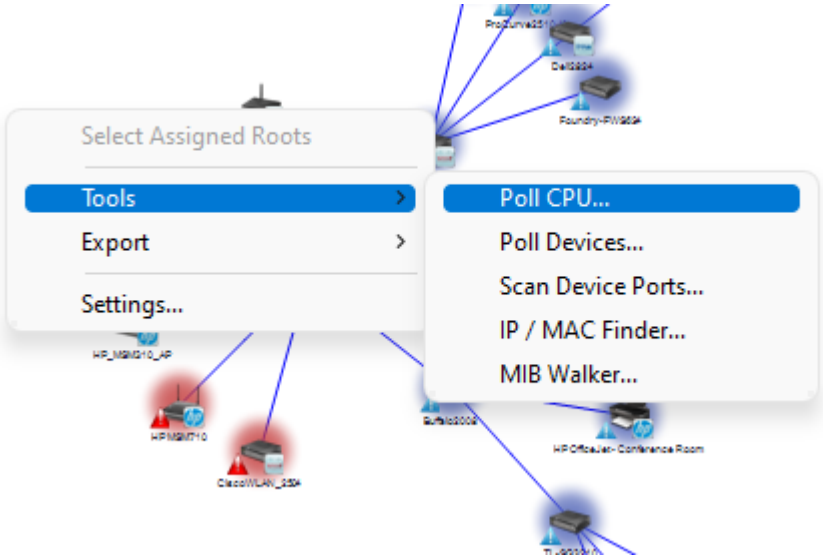
You can also add all associated devices by category type to the map using the map context menu.

Device State
If devices are monitored, they will have a monitoring state associated with them. The state of these devices will be displayed on the map as a color-coded icon. Device state will be updated automatically on the map as the state of the device changes when monitors complete.

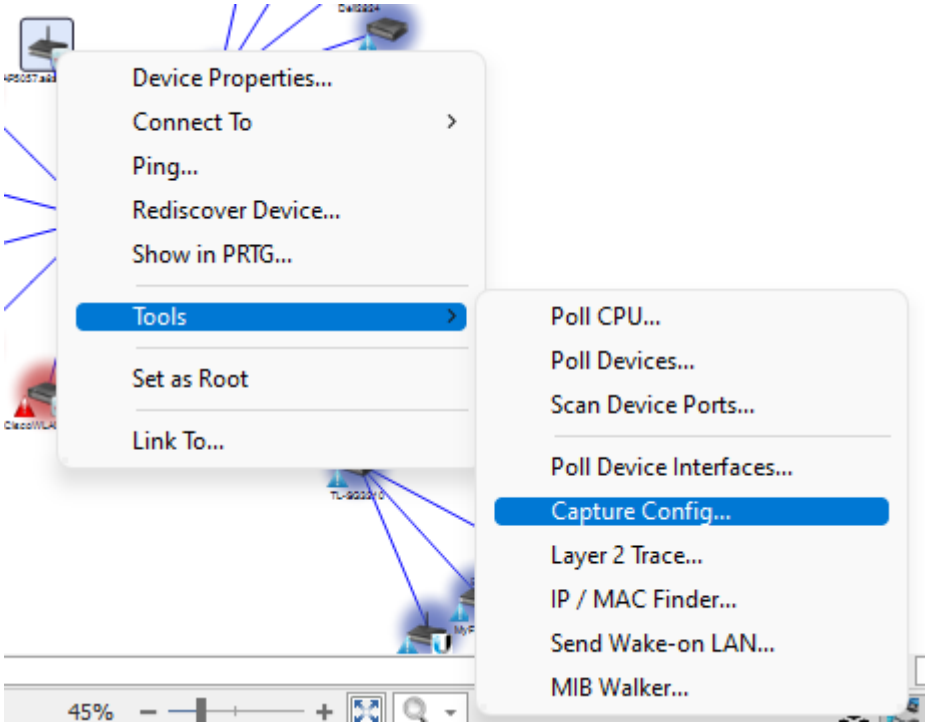


Network Tools

Tools
The map allows access to several of the network tools. This provides an intuitive way of selecting devices and performing common operations on them. The tools will either interact with all the devices on the map, or just the selected ones. You can access the map tools options from either the map or device context menu's 'Tools' option.

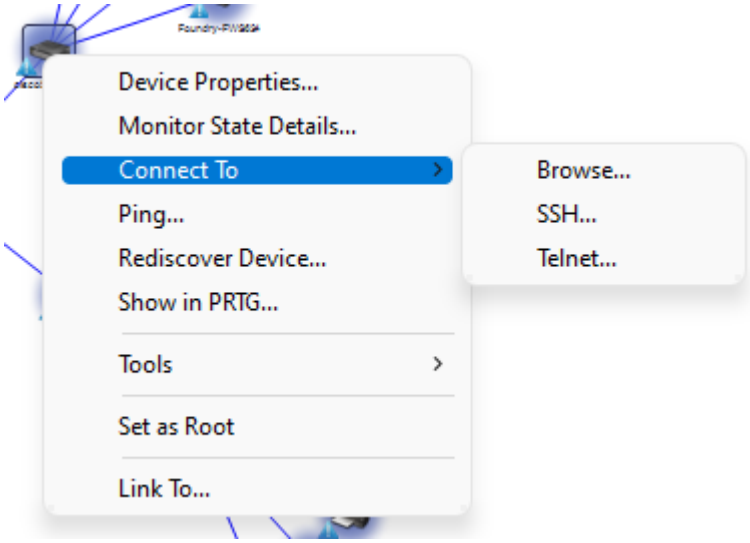


- The Poll CPU, Poll Devices, and Scan Device Ports tools will operate on all devices on the map. These tools will open pre-populated with all the devices in the group.
- The Poll Device Interfaces, Capture Config, Layer 2 Trace and Send Wake On LAN tools will display when a single device is selected. Right click the device and go to "Tools".



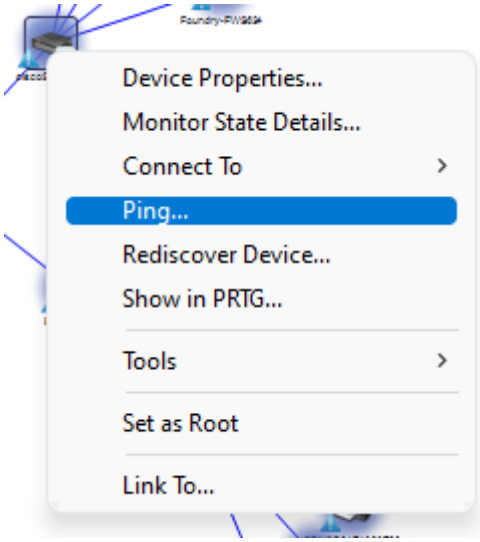
Connect To

The device context menu allows you to connect to a device using SSH, Telnet, or a Web Browser. Each of these options will open either the browser or a Putty connection to the device and will be ready for you to authenticate with the device when necessary.



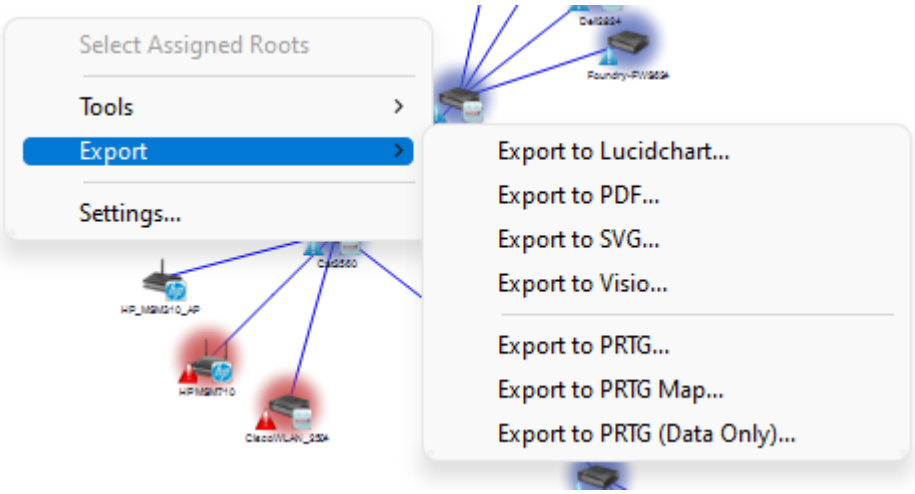
Ping

You can send a simple ping request to a device using the device context menu 'Ping' option. This will send a ping request to the device's primary IP Address. The results of the request will be displayed in a Windows command prompt.



Export

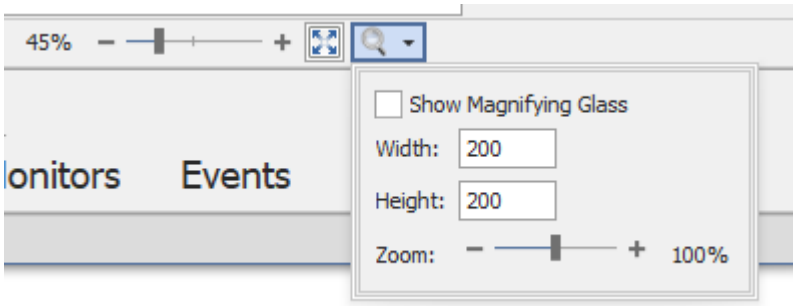
Each map can be exported to either Lucidchart, Visio, PDF, or SVG. To export a map, right click the map go to 'Export'. Dialogs with the applicable export settings will be presented to be configured before the export can be completed.



See Exporting Topology Maps for more information.

Zooming

Topology maps support zooming between close to 0% up to 200%. Several options for zooming are available.



Zoom Track Bar

A zoom track bar is available below the map. This supports zooming by either sliding the track bar or pressing the + and - buttons. You can also select a zoom value on the track bar by clicking on the track bar.

Zoom to Point

You can zoom relative to a particular point on the map by placing the mouse at the desired location, pressing, and holding the Ctrl key, and rolling mouse wheel or equivalent in and out.

Fit and Center

You can zoom the map to the best scale level to fit the map by pressing the Fit and Center button located to the right of the zoom track bar. This will zoom the map to the best scale value to fit the map as well as centering the map in the window.

Zoom Magnifying Glass

The zoom magnifying glass when enabled will display a zoom pane near the mouse containing the contents of the map at the mouse point, scaled to the specified zoom value. The zoom magnifying glass is located to the right of the zoom track bar and contains a drop down with the magnifying glasses zoom settings. The drop down contains the following settings.

Show Magnifying Glass

A checkbox indicating whether to display the zoom magnifying glass pane. When checked the pane will display near the mouse whenever it is placed over the map.

Width and Height

The width and height values determine the size of the magnifying glass pane in pixels.

Zoom

The zoom track bar determines the zoom scale of the map magnifying glass pane. This value is separate from the map's primary zoom level.

Panning

If the map is zoomed such that the entire map does not fit in the map view, you can pan to the areas outside of the view.

Pan using scroll bars

You can pan the map using the scroll bars like scrolling documents and other items that do not fit in their view.

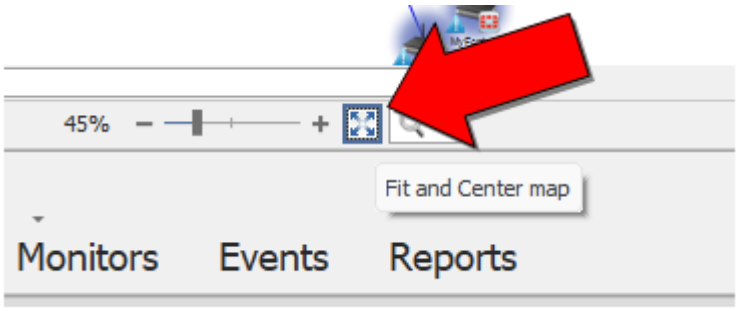
Pan by dragging

You can also drag the map to pan to a new area. To pan select a point on the map and drag the mouse. The map will pan/move as if you picked up the map and moved it in that direction. This should be like other map software you may be familiar with.

Note: Be careful not to grab a node when wanting to drag the map doing so will drag the node instead.

Fit and Center

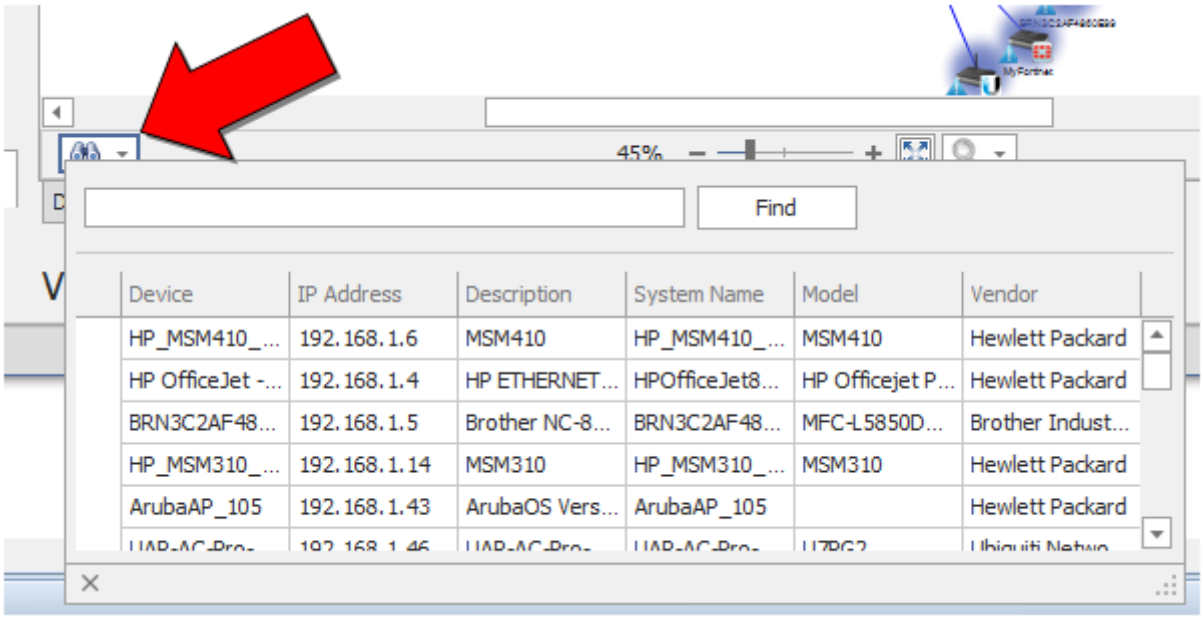
You can zoom the map to the best scale level to fit the map by pressing the Fit and Center button located to the right of the zoom track bar. This will zoom the map to the best scale value to fit the map as well as centering the map in the window.



Find on Map

You can find the location of a device on the map using the Find on Map feature. The Find on Map tool is in the lower left corner of the map. It is a drop-down pane with a binocular image. Find on Map allows you to use partial word matching based on several device values.

To open the Find on Map tool, click on the binocular drop down. All devices on the map will be displayed in a grid below a find text area. The devices can be filtered by typing a word or partial word to match on into the find text area. The search word will be matched to all columns in the device grid. Any devices with available attributes matching the find word will remain in the device list. Once you have located the device you would like to find on the map in the device list, click on the device, and the map will select that device and pan and zoom to that device's location.

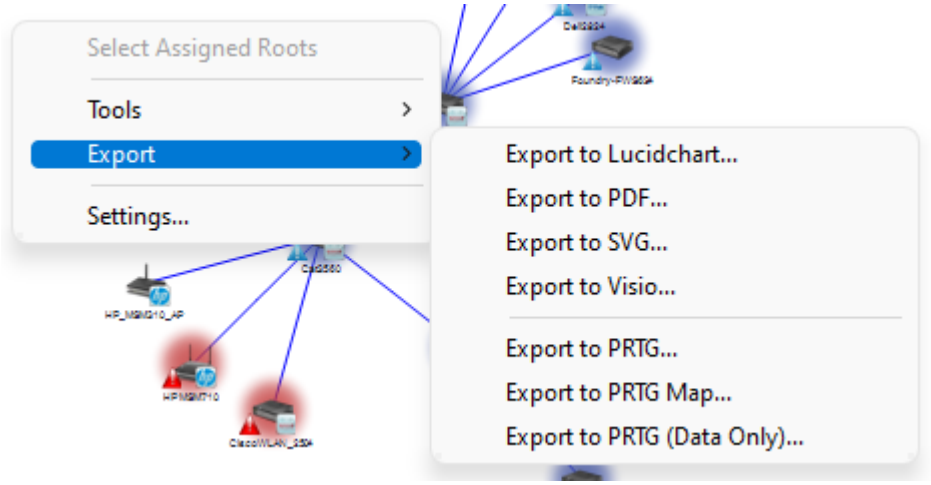


Map Draw Settings

Topology maps support application wide drawing settings that allow you to specify how links and labels are drawn on maps. See Map Draw Settings for more information.

Exporting Topology Maps

Topology maps can be exported to Lucidchart, Visio, PDF and SVG files. To export maps, open the map and select the 'Export' option on the map context menu. A dialog will be presented containing export configuration settings. Once the settings are configured you will be prompted with a dialog to choose the file name and location to save the map. After a name has been provided, a document of the specified export type will be generated and saved. If an application is available for viewing files of the given format, the file will be opened for viewing in the system's default viewer for that file type.

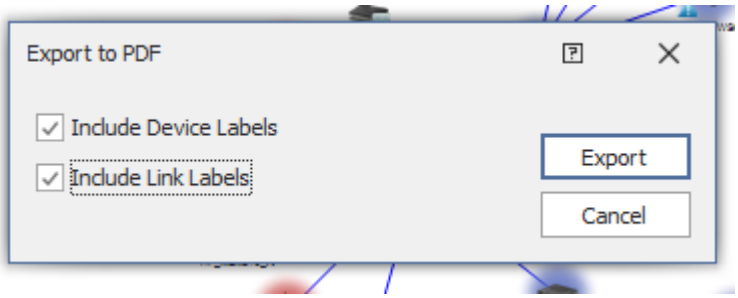


Export Settings

The following settings are available when exporting.

Include 'Device and Link Labels'

The 'Include Device and Link Labels' option determines whether to include the device and link labels in the exported maps. Occasionally the device and link labels make the map look cluttered; this setting allows you to export the map without them.



Export to Lucidchart

Lucidchart is an online diagramming solution that can be used to create and visual detailed network diagrams. UVexplorer automates the creation of these diagrams by providing functionality that will generate a Visio XML file (.vdx file) and then automatically import that document into the Lucidchart diagram editor. This document can then be saved by simply logging into your Lucidchart account. In addition to the 'Include Device and Link Labels' setting, Lucidchart documents provide the additional following settings.

Sheets Across and Down

Lucidchart documents can be generated to span multiple pages. The Sheets Across and Sheets Down settings indicate how many pages to fit the map to.

Include Device and Link Properties

Lucidchart documents support including shape properties with device shapes. When topology maps are exported to Lucidchart, you can choose to include link and device properties as shape properties on the shapes. The properties include device system information and details about devices and interfaces associated with device links.

Export to Visio

Visio documents are created as Visio XML files saved as .vdx files. The generated .vdx files should be compatible with Visio 2003, 2010 and 2013 Visio applications. In addition to the Include Device and Link Labels setting, Visio documents provide the additional following settings.

Sheets Across and Down

Visio documents can be generated to span multiple pages. The Sheets Across and Sheets Down settings indicate how many pages to fit the map to.

Include Device and Link Properties

Visio documents support including shape properties with Visio shapes. When topology maps are exported to Visio, you can choose to include link and device properties as shape properties on the shapes. The properties include device system information and details about devices and interfaces associated with device links.

Export to PDF

When topology maps are exported to PDF, they are generated as basic PDF files. The resulting PDF files will support text searching.

NOTE: Large maps that do not fit on a standard PDF page may not display correctly in some PDF viewers. Occasionally these files will display correctly when opened in a web PDF viewer such as Chrome.

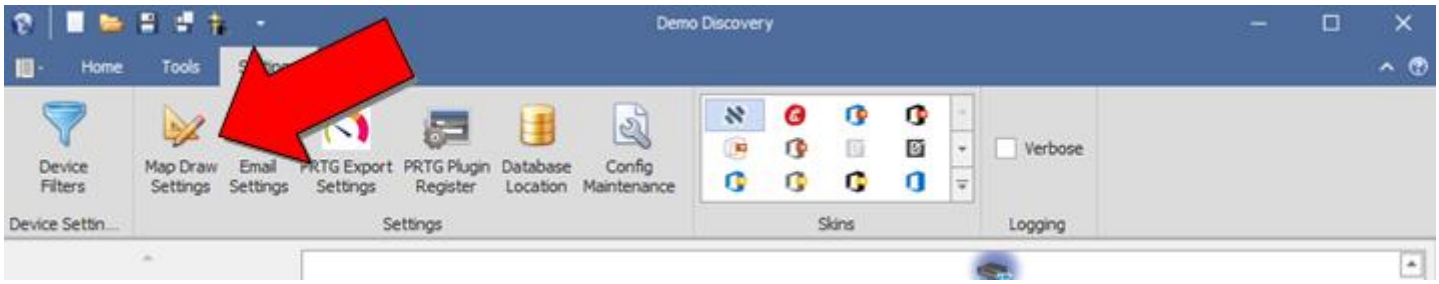
Export to SVG

SVG is a scalable vector graphics format that supports sizing images without losing quality. SVG graphics are often used in web applications. When topology maps are exported to SVG, they will generate compliant SVG files with common fonts and embedded images that should be viewable in most SVG viewers, including web browsers.

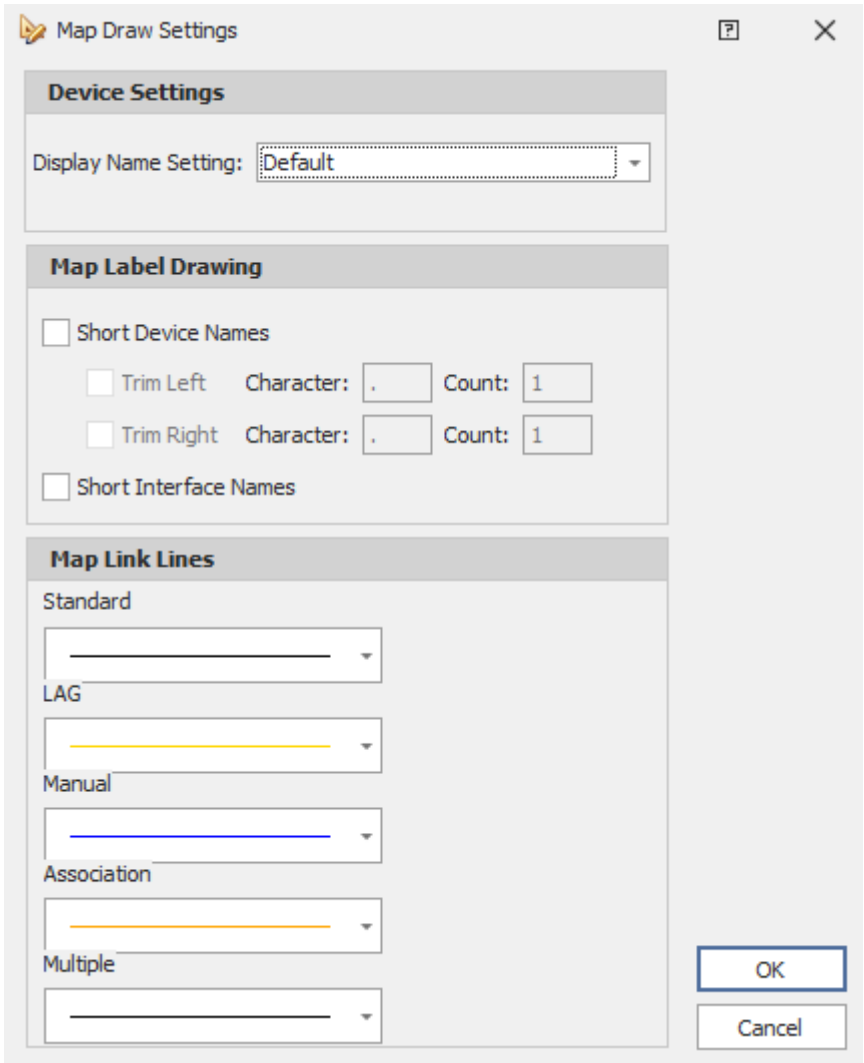
Map Draw Settings

Topology maps support drawing links with different colors and patterns. Maps can also be configured to use short device and interface names to avoid crowding on the map.

To open the map draw settings, use the 'Map Draw Settings' menu item on the 'Settings' menu tab available in the applications main view.



The following map draw settings are available:



Short Device Names

Device names can be shortened from either the right or left using a character as a pattern to match on and trim. For example, trimming the device name 'my.network.device.host.com' using the '.' character trimming 2 from the right would remove all text to the right of the first two '.' starting at the right resulting in the trimmed name 'my.network.device'. Device names can be trimmed from the right or left or both.

Short Interface Names
When short interface names are used the link labels will only use the interface name or index without the interface description.

Map Link Lines
Topology maps support displaying five link types. By default, all link types will be drawn with a simple black line. The map draw settings allow you to draw links of different types with different colors or patterns. Each link type is presented as combo box containing a preview of the line in the map draw settings editor.

Link Types
Topology maps support the following link types:

Standard
Standard link lines represent a connection between two devices on one interface per device.

LAG
LAG links represent Link Aggregation links as configured on the devices.

Manual
Manual links represent user defined links between two devices.

Association
Association links represent an association link between two devices. Associations represent a relationship between two devices that are not necessarily physically connected. Such as a wireless controller and a wireless access point.

Multiple
Multiple links represent a situation where two devices are connected on multiple interfaces without being configured as a LAG link.

Link Draw Settings
To change the way a link type is drawn open the link draw editor by pressing the link type combo box. The link settings and a preview will be presented in the editor. The following link settings are available:

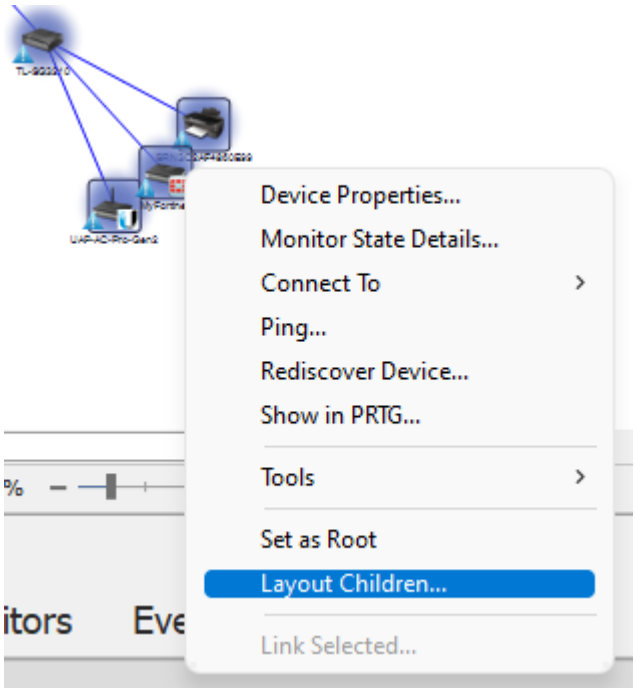
Color
The color setting determines the color used for the link line.

Weight
The weight settings determine how thick the line is.

Dash Type
The dash type setting determines the line pattern used for the link line.

Layout Map Node Children

Manual layout maps allow you to lay out all the descendants of a device using the available layout algorithms. Also, as new nodes are added to manual maps, they can be positioned on the map using layouts as well. To layout a map nodes children, use the node context menu's 'Layout Children' menu item. The dialog will also be presented when the add connected or associated devices options are used.

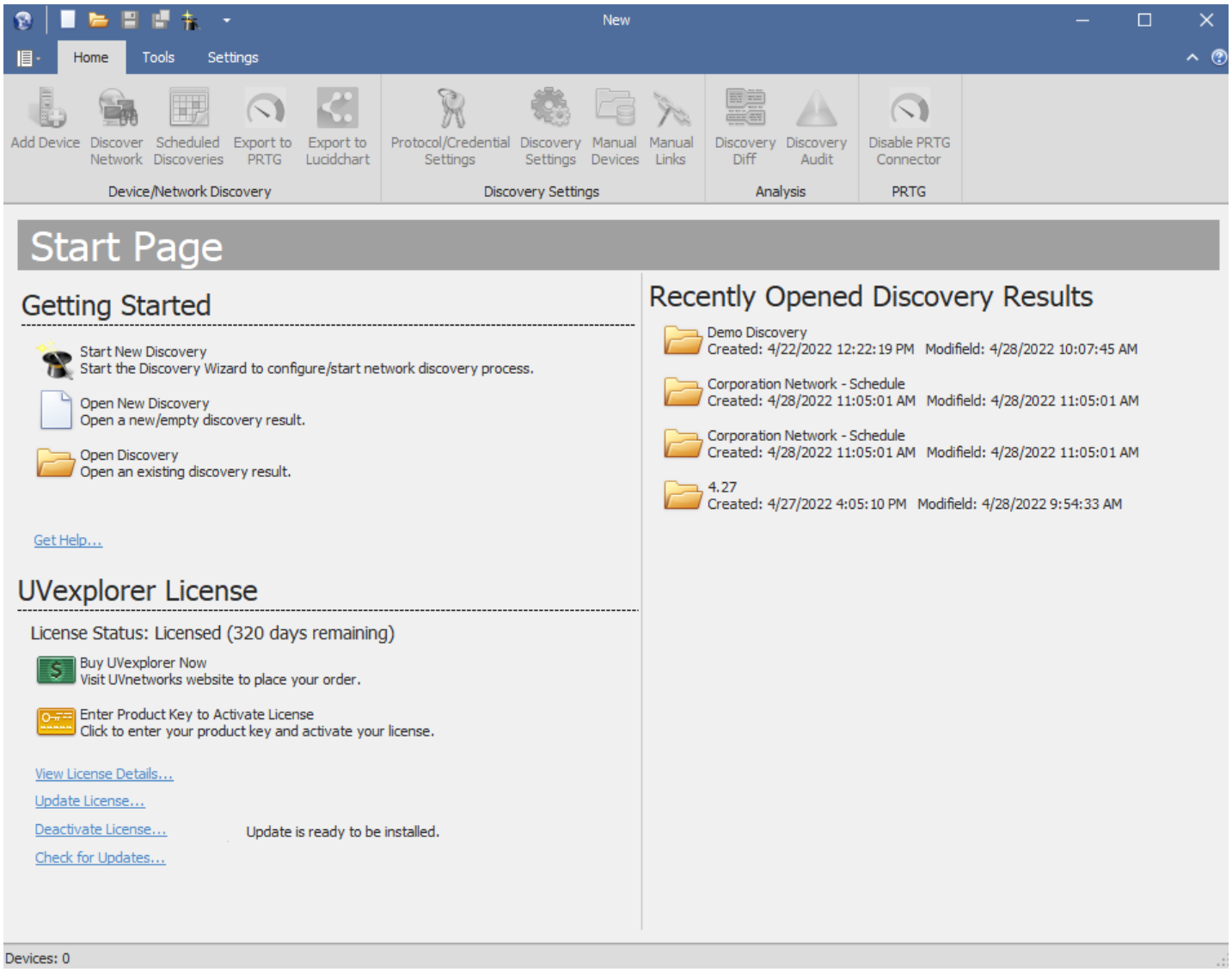


The layout map children dialog contains the same layout options available in the map's settings. See Network Topology Maps for more information.

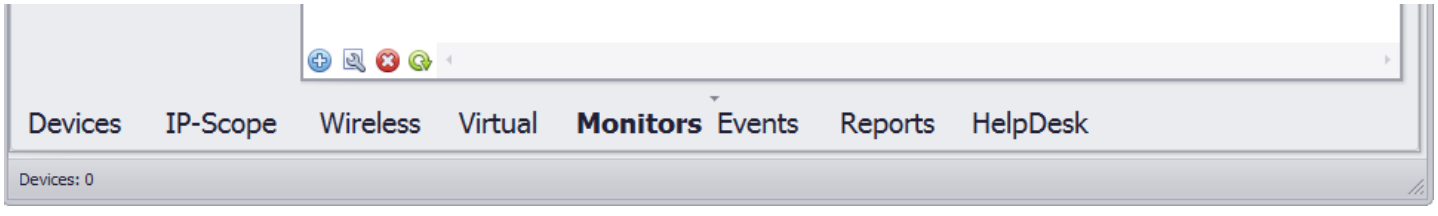
UVexplorer Views

UVexplorer provides several views for configuring the application and discovering and interacting with discovered networks.

When the application starts the Startup Page is presented. The startup page can also be accessed from the backstage view. See Startup Page for more information about the startup page.



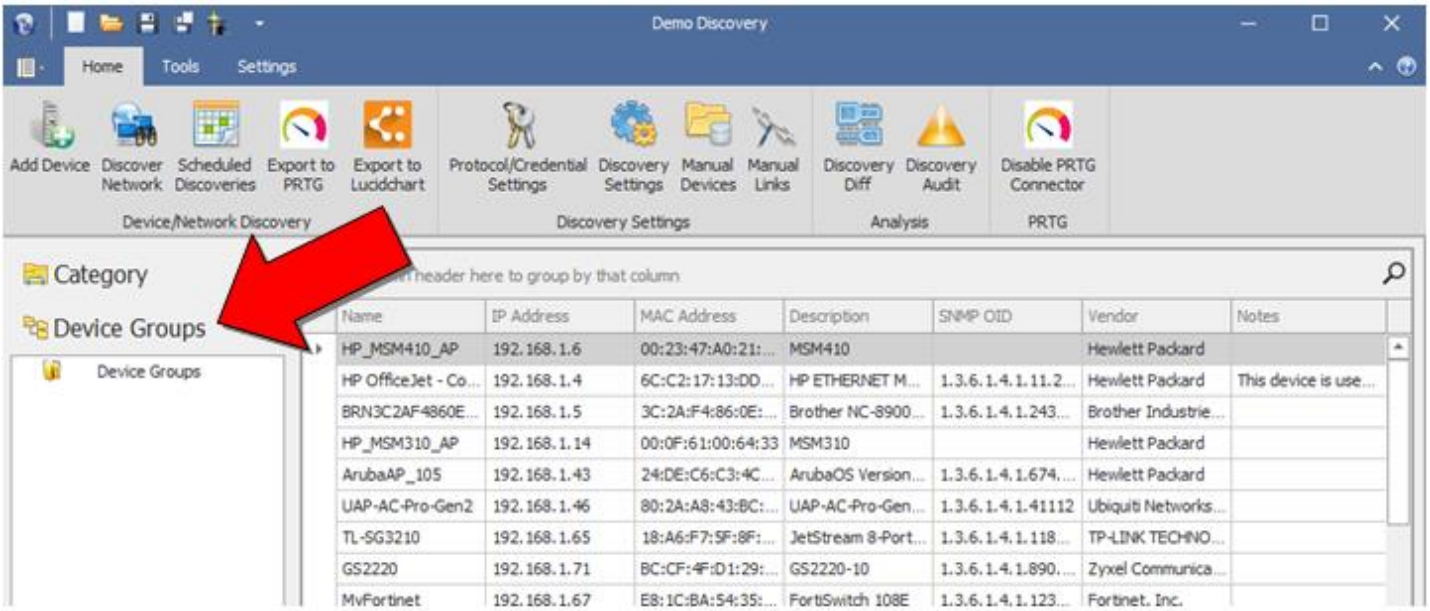
UVexplorer has several different primary views available for viewing network discovery results, events, reports, and a page for our Group Link HelpDesk tie-in. The available views can be changed by selecting the view links in the lower portion of the application. The currently selected view will display with larger bold text. The view links can be hidden by pressing the collapse button in the upper middle portion of the links. To restore the collapsed links, press the expand button.



Devices - Device Group/Category views

UVexplorer provides two primary views for viewing network discovery results: the device properties view, and the network topology map. To reduce/filter the number of devices presented in these two

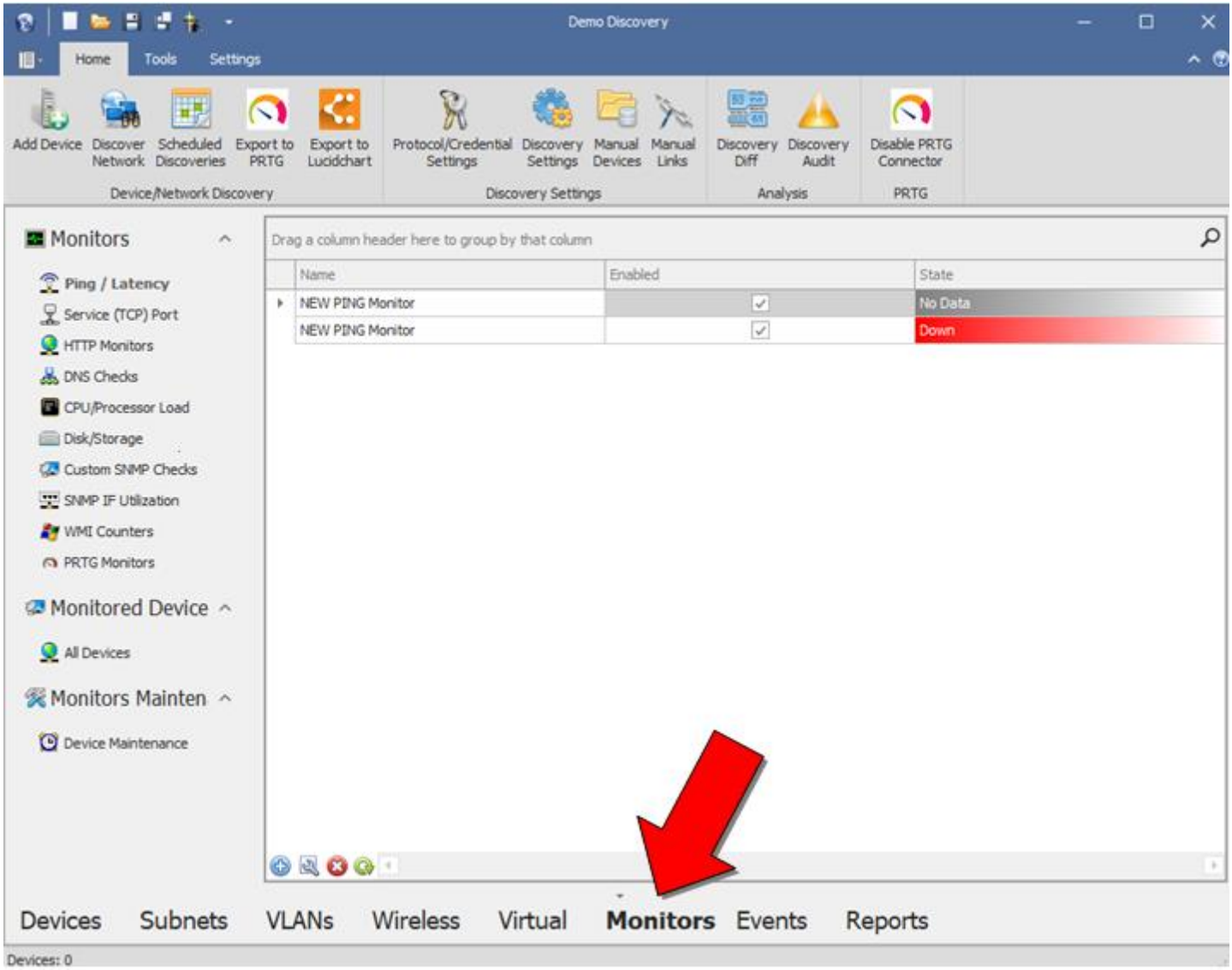
views network discovery results can be segmented into logical groups. The groups are presented in a navigation pane on the left side of the main view. When a group is selected the devices in the group will be displayed in the 'Devices' and 'Map' views in the center pane.



See Device Group/Category views for more information.

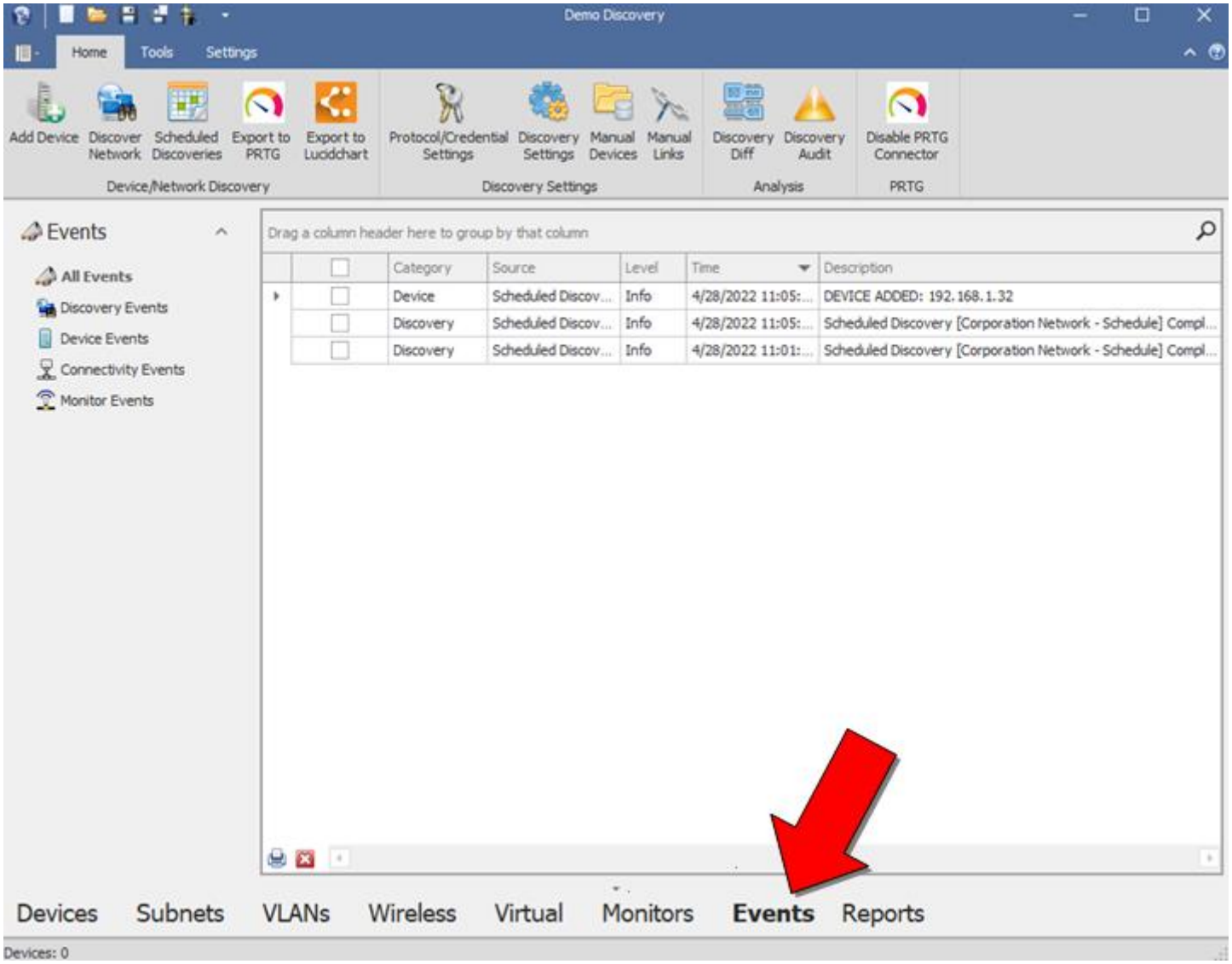
Monitors

The Monitors page allows you to create, configure, and view the results of the available monitors. See Monitors for more information.



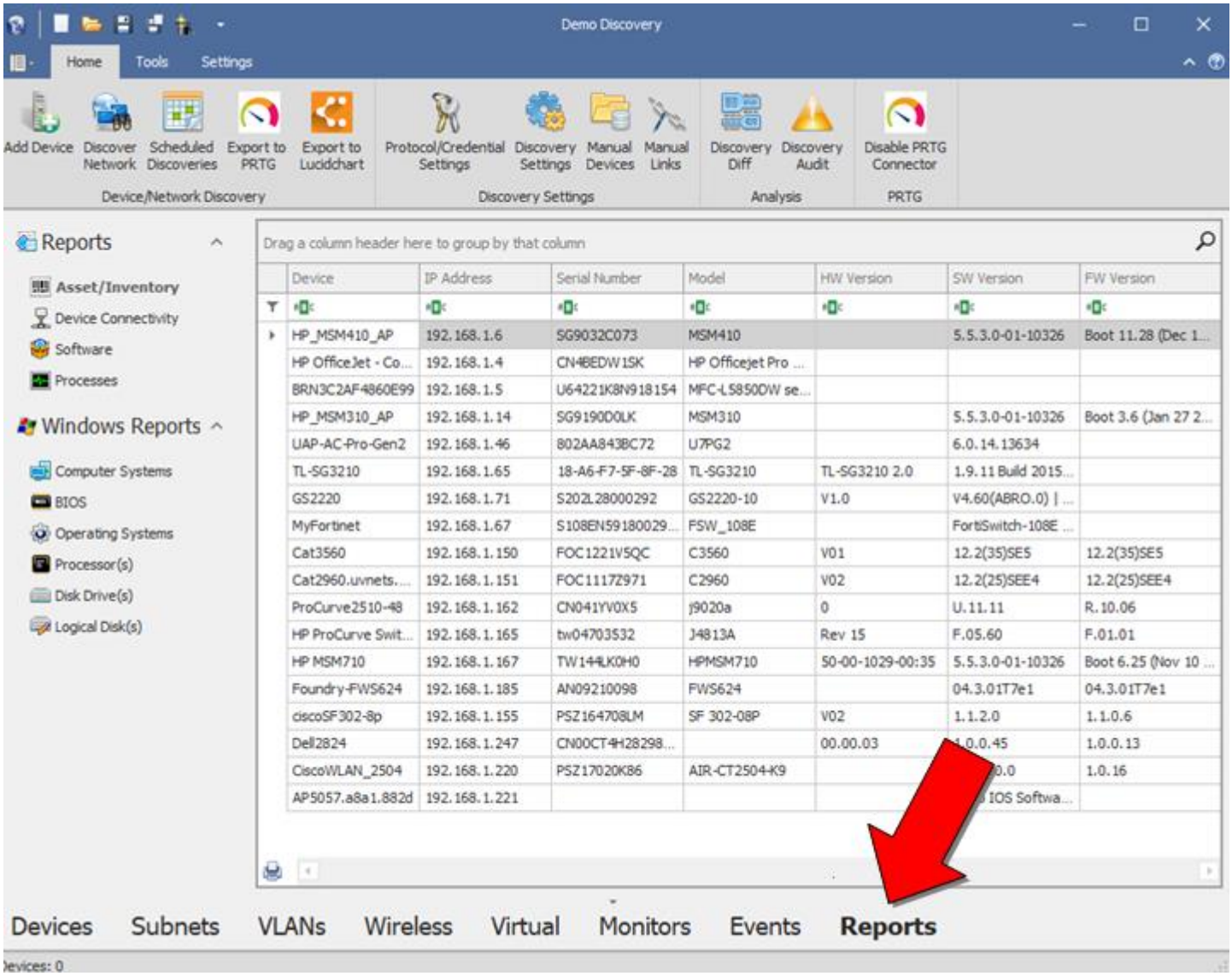
Events

The Events page displays a log of events related to scheduled discoveries. See Events for more information.



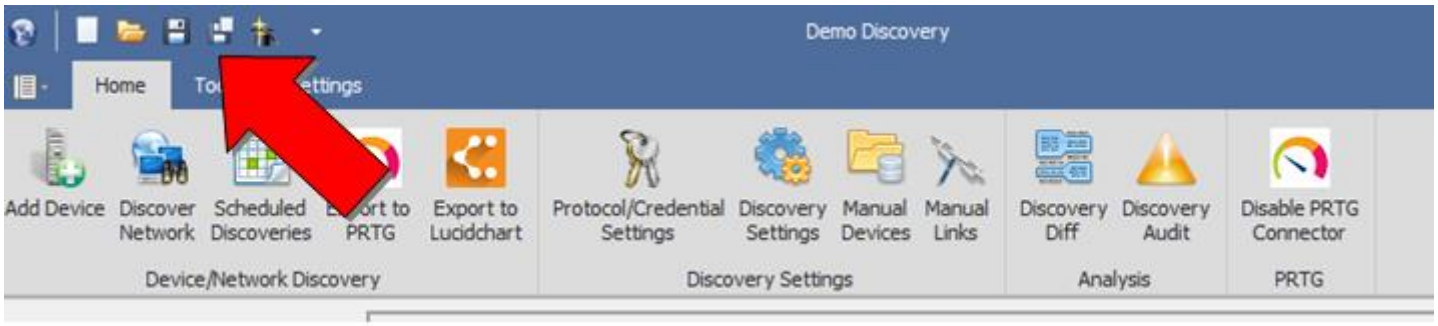
Reports

The Reports page contains reports for documenting the network device asset information collected from the network devices. The reports can be viewed and exported to multiple file formats. See Reports for more information.



Quick Access Toolbar

The quick access toolbar is located at the top of the application by default. The toolbar can be moved below the ribbon menu by clicking the drop-down icon on the left of the toolbar and selecting the 'Show Quick Access Toolbar Below the Ribbon' option. To return the toolbar select the 'Show Quick Access Toolbar Above the Ribbon' option.



The quick access toolbar contains options to open a new or previously discovered discovery result, save discovery results, and run the discovery wizard.

Ribbon Menu

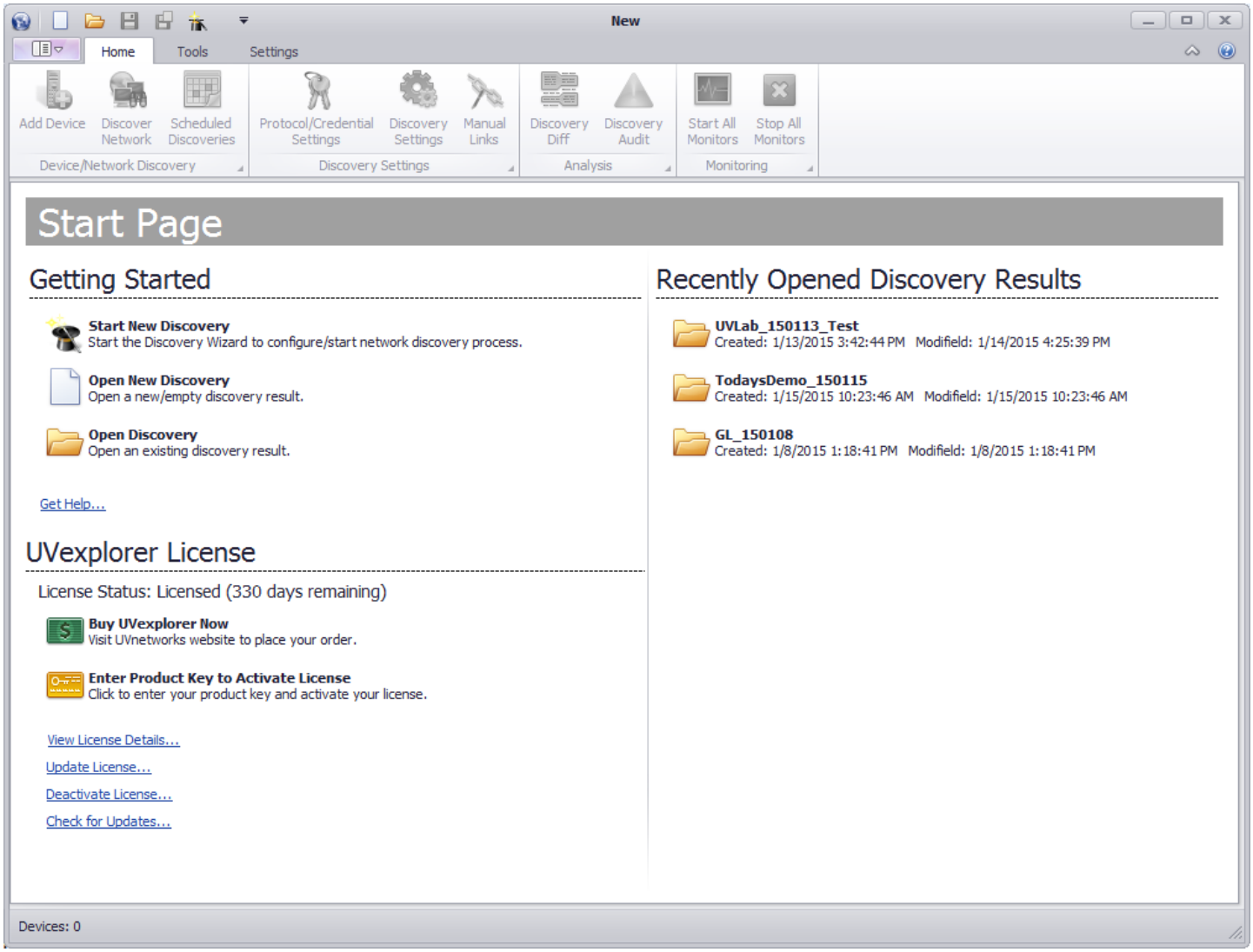
The ribbon menu is the main application menu presented as a tabbed ribbon menu at the top of the application. The ribbon menu contains tabs for the Backstage View, common operations on the 'Home' tab, network tools on the 'Tools' tab, and application settings on the 'Settings' tab. To

change menus, select any of the tabs. To hide the menu, press the collapse icon on the right of the ribbon. If the ribbon is collapsed it can be restored by pressing the expand icon on the right of the ribbon.

See Ribbon Menu for more information.

Startup Page

UVexplorer has a startup page that is presented when the application is first opened. The startup page provides easy access to common operations such as discovering networks and opening discovery results.



Accessing the Startup Page

The startup page is presented when the application is first started. To startup page can also be accessed from the backstage view, by pressing the 'Getting Started' menu option in the left navigation pane.

Getting Started

The getting started section of the startup page allows you to start the discovery wizard, open a new discovery or open an existing discovery result.

Recently Opened Discovery Results

The recently opened discovery results section contains the last five recently opened discoveries.

UVexplorer License

The license section displays the current license status along with the options to change the license. The license section contains the following settings:

Buy UVexplorer now

This option will take you to the UVnetworks website where you can buy and update your license.

Activate License
This option will allow you to enter your product license key to license the application. If the product is already licensed it must first be deactivated to change the license.

View License Details
This option will take you to the help/support section of the backstage view which contains the current license information.

Update License
This option will launch the update license wizard. See Updating UVexplorer License for more information.

Deactivate License
This option will launch the deactivate license wizard. See Deactivating UVexplorer for more information.

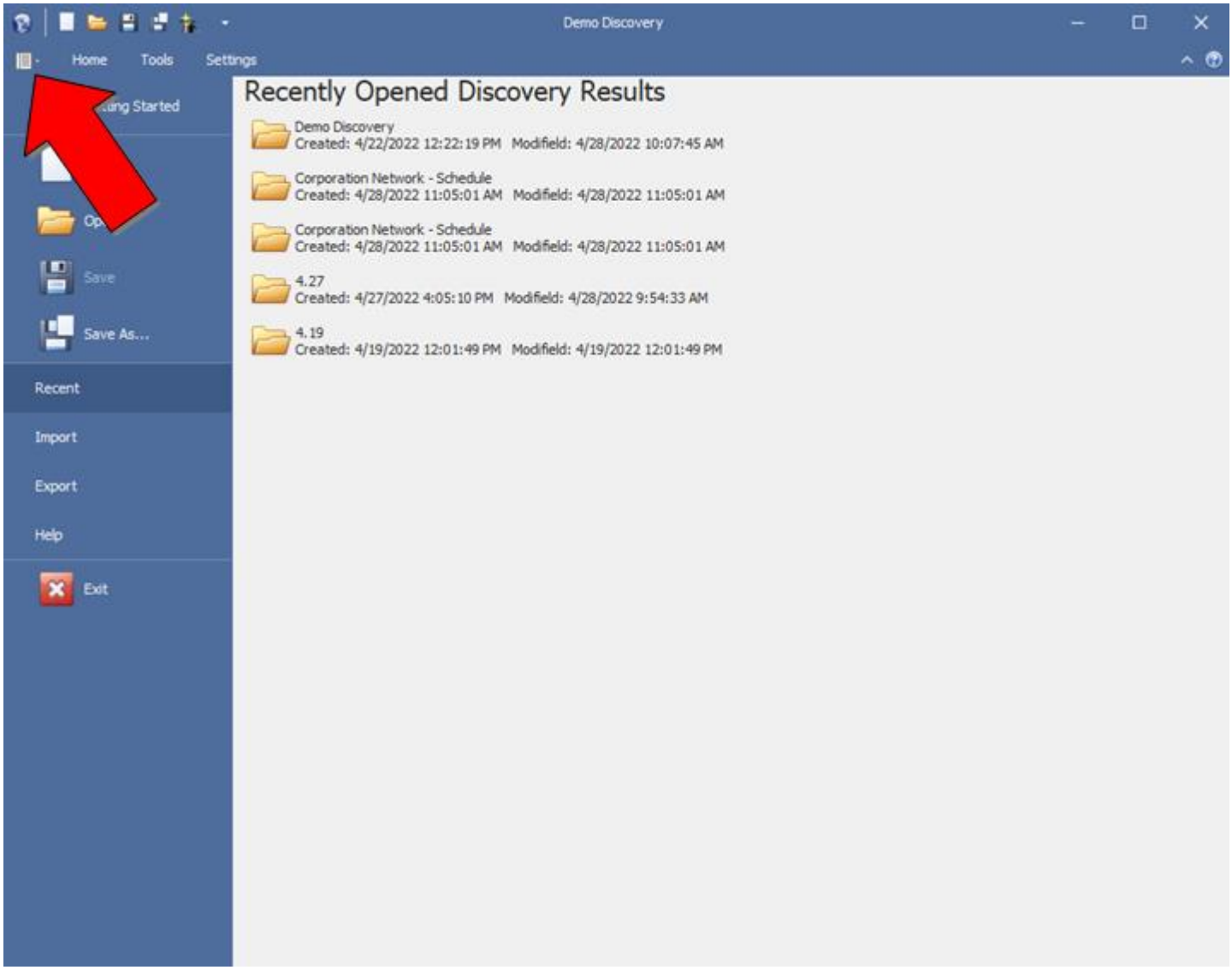
Check for updates
This option will send a request to the UVexplorer update server to check whether you have the latest version of the application. If the application is current a message will be displayed. If the application is not current an option to update will be presented. See Updating UVexplorer for more information.

Backstage View

The UVexplorer backstage view provides easy access to application operations such as managing discovery results and viewing application version and licensing information.

Accessing the Backstage View

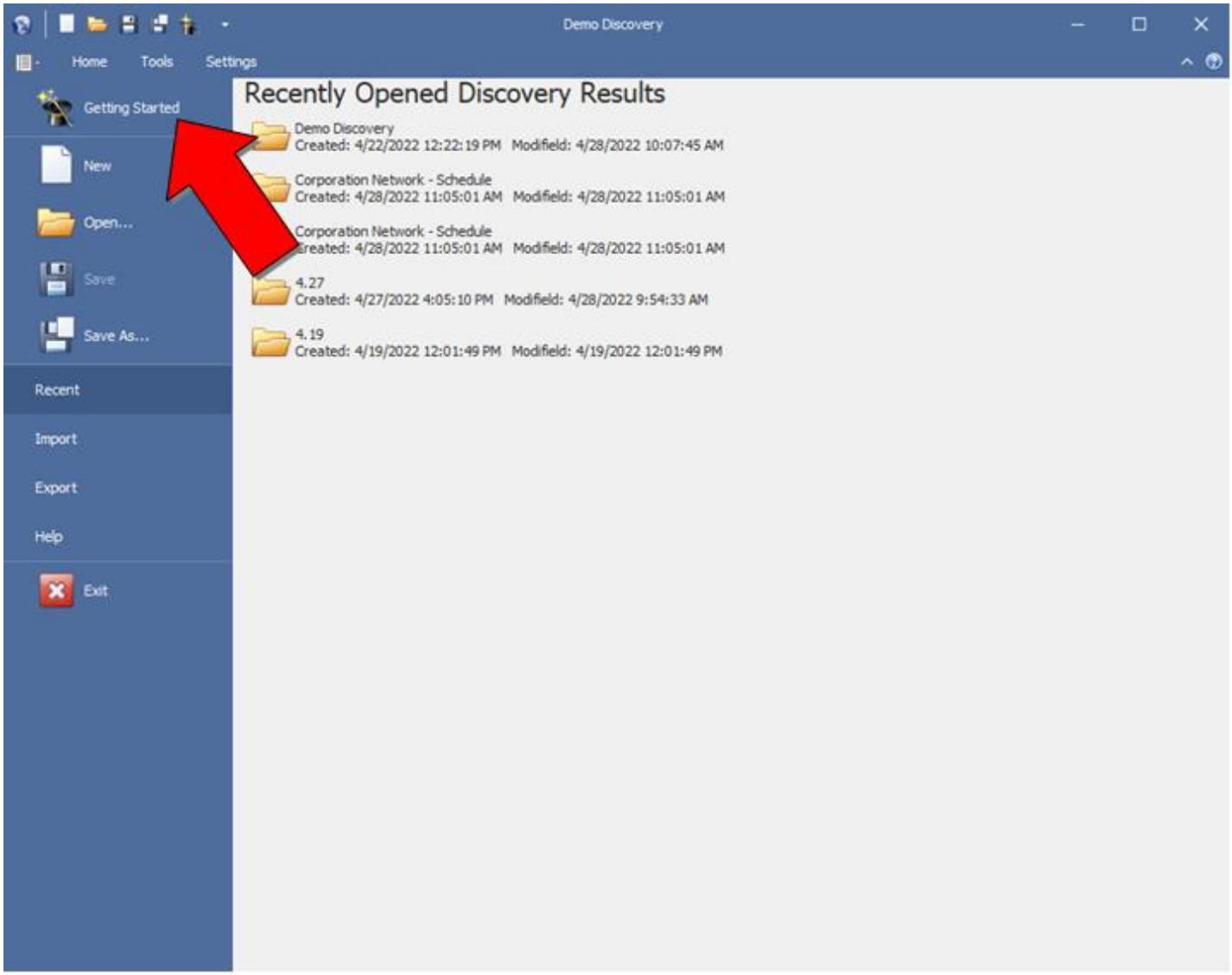
To access the backstage view, press the backstage view button on the far left of application near the main views tab menu.



Backstage View Menu Options

Getting Started

Selecting the getting started menu item will open the getting started view. See Startup Page for more information.



New
The new menu item will close any currently opened discovery results and open a new empty discovery result.

Open
The open menu item will open the open discovery results dialog. The dialog will present previously discovered networks available to open within the application. The selected network will be opened and the application will return to the main view.

Save
The save menu item will save any changes to the current network, whether they were changes that occurred from a discovery or by working with the discovered network result. If the current network has never been saved the Save As dialog will be presented.

Save As
The save as menu item will save the current network to the database as new network with a new name. When pressed a save as dialog is presented that allows you to specify the name of a new network.

Recent
The recent menu item will display a list of the five most recent discovery results opened within the application. The recent discoveries will be presented in the pane to the right and can be opened by clicking on one of them. When opened the application will open the network and return to the main

view.

Import

The import menu item allows you to import a discovery result that has previously been exported from UVexplorer. The import option allows you to share discovery results with other computers or network administrators.

To import a discovery file press the import button. A dialog will be presented allowing you to select a '.dis' file that has been previously exported from UVexplorer.

Export

The export menu item allows you to export devices from a discovery result to make them available to import into UVexplorer later or on another machine. The discovery result is exported to a '.dis' file which is an encrypted and compressed serialization format of the network devices.

To export devices select them in the device list and press the export button. A dialog will be presented to allow you to name the discovery file in the file system.

Help

The help menu item opens a view containing licensing and application version information and other options

Support

The support section provides links to launch the application help, present the Startup Page, or direct you to UVnetworks support web page.

Help on the Web

The help on the web section provides a link to the UVexplorer help documentation available on the web.

About UVexplorer

The about UVexplorer section contains the application version information.

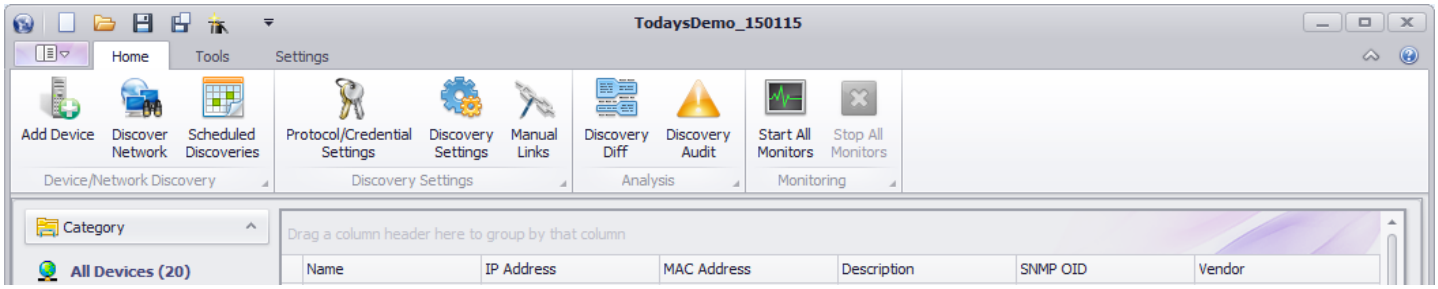
License Information

The license information section contains the current license status along with your license key.

See UVexplorer activation for more information about licensing.

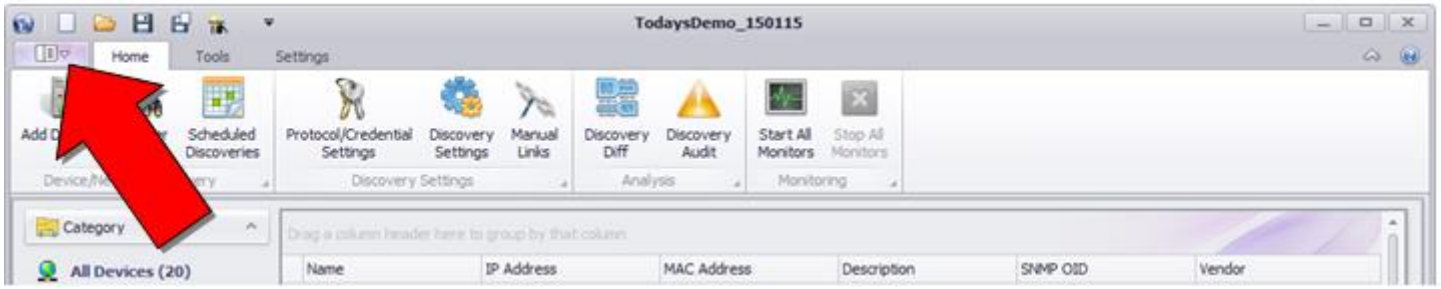
Ribbon Menu

The ribbon menu is the main application menu presented as a tabbed ribbon menu at the top of the application. The ribbon menu contains tabs for the Backstage View, common operations on the 'Home' tab, network tools on the 'Tools' tab, and application settings on the 'Settings' tab. To change menus, select any of the tabs. To hide the menu, press the collapse icon on the right of the ribbon. If the ribbon is collapsed it can be restored by pressing the expand icon on the right of the ribbon.



Backstage View

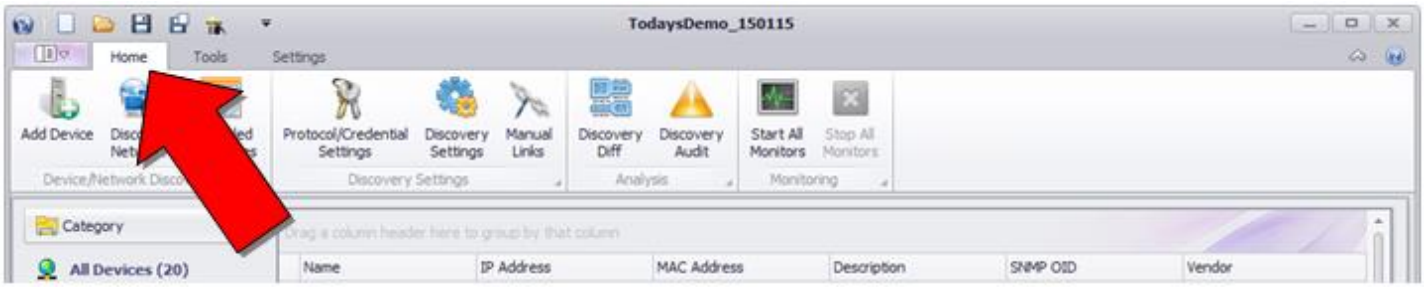
The backstage view menu is available as a drop-down tab at the far left of the ribbon menu. When the backstage view item is selected the backstage view is presented as a popup panel in front of the application. To close the backstage view complete one of the operations available in the backstage view or press on one of the other ribbon menu tabs or quick access toolbar items.



See Backstage View for more information about the

Home

The home menu provides access to the following common application operations.



Add Device

Add Device opens the single device discovery tool for discovering a single device to include in the current network discovery results. See Discovering a single device for more information.

Discover Network

Discover Network opens the network discovery tool used to discover an entire network. See Discovering Networks for more information.

Scheduled Discoveries
Scheduled Discoveries opens the scheduled discovery dialog used to run network discoveries on a scheduled basis. See Scheduling Network Discovery for more information.

Export to PRTG
This option is available if PRTG Connector is enabled and provides a wizard to walk you through exporting devices and maps to PRTG network monitor. See PRTG Connector for more information.

Protocol/Credential Settings
Protocol/Credential Settings opens the credentials manager used to manage network credentials available for communicating with network devices. See Managing Device Credentials for more information.

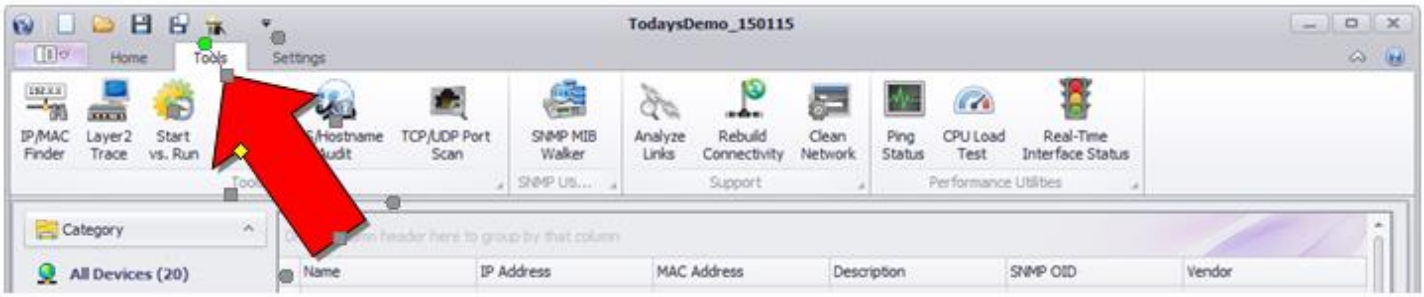
Discovery Settings
Discovery Settings opens the discovery settings library used manage discovery settings available for network discoveries. See Discovery Settings for more information.

Manual Links
Manual Links opens the manual links library used to manage user created links presented in topology maps and network connectivity summaries. See Manual Links for more information.

Discovery Diff
Discovery Diff opens the network discovery comparison which compares two discovered networks for differences. See Comparing Discovered Networks for more information.

Discovery Audit
Discovery Audit opens the discovery audit tool which provides information on ways to improve network discoveries. See Network Discovery for more information.

Tools
The tools menu provides access to the network tools.



IP/MAC Finder
IP/MAC Finder opens the IP/MAC address finder tool used to locate references to an IP or MAC address on devices in the network discovery result. See IP/MAC Address Finder for more information.

Layer 2 Trace
Layer 2 Trace opens the Layer 2 Trace tool used to track the connection path between two devices and the paths current ping and interface UP/DOWN status. See Layer 2 Trace for more information.

Start vs. Run
Start vs. Run opens the network device startup vs. running configuration tool used to compare a devices startup and running configurations. See Startup vs. Running Configuration for more

information.

Capture Config
Capture Config opens the network device configuration capture tool used to capture the startup and running configurations on a network device. See Configuration Capture for more information.

DNS/Hostname Audit
DNS/Hostname Audit opens the DNS/Hostname Audit tool used to ensure IP Addresses and Hostnames are resolving correctly on the network. See DNS/Hostname Resolver for more information.

TCP/UDP Port Scan
TCP/UDP Port Scan opens the port scan tool used to scan for open ports on a network devices. See Port Scanner for more information.

SNMP MIB Walker
SNMP MIB Walker opens the MIB walker tool used to query SNMP responses on common MIBS. See SNMP MIB Walker for more information.

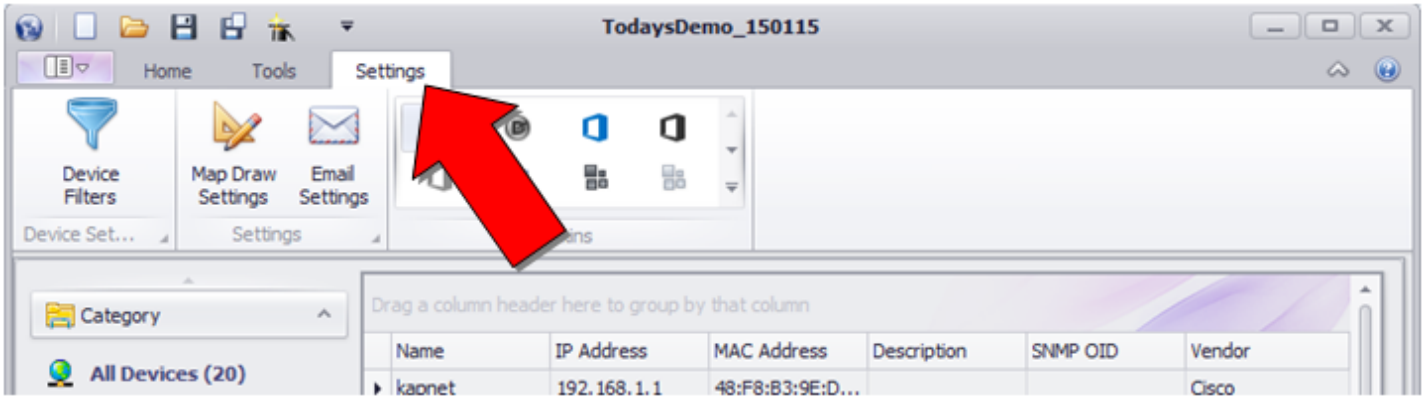
Note: The MIB Walker tool is not a full featured MIB walker. It is intended to be used as a support tool when troubleshooting incorrect or unavailable SNMP responses from devices during network discovery.

Ping Status
Ping Status opens the ping response poller used to poll ping responses on network devices. See Ping Response Poller for more information.

CPU Load Test
CPU Load Test opens the CPU Load Poller used to poll the CPU load on several network devices. See CPU Load Poller for more information.

Real-Time Interface Status
Real-Time Interface Status opens the Interface Status Poller used to poll the status of the interfaces on a device. See Interface Status Poller for more information.

Settings
The settings menu is used to configure the following application settings.



Device Filters
Device Filters opens the device filters library. Device filters are used throughout the application to create a set of devices based on device criteria. See Device Filters for more information.

Map Draw Settings
Map Draw Settings opens the map draw settings dialog used to configure application wide map draw settings. See Map Draw Settings for more information.

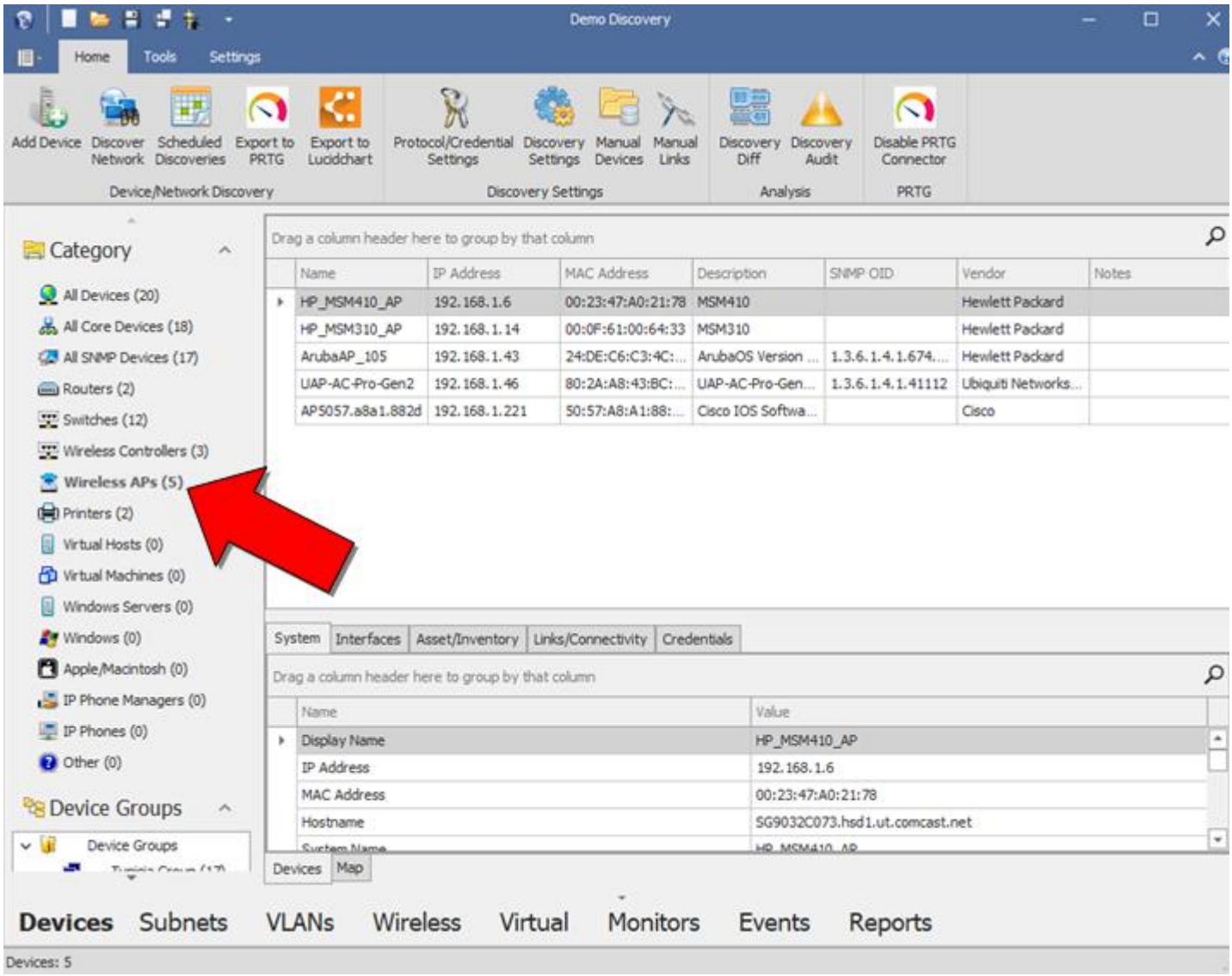
Email Settings
Email Settings opens the email settings dialog used to configure default email server and client email settings. UVexplorer uses the email server settings when sending email notifications. See SMTP Email Server Settings for more information.

PRTG Export Settings
This option is available if PRTG Connector is enabled and provides a way to manage PRTG export template settings. See PRTG Export Templates for more information.

Skins
UVexplorer can change the look and feel of the application by selecting different themes in the application skin picker. See Application Skins for more information.

Device Group Category Views

UVexplorer provides two primary views for viewing network discovery results: the device properties view, and the network topology map. To reduce/filter the number of devices presented in these two views network discovery results can be segmented into logical groups. The groups are presented in a navigation pane on the left side of the main view. When a group is selected the devices in the group will be displayed in the 'Devices' and 'Map' views in the center pane.



Devices

The 'Devices' tab contains two views: a list of the devices contained in the group, and the device properties of the device selected in the device list. To change the devices in the devices list, select a new group or change the members in the group when applicable. To change the device in the device properties view, select a device in the device list.

Devices List

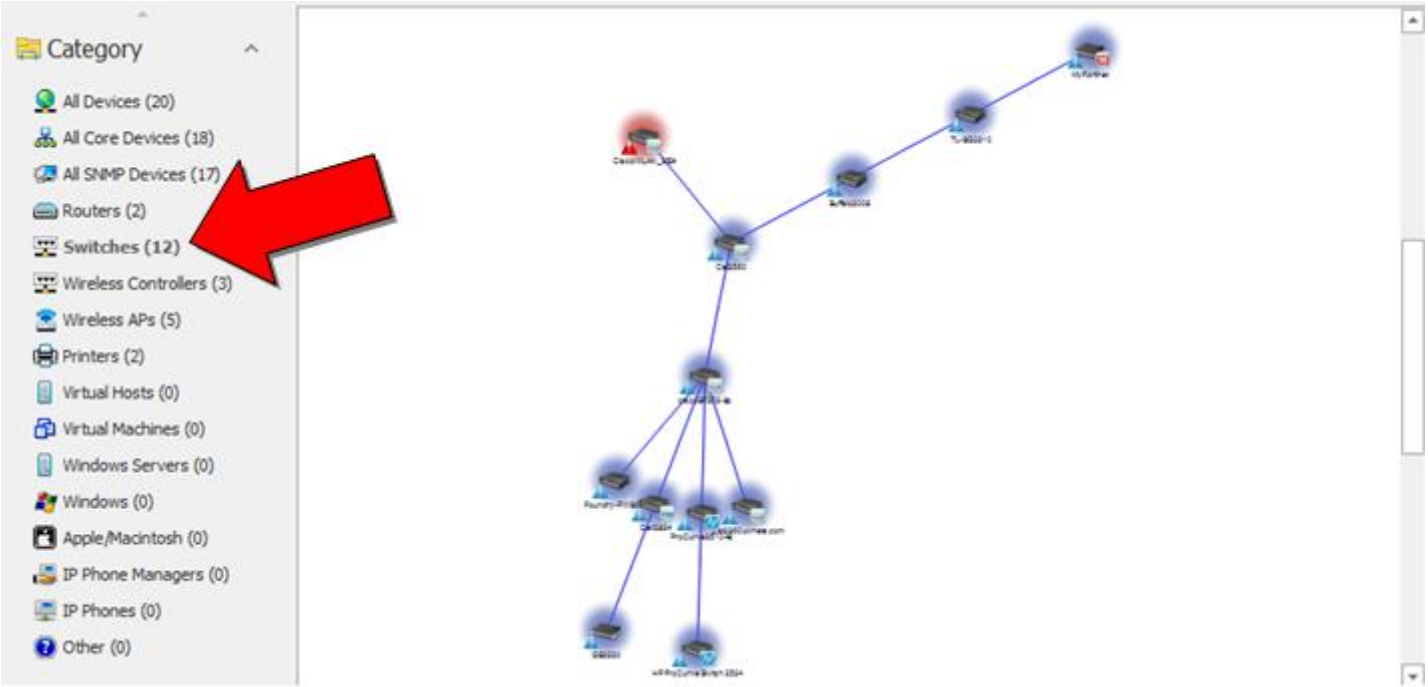
The devices list contains a list of all the devices in the group. The device entries in the list contain common device information to give an overview of the device. Each device also has a context menu that provides access to the network tools, ways to connect to the device, an option to show the device on the map, and an option to delete the device from the discovery results.

Device Properties

The device properties view displays detailed information about the device selected in the device list. See Viewing Device Data for more information.

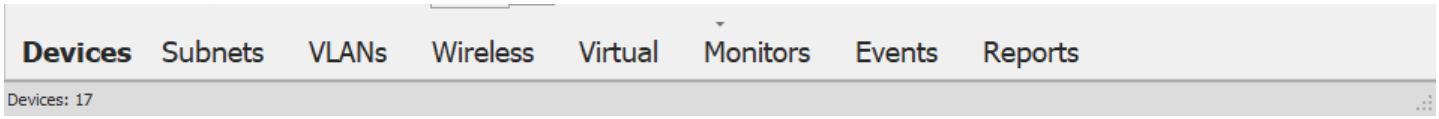
Map

Each group has an option to display a network topology map for the group. The map will contain all the devices in the group and lines representing the connections between the devices. See Network Topology Maps for more information.



Groups and Categories

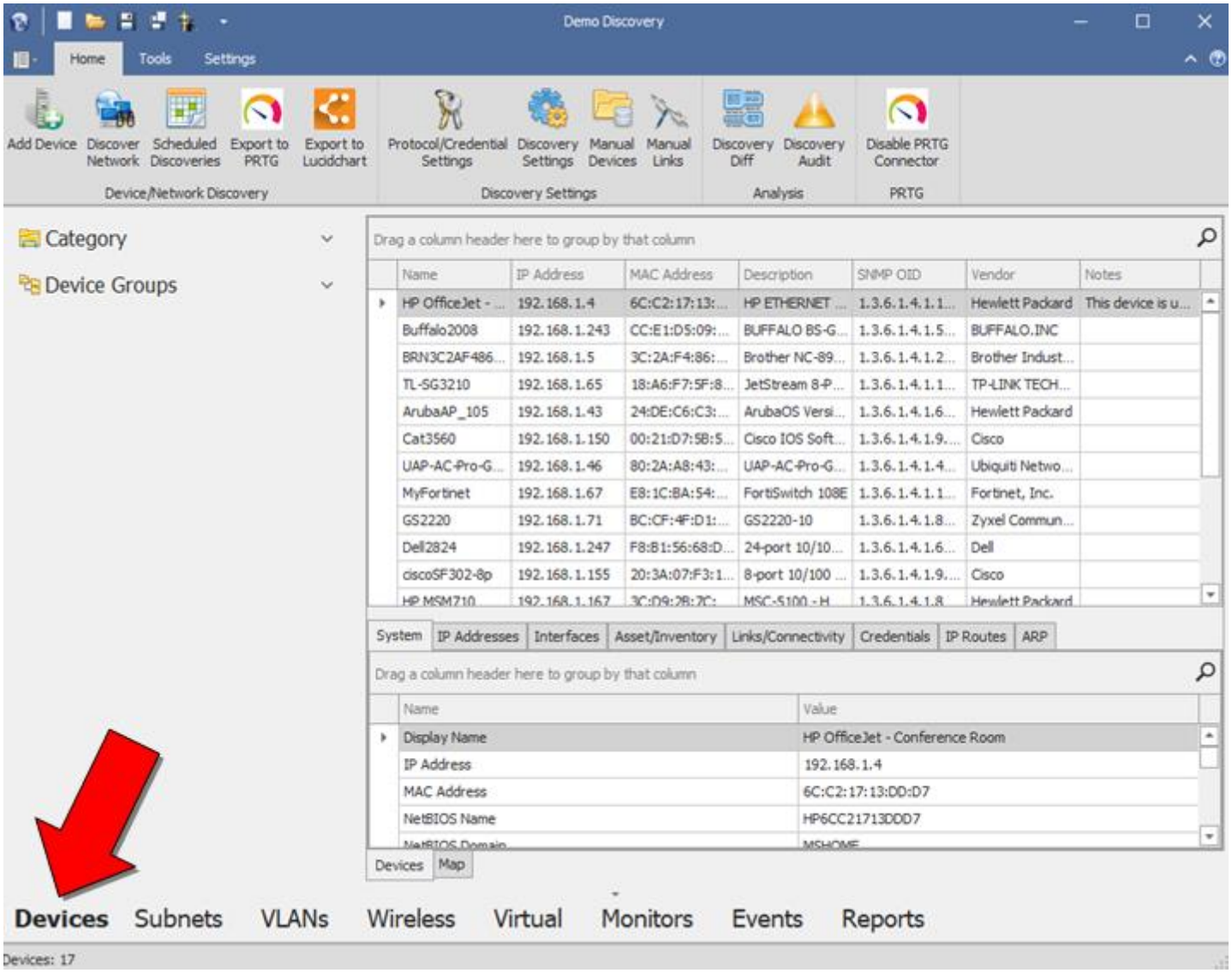
UVexplorer allows you to define your own groups or use dynamic predefined groups whose membership is based on predefined device criteria. Device membership in predefined groups is determined dynamically based on the predefined criteria and cannot be changed. Each predefined group contains a map whose settings can be configured or turned off.



The following groups are available in the Devices, IP-Scope, Wireless, and Virtual pages.

Devices

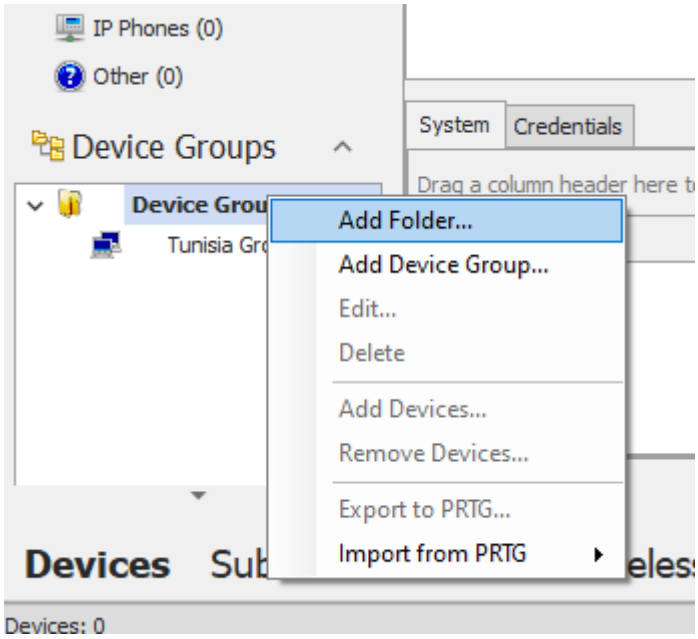
The devices page contains the following device group types:



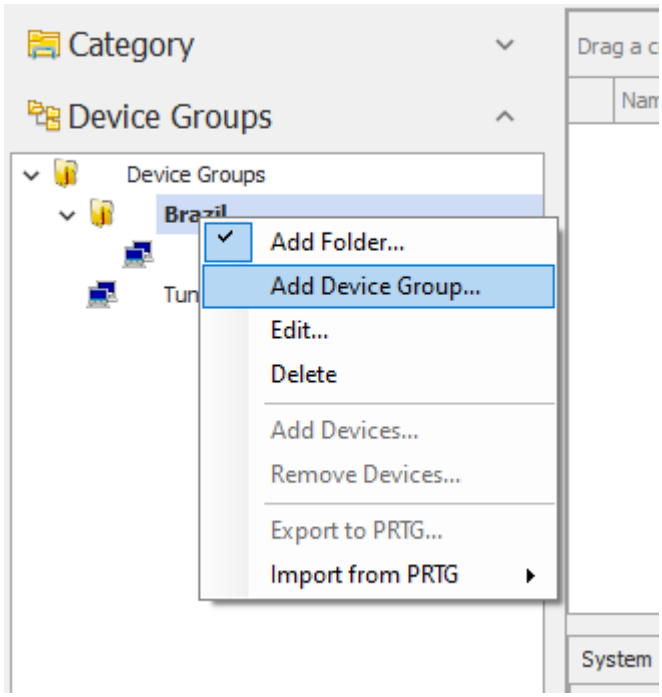
Categories
Device categories determine group membership based on the category type of the device. Device categories cannot be changed. The option to change whether to display a map for a category

Groups
Device groups are user defined groups. The user device groups are contained in tree that can hold device groups or device group folder. Device group folders allow you to logically organize your user defined groups in a hierarchy.

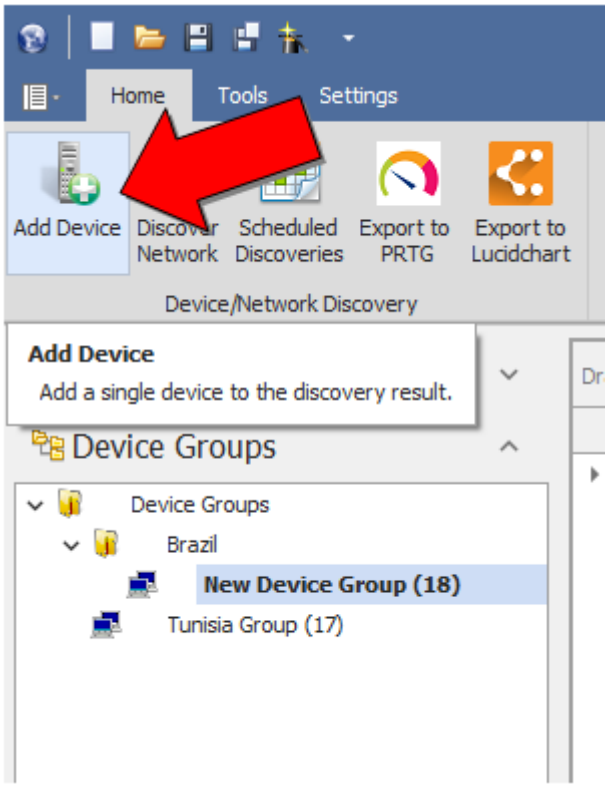
To create a device group folder right click on the groups tree and select the 'Add Folder' option. A dialog will be opened to allow you to set the name of the folder. To change the name a folder use 'Edit' menu item the folders context menu. To add a folder as a child of another folder right click on the folder and select the 'Add Folder' option. To delete a folder, use the folder 'Delete' menu item. When a folder is deleted all its descendant folders and groups will be deleted as well.



To create a device group right click on the group tree or a group folder and select the 'Add Device Group' option. A dialog containing the settings to configure the membership of the group and the maps topology map layout settings, along with the group's name will be presented.



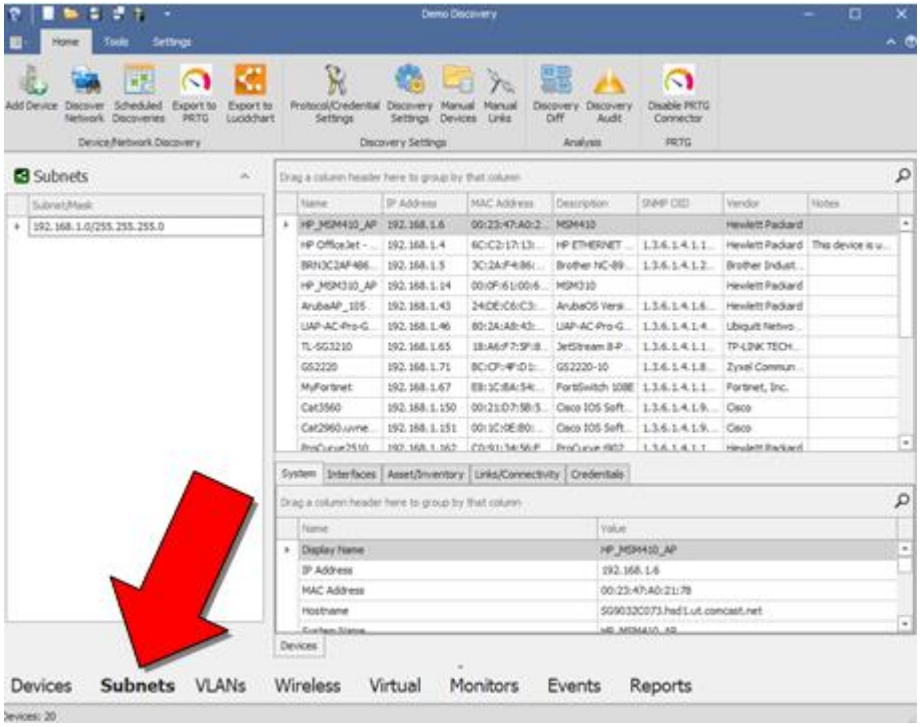
To delete a group, use the 'Delete' menu item in the group's context menu. To edit a group double click it or use the 'Edit' menu item in the group's context menu. If the group has dynamic membership the option to add devices to and remove devices from the group will also be available. These options will open a device picker to use to select the devices to add or remove. When adding devices, you can only add devices already discovered and present in the discovery result. To add a new undiscovered device, use the 'Add Device' option available in the 'Home' ribbon menu.



See Device Groups for more information.

Subnets

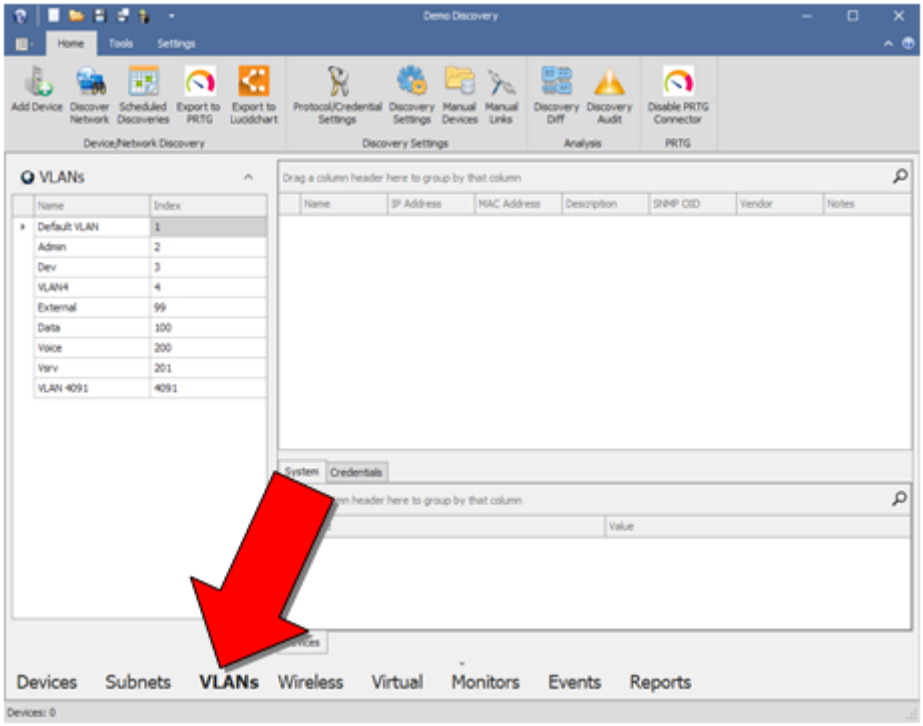
The Subnets page contains groups based on the subnets available in the network discovery results. A group is created for each subnet containing devices in the network discovery result. Subnet groups are not persisted and do not support changing the map layout settings.



VLANs

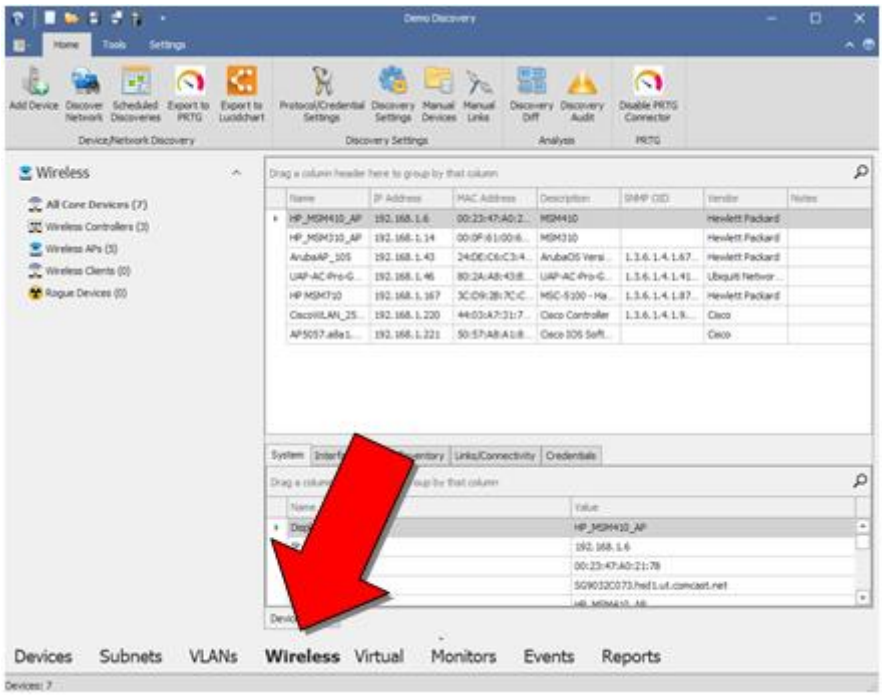
The VLANs page contains groups based on the VLANs available in the network discovery results. A

group is created for each VLAN containing devices in the network discovery result. VLAN groups are not persisted and do not support changing the map layout settings.



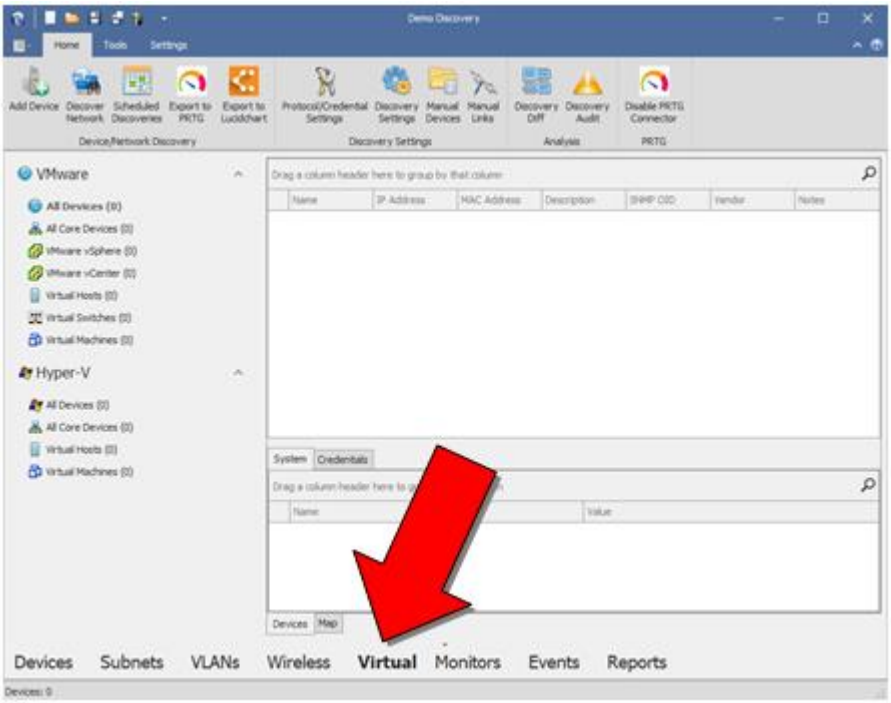
Wireless

Wireless groups are predefined groups representing the wireless infrastructure of the network. The groups include wireless controllers, Access Points and Clients. The 'All Core Devices' group contains the wireless controllers and access points and their connections when available.



Virtual

Virtual groups are predefined groups representing the virtual infrastructure of the network. The groups include virtual hosts, and machines. The groups are also categorized by the supported virtual machine types, VMware and Hyper-V.


Demo Discovery
Home
Tools
Settings
Add Device
Discover Network
Scheduled Discoveries
Export to PRTG
Export to Lucidchart
Device/Network Discovery
Protocol/Credential Settings
Discovery Settings
Manual Devices
Manual Links
Discovery Settings
Discovery Diff
Discovery Audit
Analysis
Disable PRTG Connector
PRTG
VMware
All Devices (0)
All Core Devices (0)
VMware vSphere (0)
VMware vCenter (0)
Virtual Hosts (0)
Virtual Switches (0)
Virtual Machines (0)
Hyper-V
All Devices (0)
All Core Devices (0)
Virtual Hosts (0)
Virtual Machines (0)
Drag a column header here to group by that column
Name
IP Address
MAC Address
Description
SNMP OID
Vendor
Notes
System
Credentials
Name
Value
Devices
Map
Devices
Subnets
VLANs
Wireless
Virtual
Monitors
Events
Reports
Devices: 0

Device Groups

If your network contains a lot of devices, it can be helpful to organize your devices into smaller groups that can be viewed and managed separately. By default, UVexplorer provides many built-in device groups that represent common types of devices found on a network, such as 'All Devices', 'All Core Devices', 'All SNMP Devices', 'Switches', 'Printers', etc. UVexplorer also provides built-in device groups for subnets, VLANs, wireless devices, and virtual devices.

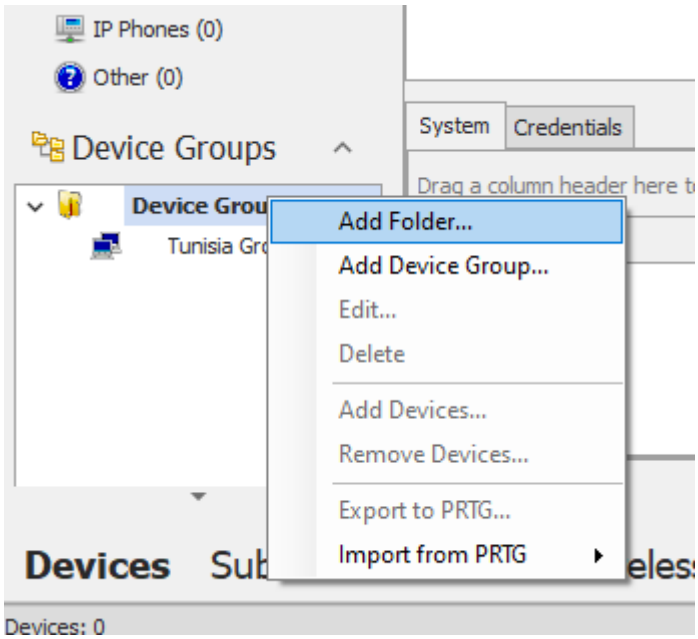
After selecting a device group on the left, you can then select the 'Devices' tab at the bottom to view a list of devices in the group, and all of the inventory information for each device. After selecting a device group on the left, you can also select the 'Map' tab at the bottom to view a topology map showing all the devices in the group and how they are connected.

While many of the device groups you will need are already provided by UVexplorer, you can also create custom device groups to represent collections of devices that are interesting and useful to you. For example, you could create a device group named 'Servers' that contains all of the server devices in your network. Or, you might create a device group named 'Firewalls' that contains all of the firewall devices in your network. By grouping related devices together, you can more easily view and otherwise manage those devices.

Device groups can be organized into folders, much like files can be organized into folders in a file system. By default, all device groups are in a folder named 'Device Groups', but additional folders can be created as needed. Each device group is in exactly one folder. Folders are organized into a hierarchy, with folders containing other folders to any number of levels. If you have a lot of device groups, folders can be very helpful in keeping them organized.

Creating a Folder

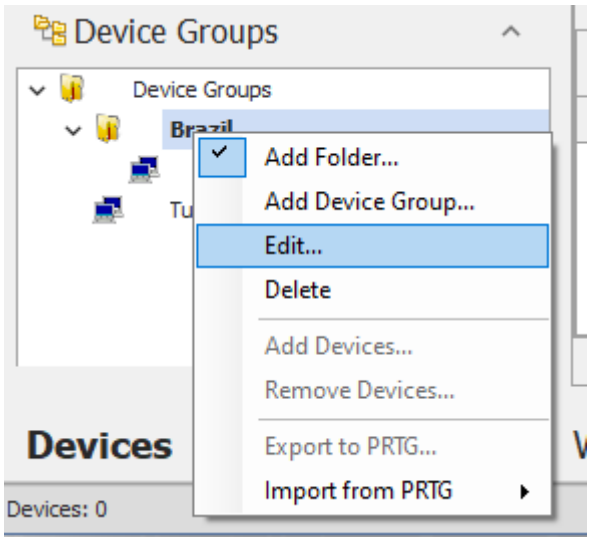
By default, all device groups are contained in a folder named 'Device Groups'. Additional folders can be created by right-clicking on the parent folder, and selecting 'Add Folder'. This will display a form that lets you enter a name for the new folder. A folder's name cannot be empty. The new folder will be created in the specified parent folder.



Editing a Folder

To change the properties of a folder, do one of the following:

- Double-click on the folder
- Right-click on the folder, and select 'Edit' from the context menu



Both of these operations will display a form that lets you modify the name of the folder. A folder's name cannot be empty.

Deleting a Folder

To delete a folder, right-click on the folder and select 'Delete' from the context menu. This operation cannot be reversed, and deleting a folder will delete all folders and device groups contained within the folder, so make sure you really want to delete the folder. If you want to preserve the contents of the folder, move the folder's contents to another folder before deleting it.

Moving Folders and Device Groups

To move a device group or folder to a different folder, simply click on the group or folder to be moved, and drag it to the folder you want to move it to.

Adding a Device Group

To create a new device group, right-click on the folder that will contain the new group, and select 'Add Device Group' from the context menu. This will display the Device Group Editor, which lets you configure the new device group. See Device Group Editor for more details.

Editing a Device Group

To change the properties of a device group, do one of the following:

- Double-click on the device group
- Right-click on the device group, and select 'Edit' from the context menu

Both of these operations will display the Device Group Editor, which lets you modify the properties of an existing device group. See Device Group Editor for more details.

Deleting a Device Group

To delete a device group, right-click on the group and select 'Delete' from the context menu. This operation cannot be reversed, so make sure you really want to delete the group.

Adding and Removing Devices To/From a Static Device Group

For static device groups, you manually add and remove devices to/from the group. There are several ways to add and remove group devices.

Here are the different ways you can add devices to a static device group:

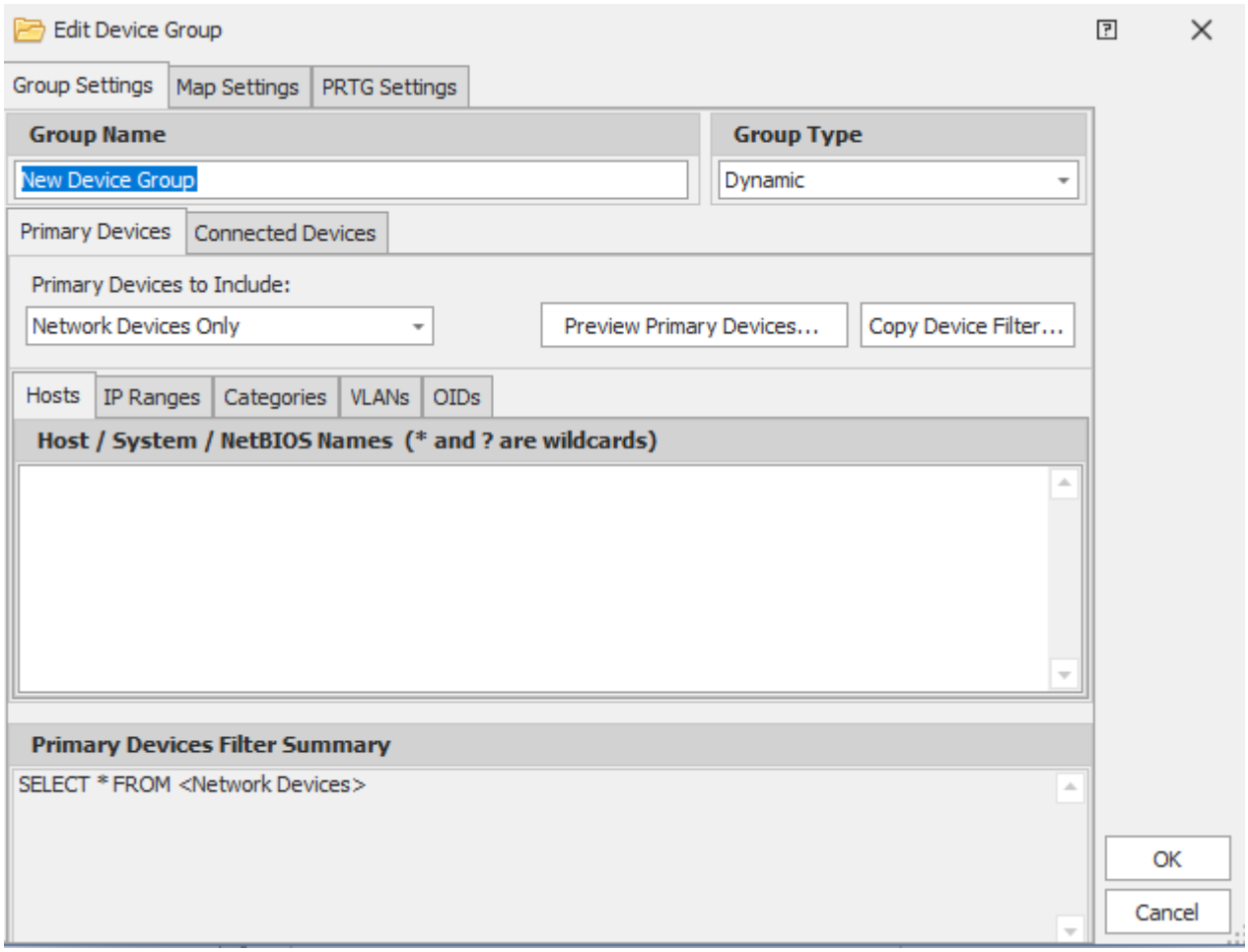
- Right-click on the device group in the Device Groups hierarchy, and select 'Add Devices' from the context menu.
- Right-click on the device group's connectivity map, and select 'Add Devices' from the context menu.
- Right-click on the device group's connectivity map, and select either 'Add Connected' or 'Add Associated' from the context menu. To perform these operations on all devices on the map, right-click on the map background (i.e., not a device). To perform these operations on a single device, right-click on the device.

Here are the different ways you can remove devices from a static device group:

- Right-click on the device group in the Device Groups hierarchy, and select 'Remove Devices' from the context menu
- Right-click on the device group's connectivity map, and select 'Remove Devices' from the context menu
- Right-click on the device group's connectivity map, and select either 'Remove Connected' or 'Remove Associated' from the context menu. To perform these operations on all devices on the map, right-click on the map background (i.e., not a device). To perform these operations on a single device, right-click on the device.
- Select one or more devices on the device group's connectivity map, right-click on one of the selected devices, and select 'Remove Selected' from the context menu.
- Select one or more devices on the device group's connectivity map, press the DELETE key on your keyboard.

Device Group Editor

The Device Group Editor is used to specify the properties of a device group. This applies when you create a new device group, or modify the properties of an existing device group. A device group's properties are divided into Group Settings and Map Settings. The Group Settings tab contains the basic properties that define the group's name, type, and device membership. The Map Settings tab defines properties that control how (and if) the topology map for the group is drawn.



Group Settings

Group Name

A device group must have a name. It can be anything you want, as long as it's not empty.

Group Type

A device group must have a type. There are two types to choose from, 'Dynamic' and 'Static'.

For dynamic device groups, you provide an abstract description of the devices that are in the group, and UVexplorer will automatically match your abstract description against each device to determine which devices are in the group. For example, a group's abstract description might be, "This group contains all SNMP-enabled devices in the 192.168.5.0/24 subnet". Given that description, UVexplorer will automatically compute which devices in the currently-open discovery result are in the group.

For static device groups, you manually manage the device membership of the group. That is, you manually add and remove specific devices to/from the group, giving you complete control over which devices are in the group. In this case, UVexplorer will not try to automatically determine which devices are in the group. Instead, it will just use the devices you have manually put in the group.

Device Membership

For dynamic device groups, you provide an abstract description of what devices are in the group. This is done in two steps:

1) Specify the 'Primary' devices for the group. These are the main devices that should be included in the group.
2) Specify which devices that are connected to the primary devices that should be included in the group. These are called 'Connected' devices.

For example, suppose that you want to create a group containing all switches in your network, and all servers and printers connected to those switches. The group would be defined as follows:
Primary Devices = Switches
Connected Devices = Servers, Printers

Notice that this group would contain servers and printers that are connected to a switch, but not contain servers and printers that are not connected to a switch. If you wanted the device group to contain all servers and printers regardless of whether they are connected to a switch, the group would be defined as follows:

Primary Devices = Switches, Servers, Printers
Connected Devices = None

The 'Primary Devices' tab lets you specify the group's primary devices, and the 'Connected Devices' tab lets you specify the group's connected devices. For both the Primary and Connected devices, you must specify which devices should be included in the group. This is done in two steps:

1) Select a base set of devices to be included in the group. The choices are: All Devices, SNMP Devices Only, Network Devices Only, and No Devices. This selection defines which devices could potentially be included in the group (i.e., devices outside the base set will not be included in the group).
   a) All Devices – All devices can be included in the group
   b) SNMP Devices Only – Only SNMP devices can be included in the group
   c) Network Devices Only – Only network devices can be included in the group (routers, switches, wireless access points, etc.)
   d) No Devices – No devices can be included in the group
1) Starting with the base device set selected in step 1, you may optionally specify additional criteria to narrow down the base set even further. The following additional filtering criteria may also be specified:
   a) Host/System/NetBIOS Name – You can specify one or more patterns to be matched against a device's names. For example, the pattern fileserver will match any device that has a DNS host name, SNMP system name, or NetBIOS name with the value fileserver. You can also include wildcard characters in a name pattern. For example, the pattern *.acme.com will match any device with a name ending in .acme.com. In general, an asterisk * will match zero or more adjacent characters, and a question mark ? will match exactly one character. If any device name patterns are specified, a device's names must match at least one of the name patterns in order to be included in the group.
   b) IP Ranges – You can specify one or more IP addresses to be matched against a device's IP addresses. You can specify individual IP addresses, such as 172.16.3.25; ranges of IP addresses, such as 192.168.3.1 – 192.168.3.127; or IP subnets, such as 10.5.0.0/16. If any IP address constraints are specified, a device must have at least one IP address that matches at least one of the constraints.
   c) Categories – You can specify one or more device categories to be included in the group. A list of all possible device categories is presented for you to choose from. Simply check the device categories that should be included in the group. For example, if you select the 'printer'

category, then printer devices will be included in the group. If any device categories are specified, a device must be in at least one of the selected categories in order to be included in the group.

d) VLANs - You can specify that devices in particular VLANs should be included in the group. This is done by listing one or more patterns to be matched against the names of a device's VLANs. For example, the pattern Sales will match any device that is in the VLAN named Sales. You can also include wildcard characters in a VLAN name pattern. For example, the pattern Marketing* will match any device that participates in a VLAN whose name begins with Marketing. In general, an asterisk * will match zero or more adjacent characters, and a question mark ? will match exactly one character. If any VLAN patterns are specified, a device's VLANs must match at least one of the patterns in order to be included in the group.

e) OIDS - You can specify that devices with an OID matching the provided OID pattern should be included in the group. An OID is an unique object identifier provided by the manufacturer of a device or asset. The first portion of an OID is specific for a vendor and often a model. Multiple OID patterns can be provided, separated by a space or comma. Wild card's of '*' and '?' can be used when specifiying a match pattern. In general, an asterisk * will match zero or more adjacent characters, and a question mark ? will match exactly one character. If any OID patterns are specified, a device's OID must match at least one of the patterns in order to match the filter.

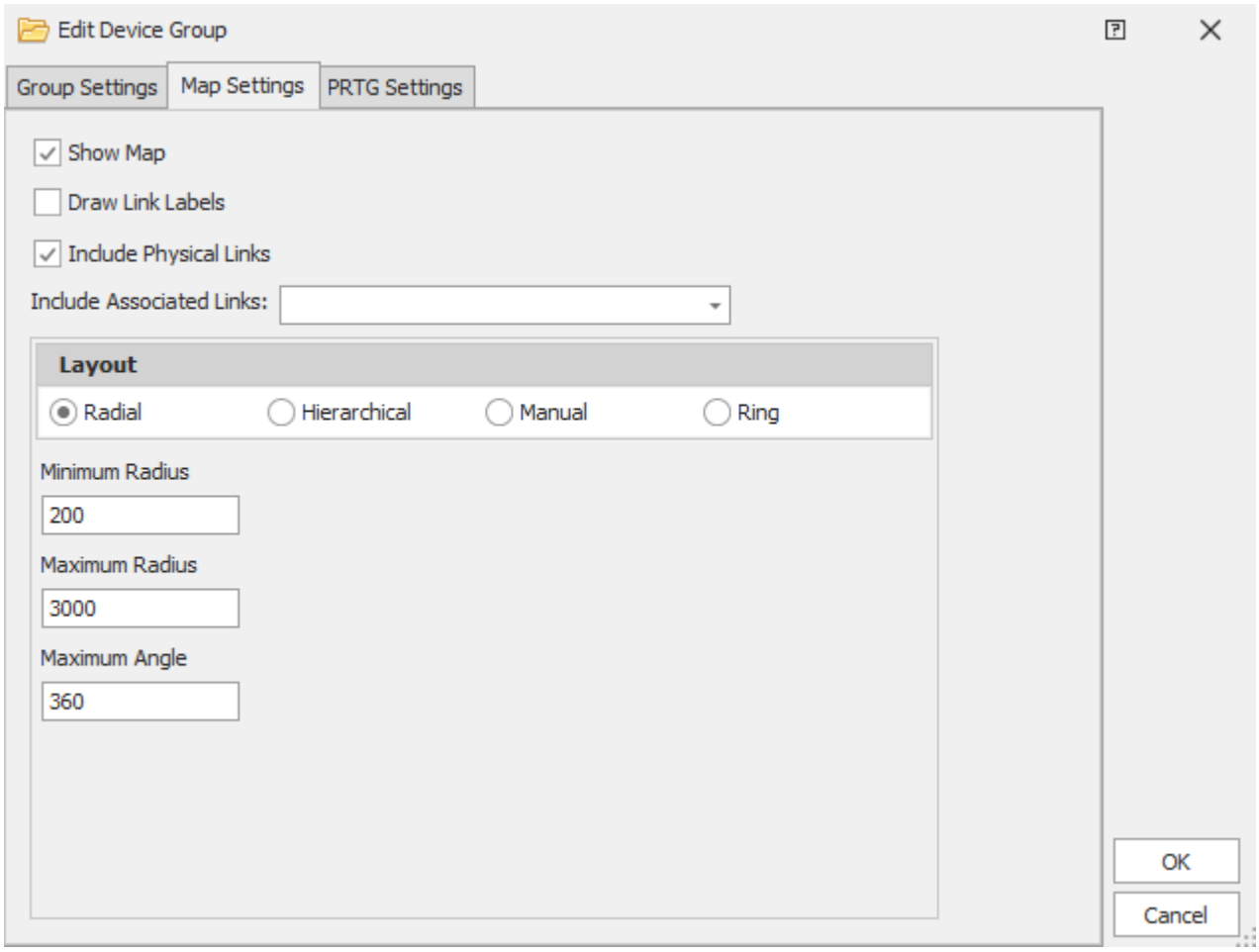
If you are familiar with device filters, you will notice that the 'Primary Devices' and 'Connected Devices' tabs contain the same settings as a device filter. Therefore, when specifying the Primary or Connected devices for a group, there is a 'Copy Device Filter' button that lets you copy the settings from an existing device filter. This can be helpful if there is an existing device filter that contains settings similar to the ones you want to enter for the Primary or Connected devices. See Device Filters for more information.

After modifying the Primary or Connected device settings, there are two things you can do to make sure you have done so correctly:

1) Review the Filter Summary at the bottom of the form. The Filter Summary field always displays a summary of the settings you have entered. This Filter Summary uses a SQL-like syntax to display all of the current settings in one place. It is updated any time the filter settings are modified.
2) Click the Preview button, which will display a list of devices in the currently-open discovery result that will be included in the group

Map Settings

The map settings provide an option of whether to display the map. For larger groups the topology map may not be useful and drawing the map can slow the time required to load and work with the groups. If you have a large group that makes the application slow to respond, and you don't need the map for that group, disabling drawing the map could speed up the application.



Map Layout

Topology maps can be laid out automatically using layout algorithms or manually. When maps are laid out automatically, the layout of each cluster of connected devices is placed on the map from left to right until all the clusters are placed. Any unconnected devices are laid out in a grid above the clusters.

Device Group Folder Editor

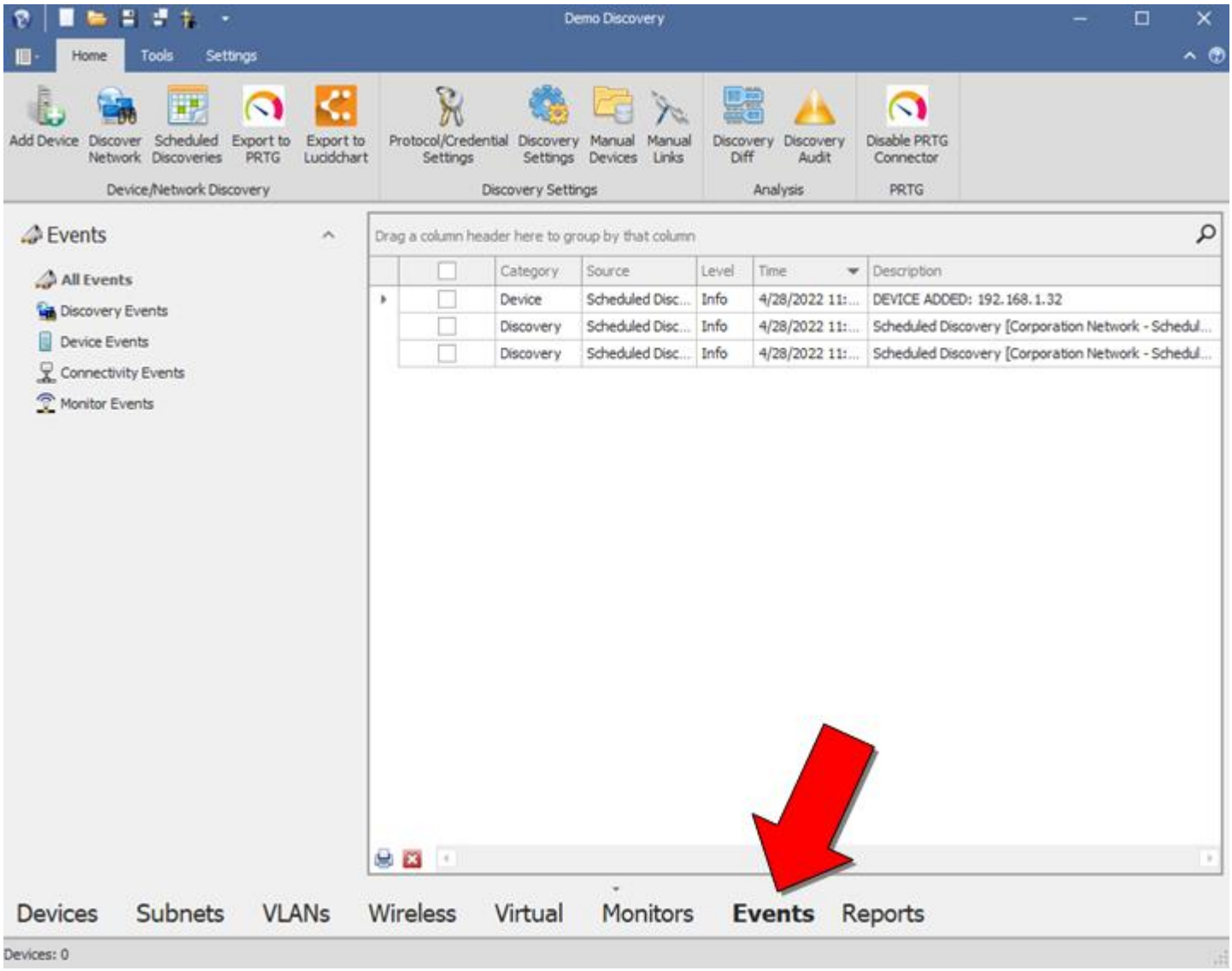
The Device Group Folder Editor is used to specify the properties of a device group folder. This applies when you create a new device group folder, or modify the properties of an existing folder.

Folder Name

The only property you can set for a device group folder is the folder's name. A folder must have a name. It can be anything you want, as long as it's not empty.

Events View

The events tab contains a log of events generated by UVexplorer tasks. As tasks run and generate relevant information, they are configured to log an event is created and posted to the event log. The events can be viewed in the log filtered by type based on the item selected to the left of the grid.



Event Types

All Events

All events are a list of all of the events currently in the event log.

Discovery Events

Discovery events is a filtered view of all the events created by discovery. See Scheduled Discovery Events for more information about events generated by discovery.

Connectivity Events

Connectivity events is a subset of discovery events and is specific to those events related to the network connectivity.

Monitor Events

Monitor events is a filtered view of all of the events created by monitors. See Monitors for more information about events generated by monitors.

Event Grid Operations

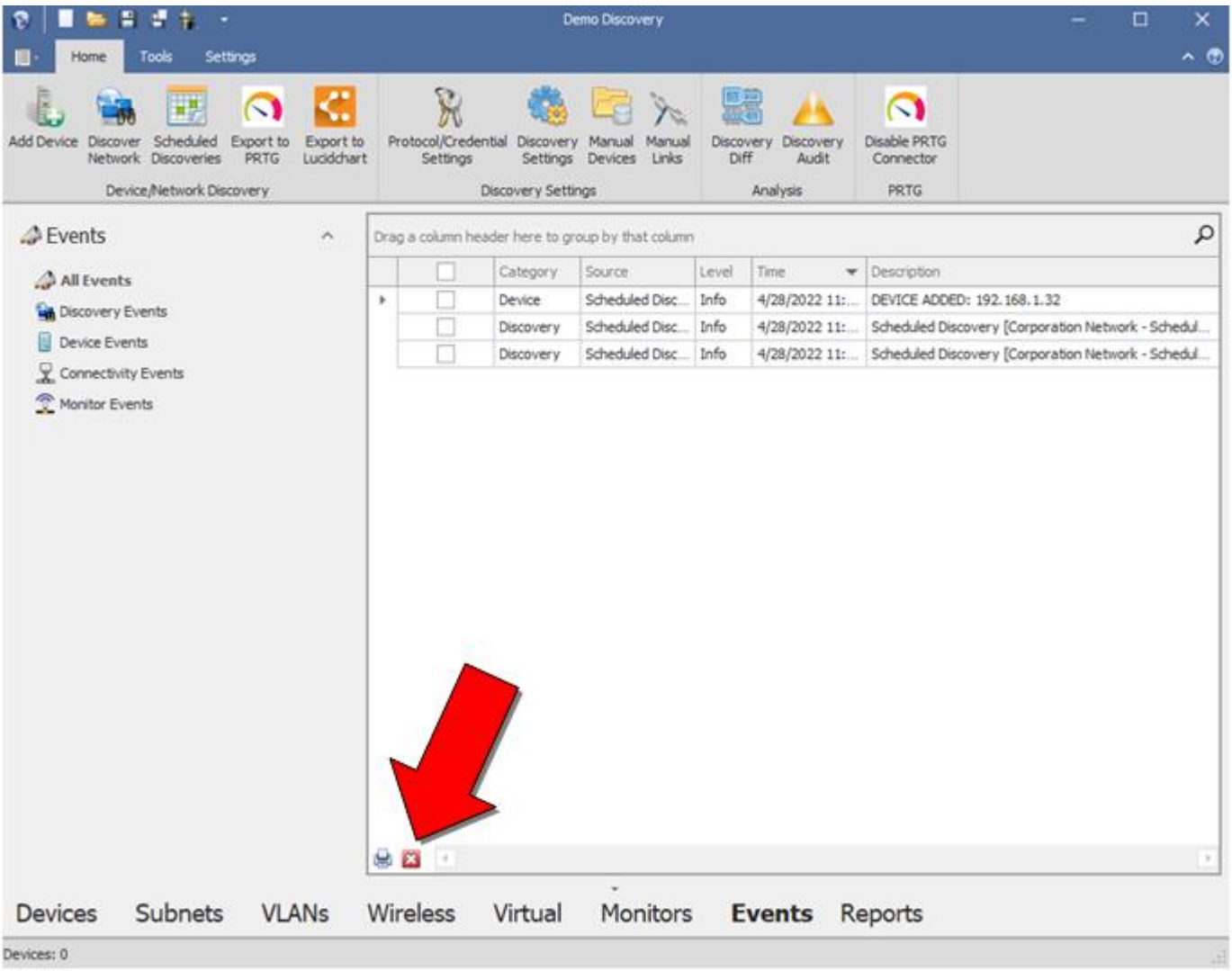
The bottom-left corner of the Events tab contains buttons for performing the following actions:

Refreshing Events

When new events are generated, they are not automatically loaded into the event list. Rather, you can control when the event list is updated with new events. This is done by clicking the Refresh (i.e., circular green arrow) button.

Deleting Events

You can delete events that you no longer want by selecting them, and then clicking the delete button . The row for each event in the list has a check box that can be used to select the event. The check box in the row headings can be used to easily select or de-select ALL events.

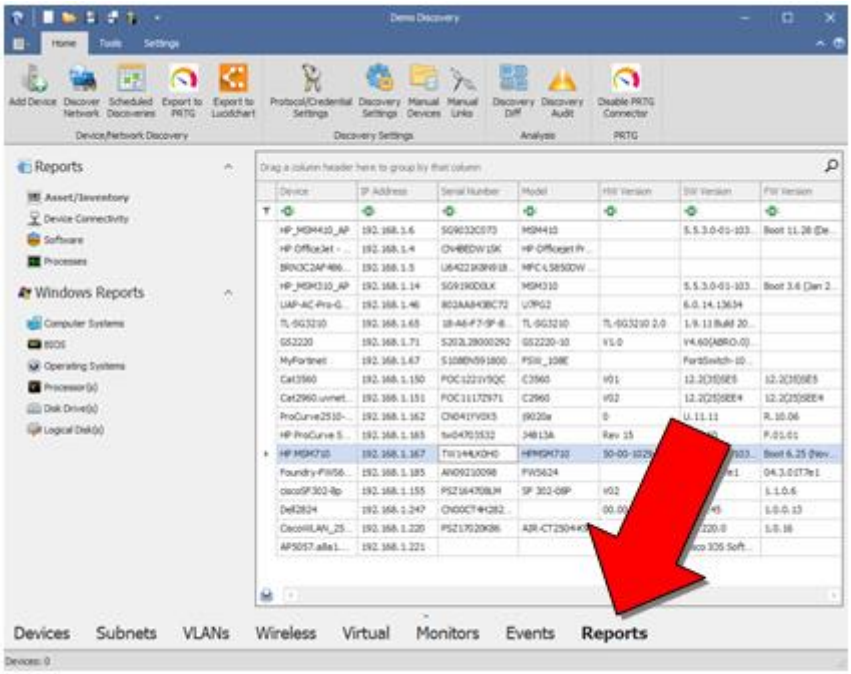


Printing Events

Events can be printed or exported to a PDF file by clicking the print button .

Reports

UVexplorer reports combine specific information from devices in the network into an easy to view and export report.



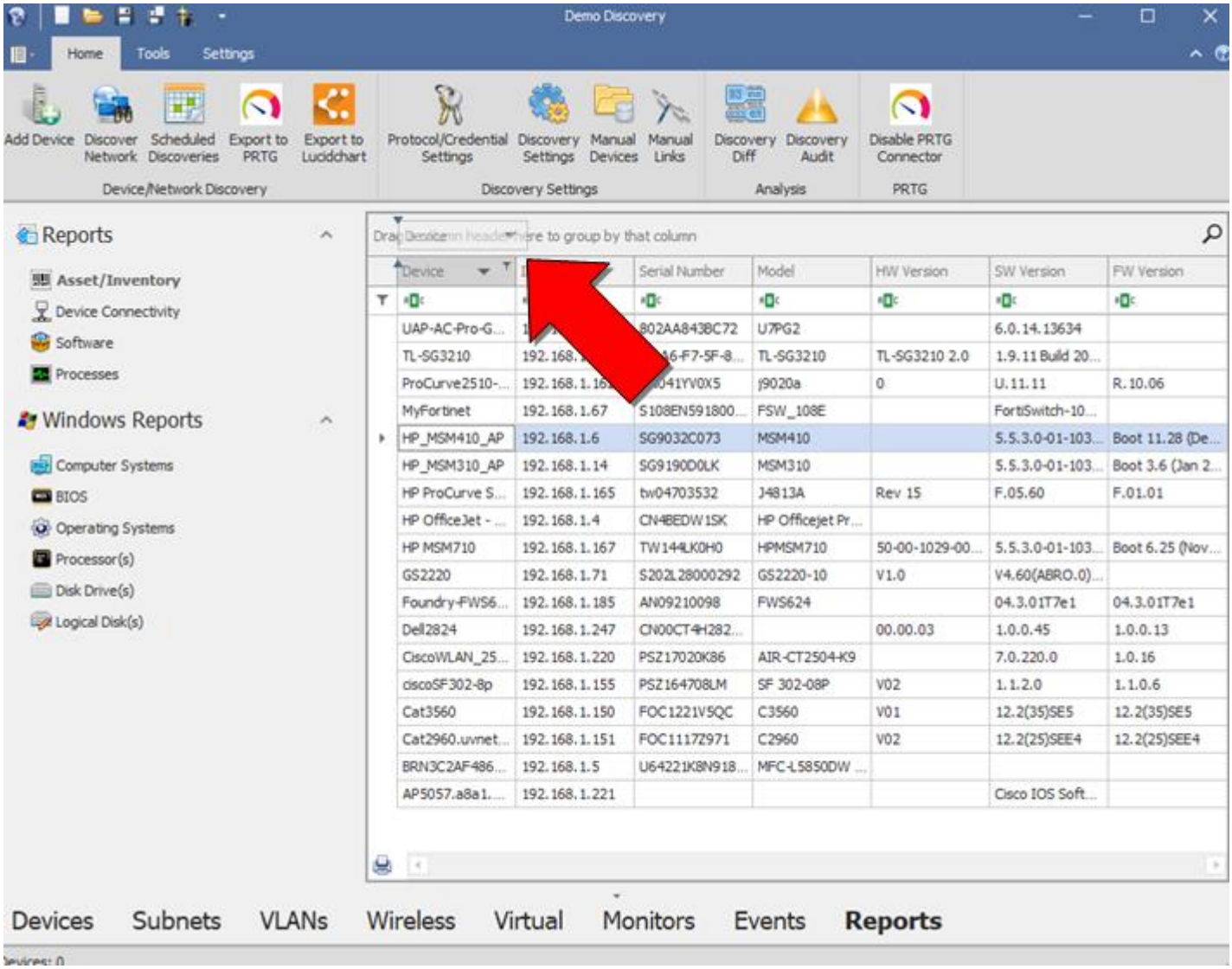
Reports are limited by the number of network interfaces allowed in the license. For example, the 500 network interface license will provide up to 500 network interfaces to be displayed and exported.

Report Operations

Each report contains entries in grid that can be grouped, sorted, filtered, and exported.

Grouping

To group the report by a column, drag the column into the group header at the top of the report. The report entries will be grouped into sections based on the values of the grouped-on column. To group on multiple columns, drag each column to the header in the order you would like them grouped.



Sorting

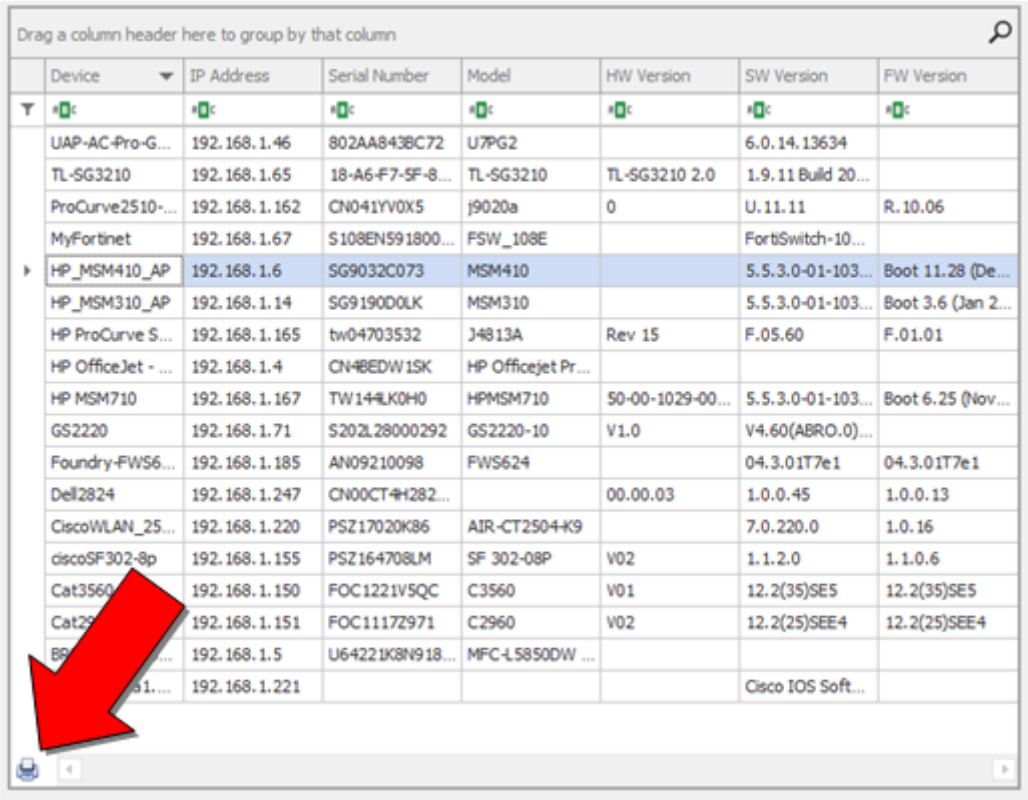
To sort report entries, click on the column headers. To sort multiple columns, sort each column in the order you want them sorted.

Filtering

To filter the values of a column, select the filter icon in the right corner of the column header. A list of values to filter by will be presented. When a value is selected only entries containing that value will remain in the displayed results.

Exporting

To export a report group, sort, and filter it as desired then press the print button in the lower left corner of the report. A print/export dialog will be opened with the current contents of the report grid. The print dialog provides a lot of features to format and customize the report. To print the report, select the 'Print' button in the upper ribbon or the file menu. To save it to a file select the 'Export' button in the upper ribbon or the file menu. The print dialog supports exporting to several file formats including image, csv, html, and xsl.



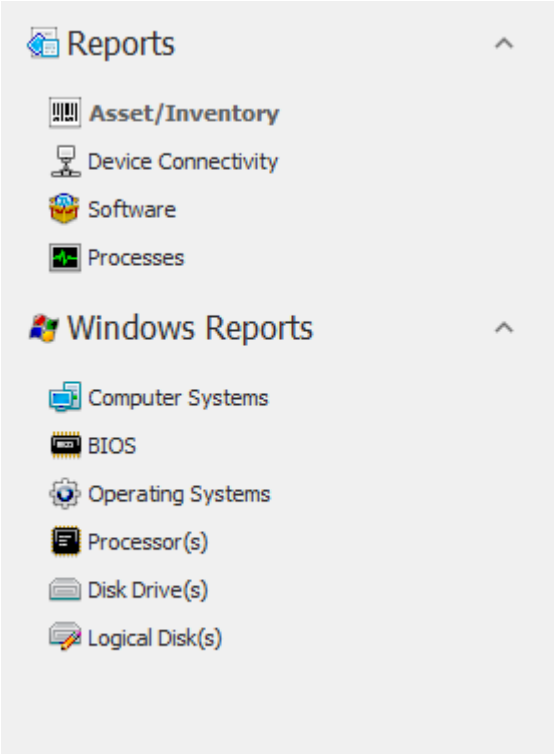
Report Types

UVexplorer reports are categorized into data collected from windows machines using windows protocols and data collected from other devices typically using SNMP standard MIBs. To capture information presented in the reports valid SNMP and Windows credentials must be provided during discovery.

Reports

The reports in the reports section contain device data typically collected from network devices using SNMP standard MIBs.

The available reports include:



Asset/Inventory
The asset and inventory report contains device system information such as the Serial Number, Model, Software Version, and Hardware Version.

Device Connectivity
The device connectivity report contains the network device connectivity links including the devices in the link and the interfaces they are connected on.

Software
The software report contains entries for installed software on devices in the discovery result.

Processes
The processes report contains entries for the running processes on devices in the discovery result.

Windows Reports

The report in the windows reports section contain device data collected from windows machines using data read from standard windows tables

Computer Systems
The computer systems report contains the device computer system information including the model, manufacturer, and warranty.

BIOS
The BIOS report contains the BIOS information of the device including the version, serial number, and install date.

Operating Systems
The operating systems report contains the operating system information of the device including the version, serial number, and install date.

Processors
The processors report contains the processor information of the device including the name and description of each processor on the device.

Disk Drives
The disk drives report contains the hard disk drive information of the device including the name, serial number, model, and size.

Logical Disks
The logical disk drives report contains the logical disk drive information of the device including the name, size, and free space.

GroupLink HelpDesk

The GroupLink HelpDesk page provides a way to export discovery data from UVexplorer into a GroupLink everything HelpDesk instance.

The HelpDesk page provides the following navigation pane options:

GroupLink eHD

The GroupLink eHD page provides information and links on buying an everything HelpDesk solution.

Settings

In-order to export information to an everything HelpDesk instance UVexplorer must be configured with the correct settings necessary to connect with the HelpDesk server. Selecting the 'Settings' item will open a dialog for configuring the base URL of the HelpDesk server and the start URL of the API for importing data into the HelpDesk server.

Export Assets

The export assets item will open the export dialog used to export the network asset information to everything HelpDesk.

The export dialog contains the following settings:

Target HelpDesk Settings

The target HelpDesk settings contains the Base URL of the HelpDesk server instance and the help desk user credentials required to authenticate with the server.

Asset Settings

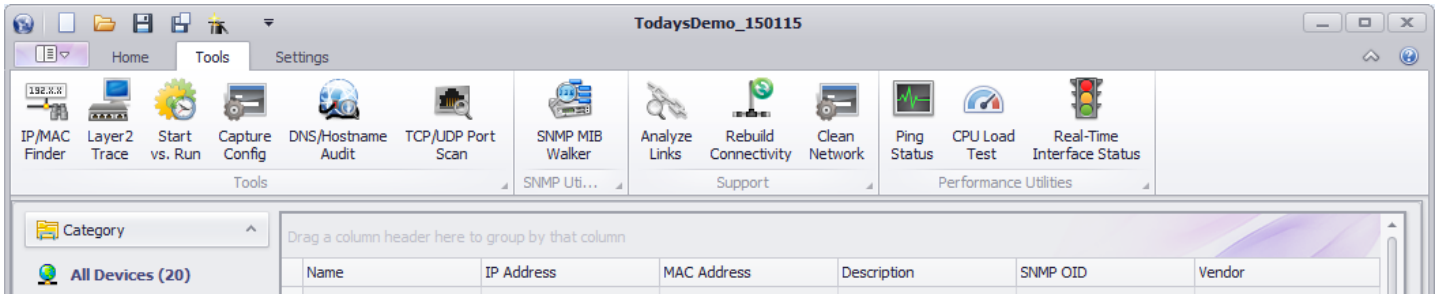
The asset settings allow you to define the attributes associated with the exported settings when they are imported into the help desk instance. The available values for the assets are read from the HelpDesk instance after the connect button is pressed.

Devices

The devices list is a device picker to select which devices to export to the help desk server.

Using Network Tools

Network tools allow network administrators to perform common device operations and queries from one simple location. By using UVexplorer discovery results, together with device groups, filters, and topology maps, administrators can easily see and filter devices into groups for performing operations such as checking real time statistics and capturing configurations.



Accessing Tools

Network tools are available in the Tools tab on the main view of UVexplorer, or through context menus on the device grid or the topology map.

Network Tools

For details about the available network tools see the following:

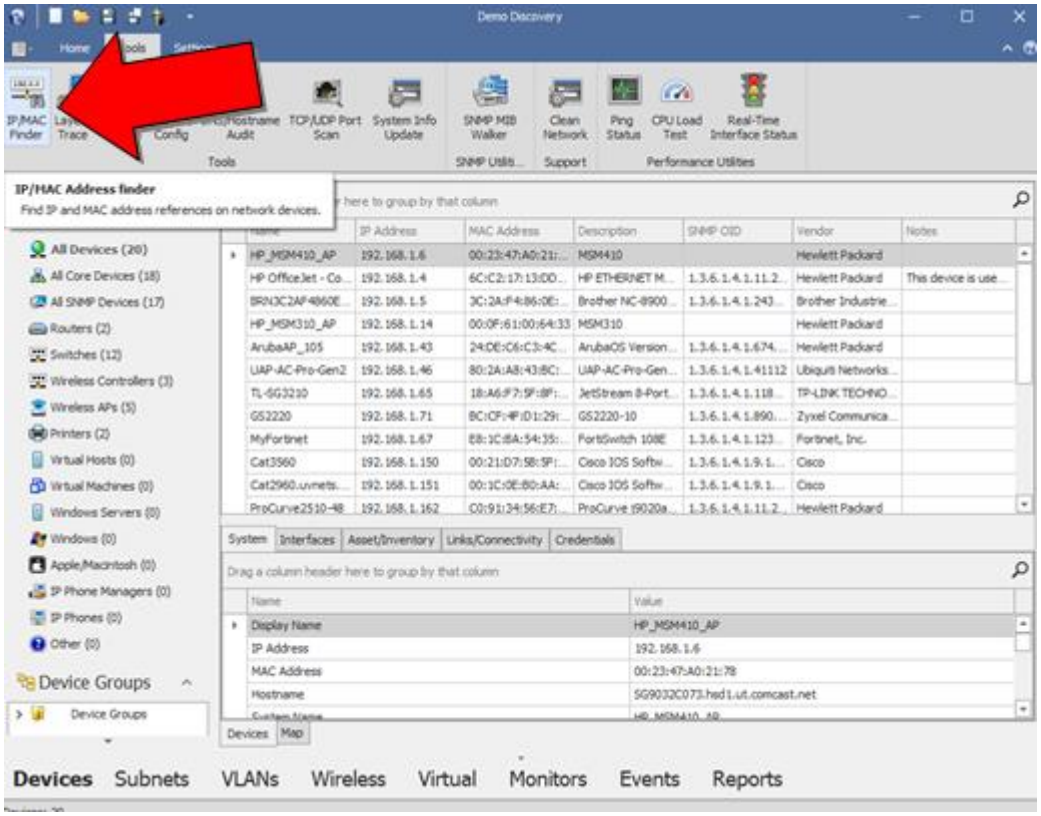
IP/MAC Address Finder
Layer 2 Trace
Startup vs. Running configuration
Configuration Capture
DNS/Hostname Resolver
Port Scanner
SNMP MIB Walker
Ping Response Poller
CPU Load Poller
Interface Status Poller

IP/MAC Address Finder

The IP/MAC Address finder tool allows you to find all references to an IP or MAC Address within the discovery results. In addition, this tool will help identify any device or interface that may own the address. Find results will also include references to the where the address was "found" including but not limited to ARP caches, forwarding databases, or discovery protocol tables.

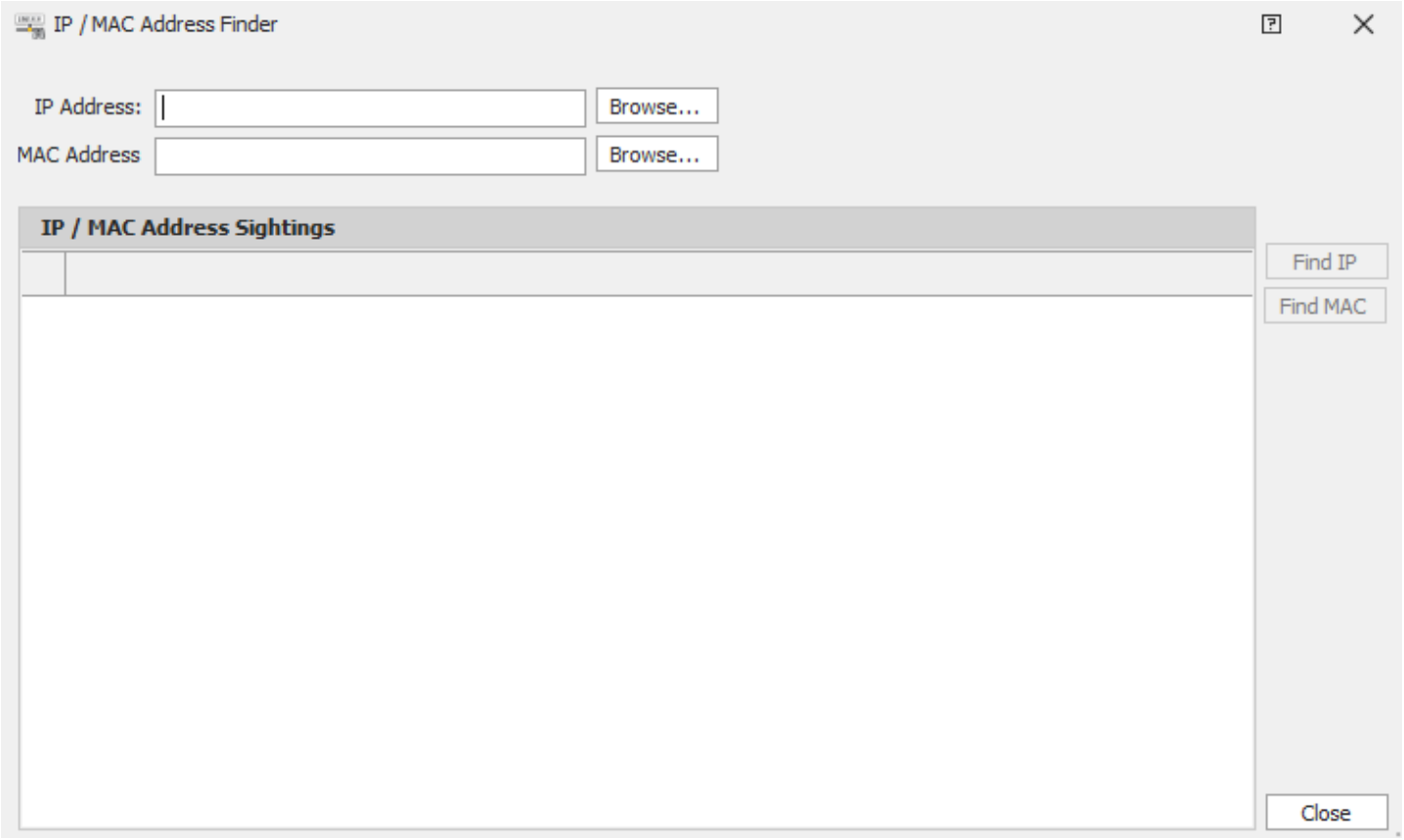
Launching the IP/MAC Address Finder

The IP/MAC address finder can be launched from the 'Tools' tab available on the main page of UVexplorer.



Using the IP/MAC Address Finder

The address finder can use either an IP or a MAC address or both. If both an IP address and a MAC address are provided all find results will be for references that include both the IP and MAC address.



IP Address

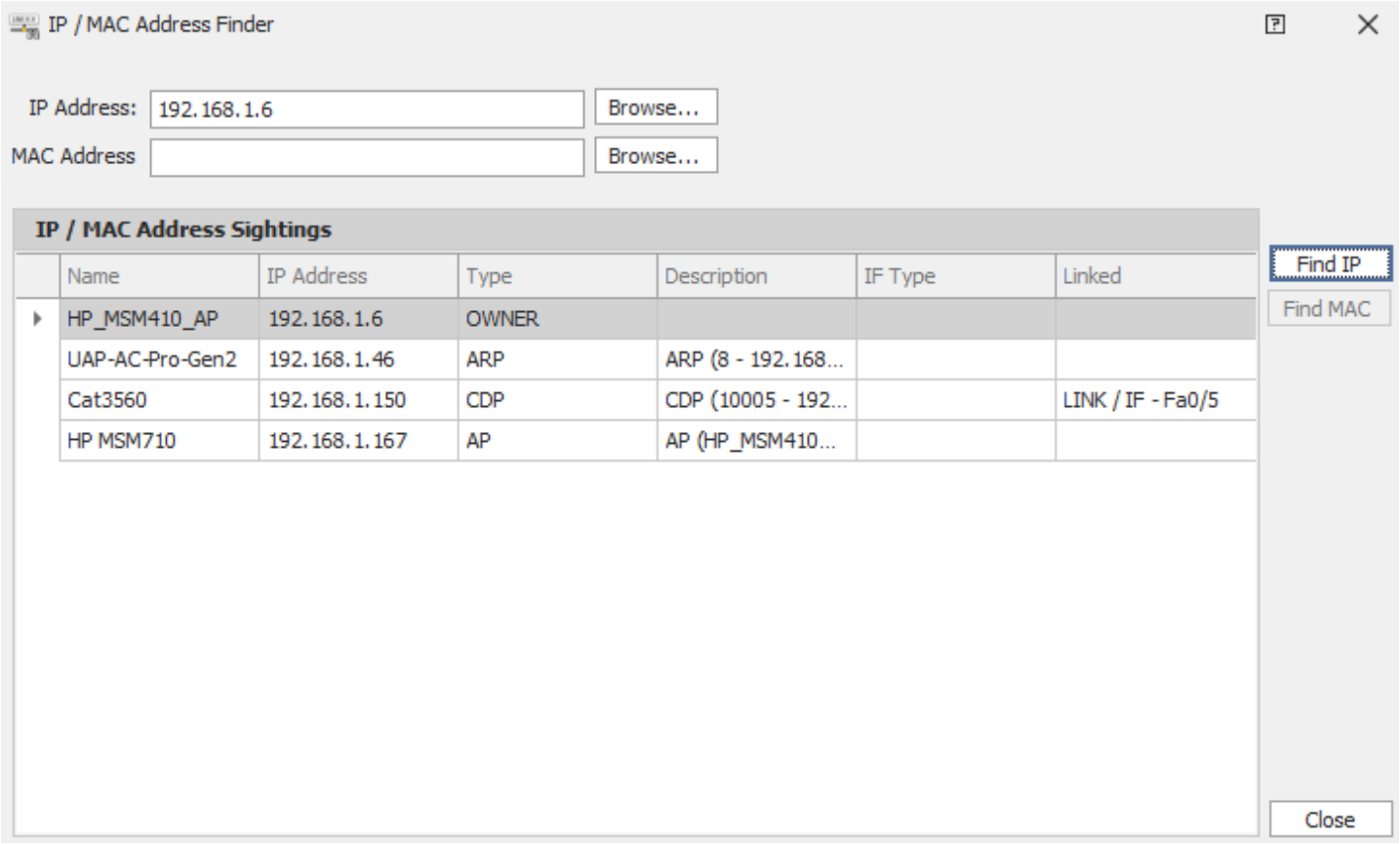
To provide an IP address you can either type in the address manually or select one using device selector. When using the device selector, the IP address used will be the primary IP address of the selected device.

MAC Address

To provide a MAC address you can either type in the address manually or select one using the device selector. When using the device selector, the MAC address used will be the primary MAC address of the selected device.

Searching

To begin the search, after providing a valid IP or MAC address, press the 'Find' button. The address finder will search the discovery result for any devices with a reference to that address. When the search is completed, the results will be displayed in the result table.



Address finder results

Name

The 'Name' column contains the display name of the device with the reference to the searched address.

IP Address

The 'IP Address' column contains the IP address of the device with the reference to the searched address.

Type

The 'Type' column indicates what type of sighting was used to generate the result. Possible values are:

FDB (Forwarding Database),
ARP (Address resolution protocol table),
CDP (Cisco Discovery Protocol),
IP_ROUTE (IP address route table),
AP (Wireless Access Point),
AP_CLIENT (Wireless Access Point Client),
LLDP (Link Layer Discovery Protocol),
STP (Spanning Tree Protocol),
VIRTUAL_MACHINE,
VIRTUAL_HOST,
OWNER (Address belongs to the resulting sighting device),

Description

The 'Description' column contains a description of the sighting type. In addition to the sighting type, it will contain other information relevant to the sighting type. For example, if the sighting is from a data table such as CDP it will contain the entry index.

Linked

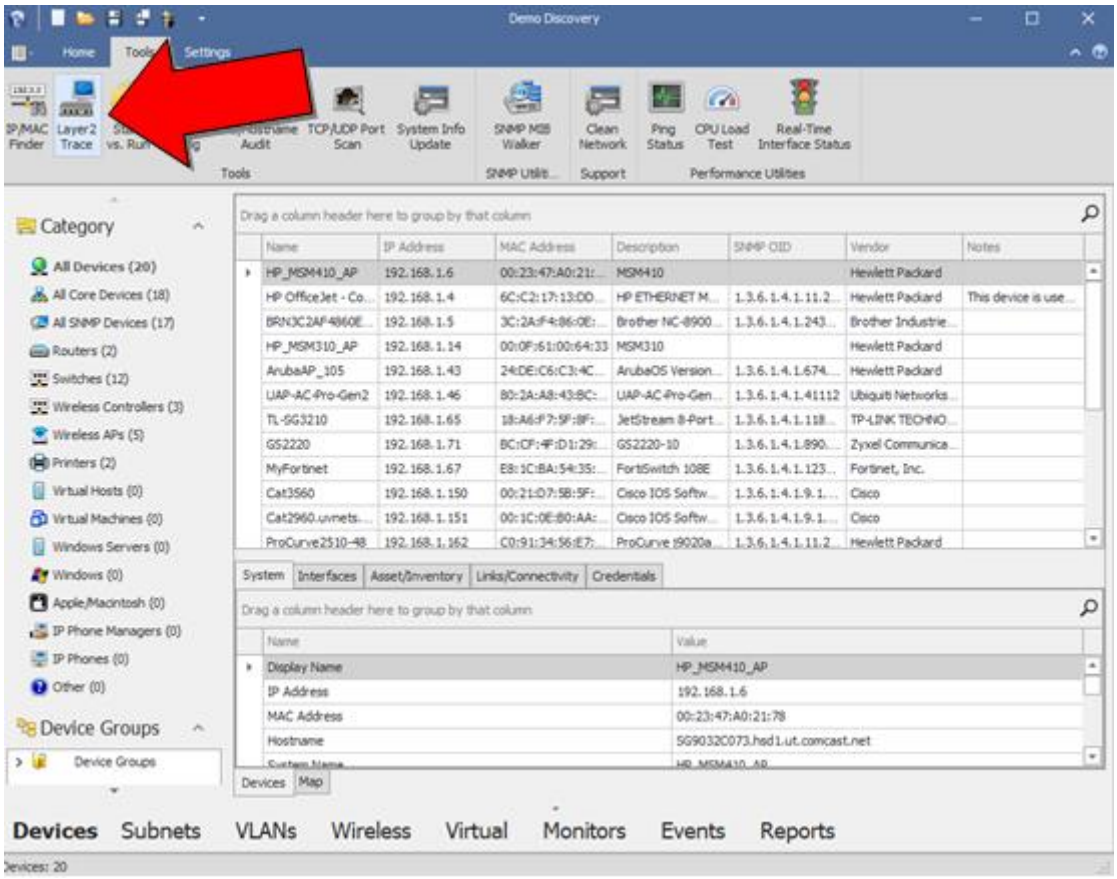
If the interfaces involved in the sighting participate in a connectivity link such as CDP and LLDP, the linked column will contain details about the members of that link.

Layer 2 Trace

The Layer 2 Trace tool uses the network discovery results to calculate the path between two devices. The path is calculated using the connectivity results for the currently loaded discovery result.

Launching Layer 2 Trace

The Layer 2 Trace tool can be launched from the 'Tools' tab available on the main page of UVexplorer. Layer 2 Trace is also available from the device context menu in either the device grid or the topology map. When launched from the map the layer 2 trace tool is populated with the selected device. When launched from the map if two devices are selected both devices are populated in the tool. If more than three devices are selected the tool will not be populated with any devices.

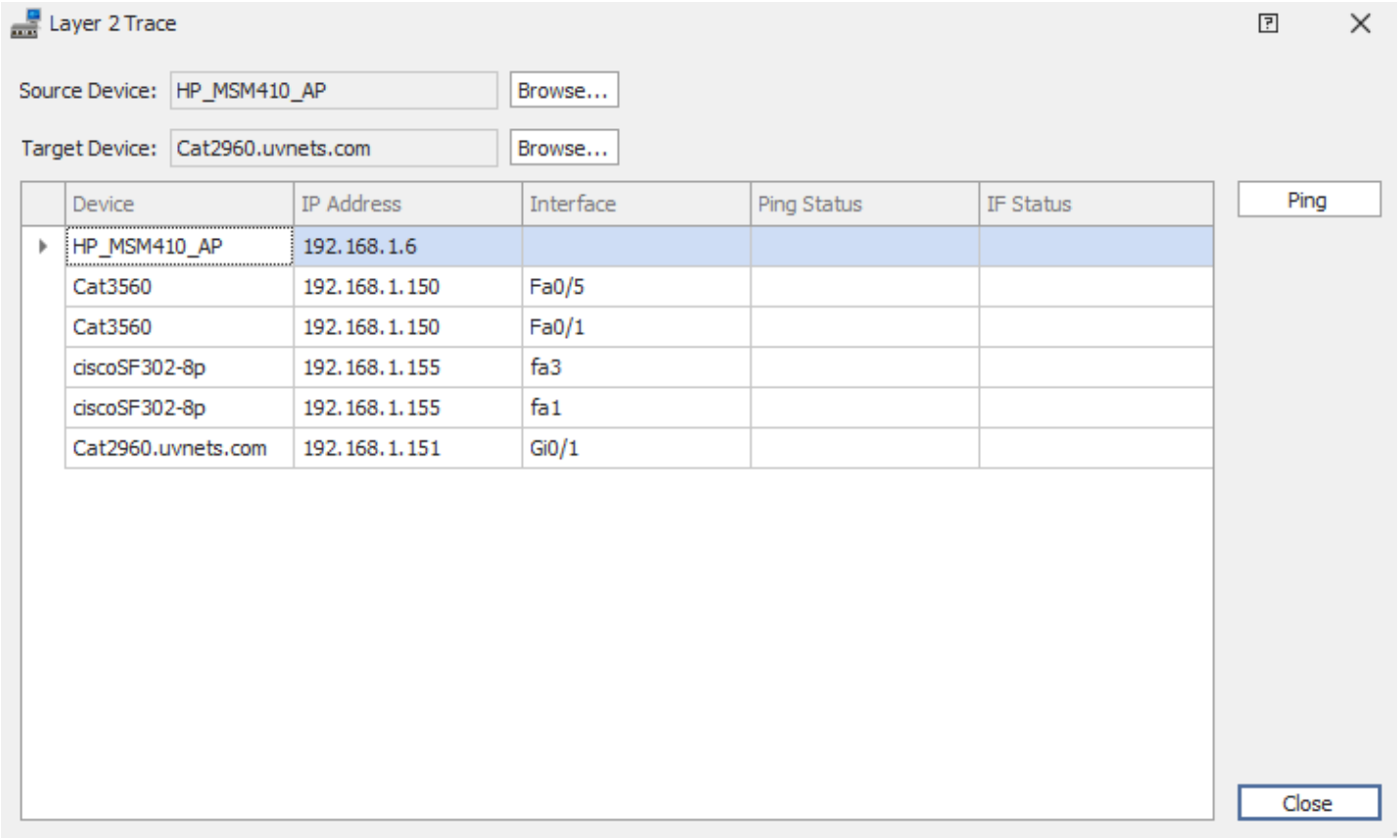


Using Layer 2 Trace

To perform the trace both a source and target device must be selected. The device that is chosen as the source will not affect the results other than to reverse the direction of the trace. If there is no calculated path between the devices the results will display a message indicating such. Once both devices are selected the results of the trace will be displayed in the results grid. The trace results contain each device participating in the trace path beginning with the source device and ending with the target. If any network devices are involved in the path they will be displayed in-order. A network device will usually participate in the path twice once on the interface connecting to the source path and once on the interface connecting to the target path; in some cases, these interfaces will be the same and will appear only once. Since the path represents an ordering sorting of the results is unsupported.

Once the devices are selected and the trace is displayed, the status of the current path can be found by pressing the 'Ping' button. The ping operation will attempt to both ping the device and query the interface status of the device (where available). The interface status query will only be performed if the device has an interface involved in the link and valid SNMP credentials are associated with the device. See Managing Device Credentials for more information about associating credentials.

Layer 2 Trace results



Device

The 'Device' column contains the display name of the device participating in the trace path.

IP Address

The 'IP Address' column contains the primary IP address of the device participating in the trace path.

Interface

The 'Interface' column contains the display name of the device interface participating in the trace path.

Ping Status

The 'Ping Status' column displays the UP or DOWN status of the ping attempt. This column will only be populated if the ping operation has been performed.

IF Status

The 'IF Status' column displays the interface UP or DOWN status for the interface participating in the

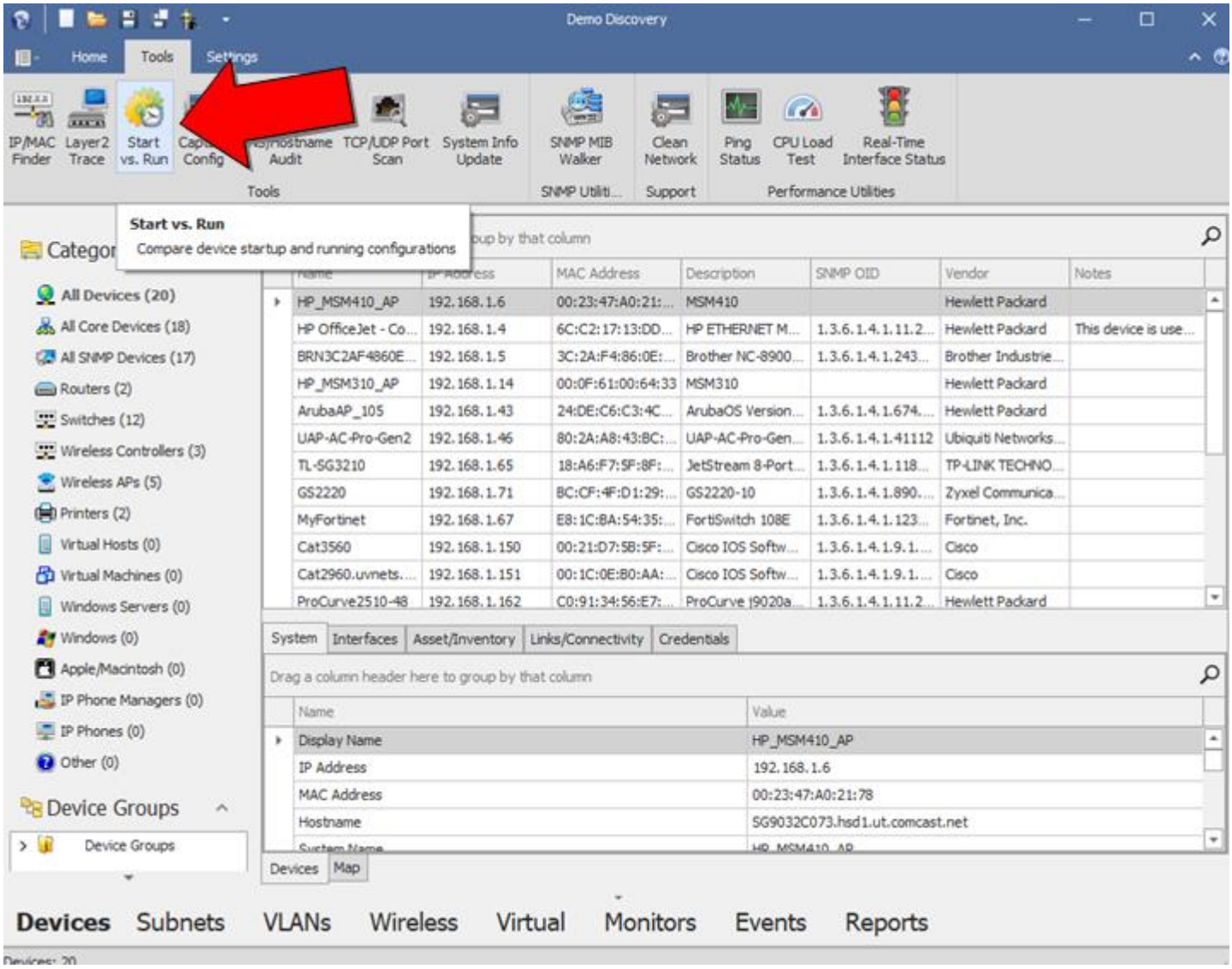
trace path.

Startup vs. Running Configuration

The startup vs. running configuration provides a quick way to compare the startup and running configurations of the device. See Capturing Device Configurations to learn more about device configurations and how UVexplorer collects and stores them.

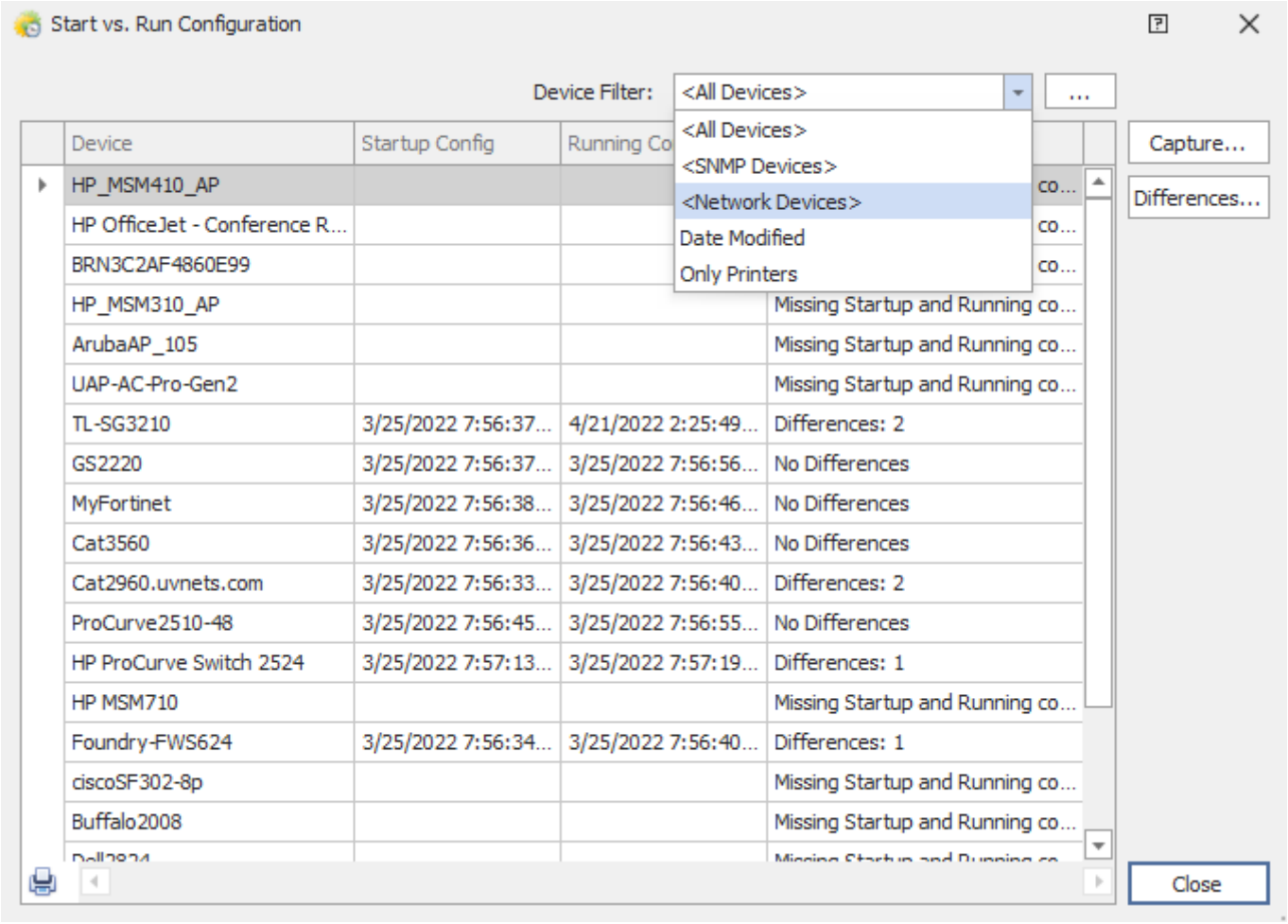
Launching Start vs. Run tool

The start vs. run tool can be launched from the 'Tools' tab in the main UVexplorer view.



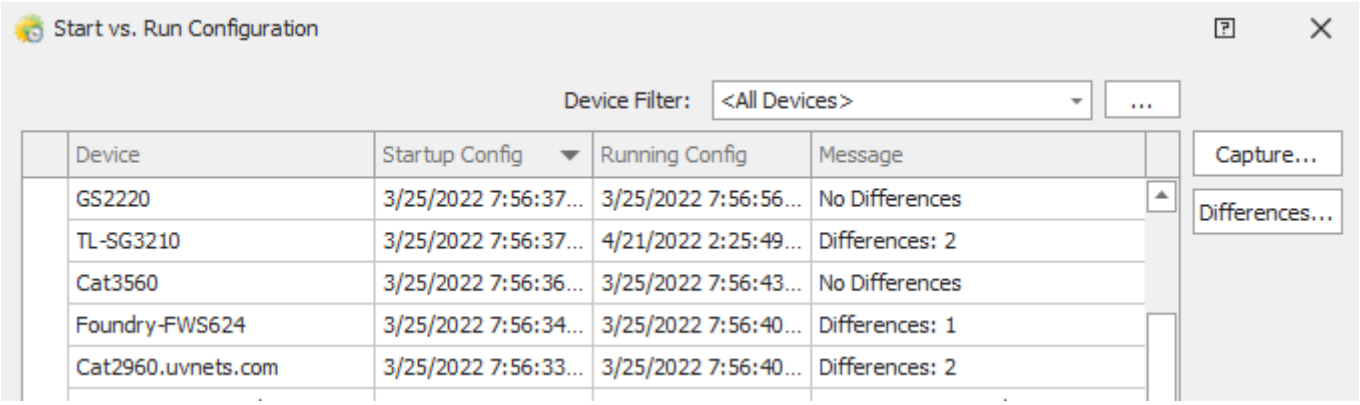
Using Start vs. Run

The start vs. run tool operates on a group of filtered devices. To filter which devices to include in the comparison change the device filter using the 'Device Filter' combo box. Filters can be managed by selecting the button next to the filter combo box. See Device Filters for more information about managing device filters.



Start vs. Run Results

Once a group of filtered devices is selected the start vs run configuration comparison is performed. Each device in the group will be displayed in the results grid with the accompanying comparison summary.



Device

The 'Device' column contains the display name of the device.

Startup Config

The 'Startup Config' column will display the time the startup configuration was captured.

Running Config

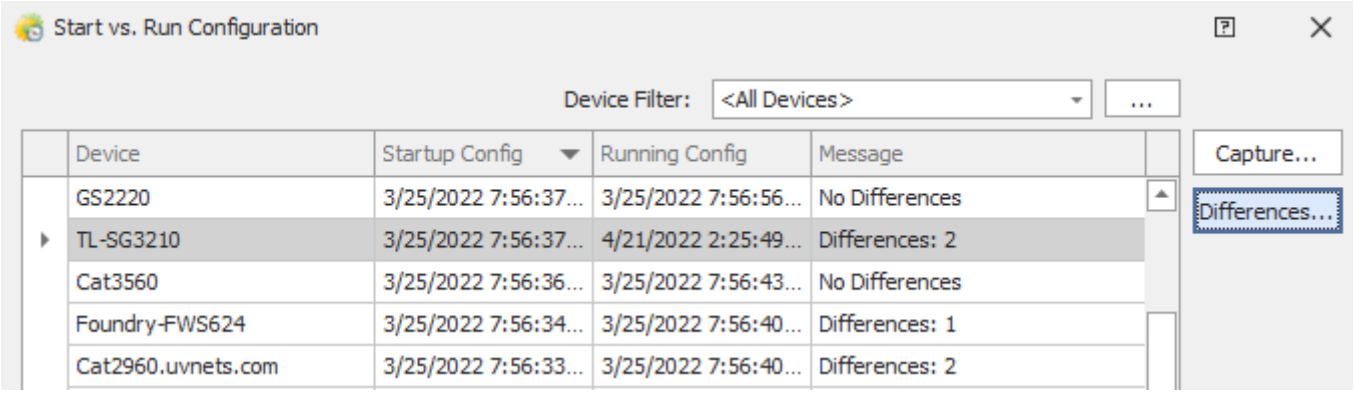
The 'Running Config' column will display the time the running configuration was captured.

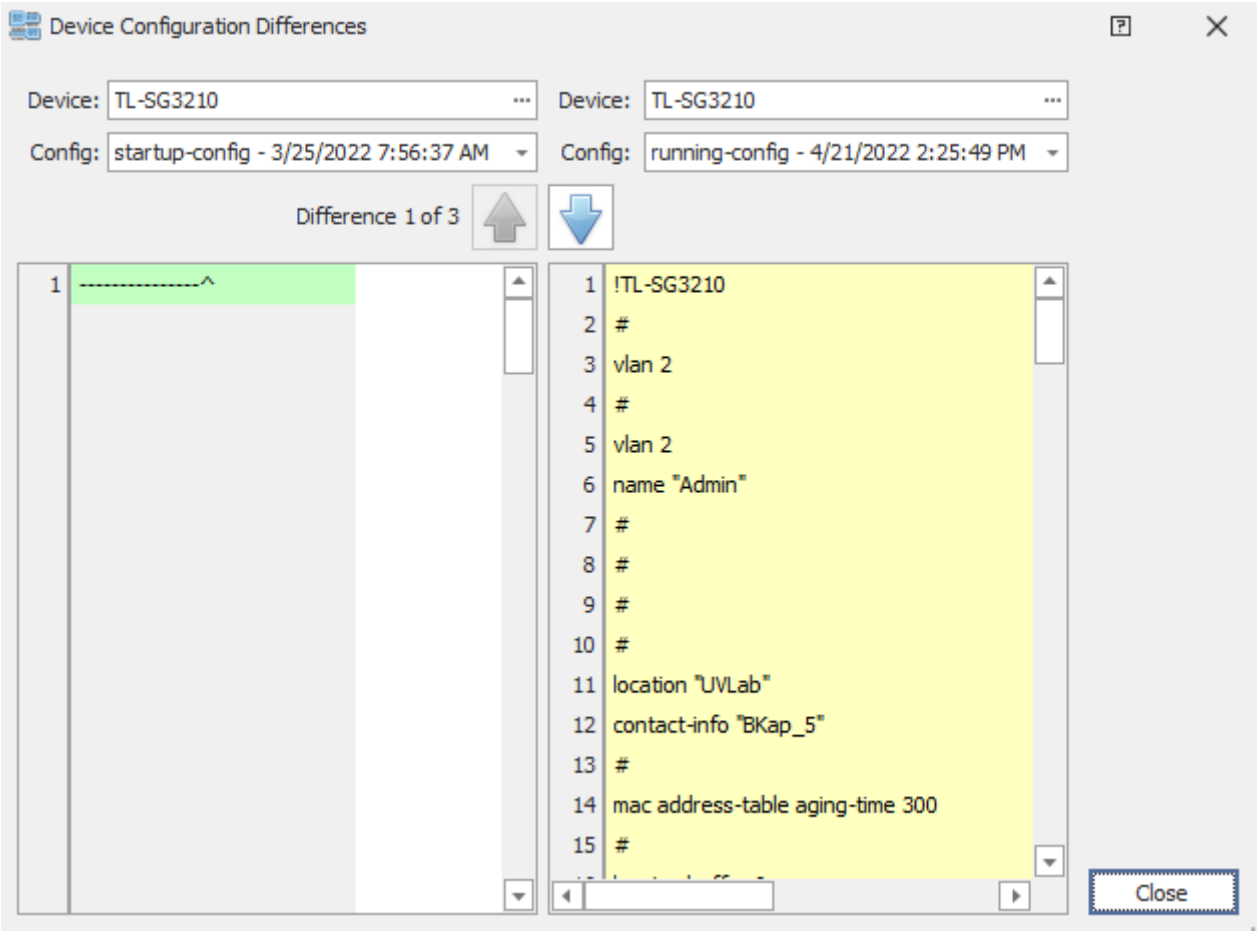
Message

The 'Message' column will display a message about the comparison result. The message will tell you if there is a missing configuration, if there are no differences, or the number of differences.

Viewing Differences

To view a side-by-side comparison of the differences select a device and press the 'Differences' button. See Comparing Device Configurations for more information about configuration differences.

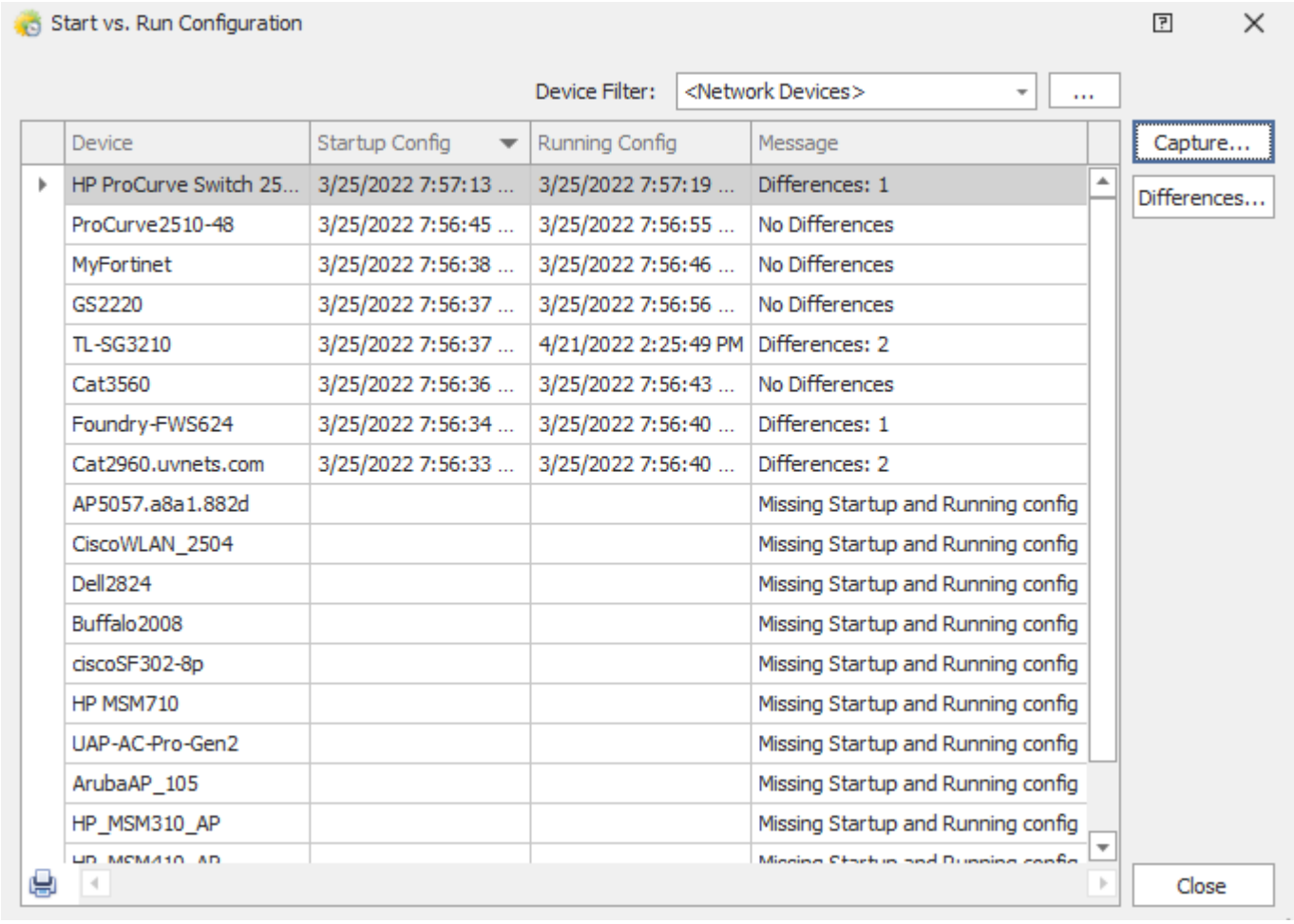


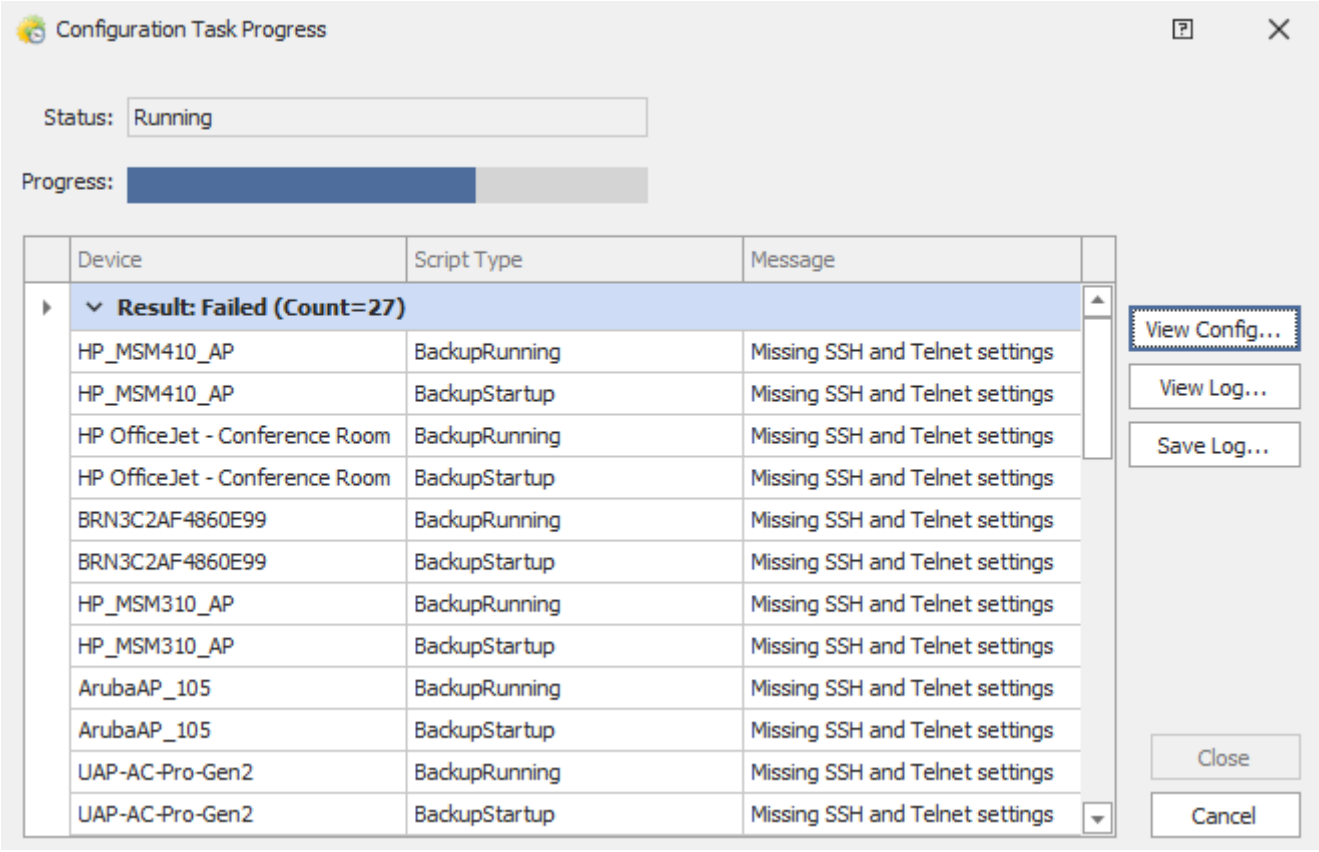


Capturing Configurations

If either configuration is missing, or if you would like to collect more recent configurations for the

device, you may capture the configurations by pressing the 'Capture' button. The capture button will attempt to collect the startup and running configurations for all the devices in the filtered device set. The configuration task progress form will be displayed. Once the captures are completed, and the progress form closed, the configuration comparison results will be updated. Devices must have Telnet or SSH credentials assigned to them for the capture to work.





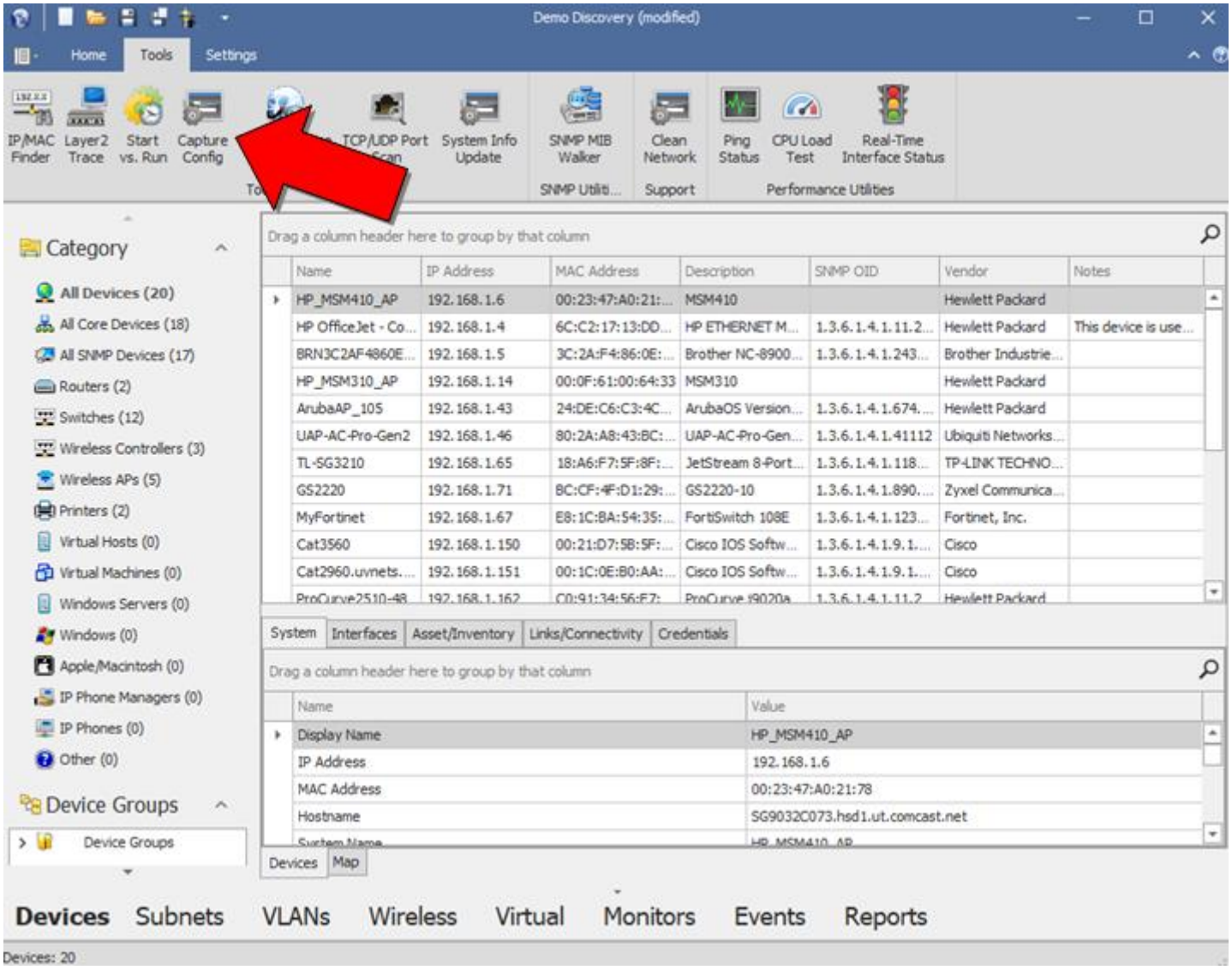
See Configuration Task Progress for more information on configuration capture progress.
See Capturing Device Configurations for more information about capturing configurations.

Configuration Capture

Device configurations can be captured for a single device using the Capture Configuration tool.

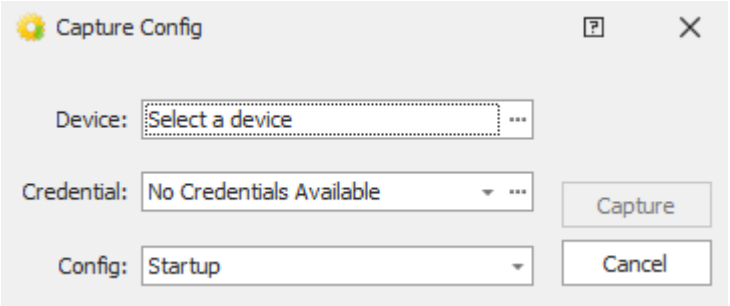
Launching Configuration Capture

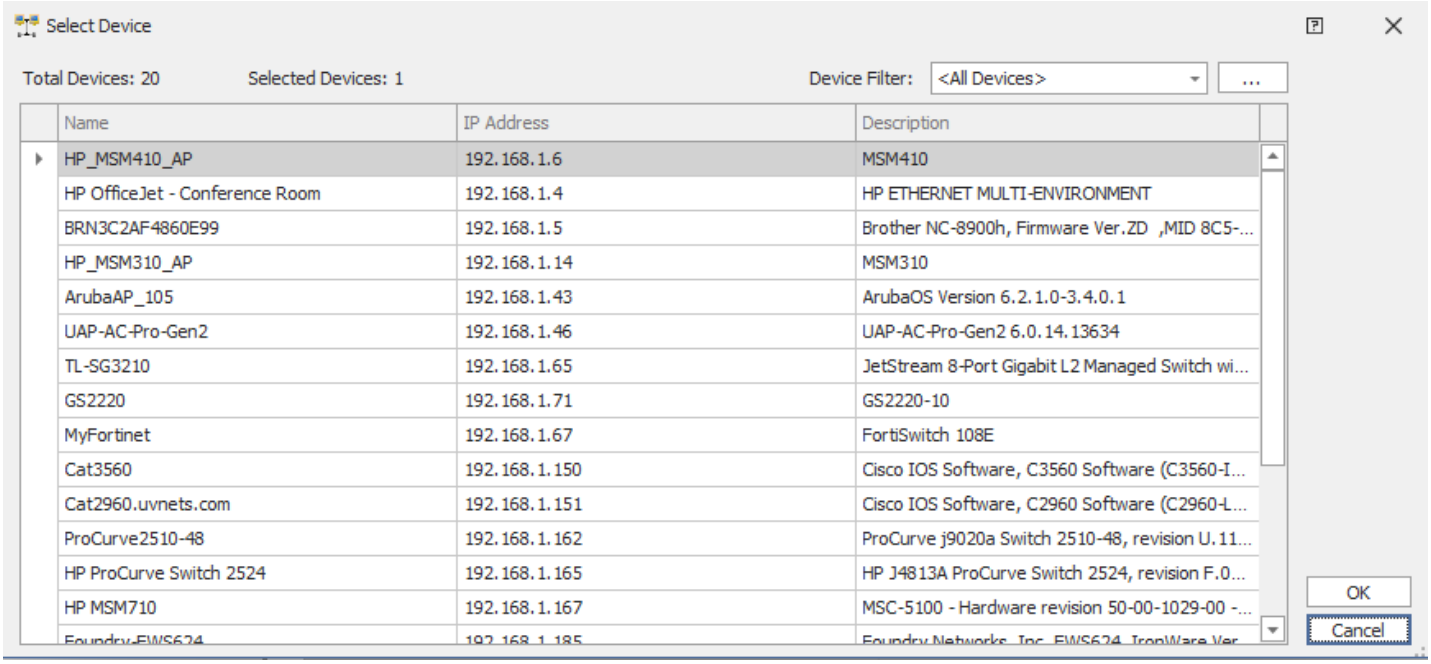
The configuration capture tool can be launched by selecting the 'Capture Config' context menu item from the device context menu. The device context menu is available by right clicking the device in the Device List, or on the Topology Map. The tool is also available in the 'Tools' tab on the main view of UVexplorer.



Using Configuration Capture tool

In the capture configuration tool, you can select the device and the credential to use during the configuration capture. Either Telnet or SSH credentials must be used to connect with the device. Devices that do not provide a command line terminal are not supported at this time. You can choose to capture either the Startup or Running configuration or both. Once you have selected the device, credentials, and configurations you want to capture select the 'Capture' button and the configuration capture process will begin. The task progress form will be launched to display the task progress.





When the configuration capture is complete the configuration will be available for viewing on the device properties configuration tab.

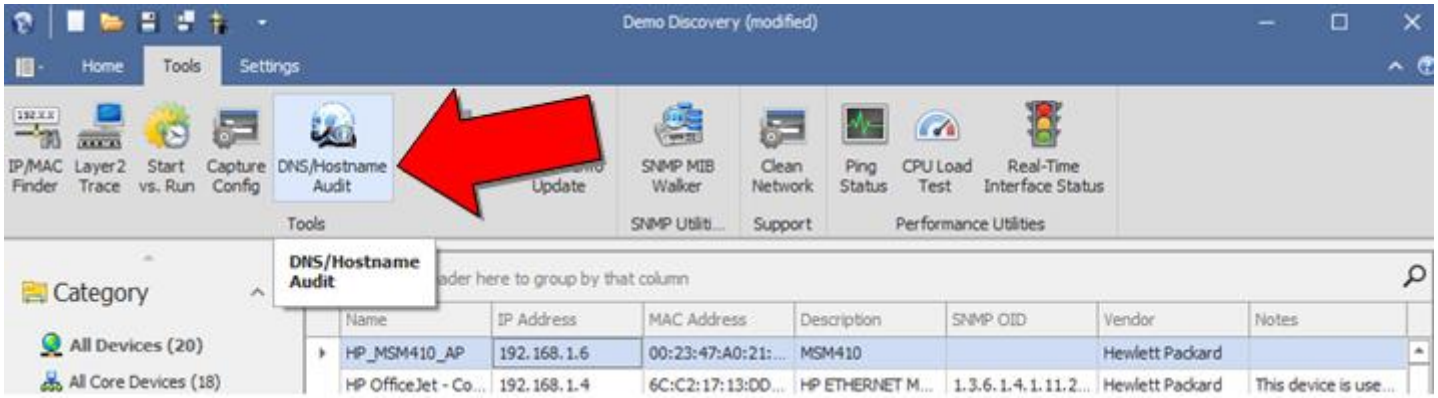
See Configuration Task Progress for information on the task progress.
See Viewing Configuration Captures for more information on viewing configurations.
See Saving Configuration Captures for more information on how configurations are stored.

DNS/Hostname Audit

The DNS/Hostname Audit tool provides a simple interface for resolving IP Addresses and Hostnames to the DNS server for a range of IP Addresses. The resolver will perform a reverse and forward lookup for the IP Address and the DNS name. The results will allow you to audit whether IP Addresses and HostNames are resolving correctly.

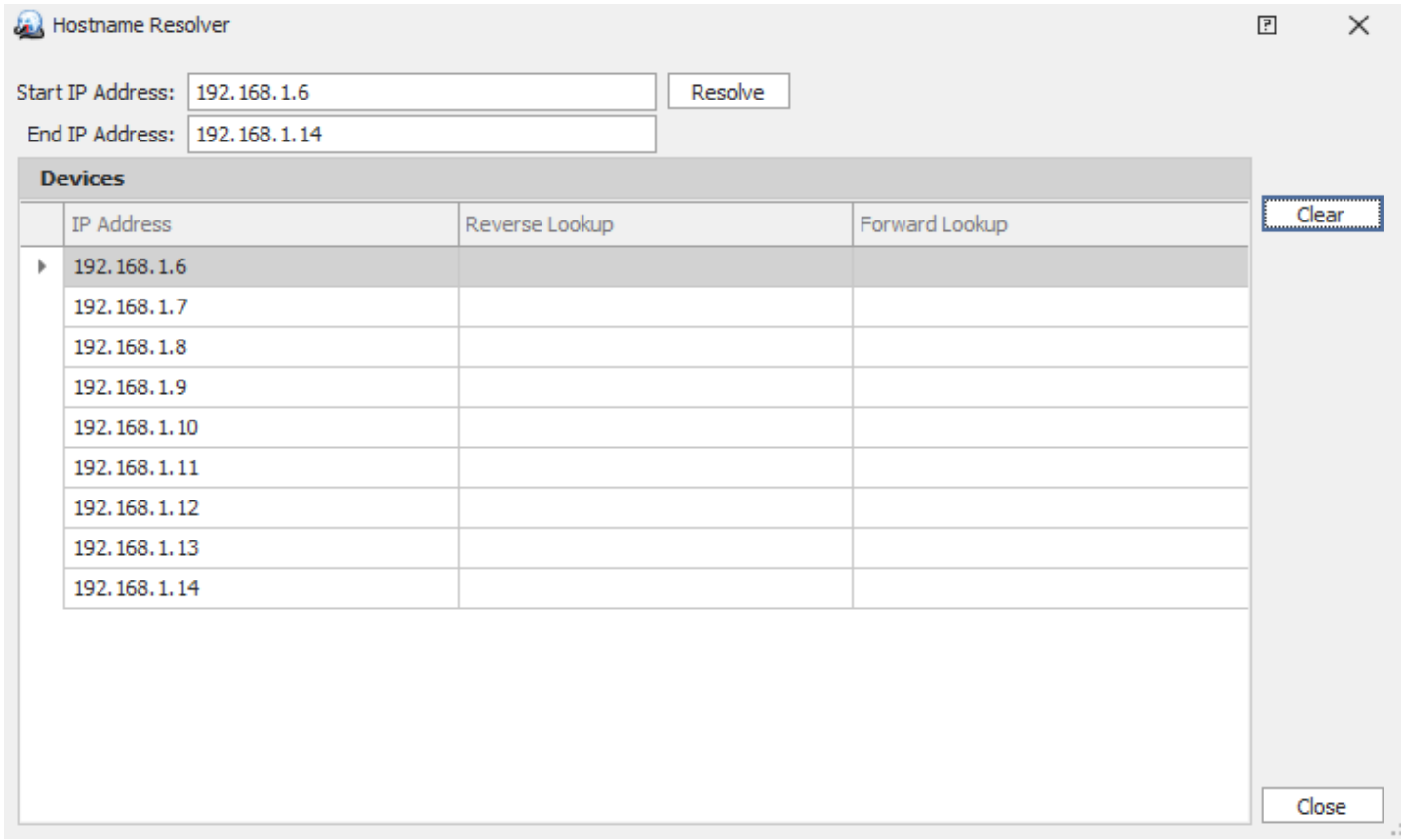
Launching the Audit

The DNS/Hostname resolver can be launched from the 'Tools' tab in the main view of UVexplorer.



Using the resolver

To resolve a range of IP addresses you provide a start and end IP address for the range. Once a valid start and end IP address are provided select the resolve button to resolve the IP addresses in the address range. When the resolution is complete, the results will be displayed in the results grid.



Viewing the results

IP Address

The 'IP Address' column contains the IP address from the resolution range.

Reverse Lookup

The 'Reverse Lookup' column displays the name the IP Address resolved to in the reverse DNS lookup.

Forward Lookup

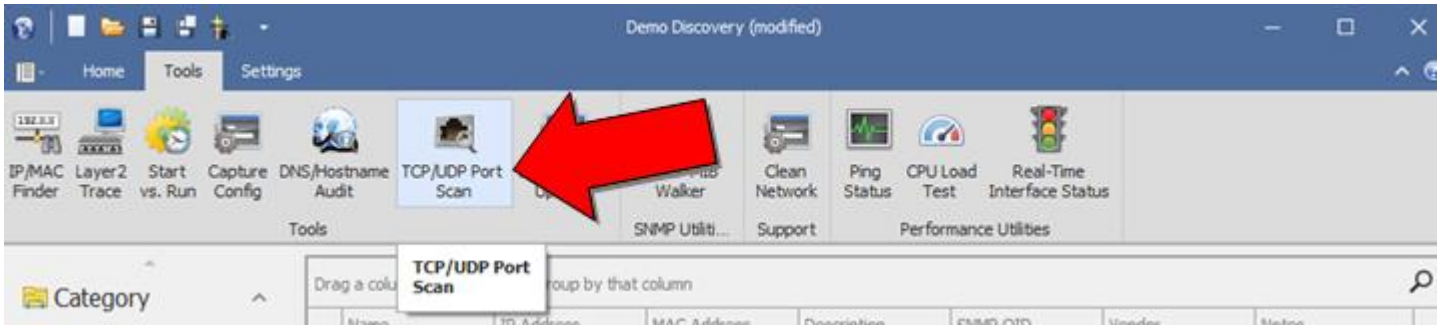
The 'Forward Lookup' column displays the IP Address the host name resolved to in the forward DNS lookup.

Port Scanner Tool

The port scanner tool provides the ability to scan specific ports on multiple devices in one simple interface.

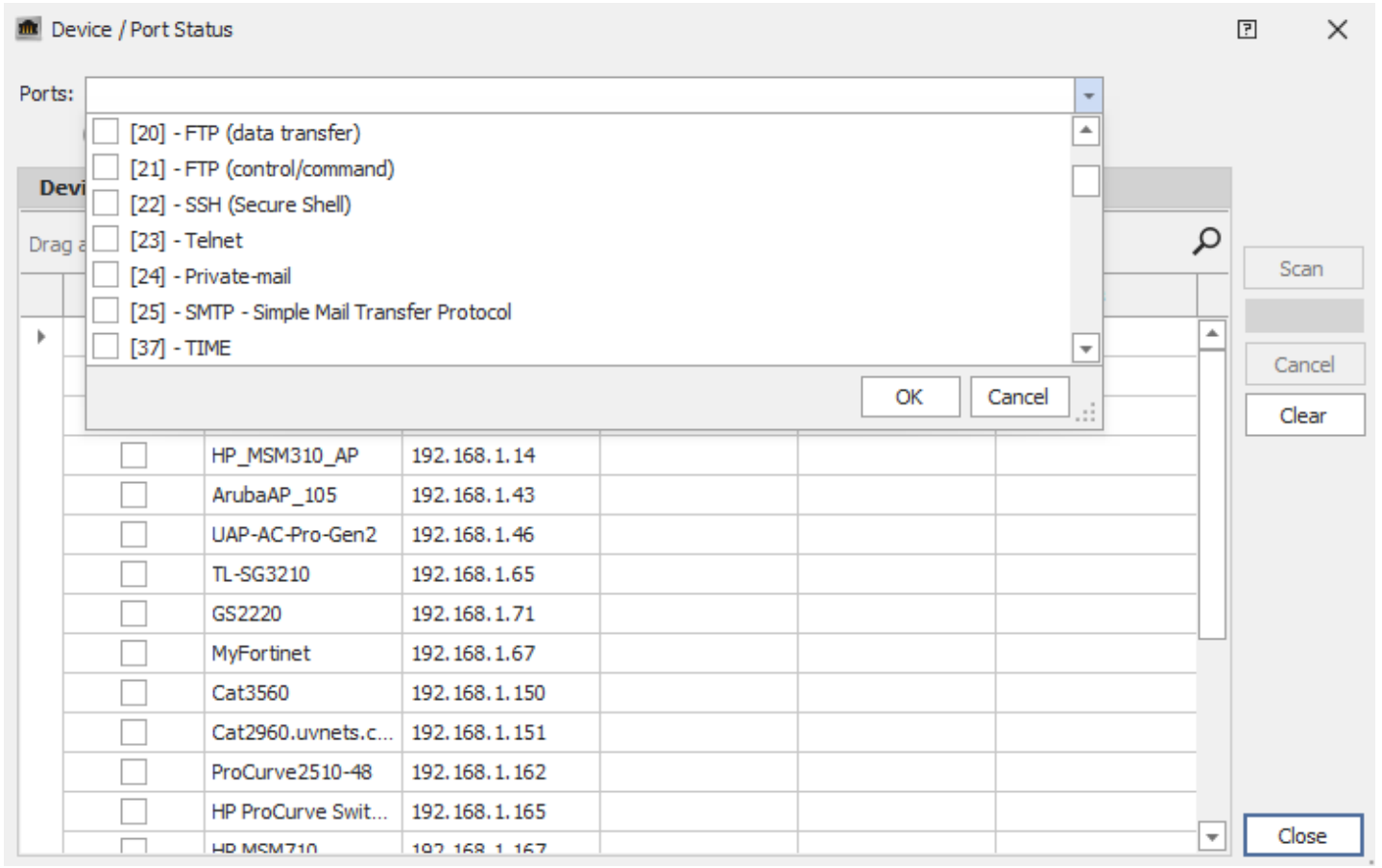
Launching the Port Scanner tool

The port scanner tool can be launched from the 'Tools' tab on the main view of UVexplorer. It can also be launched from the device context menu available on the device grid and the topology map.



Using the Port Scanner tool

To scan ports with the port scanner tool you need to select the ports and devices to scan, choose the protocol and then select the scan button.



Ports

To select ports, use the check list combo box available at the top of the control. The combo box

contains a list of common ports with their port numbers and descriptions. To select the ports, expand the list and select the checkbox next to the ports you would like to include in the scan.

Protocol

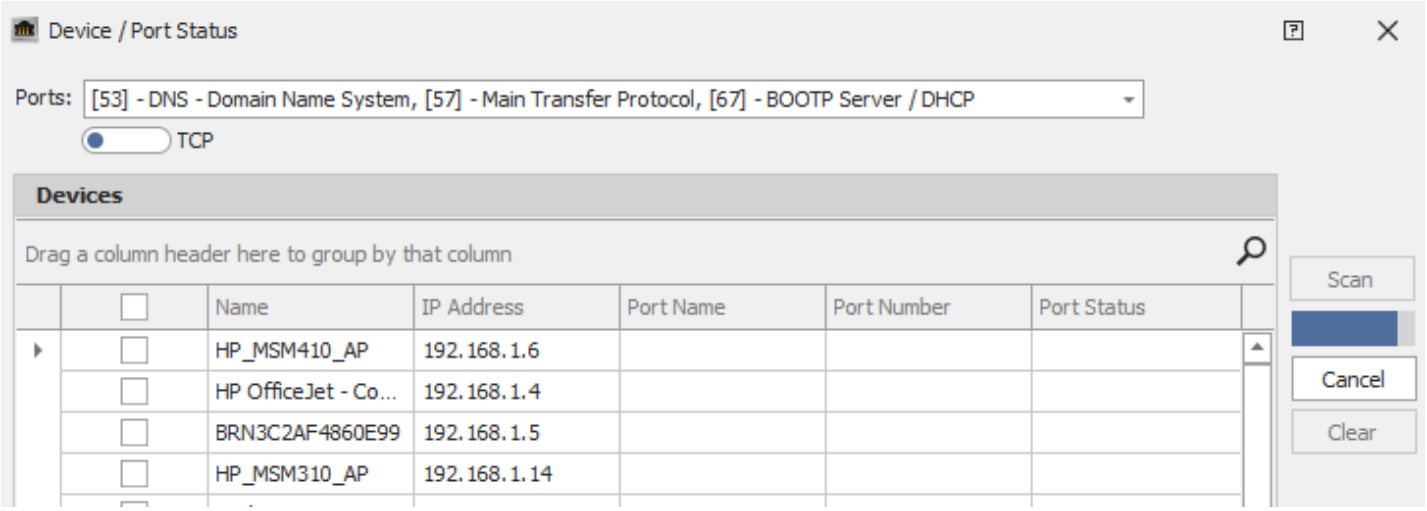
Each service running on a port can choose to use either TCP or UDP as the communication protocol. To scan the ports, you must choose which protocol to use while scanning.

Devices

The port scanner tool is populated with all of the devices in the discovery result. To scan the selected ports on a device the check box in the device list must be selected.

Scan

Once the ports, protocol, and devices are selected you press the scan button to begin the scan. The port scanner tool attempts to connect to each port using the selected protocol. If the connection is successful, the port is considered open.



Viewing Results

When the scan is completed the result of the scan for each device and port is listed in the results view. When wanting to perform additional scans the results of the previous scan can be cleared using the clear button.

Name

The 'Name' column contains the display name of the scanned device.

IP Address

The 'IP Address' column contains the primary IP address of the scanned device.

Port Name

The 'Port Name' column contains a description of the commonly known service run on the provided port.

Port Number

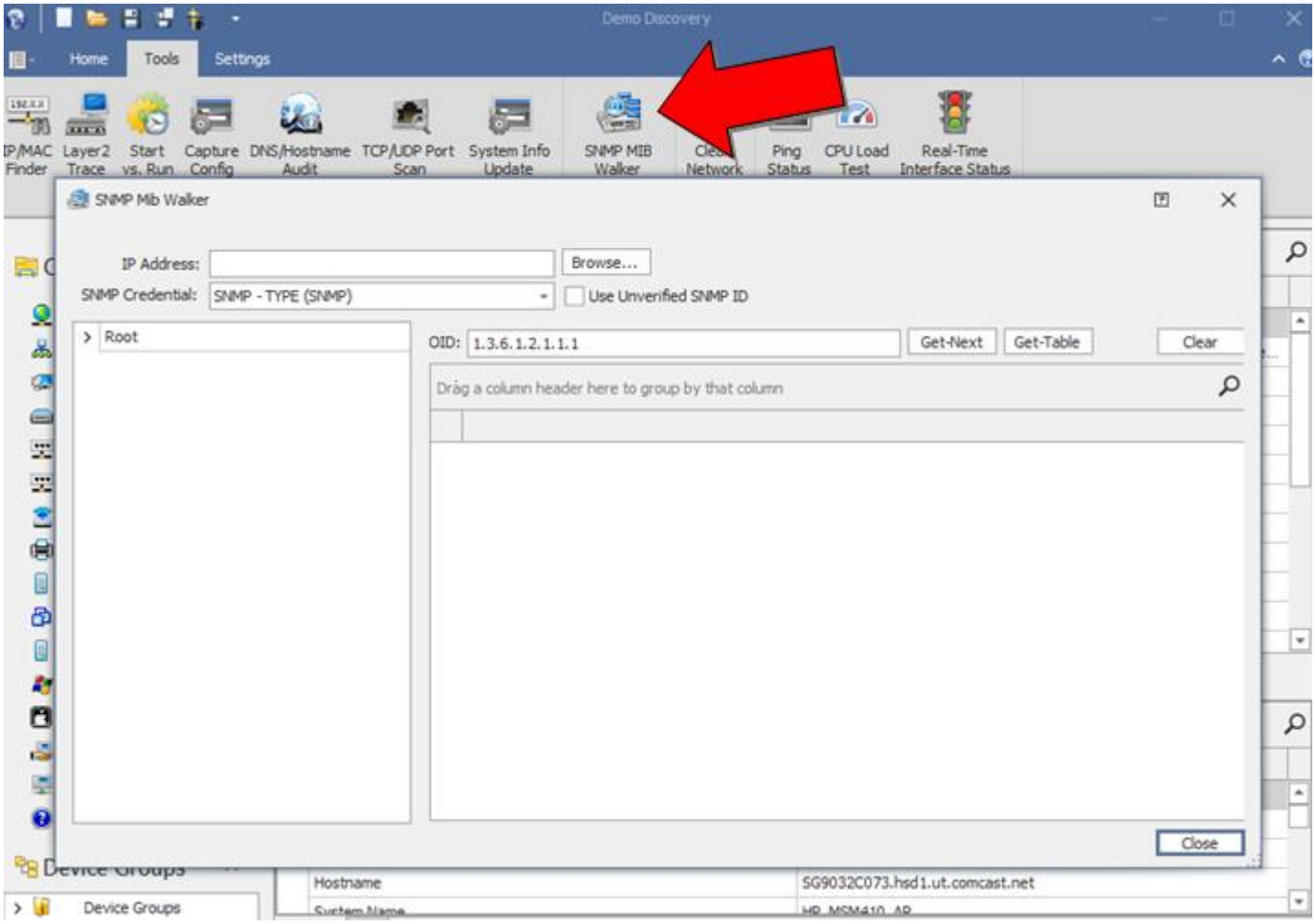
The 'Port Number' column contains the number of the scanned port.

Port Status

The 'Port Status' column contains the status of scan results. The port is either OPEN or CLOSED. If the scanner can connect to the device port with the selected protocol the port is considered open.

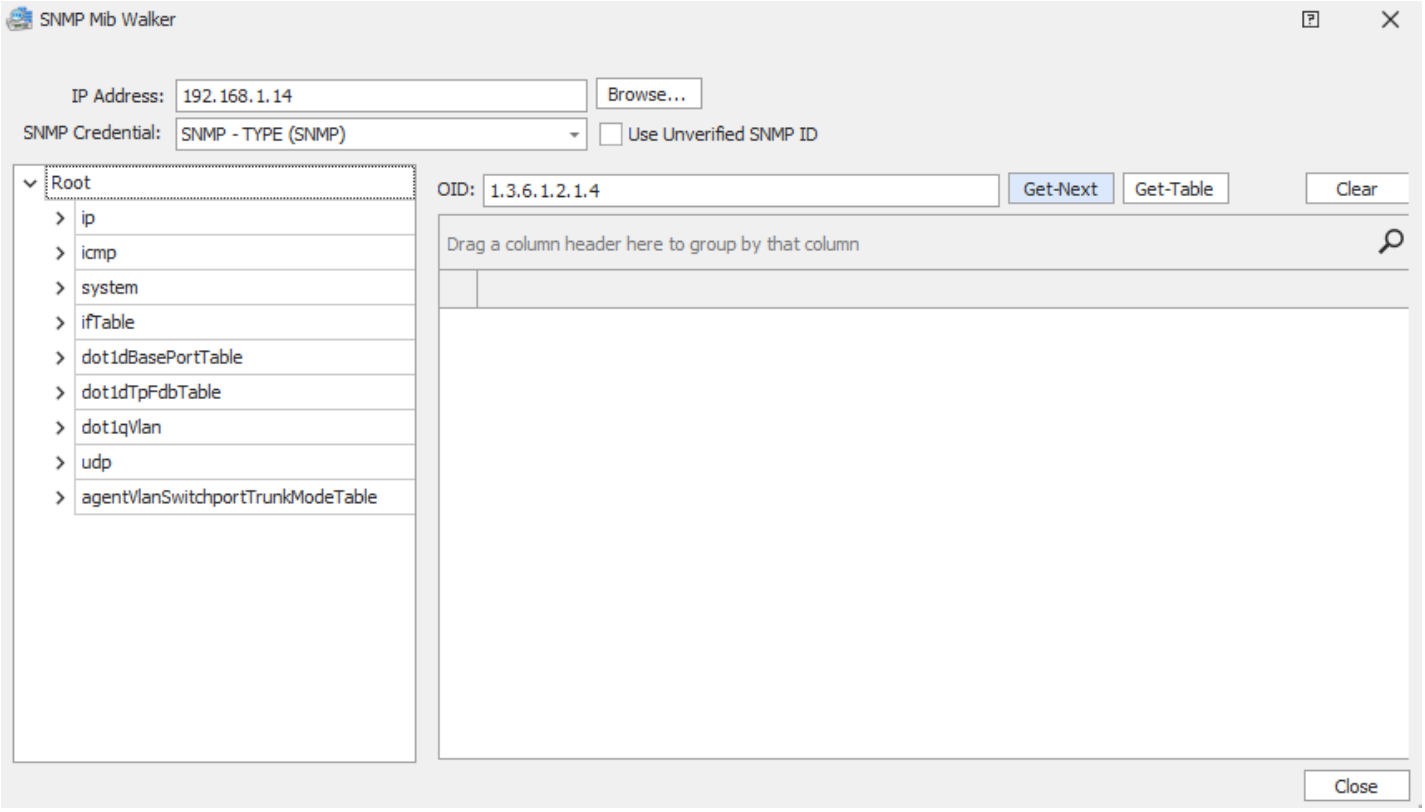
SNMP MIB Walker

The SNMP MIB Walker is simple tool to help test and trouble shoot SNMP data on any SNMP enabled device.



This is accomplished by the following steps:

1) Select an IP device from the current discovery results (or manually entering an **IP Address:** field)
2) Select a **SNMP Credential** to use when querying the device.
3) Select a MIB OID from the MIB Tree on the left (the selected value will show in the **OID:** field)
   a) **NOTE:** You may also enter any known OID in the OID field to test whether the device has any data under that OID value.
1) Use one of the following actions:
   a) **Get-Next** : Perform a SNMP Get-Next request given the current OID value.
   b) **Get-Table**: Perform successive SNMP Get-Next requests to query all values under the selected OID root.



1) The SNMP query results will be shown in the right table.

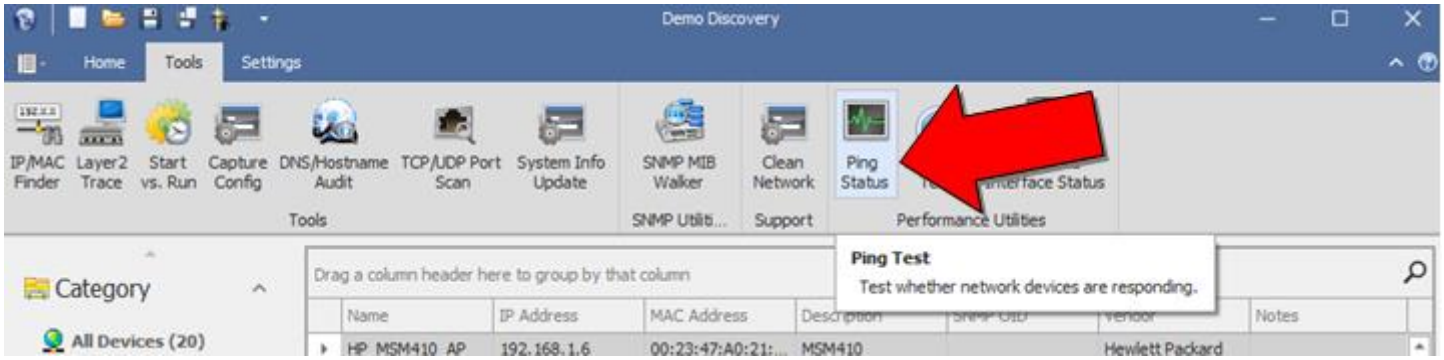
NOTE: This SNMP MIB walker is not yet a full featured SNMP MIB tool. It currently supports operations that are mainly focused on troubleshooting SNMP devices so as to gather the necessary SNMP values to ensure UVexplorer is providing its greatest level of functionality.

Ping Response Poller

The ping response poller tool allows you to monitor the real time ping response of devices on a timed interval.

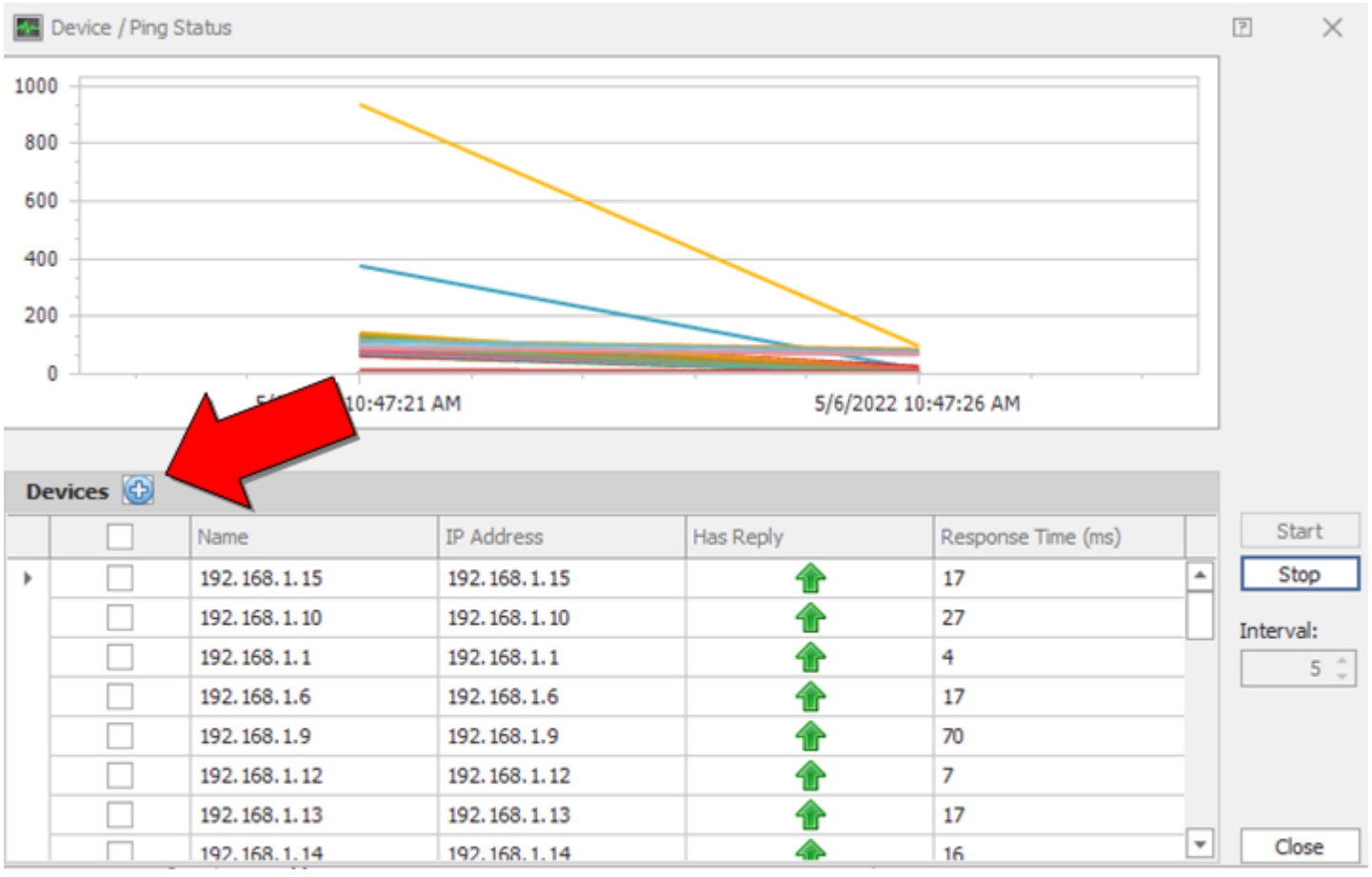
Launching the Ping Poller

The ping poller can be launched from the 'Tools' tab on the main view of UVexplorer. It can also be launched from the device context menu available on the device grid and the topology map.



Using the Ping Poller

To ping devices with the ping poller you add and select devices in the device grid, set the poll interval, and press the start button. The poller will continue to ping the devices, keeping track and graphing the response time, until the dialog is closed, or the stop button is pressed.



Devices

To add devices to the poller press the add button above the device grid. Devices added to the poller will only be polled when they are selected using the checkbox next to the device. If a poll is in process when a new device is added and selected the poller must be restarted before the newly selected device will be included in the poll.

Interval

The interval sets the frequency of the poll in seconds; the max interval is 120 seconds. The interval can only be changed when the poller is not running.

Ping Response Chart

The results chart contains the response times and poll intervals of the devices being polled. The response times are displayed in milliseconds. The interval contains the time the poll was performed. The legend maps the devices to the response time lines in the chart.

Ping Response Grid

The result grid displays the devices and their UP or DOWN status of the ping response along with the response time.

Name

The 'Name' column contains the display name of the polled device.

IP Address

The 'IP Address' column contains the primary IP address of the polled device.

Has Reply

The 'Has Reply' column contains an up or down arrow indicating UP for a ping response, and DOWN for no response.

Response Time (ms)

The 'Response Time' column contains the time in milliseconds it took for the device to respond. If the device did not respond the response time is empty.

CPU Load Poller

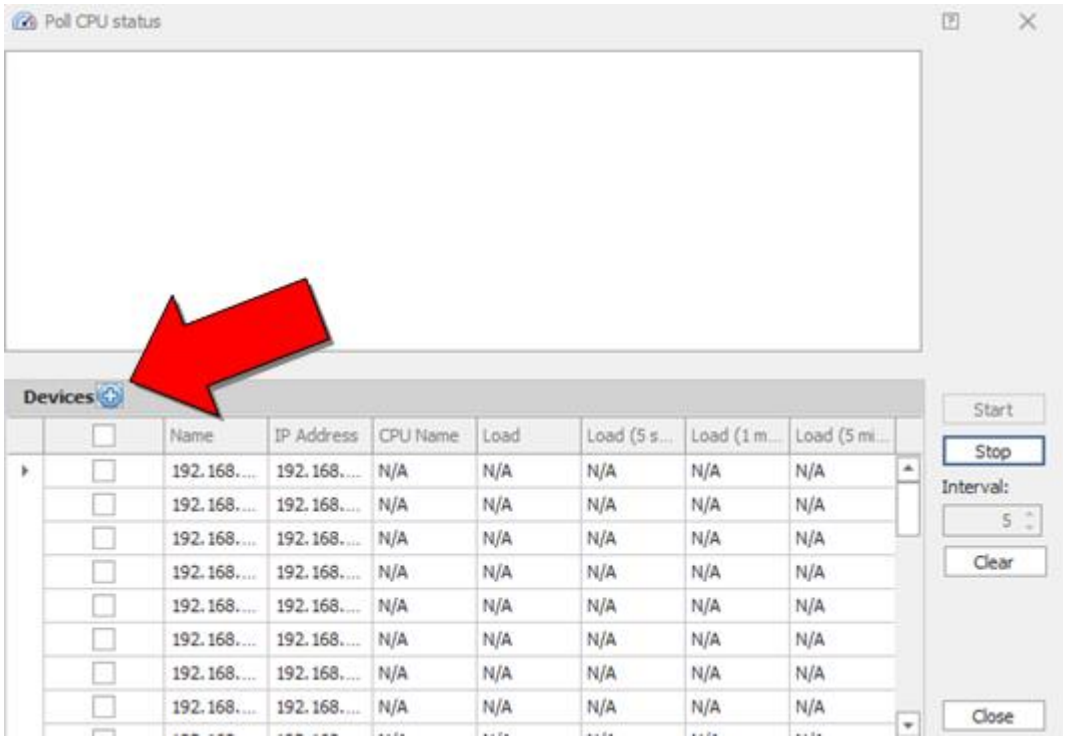
The CPU Load poller allows you to monitor the real time CPU load of devices on a timed interval.

Launching the CPU Poller

The CPU poller can be launched from the 'Tools' tab on the main view of UVexplorer. It can also be launched from the device context menu available on the device grid and the topology map.

Using the CPU Poller

To poll the device CPU load with the CPU poller you add and select devices in the device grid, set the poll interval, and press the start button. The poller will continue to poll the devices until the dialog is closed or the stop button is pressed. The CPU load query uses SNMP to query the CPU load from the devices. Devices must have SNMP credentials assigned to them for the query to succeed. See Managing Device Credentials for more information about managing credentials.



Devices

To add devices to the poller press the add button above the device grid. Devices added to the poller will only be polled when they are selected using the check box next to the device. If a poll is in process when a new device is added and selected the poller must be restarted before the newly selected device will be included in the poll.

Interval

The interval sets the frequency of the poll in seconds; the max interval is 120 seconds. The interval can only be changed when the poller is not running.

CPU Load Results Chart

The results chart contains the CPU load and poll intervals of the devices being polled. The CPU load is displayed as a percentage. The interval contains the time the poll was performed. The legend maps the devices to the load percentage lines in the chart.

CPU Load Results Grid

The results grid displays the devices and their CPU load percentages over time.

Name

The 'Name' column contains the display name of the polled device.

IP Address

The 'IP Address' column contains the primary IP address of the polled device.

CPU Name

The 'CPU Name' column displays the name of the processor when available. If there isn't a name the processor index may be used.

Load

The 'Load' column displays the CPU load as a percentage of the processor's capacity. Historical load values are also presented over a period.

Load (5 sec)
Load (1 min)
Load (5 min)

All these respective load columns display CPU loads based on their average over the indicated time (i.e., 5 seconds or 5 minutes). Not all devices support querying this information; but when it is available, the tool will display the collected values.

Interface Status Poller

The interface status poller allows you to monitor the real time interface status of a device on a timed interval.

Launching the Interface Status Poller

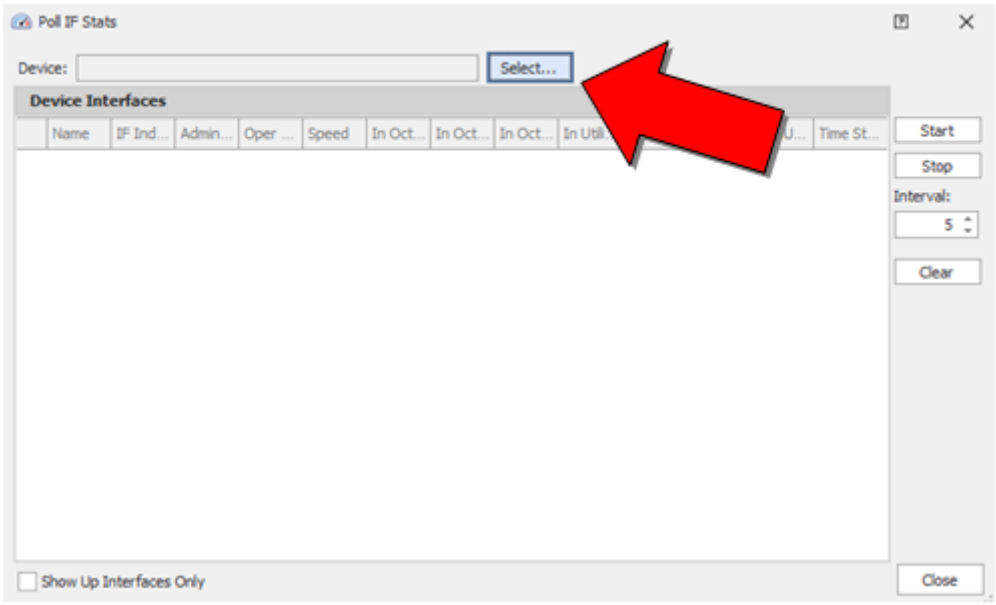
The interface status poller can be launched from the 'Tools' tab on the main view of UVexplorer. It can also be launched from the device context menu available on the device grid and the topology map.

Using the Interface Status Poller

To poll the device interface status with the interface status poller select a device with interfaces and press the 'Poll' button. The interface status query uses SNMP to query the interface status from the device. The device must have SNMP credentials assigned to them for the query to succeed. See Managing Device Credentials for more information about managing credentials.

Selecting a Device

To select a device, press the browse device button. The device selector will only allow devices with interfaces to be selected. The device must also have SNMP credentials assigned to it for the queries to be made.



Viewing Results

After a device is selected and the poll button pressed the results are displayed in the results grid. The grid contains an entry for each interface on the device containing the interface status query results.

Name

The 'Name' column contains the interface name of the polled interface.

IF Index

The 'IF Index' column contains the index of the polled interface.

Admin State

The 'Admin State' column displays the administrator status of the interface. Possible values are: up, down, testing, unknown, dormant, not present, lower layer down.

Oper State

The 'Oper State' column displays the operating status of the interface. Possible values are: up, down, testing, unknown, dormant, not present, lower layer down.

Speed

The 'Speed' column displays the bandwidth of the interface in bits per second.

In Octets

The 'In Octets' column displays the number of octets of data received on the interface.

In Octets Usage (Mbps)

The 'In Octets Usage' column displays the number of octets being received as a calculation of Mbps (Mega-bits-per-second). For this calculation to work, there must be more than 1 poll result.

Out Octets

The 'Out Octets' column displays the number of octets of data sent on the interface.

Out Octets Usage

The 'Out Octets Usage' column displays the number of octets being sent as a calculation of Mbps (Mega-bits-per-second). For this calculation to work, there must be more than 1 poll result.

Time Stamp

The 'Time Stamp' column displays the time the interface statistics were collected.

Managing Device Credentials

Credentials can be managed in the Protocol/Credential Settings dialog.

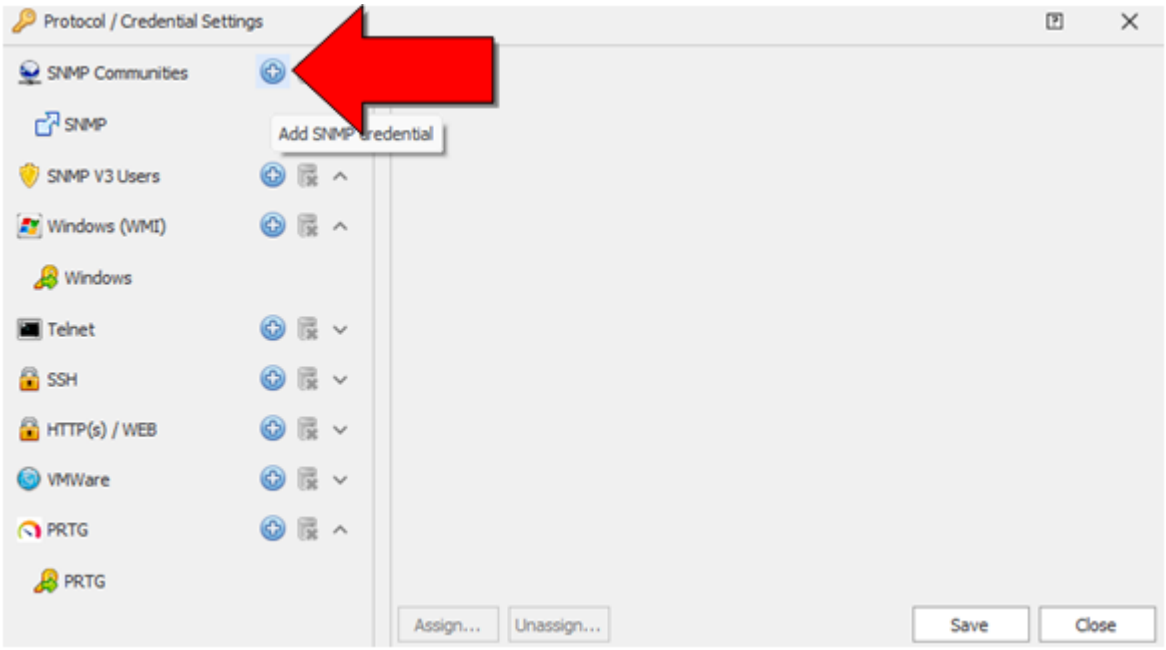
Launching the Protocol/Credential Settings dialog

The Protocol/Credential settings dialog can be launched from the 'Protocol/Credential Settings' button on the 'Home' tab of the main UVexplorer page.

Adding credentials.

UVexplorer requires a variety of credentials for use in discovering and managing various device types and device information. The protocol settings dialog contains two main views. On the left is a navigation pane that contains a header for all the protocol types. On the right is a pane that contains the settings for the protocol/credential selected in the navigation pane.

To add new credentials of any type either use the add '+' button on the credential type header, or right click the pane within that credential type and select 'Add'. A new credential of that type will be created and added to the credential store. The credential settings will then be displayed in the right pane where changes can be made.



Removing credentials

To remove a credential you can either right click on the credential and select 'Delete' or press the

delete 'X' button to delete the selected credential. The selected credential will be permanently deleted from the credential store.

Editing credentials

A credential can be edited by selecting the credential and making changes to the settings displayed in the right credential settings pane. When you have completed your changes select the 'Save' button to persist the changes to the credential store. If you attempt to leave the credential settings dialog or select a new credential without saving changes to the current settings, you will be prompted to save them before continuing. If you did not intend to make changes, or want to cancel your changes, select 'No' when prompted to save your changes.

Credential Settings Details

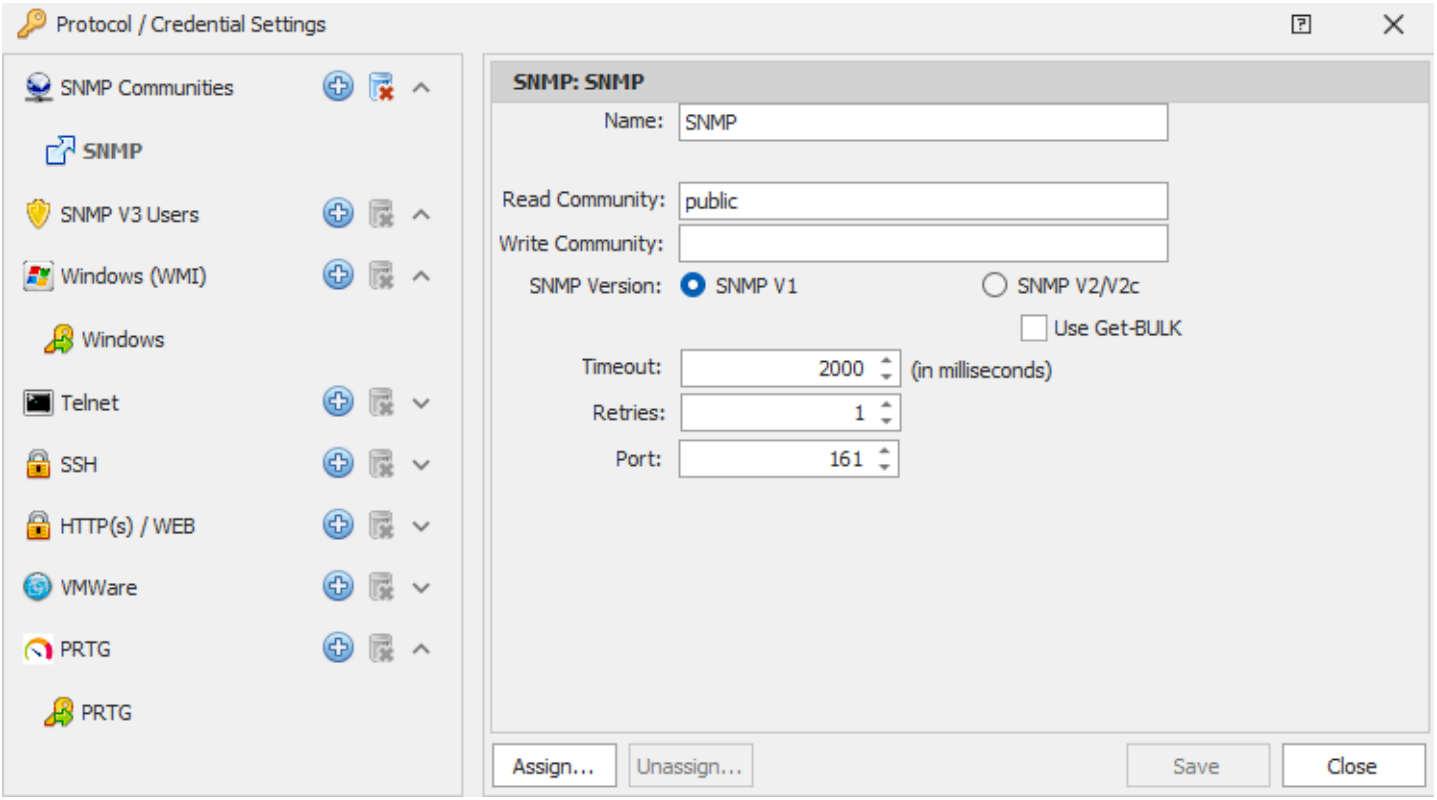
For details about the available credentials see the following:

SNMP Communities
SNMP V3 Users
Windows (WMI)
Telnet
SSH
VMWare

Configuring SNMP Credentials

Understanding SNMP Community Strings

SNMP is the Simple Network Management Protocol used by many network devices to provide device information. SNMP community strings are like passwords, the correct community string must be provided to the device SNMP agent before it will respond to requests for information.



SNMP credential settings

Name

The credential name is used within UVexplorer to refer to the SNMP credentials

Read Community

The read community string is the community string UVexplorer uses when reading information from a device. This value should be set to the read community string value set on the device.

Write Community

The write community string is the community string UVexplorer uses when writing information to the device. This value should be set to the write community string value set on the device.

SNMP Version

The SNMP protocol currently has three versions. SNMP v3 has enough differences from v1 and v2 that it requires a different editor. See Configuring SNMP V3 Users for help creating SNMP V3 credentials.

SNMP V2 added performance, and security improvements that require a different SNMP agent. View the device configuration to determine which SNMP version is required by your device.

Timeout

When making requests to SNMP agents, UVexplorer must wait for a response. The timeout setting is used to configure how long UVexplorer will wait for a response. The timeout value is set in milliseconds. The default value is 2000 milliseconds or 2 seconds. Increasing the timeout could improve the number of responses UVexplorer receives. Longer timeouts may increase the amount of time required for a discovery.

Retries

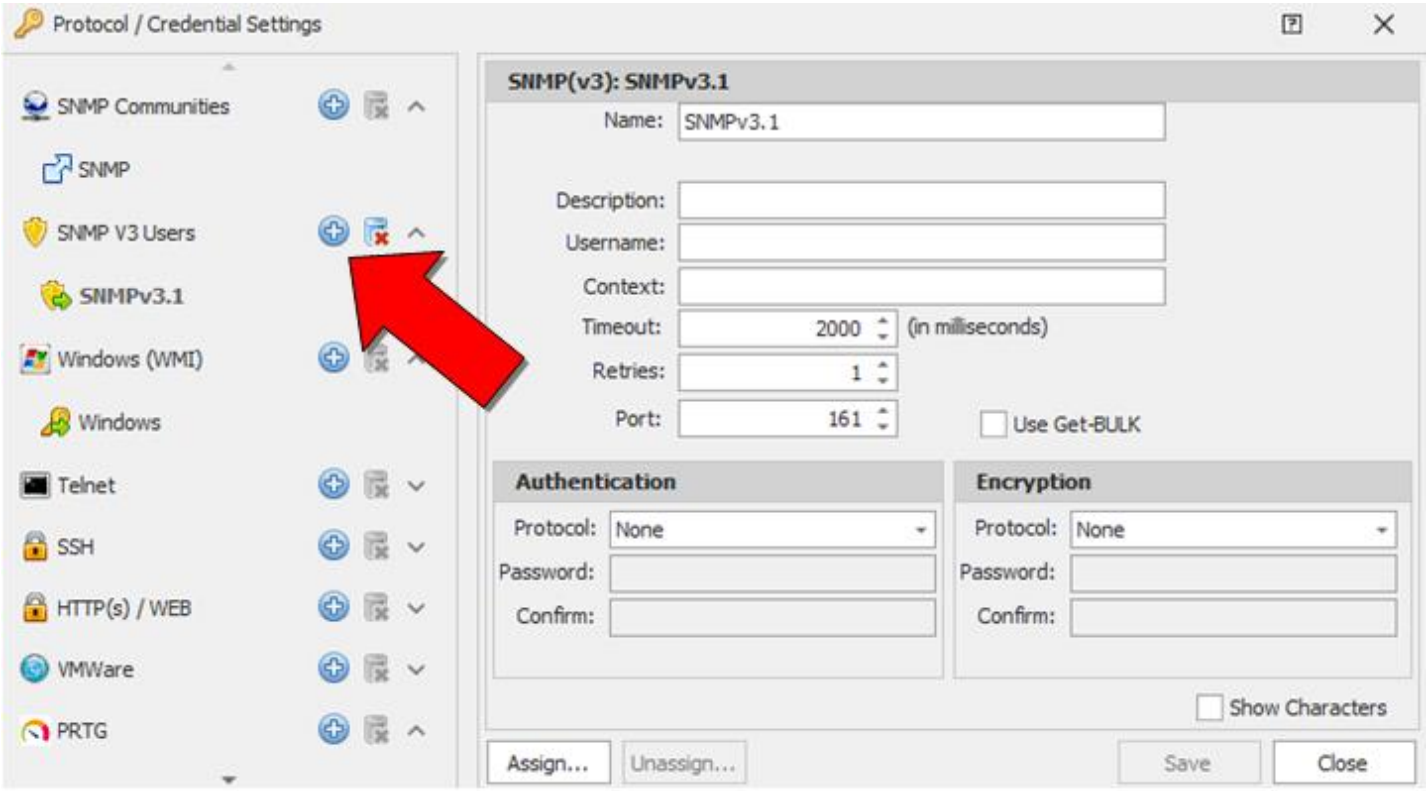
If an SNMP request fails to receive a response, UVexplorer can send the request again. The retries setting is used to configure the number of times to resend the request. Increasing the retries may increase the amount of time required for a discovery but may also improve the results.

Configuring SNMP V3 Users

SNMP V3 Credential Settings

Name

The credential name is used within UVexplorer to refer to the SNMP V3 credentials



Description

The description field contains a description of the SNMP V3 credentials

Username

The username used when sending requests to the device's SNMP V3 agent. The username is used to identify who is making the request. This should be set to the value of an SNMP V3 user configured on the device.

Context

SNMP V3 supports the idea of defining an object context that an SNMP V3 user can access. Context can be used to restrict an SNMP V3 user to specific information on the device. This field typically should be set the name of an SNMP V3 group configured on the device.

Authentication

The authentication settings are used to authenticate an SNMP V3 user with the device. Authentication is the process of verifying that the user is who they say they are. In this case authentication is performed by providing a password. SNMP V3 authentication can be disabled; in this case no password is required. If authentication is disabled on your device, select 'None' as

the protocol type to indicate that authentication is not required.

Protocol

SNMP V3 authentication provides two protocols for sharing the password: SHA-1 and MD5. This setting should be set to match the configuration of the SNMP V3 agent/user of the device.

Password

Password is the token used to authenticate the user with the device SNMP agent. This setting should be set to match the authentication password of the SNMP V3 user on the device.

Confirm

Confirm password is used to ensure that the correct password is supplied. This settings should match the password exactly.

Encryption

One advantage SNMP V3 has over older SNMP versions is the ability to encrypt SNMP agent communication. When encryption is used, all communication with the device is encrypted making it harder for others on the network see the information being sent and received. If SNMP V3 encryption is disabled on your device, select 'None' as the protocol type to indicate that encryption is not required.

Protocol

SNMP V3 encryption provides two protocols for performing the encryption: DES and AES256. This setting should be set to match the configuration of the SNMP V3 agent/user of the device.

Password

Password is the shared key used to initiate the encryption session. This setting should be set to match the encryption password of the SNMP V3 user on the device.

Confirm

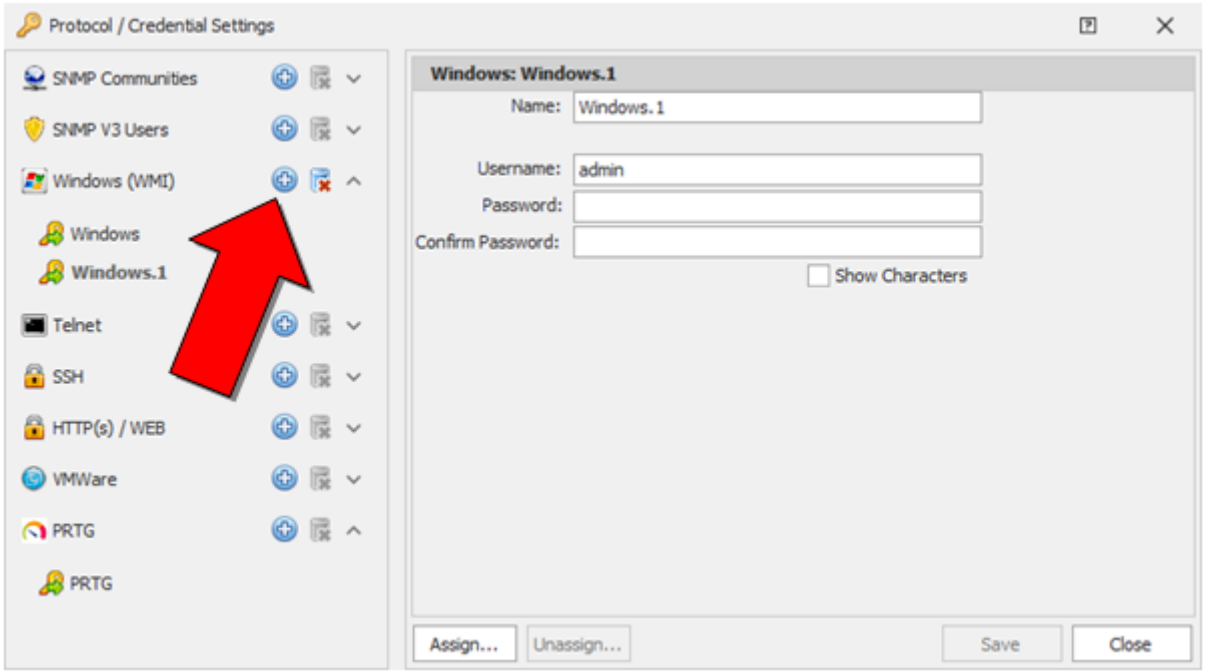
Confirm password is used to ensure that the correct password is supplied. This setting should match the password exactly.

Show Characters

The Show Characters check box can be used to ensure the passwords are entered correctly. When selected, the Authentication and Encryption passwords will be displayed. This option is only available when the credentials are initially created.

Configuring Windows (WMI) Credentials

Windows (WMI) credentials are used to authenticate with Windows machines. The settings in the Windows credential match the settings associated with a Windows user account. WMI credentials are used to collect Windows specific data from Windows machines.



Windows Credential Settings

Name

The credential name is used within UVexplorer to refer to the Windows credentials

Username

Username is the account name associated with the Windows user account.

Password

Password is the password associated with the Windows user account.

Confirm Password

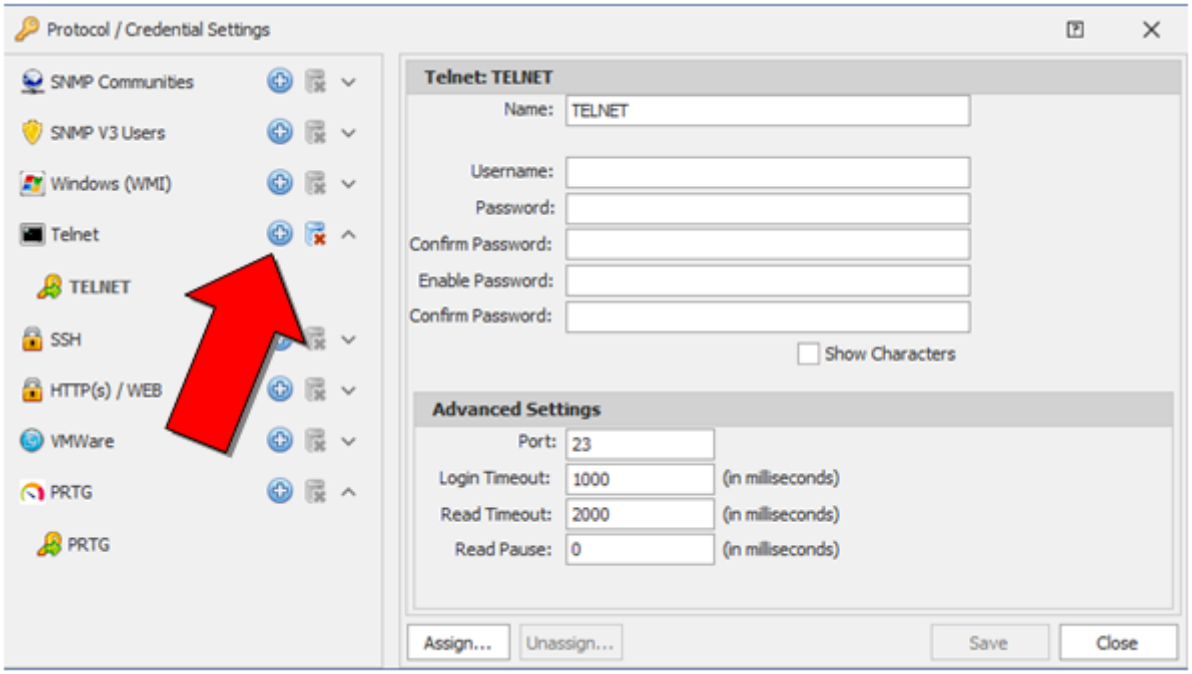
Confirm password is used to ensure that the correct password is supplied. This setting should match the password exactly.

Show Characters

The Show Characters check box can be used to ensure the passwords are entered correctly. When selected, the password text will be displayed. The Show Characters option is only available when the credentials are initially created.

Configuring Telnet Credentials

Telnet credentials are used by UVexplorer to connect to the device command line terminal. Reading from the command line terminal allows UVexplorer to collect information not available through other protocols. The Telnet protocol does not support encryption. Consider using the SSH protocol if encrypted communication is desired.



Telnet Credential Settings

Name

The credential name is used within UVexplorer to refer to the Telnet credentials

Username

The Username setting is the Telnet username and should be set to match the username of the device Telnet user settings.

Password

The password setting is the password associated with the Telnet user and should be set to match the password of the device Telnet user settings.

Confirm Password

Confirm password is used to ensure that the correct password is supplied. This setting should match the password exactly.

Enable Password

Some devices have a privileged mode that requires an additional password. UVexplorer will use this password when prompted for a password while entering the privileged mode. The enable password must be provided to enter enabled mode even if it is the same as the user password.

Confirm Password

Confirm password is used to ensure that the correct enable password is supplied. This setting should match the enable password exactly.

Show Characters

The show characters check box can be used to ensure the passwords are entered correctly. When selected the values of the password fields will be displayed.

Port Settings

Port

Telnet uses port 23 by default. If your device has been configured to use a different port, you can configure UVexplorer to use that port here.

Login Timeout

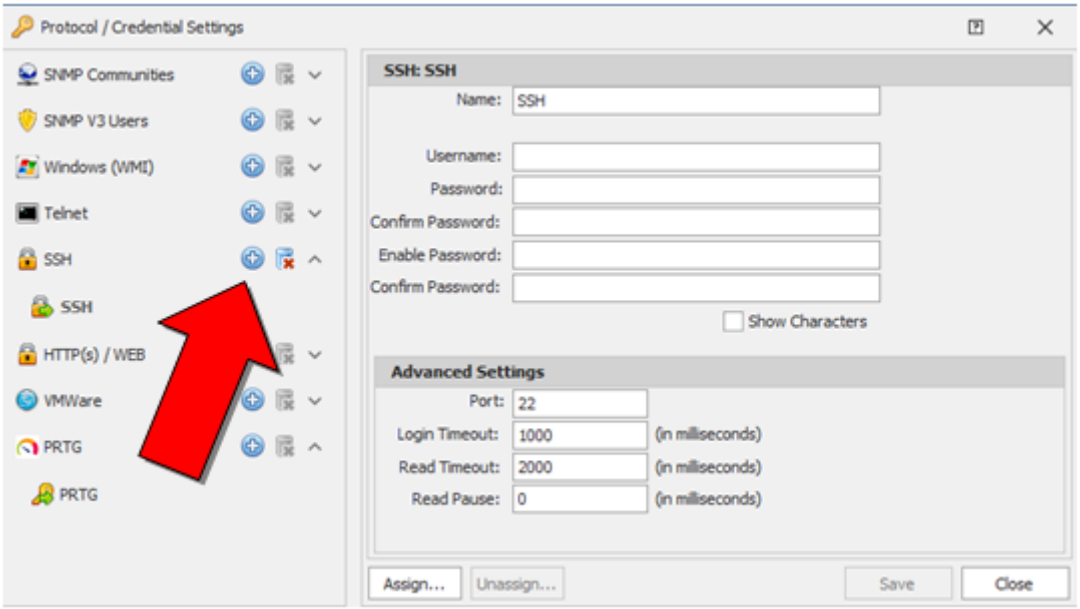
When UVexplorer sends login commands to a device, it waits for responses from the device to complete the login process. The login timeout indicates the time in milliseconds UVexplorer should wait for responses to login commands. Since login responses may take longer than regular command responses, this setting is provided separate from the Read Timeout.

Read Timeout

The read timeout is like the login timeout but is used to determine how long to wait for responses to all other commands. The read timeout indicates the time in milliseconds UVexplorer should wait for a response from the device once a command is sent. If UVexplorer is actively reading data from the device, the read timeout is not used; it is only used when the device is not responding with any data. Consider increasing the read timeout if commands to the device are failing, or the entire response is not received.

Configuring SSH Credentials

SSH credentials are used by UVexplorer to connect to the device command line terminal. Reading from the command line terminal allows UVexplorer to collect information not available through other protocols.



SSH Credential Settings

Name

The credential name is used within UVexplorer to refer to the SSH credentials

Username

The Username setting is the SSH username and should be set to match the user name of the device SSH user settings.

Password

The password setting is the password associated with the SSH user and should be set to match the password of the device SSH user settings.

Confirm Password

Confirm password is used to ensure that the correct password is supplied. This setting should match the password exactly.

Enable Password

Some devices have a privileged mode that requires an additional password. UVexplorer will use this password when prompted for a password while entering the privileged mode. The enable password must be provided to enter enabled mode even if it is the same as the user password.

Confirm Password

Confirm password is used to ensure that the correct enable password is supplied. This setting should match the enable password exactly.

Show Characters

The show characters check box can be used to ensure the passwords are entered correctly. When selected the values of the password fields will be displayed.

Port Settings

Port

SSH uses port 22 by default. If your device has been configured to use a different port, you can configure UVexplorer to use that port here.

Login Timeout

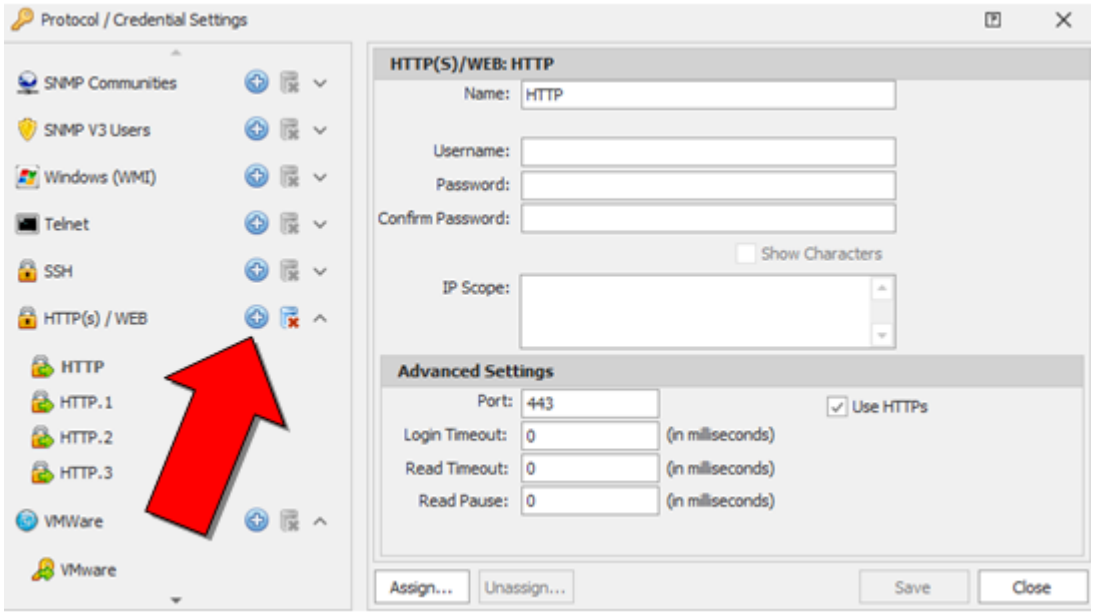
When UVexplorer sends login commands to a device, it waits for responses from the device to complete the login process. The login timeout indicates the time in milliseconds UVexplorer should wait for responses to login commands. Since login responses may take longer than regular command responses, this setting is provided separate from the Read Timeout.

Read Timeout

The read timeout is like the login timeout but is used to determine how long to wait for responses to all other commands. The read timeout indicates the time in milliseconds UVexplorer should wait for a response from the device once a command is sent. If UVexplorer is actively reading data from the device, the read timeout is not used; it is only used when the device is not responding with any data. Consider increasing the read timeout if commands to the device are failing, or the entire response is not received.

Configuring HTTP(s) / WEB Credentials

HTTP(s)/WEB credentials are used by UVexplorer to collect information not available through other protocols.



HTTP(s)/WEB Credential Settings

Name

The credential name is used within UVexplorer to refer to the HTTP credentials.

Username

The Username setting is the HTTP username and should be set to match the username of the device HTTP user settings.

Password

The password setting is the password associated with the HTTP user and should be set to match the password of the device HTTP user settings.

Confirm Password

Confirm password is used to ensure that the correct password is supplied. This setting should match the password exactly.

Show Characters

The show characters check box can be used to ensure the passwords are entered correctly. When selected the values of the password fields will be displayed.

Port Settings

Port

HTTP uses port 443 by default. If your device has been configured to use a different port, you can configure UVexplorer to use that port here.

Login Timeout

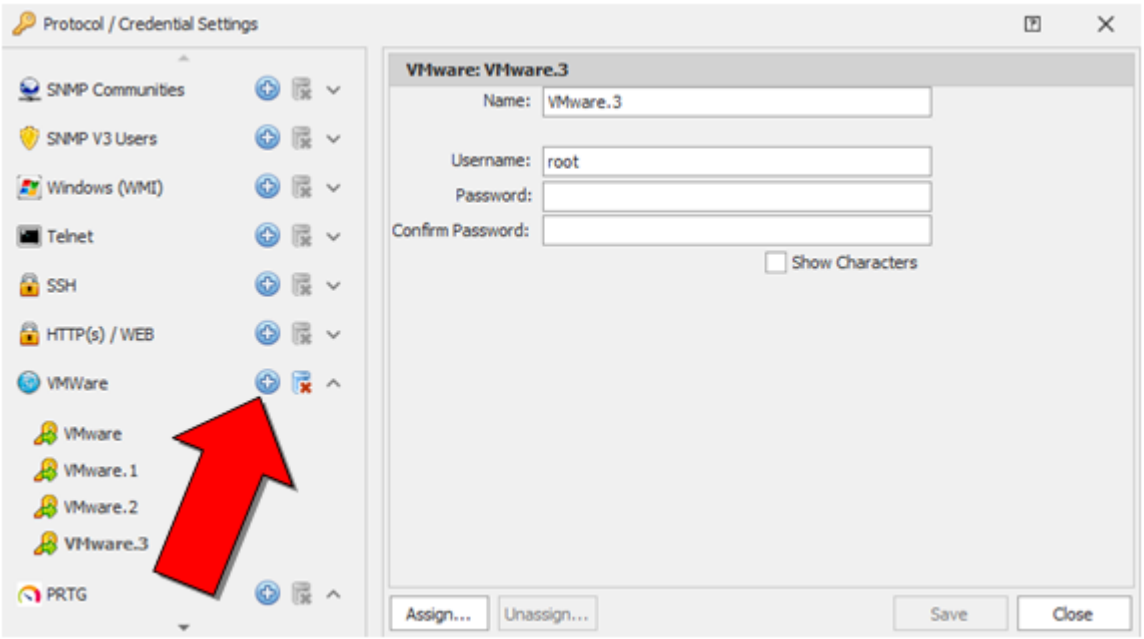
When UVexplorer sends login commands to a device, it waits for responses from the device to complete the login process. The login timeout indicates the time in milliseconds UVexplorer should wait for responses to login commands. Since login responses may take longer than regular command responses, this setting is provided separate from the Read Timeout.

Read Timeout

The read timeout is like the login timeout but is used to determine how long to wait for responses to all other commands. The read timeout indicates the time in milliseconds UVexplorer should wait for a response from the device once a command is sent. If UVexplorer is actively reading data from the device, the read timeout is not used; it is only used when the device is not responding with any data. Consider increasing the read timeout if commands to the device are failing, or the entire response is not received.

Configuring VMware Credentials

VMware credentials are used to authenticate with VMware machines.



VMware Credential Settings

Name

The credential name is used within UVexplorer to refer to the VMware credentials.

Username

Username is the account name associated with the VMware account.

Password

Password is the password associated with the VMware account.

Confirm Password

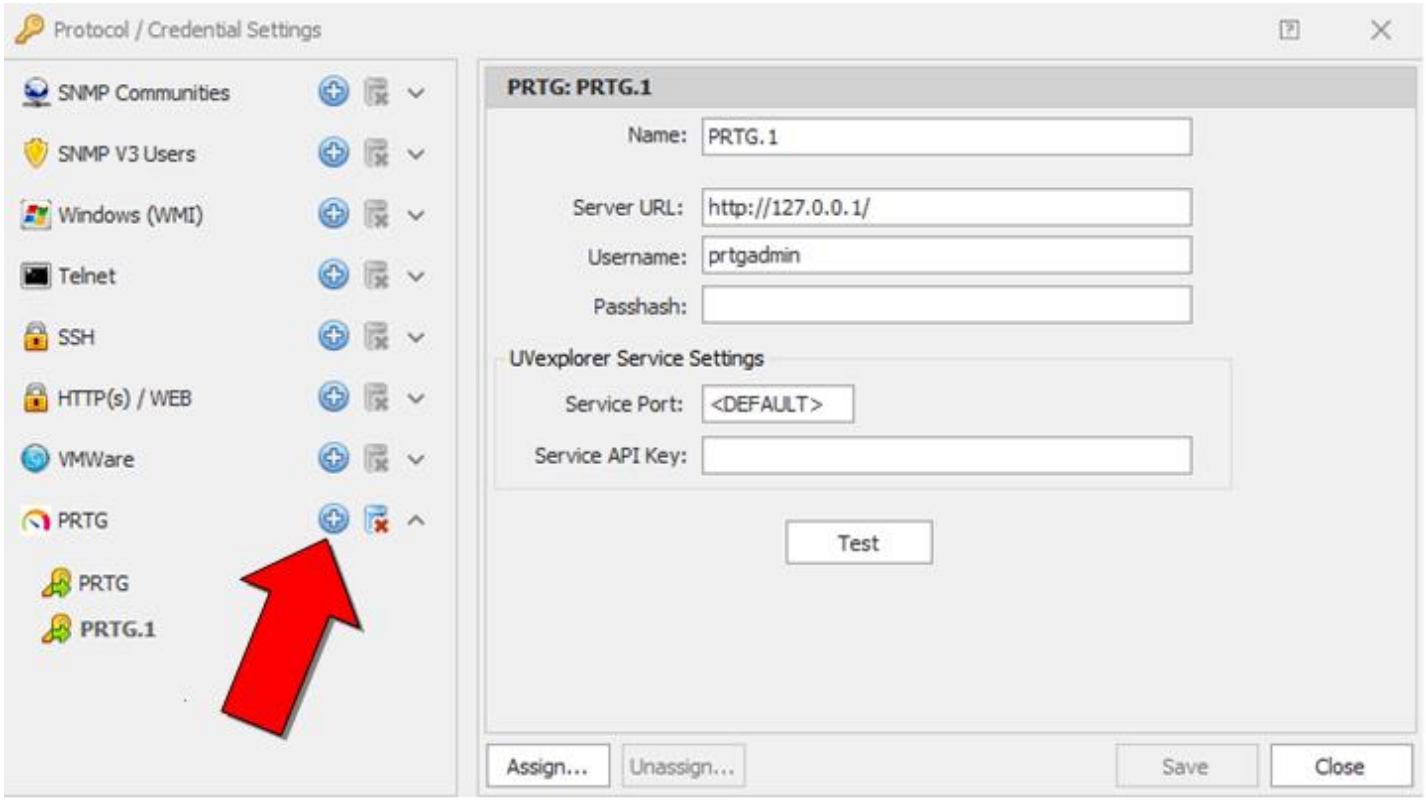
Confirm password is used to ensure that the correct password is supplied. This setting should match the password exactly.

Show Characters

The show characters check box can be used to ensure the passwords are entered correctly. When selected, the password text will be displayed. The show characters option is only available when the credentials are initially created.

Configuring PRTG Credentials

PRTG credentials are used to authenticate with the PRTG server.



VMware Credential Settings

Name

The credential name is used within UVexplorer to refer to the PRTG credentials.

Server URL

Server URL is the URL of the PRTG server.

Username

Username is the account name associated with the PRTG server.

Passhash

Passhash is the passhash associated with the PRTG server.

Service Port

Service port can be left on 'default' or enter the custom service port for your PRTG server.

Service API Key

Service API key is the API key provided from the PRTG server.

Capturing Device Configurations

Understanding Device Configuration Capture

Many network devices such as Routers, Switches, Wireless Controllers, etc... have a configuration file where the device configuration settings are stored. When the device starts for the first time, it loads the factory default configuration settings. Administrators can change the default settings using the Command Line Terminal, SNMP set commands, or a web interface. As the changes are made, they can be stored back out to the configuration file so that they are available to be used the next time the devices starts.

Most devices allow a device to run with the new configuration changes without saving those changes to the startup configuration file. This introduces the idea of a running configuration and a startup configuration. Some devices store any changes to the configuration file immediately, for these devices the startup and running configurations will always be the same.

As a network administrator it is helpful to keep backups of the device configuration once it has been properly configured so that it can be restored should the device fail. It is also helpful to compare the current startup or running configuration with a known good configuration to ensure that unexpected changes have not been made. This can be an effective way to troubleshoot and correct problems created when changes to the configuration have been made.

In this section:

Capturing Device Configurations
Selecting Configuration Capture Credentials
Saving Configuration Captures
Viewing Configuration Captures
Understanding Configuration Capture Scripts
Configuration Task Progress
Comparing Device Configurations
Supported Devices

Capturing Device Configurations

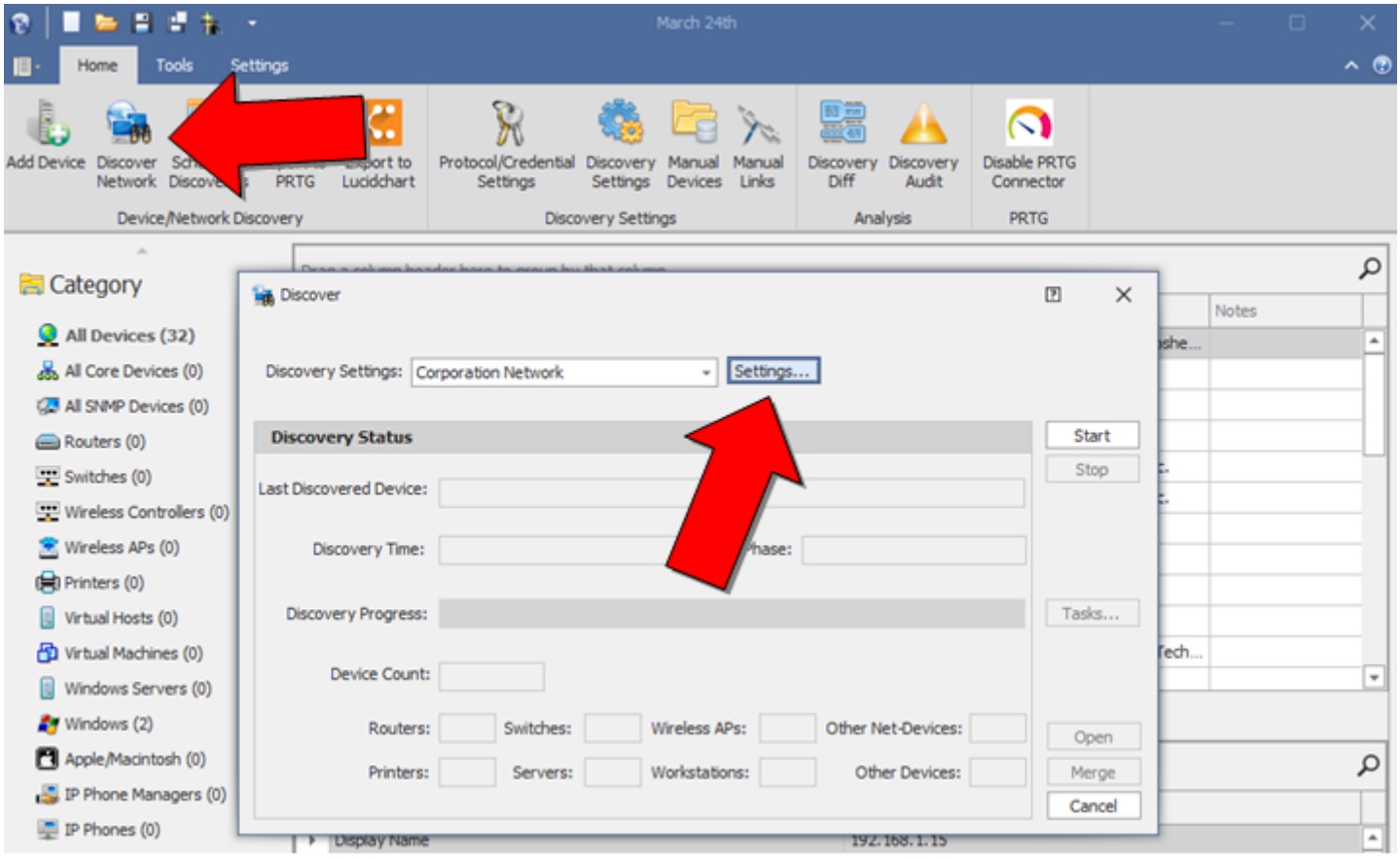
UVexplorer provides the ability to capture and compare device configurations.

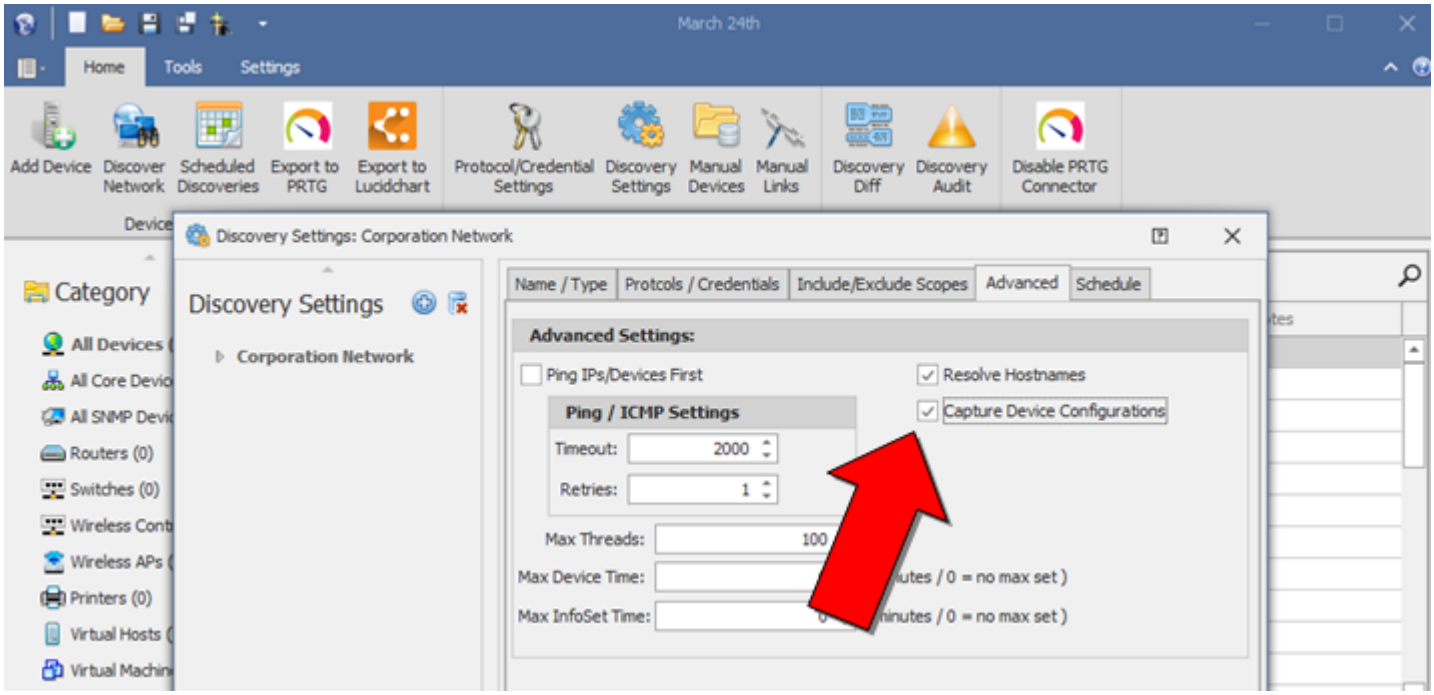
Device configurations are captured by connecting to the device Command Line Terminal using the SSH or Telnet protocols. Once connected a script is run against the device which captures the appropriate configurations to be stored in the UVexplorer database.

Configuration captures can be started during discovery, using the configuration Start vs. Run report tool, or for a single device using the Capture Configuration tool.

Capturing Configurations during Discovery

To capture device configurations during discovery, enable the 'Capture Device Configurations' setting located in the 'Advanced' tab of the discovery settings dialog. Appropriate SNMP and Telnet or SSH credentials must be provided in-order to determine the correct configuration capture script to run, and in-order to connect to the device command line terminal.



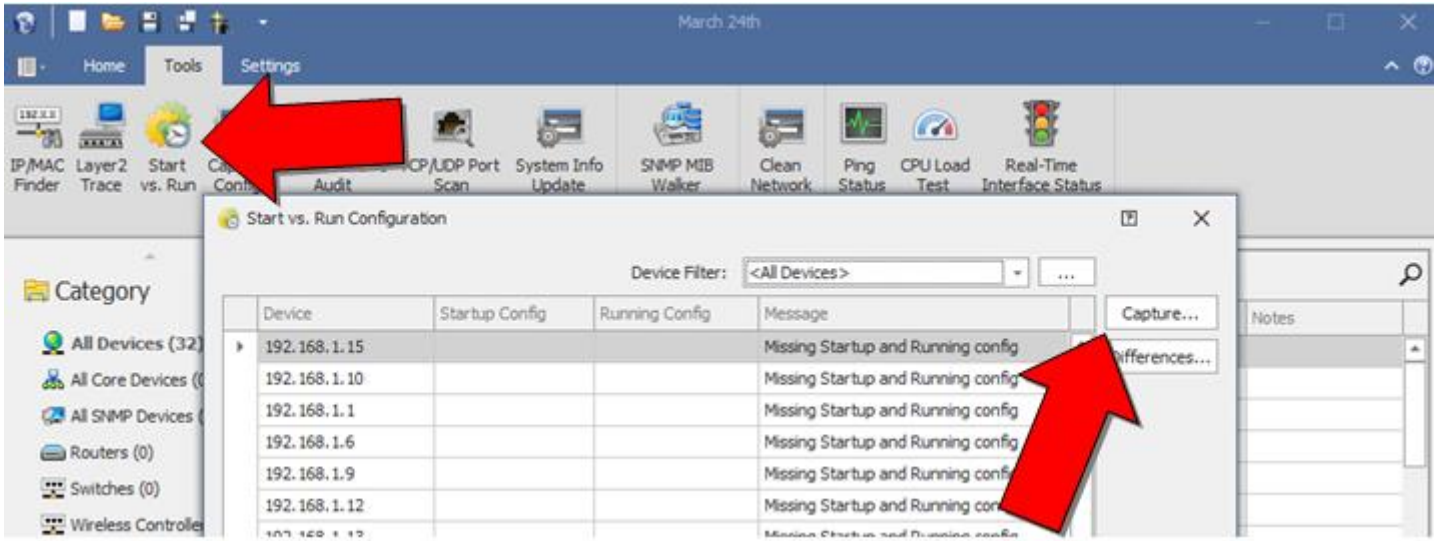


If the 'Capture Device Configurations' setting is enabled and the correct credentials are provided the Startup and Running configurations will be captured where available. The results of the configuration captures will be stored on the corresponding device properties within the discovery results.

See Discovery Settings for more information.

Capturing Configurations using the Start vs. Run tool

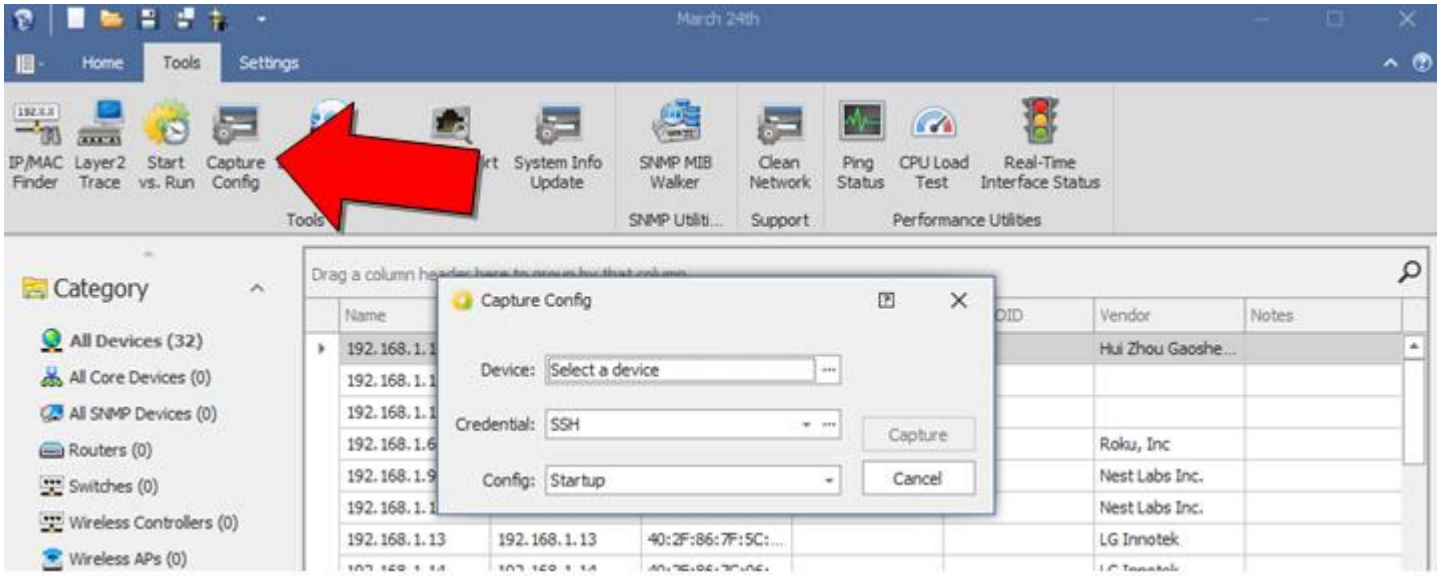
The Start vs Run configuration tool provides the ability to capture the startup and running configurations for the selected devices. Once the configurations are captured, they will be compared for differences and the results will be reported.



See Start vs Run for more information.

Capturing Configurations using Capture Configuration tool.

Device configurations can be captured for a single device using the Capture Configuration tool.



See Configuration Capture for more information about capturing configurations for a single device.

Selecting Configuration Capture Credentials

SSH or Telnet credentials must be provided to establish a command line terminal session. If no credentials are provided, the configuration capture will fail. When capturing configurations during discovery the credentials provided in the discovery settings will be used. When using the 'Start vs. Run' tool the credentials assigned to the device will be used. Credentials can be assigned to a device during discovery or manually. When using the Capture Configuration tool, the credentials selected before beginning the configuration capture will be used.

If both SSH and Telnet credentials are available, the SSH credentials will be used. If the SSH authentication fails, the Telnet credentials will not be used. The assumption is that if SSH credentials are available, then secure authentication is desired. If you want Telnet credentials to be used the SSH credentials must be removed from the device.

See Managing Device Credentials for more information.

Saving Configuration Captures

When device configurations are captured, they are stored with the device properties in the discovery result. If a configuration of that type has already been captured on the device the new configuration will be compared to the old one before it is stored. If the new one and the old one is the same as the last capture time, it will be updated, and a new entry will not be added. If the new one and the old one is different a new entry will be added containing the new configuration.

Viewing Configuration Captures

Device configuration captures are stored on the device properties. They can be viewed on the device properties 'Config' tab.

See Device Properties for more information.

Understanding Configuration Capture Scripts

When capturing device configurations UVexplorer needs to connect to the Command Line Terminal of the device and issue commands to show the appropriate configurations. When the configuration is displayed to the terminal UVexplorer can read the results and store them on the device properties.

Each device can provide different command line terminal prompts and can require a different set of commands to show the configurations. UVexplorer is configured with a set of command line settings and command scripts to run depending on the device the configuration capture is run against. Each script and command line settings contains command and settings appropriate for capturing the config of the given device.

To determine which settings and script to use UVexplorer maps the devices SNMP System Object Identifier (SNMP OID) to the corresponding script and settings. In-order for configuration capture to work the device SNMP OID must be available and the device must be supported by UVexplorer. UVexplorer will discover the device OID when valid SNMP credentials are provided during Network Discovery.

See Network Discovery for more information.

Capturing multiple configurations

When capturing multiple device configurations UVexplorer will establish a connection to the device for each configuration to be captured. Command Line Terminal sessions and commands can have a state, such as the enabled state, or the terminal state. Since configurations scripts must be written to assume the terminal session is in the initial state they could possibly fail if they are run in the same session with another script which changed the state. To avoid the possibility of this occurring a new session is created for each script.

If capturing multiple configurations at the same time fails on a device you could try increasing the timeout value for the credential/protocol or, ensure that the device is configured to allow simultaneous connections.

Configuration Capture Script Commands

When UVexplorer runs a command script against a device, it connects to the device using the provided credentials protocol. Upon connection UVexplorer typically attempts to login by waiting for a prompt for the username, sending the username, then waiting for a prompt for the password and sending the password, and finally by waiting for a prompt for the first command, referred to as the command prompt. Once the command prompt is reached UVexplorer can run the first command in the script.

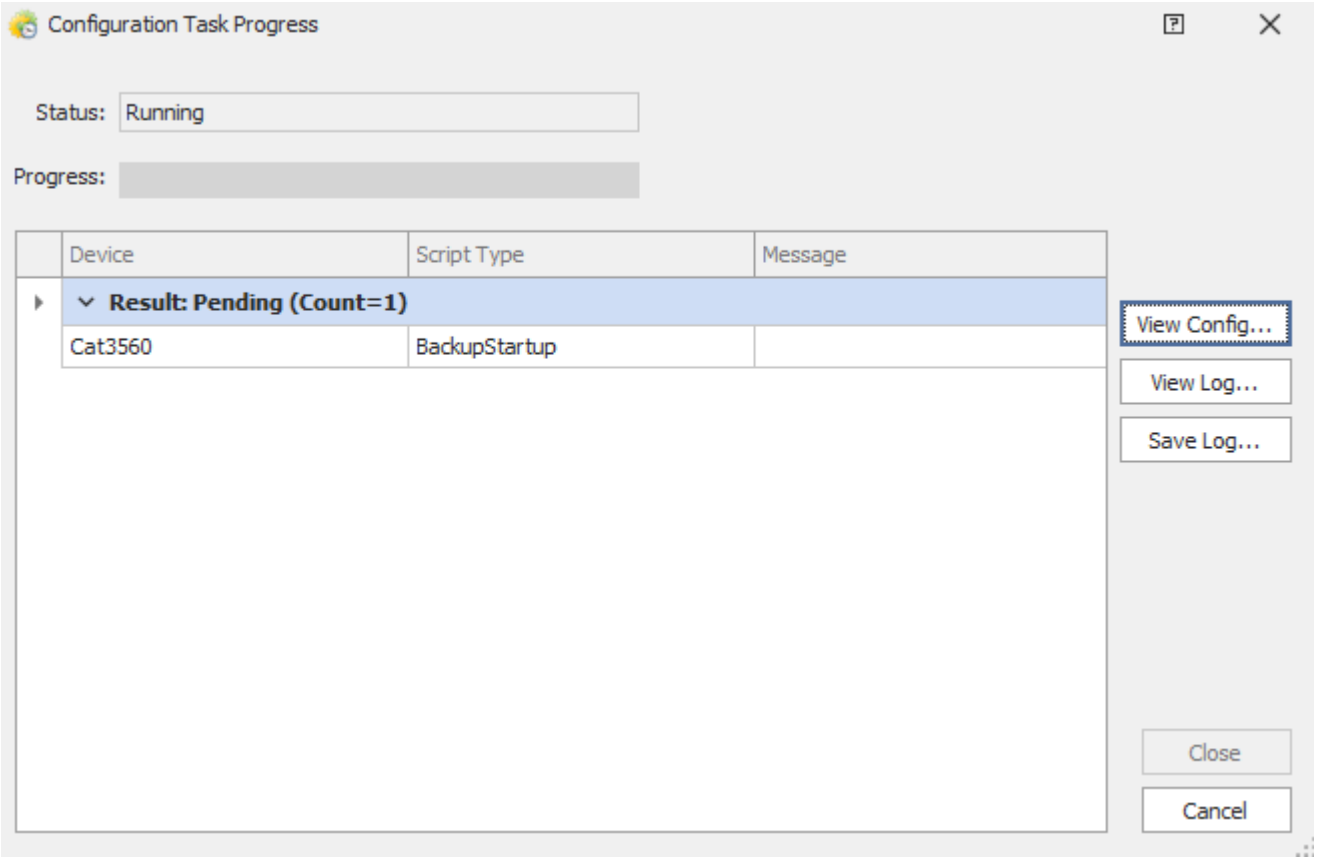
Running script commands is a similar process, when the command prompt is read, UVexplorer runs the next command, and reads the input until the next command prompt is read, at which point the next command will be run. Occasionally commands responses such as 'show run' will print a page of the configuration then prompt the user if they want more. If UVexplorer sees the more prompt, it will send the more response and continue reading the command response until the next command prompt is seen.

Since each device may have different prompts for the username, password, more and command prompts, along with different responses, UVexplorer allows command line settings for specific devices to be mapped to the configuration capture task, based on the device SNMP OID. If a

command fails, it is most likely caused by the device sending an unexpected prompt or not understanding the command or response UVexplorer sent. These settings are based on the provided device support. If your device is failing while running a command, contact UVexplorer customer support to request device support for your device.

Configuration Task Progress

When device configuration capture tasks are started the progress of the task can be seen within the Configuration Task Progress dialog.



Each device participating in the configuration task will be listed in the dialog results. The devices will be grouped within the list depending on their current task state. Task states include, Pending, Running, Succeeded, and Failed.

Understanding Failure Messages

If the configuration capture failed a message indicating the reason for the failure will be provided. Some common failures and suggested fixes are provided below.

Missing SSH and Telnet credentials

UVexplorer requires SSH or Telnet credentials to create a command line terminal session. If SSH or Telnet credentials are not provided in the settings or on the device configuration capture will not be able to continue.

See Managing Device Credentials, and Capturing Device Configurations for more information.

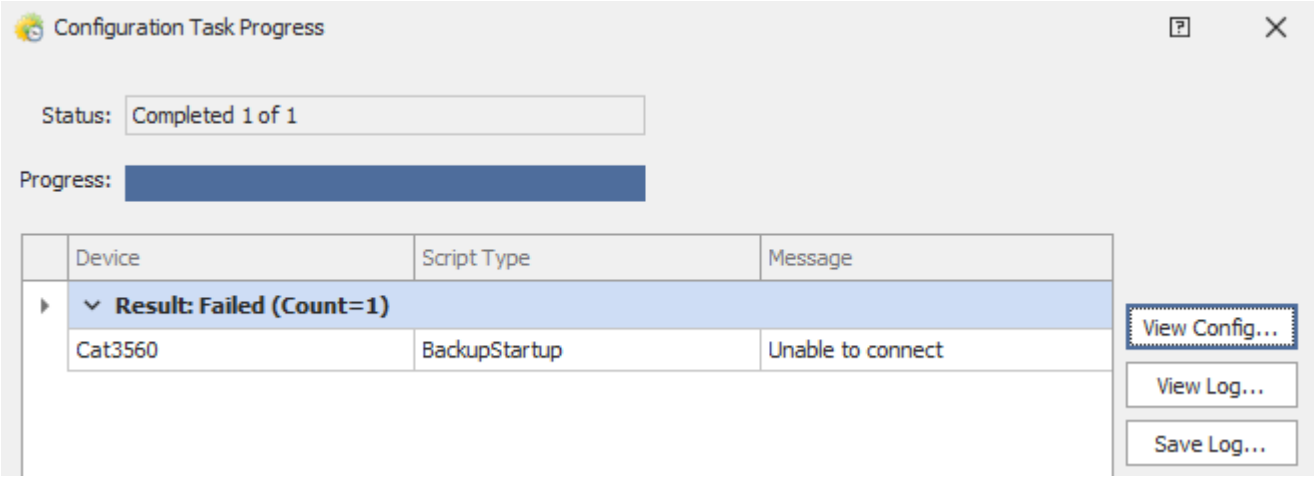
Unable to Find Script

When UVexplorer runs configuration tasks it must find the correct script to run against the device. If UVexplorer is unable to find a script for the device could be because it does not have a discovered SNMP OID or because there is no available script.

See Understanding Configuration Capture Scripts for more information.

Unable to Connect

This message indicates that UVexplorer was unable to connect to the device. This could occur because the device is unavailable, you could try pinging the device to ensure it is responding. It is also possible that the device is not configured to support the attempted SSH or Telnet protocol. You could try connecting to the device manually using a tool such as Putty to ensure the device is configured properly. If the device does not accept the manual connection the device will likely need to be configured to accept SSH or Telnet connections.



Unable to Login

This message could occur if the provided credentials are incorrect. You could verify the credentials manually using a tool such as Putty. Also, you could ensure that the correct credentials are provided and properly configured within UVexplorer. See Managing Device Credentials for more help configuring credentials.

Another cause of this error message is that UVexplorer didn't recognize the login sequence required for the device. When UVexplorer connects to a device it looks for command prompts such as 'login as:' or 'Username: ' to begin the login sequence. If the device is unsupported UVexplorer may not recognize the device login prompts and will be unable to connect to the device. If you have verified that the correct credentials are being used for the configuration task, then it is possible your device is unsupported. Contact UVexplorer customer support for help with device support.

Unable to Enter Privileged Mode

Many devices require the logged in user to have privileged access to display the device configuration. These devices typically have a command to enter privileged mode such as 'enable'. When this error occurs, UVexplorer attempted to enter privileged mode and the command failed.

One cause of this failure could be that the privileged command prompted for a password and the wrong password was provided. To fix this ensure that the correct privileged password is provided with the device credential.

Another problem could be that the UVexplorer command line settings were unable to recognize the privileged password prompt or command prompt, or the device didn't understand the response to these prompts that UVexplorer sent.

Another potential cause of this error message is that the device does not support a privileged mode

or requires a privileged command different from the one being sent by UVexplorer if this is the case there is an issue with device support.

See Understanding Configuration Capture Scripts for more help with this error.

Error Running Command

This message occurs when an error occurs while running a command within the script.

See Understanding Configuration Capture Scripts for help with this error message.

Canceling Configuration Capture Tasks

Configuration capture tasks started manually can be canceled in the task progress dialog by selecting the cancel button. Canceling a configuration task will keep any pending device captures from starting. For any running captures the next command will not be run but UVexplorer will wait for the currently running command to complete before it can cancel the task entirely. If a configuration capture task is canceled the results of any completed captures will not be stored on the device.

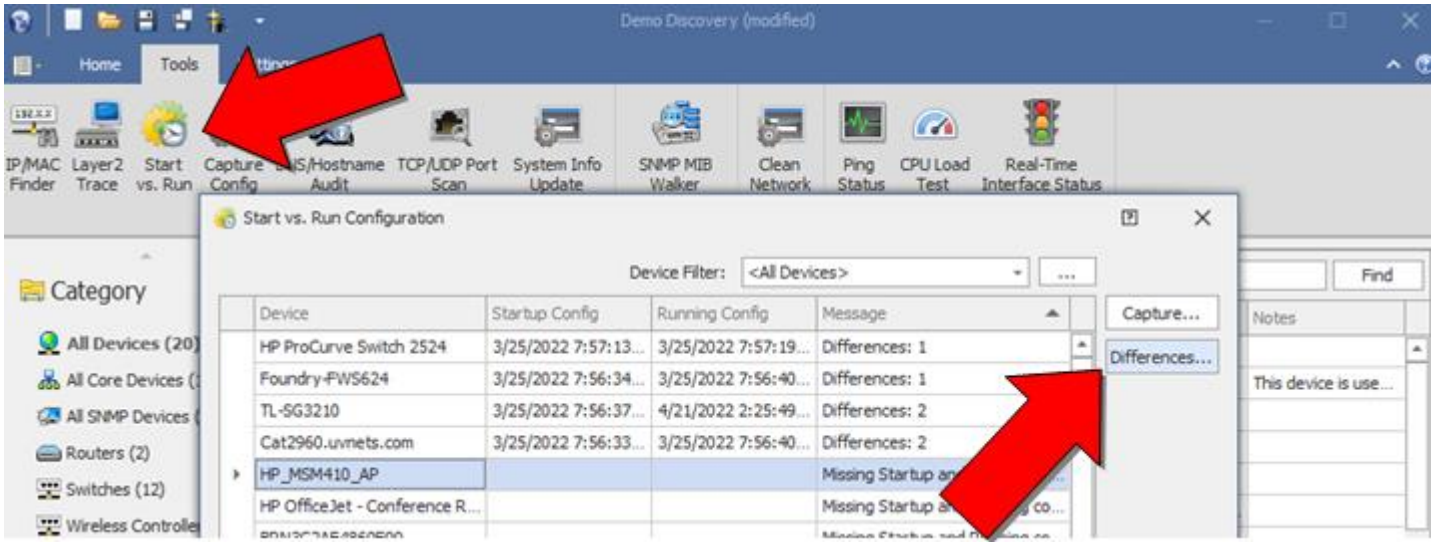
Comparing Device Configurations

UVexplorer allows you to compare configurations on the same device or on other devices.

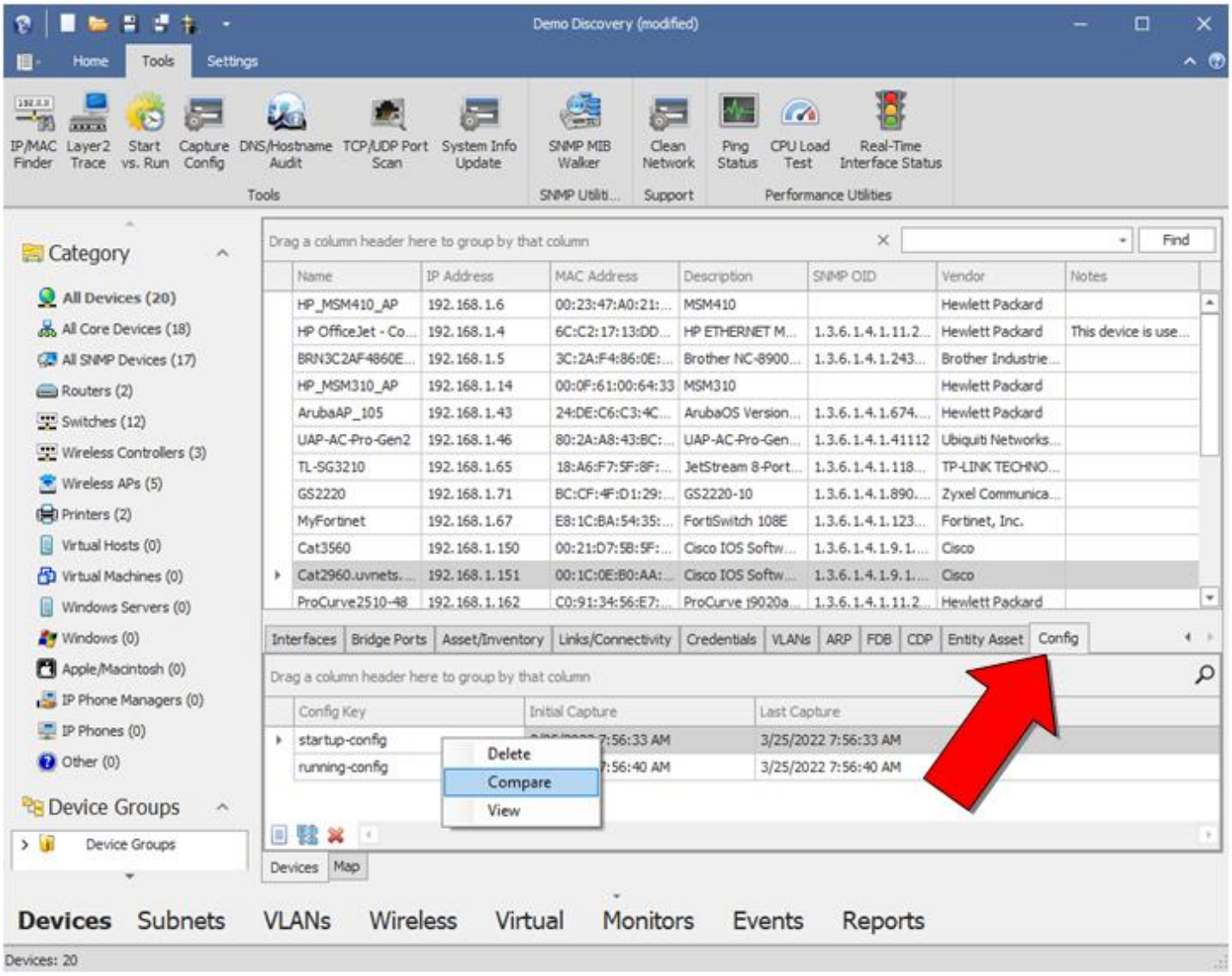
Launching the configuration difference viewer

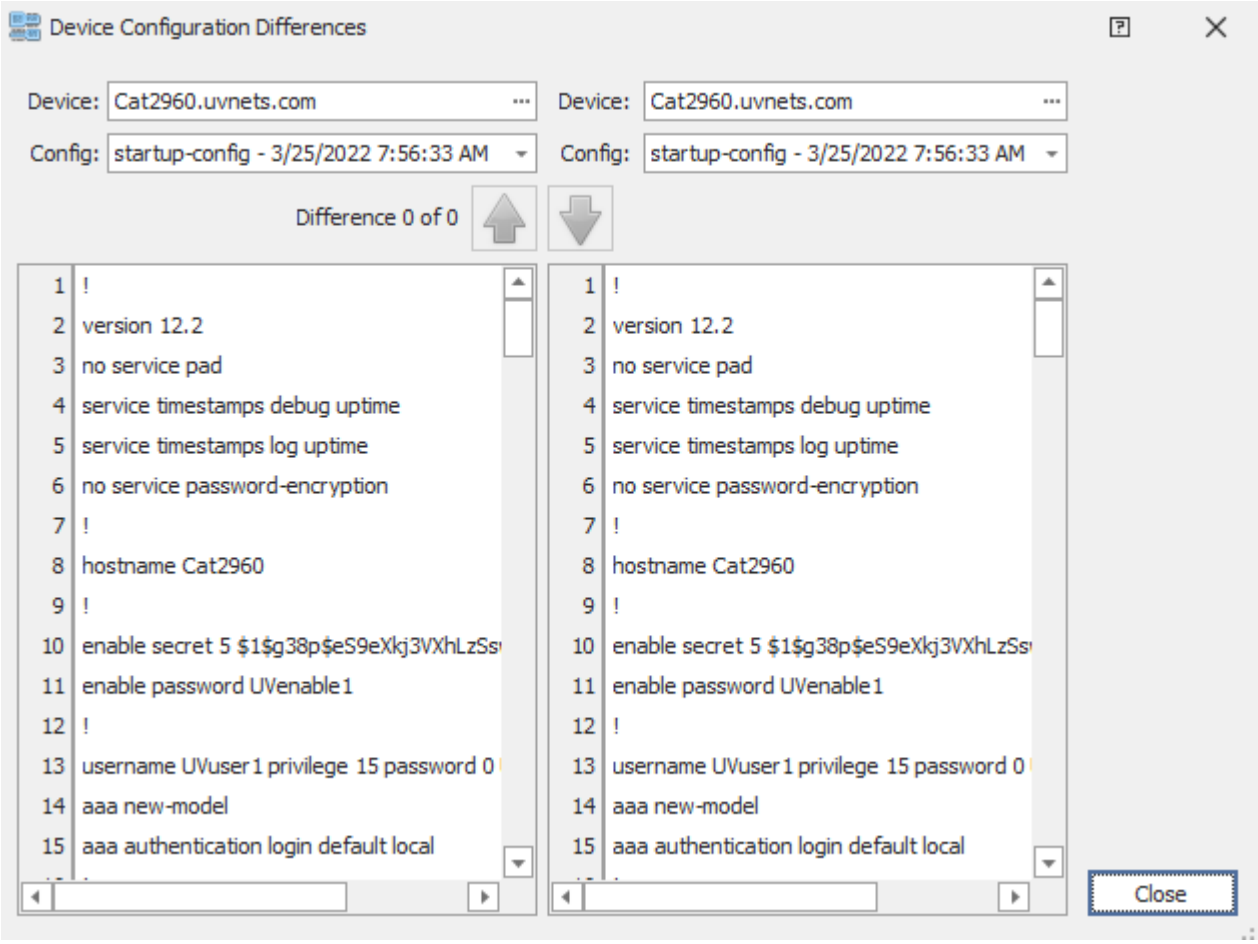
The configuration difference viewer can be launched from the 'Start vs. Run' Tool or from the Device Properties 'Config' tab.

From the Start vs. Run tool; select the device whose configurations you want to compare and select the 'Differences' button.



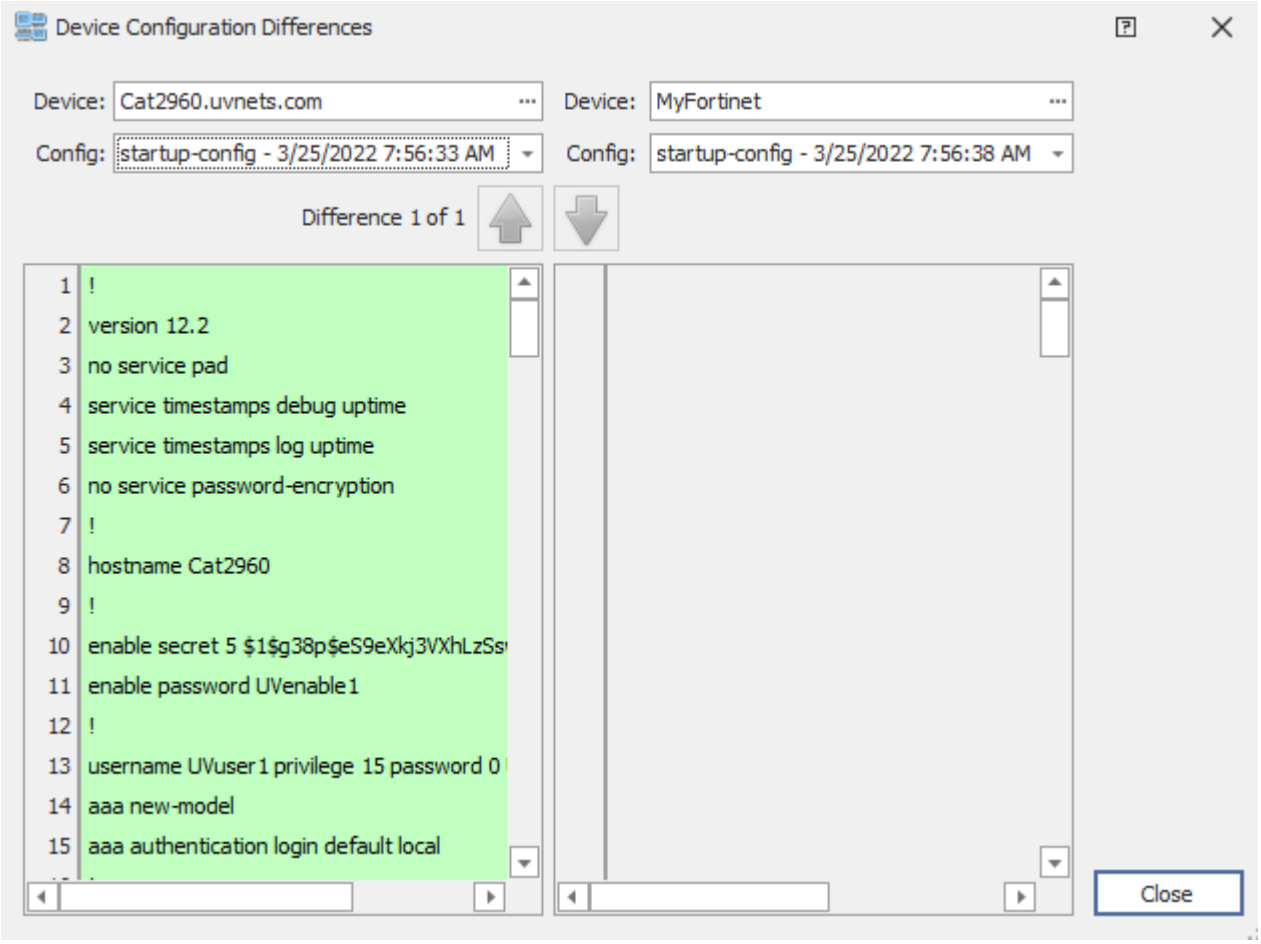
From the Device Properties 'Config' tab; select the configuration entry in the list and either use the right click context menu 'Compare' or select the compare button in the lower left corner of the grid.


Demo Discovery (modified)
Home
Tools
Settings
IP/MAC Finder
Layer2 Trace
Start vs. Run
Capture Config
DNS/Hostname Audit
TCP/UDP Port Scan
System Info Update
SNMP MIB Walker
Clean Network
Ping Status
CPU Load Test
Real-Time Interface Status
Tools
SNMP Utiliti...
Support
Performance Utilities
Category
All Devices (20)
All Core Devices (18)
All SNMP Devices (17)
Routers (2)
Switches (12)
Wireless Controllers (3)
Wireless APs (5)
Printers (2)
Virtual Hosts (0)
Virtual Machines (0)
Windows Servers (0)
Windows (0)
Apple/Macintosh (0)
IP Phone Managers (0)
IP Phones (0)
Other (0)
Device Groups
Device Groups
Drag a column header here to group by that column
Find
Name
IP Address
MAC Address
Description
SNMP OID
Vendor
Notes
HP_MSM410_AP 192.168.1.6 00:23:47:A0:21:... MSM410 Hewlett Packard
HP OfficeJet - Co... 192.168.1.4 6C:C2:17:13:DD... HP ETHERNET M... 1.3.6.1.4.1.11.2... Hewlett Packard This device is use...
BRN3C2AF4860E... 192.168.1.5 3C:2A:F4:86:0E:... Brother NC-8900... 1.3.6.1.4.1.243... Brother Industrie...
HP_MSM310_AP 192.168.1.14 00:0F:61:00:64:33 MSM310 Hewlett Packard
ArubaAP_105 192.168.1.43 24:DE:C6:C3:4C... ArubaOS Version... 1.3.6.1.4.1.674.... Hewlett Packard
UAP-AC-Pro-Gen2 192.168.1.46 80:2A:A8:43:BC:... UAP-AC-Pro-Gen... 1.3.6.1.4.1.41112 Ubiquiti Networks...
TL-SG3210 192.168.1.65 18:A6:F7:5F:8F:... JetStream 8-Port... 1.3.6.1.4.1.118... TP-LINK TECHNO...
GS2220 192.168.1.71 BC:CF:4F:D1:29:... GS2220-10 1.3.6.1.4.1.890.... Zyxel Communica...
MyFortinet 192.168.1.67 E8:1C:BA:54:35:... FortiSwitch 108E 1.3.6.1.4.1.123... Fortinet, Inc.
Cat3560 192.168.1.150 00:21:D7:5B:5F:... Cisco IOS Softw... 1.3.6.1.4.1.9.1.... Cisco
Cat2960.uvnets.... 192.168.1.151 00:1C:0E:B0:AA:... Cisco IOS Softw... 1.3.6.1.4.1.9.1.... Cisco
ProCurve2510-48 192.168.1.162 C0:91:34:56:E7:... ProCurve j9020a... 1.3.6.1.4.1.11.2... Hewlett Packard
Interfaces
Bridge Ports
Asset/Inventory
Links/Connectivity
Credentials
VLANs
ARP
FDB
CDP
Entity Asset
Config
Drag a column header here to group by that column
Config Key
Initial Capture
Last Capture
startup-config 3/25/2022 7:56:33 AM
running-config 3/25/2022 7:56:40 AM
Delete
Compare
View
Devices
Map
Devices
Subnets
VLANs
Wireless
Virtual
Monitors
Events
Reports
Devices: 20

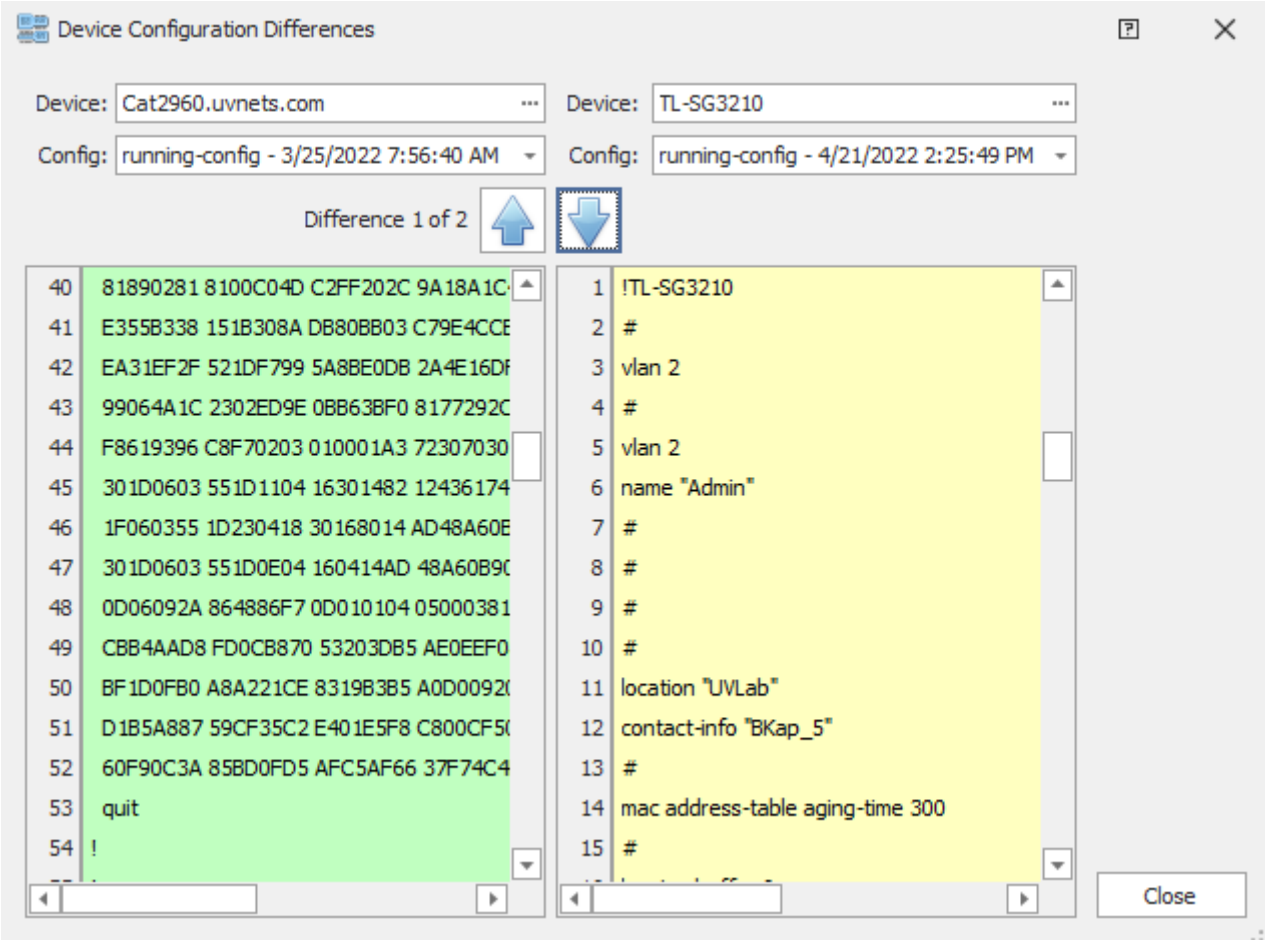


Using the Configuration Difference Viewer

The difference viewer has a device and configuration entry selector for two devices and configurations. Each selector must have a device and configuration selected before the configurations will be displayed in the difference comparer. The same or different devices may be selected in the device selectors. The configuration selector will display all available configurations for the device. If no configurations are available, the selector will be empty.



Once two configurations are selected the number of differences will be displayed next to the navigation buttons above the configurations. The differences can be viewed using the next or previous navigation buttons or by scrolling both configurations.



Supported Devices

UVexplorer will attempt to run a default/generic script against any device that has an SNMP OID beginning with "1.3.6.1.4.1". If the device is supported and more specific commands are necessary/available alternative scripts and settings will be used.

The currently supported devices include:

Aruba
Cisco
D-Link
Dell
HP
Extreme
Juniper
Nortel
3Com

Other devices/vendors not listed will likely work with the default scripts and settings.

PRTG Connector

PRTG Network Monitor™ is an industry leading network monitoring solution provided by Paessler AG. UVexplorer can export your discovered networks and devices to PRTG, improving the discovery experience and automating the creation of device groups, topology maps and monitors within PRTG. UVexplorer also supports displaying the status of PRTG monitors within UVexplorer.

Exporting to PRTG
PRTG Monitor
PRTG Server Settings

Exporting to PRTG

UVexplorer can export your discovered devices and topology maps to PRTG Network Monitor™, improving the discovery experience and automating the creation of device groups, topology maps and monitors within PRTG. Your discovered devices can be exported manually or on a scheduled basis at the completion of a scheduled discovery.

PRTG Export Wizard
Scheduled Discovery PRTG Export
Topology Map PRTG Export

Beginning PRTG export

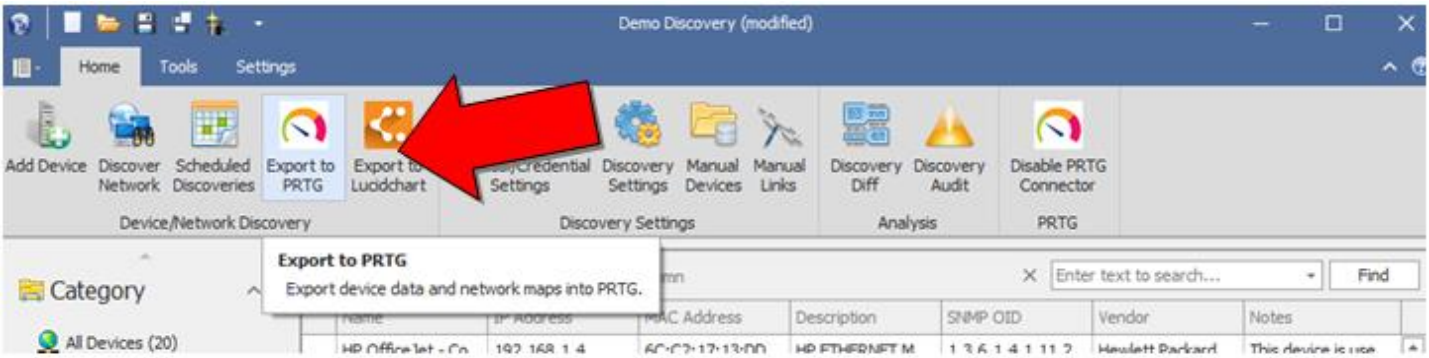
Scheduled Discovery Export

UVexplorer can be configured to export discovery results to PRTG at the completion of a scheduled discovery. The scheduled export configuration settings are available in the 'PRTG Export' tab of the Scheduled Discovery configuration and are described below. The export will occur at the completion of each scheduled discovery if changes are detected. Each export will update any prior export synchronizing the results.

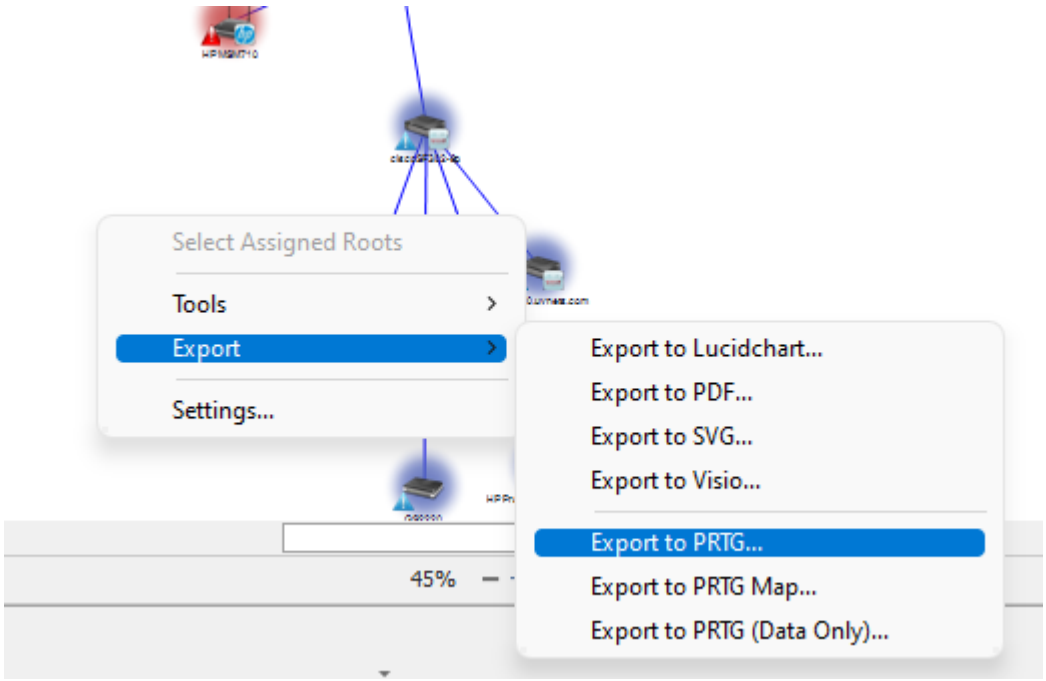
See Scheduling Network Discoveries for more information on scheduled discoveries.

Manual Export

UVexplorer provides a wizard to step you through the process of exporting your devices to PRTG. The wizard can be accessed by clicking the 'Export to PRTG' button in the 'Home' ribbon; this option is only available if you have a network with at least one device open in UVexplorer.



You can also export using the export dialog, which is accessed from the topology map context menu by right clicking on a topology map and selecting 'Export - Export to PRTG...'.



Configuring PRTG Export

The settings available in the PRTG export dialogs are described below.

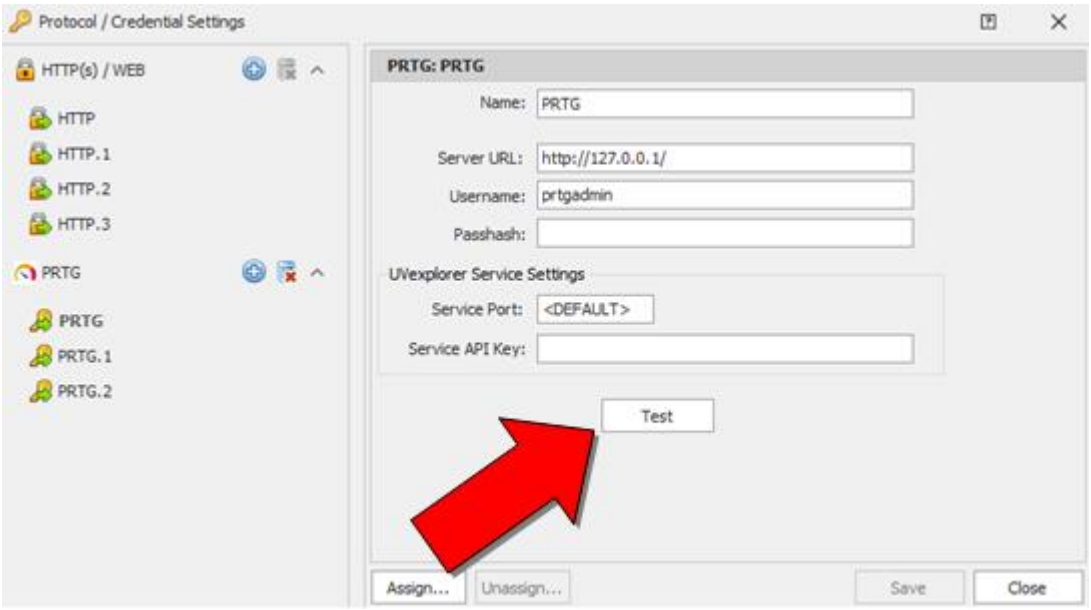
PRTG Server Settings

To export to PRTG, UVexplorer needs to communicate with your PRTG server.

See PRTG Server Settings for more information on configuring the server settings.

Testing Server Configuration

PRTG server configuration can be tested within the PRTG export wizard by selecting the 'Test' button. UVexplorer will attempt to communicate with the PRTG server using the URL, username and passhash provided. If the server is available a message displaying the PRTG version will be displayed.



Device Group

The device group is the Group on the PRTG server the devices will be exported to.

Parent Group

Parent Group is the parent group of the new or exported group. The parent group must be chosen by selecting the 'Browse' button, a list of Groups available on the PRTG server will be presented.

Group Name

This is the Group the devices will be exported to. If you are creating a new group, type the name of the group here and ensure the 'Create New Group' check box is selected. If you are using an existing group, select the group using the 'Browse' button and ensure the 'Create New Group' box is not selected.

Create A Matching Topology Map

PRTG provides maps of device groups. When groups are exported from UVexplorer the map associated with that group can be exported as well. When this option is selected a layer 2 map containing devices and links will be included as part of the export.

Overwrite Existing Map

If this option is selected the existing PRTG map will be replaced by the new map.

Devices To Export

When exporting a topology map to PRTG the exported devices are those included in the map. When exporting using the PRTG wizard the devices are selected by pressing the '+' button and choosing the devices from the picker.

PRTG Monitor Settings

When devices are exported to PRTG, UVexplorer can automatically create monitors for those devices. Monitors are created using detailed knowledge of the devices, such as creating interface monitors only for interfaces that have connections. To create monitors on export, select which

monitors you would like to include and UVexplorer will make sure those monitors are only created for devices where it makes sense.

PRTG Status Monitor

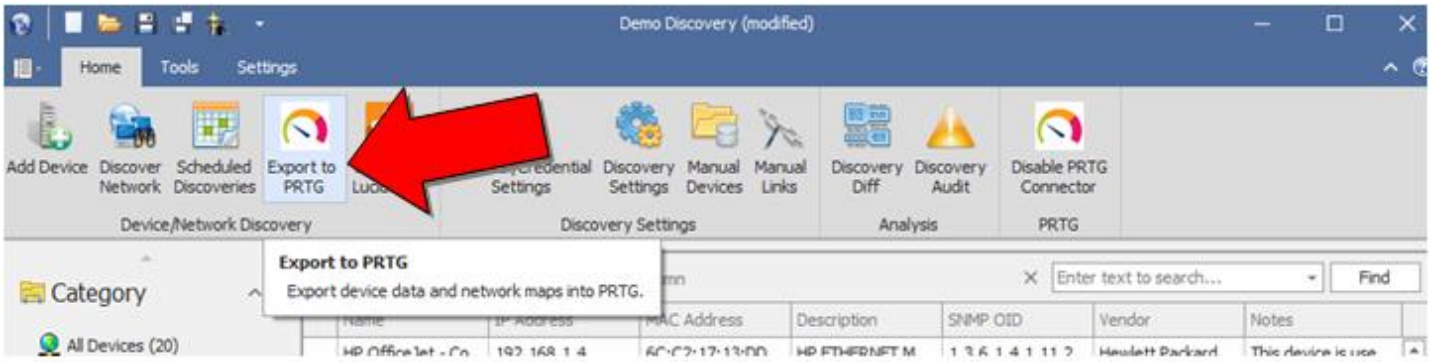
UVexplorer can report the status of PRTG monitors on devices exported to PRTG.

See PRTG Status Monitor for more information.

PRTG Export Wizard

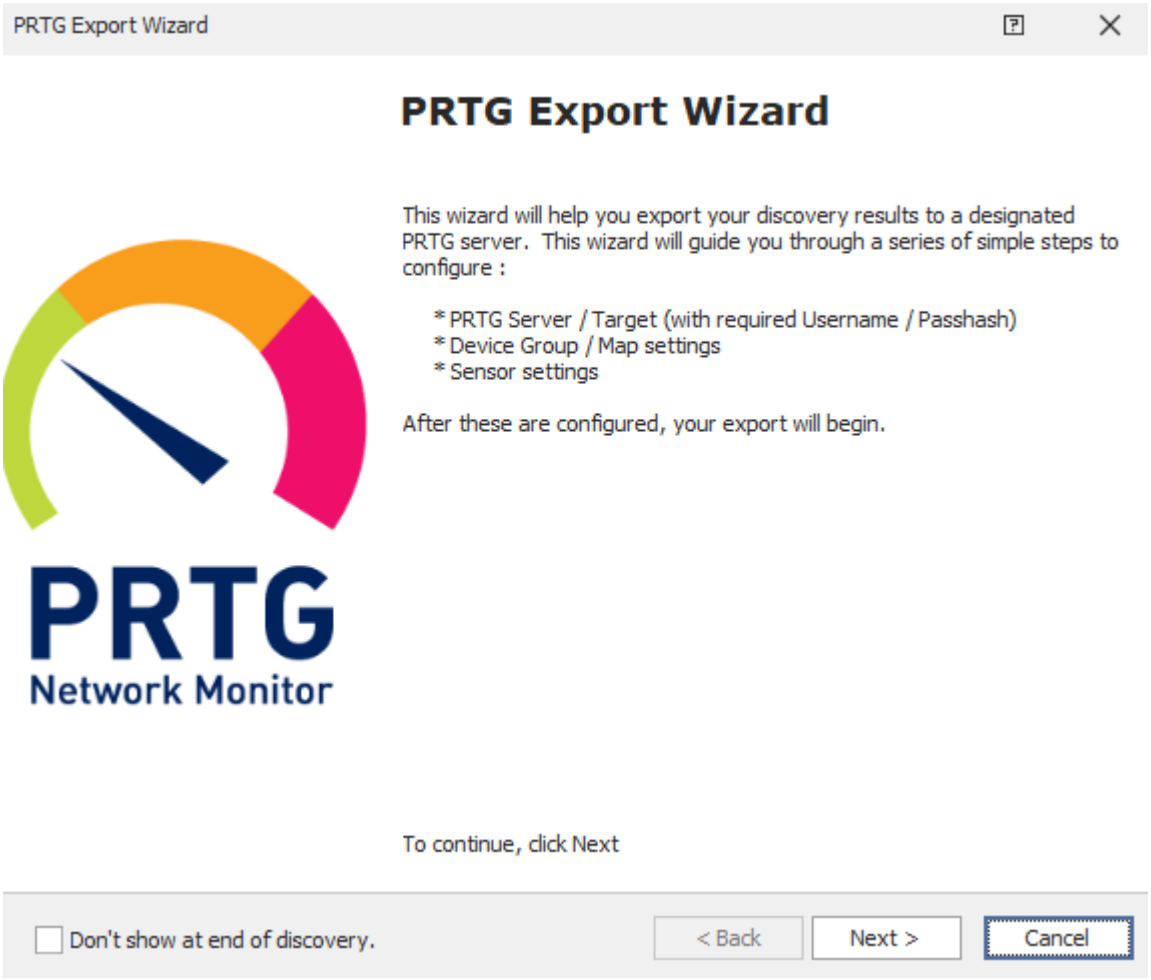
The PRTG Export wizard walks you through the process of manually exporting a device group to PRTG

The wizard can be opened by selecting the 'Export To PRTG' button on the 'Home' ribbon.



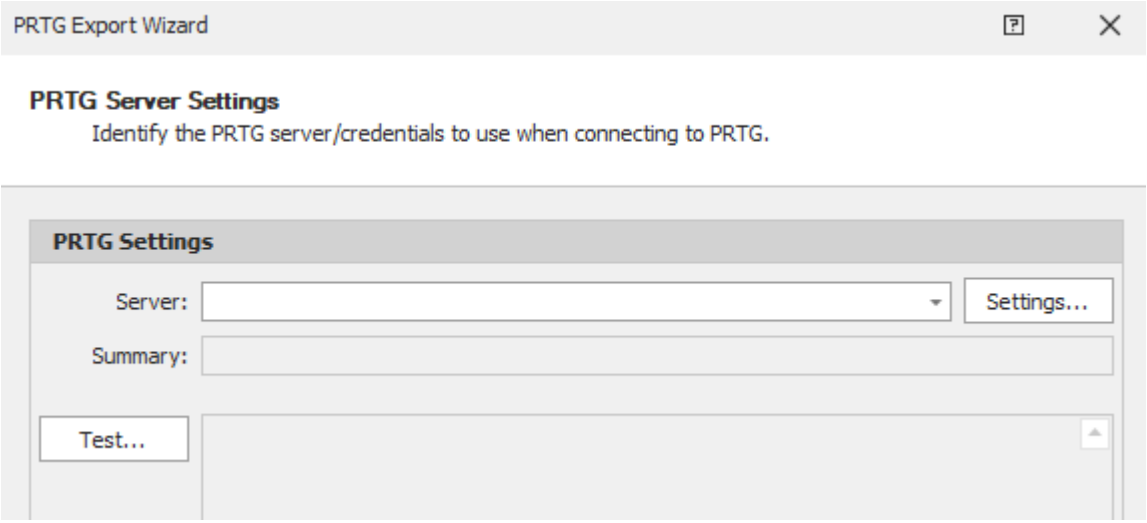
Running the Wizard

The settings on the export wizard pages are described below.



PRTG Server Settings

To export to PRTG, UVexplorer needs to communicate with your PRTG server.



Server
The server settings drop down list is used to select an available PRTG server to export to. If your server is not shown in the list, you will need to configure the PRTG server settings using the 'Settings' button to the right of the list.

See PRTG Server Settings for more information on configuring the server settings.

Summary
The summary provides a brief description of the configuration of the selected PRTG server settings.

Test
PRTG server configuration can be tested by selecting the 'Test' button. UVexplorer will attempt to communicate with the PRTG server using the URL, username and passhash provided. If the server is available a message displaying the PRTG version will be displayed.

Device Group / Map

Parent Group
Parent Group specifies the parent of the PRTG group the devices will be exported to. The parent group must be chosen by selecting the 'Browse' button, a list of Groups available on the PRTG server will be presented.

Device Group
Device group specifies the group the devices will be exported to. If you are creating a new group, type the name of the group here and ensure the 'Create New Group' check box is selected. If you are exporting to an existing group, select the group using the 'Browse' button and ensure the 'Create New Group' box is not selected.

Create New Group
Create new group specifies whether the export will be to a new or existing group. If create new is not specified and an existing group is not found under the parent group, then a new group will be created.

Create Topology Map
Create topology map specifies that the topology map associated with the device group being exported, in this case the map used to launch the export dialog, should be exported as a new PRTG map. When a UVexplorer topology map is exported all the devices, background images, and links are exported as a PRTG map.

Overwrite Existing Map

Overwrite existing map specifies that rather than creating a new map, the existing PRTG map associated with the device group being exported should be overwritten.

Note: This will replace the PRTG map and may result in loss of data, including any changes you have made within PRTG to a previously exported map.

Devices to Export

When exporting using the wizard you specify which devices to export by pressing the 'plus' button in the bottom left of the device list.

PRTG Sensor Settings

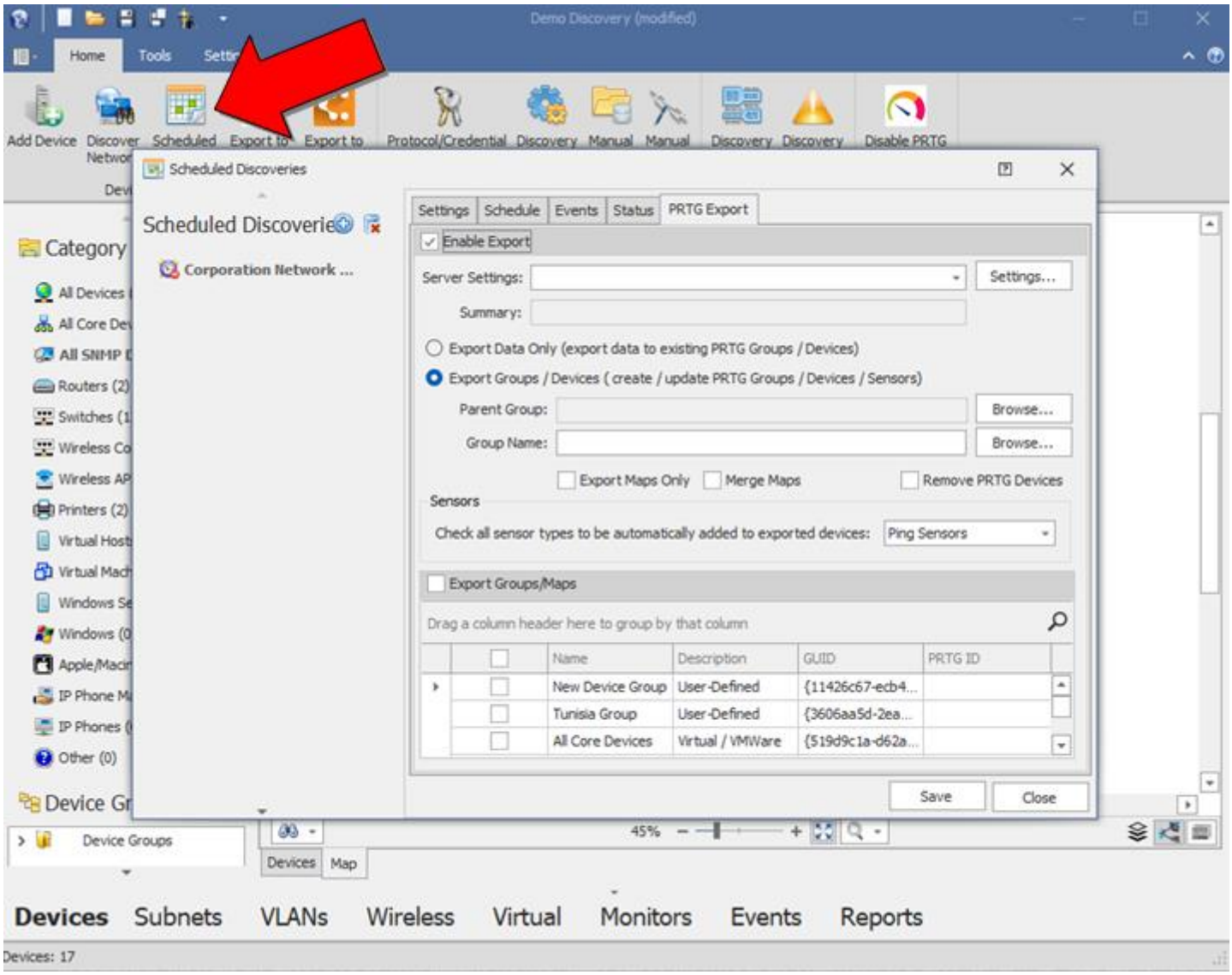
When devices are exported to PRTG UVexplorer can automatically create monitors for those devices. Monitors are created using detailed knowledge of the devices, such as creating interface monitors only for interfaces that have connections. To create monitors on export, select which monitors you would like to include and UVexplorer will make sure those monitors are only created for devices where it makes sense.

PRTG Status Monitor

UVexplorer can report the status of PRTG monitors on devices exported to PRTG. See PRTG Status Monitor for more information. Select this option to create a status monitor for the exported devices.

Scheduled Discovery PRTG Export

When a scheduled discovery completes the discovered devices and selected topology maps can be exported to PRTG. This allows UVexplorer to update devices in PRTG as changes are discovered.



Export Configuration

Enable Export
Specifies whether to export at discovery completion. This also provides a convenient way to pause export if needed.

Server Settings
To export to PRTG, UVexplorer needs to communicate with your PRTG server.

The server settings drop down list is used to select an available PRTG server to export to. If your server is not shown in the list, you will need to configure the PRTG server settings using the 'Settings' button to the right of the list.

See PRTG Server Settings for more information on configuring the server settings.

Summary
The summary provides a brief description of the configuration of the selected PRTG server settings.

Parent Group
Parent Group specifies the parent of the PRTG group the devices will be exported to. The parent group must be chosen by selecting the 'Browse' button, a list of Groups available on the PRTG server will be presented.

Group Name
This specifies the group the devices will be exported to. Type the name of the group here. A new group will be created on the initial discovery and updated thereafter.

Sensors
When devices are exported to PRTG UVexplorer can automatically create monitors for those devices. Monitors are created using detailed knowledge of the devices, such as creating interface monitors only for interfaces that have connections. To create monitors on export, select which monitors you would like to include and UVexplorer will make sure those monitors are only created for devices where it makes sense.

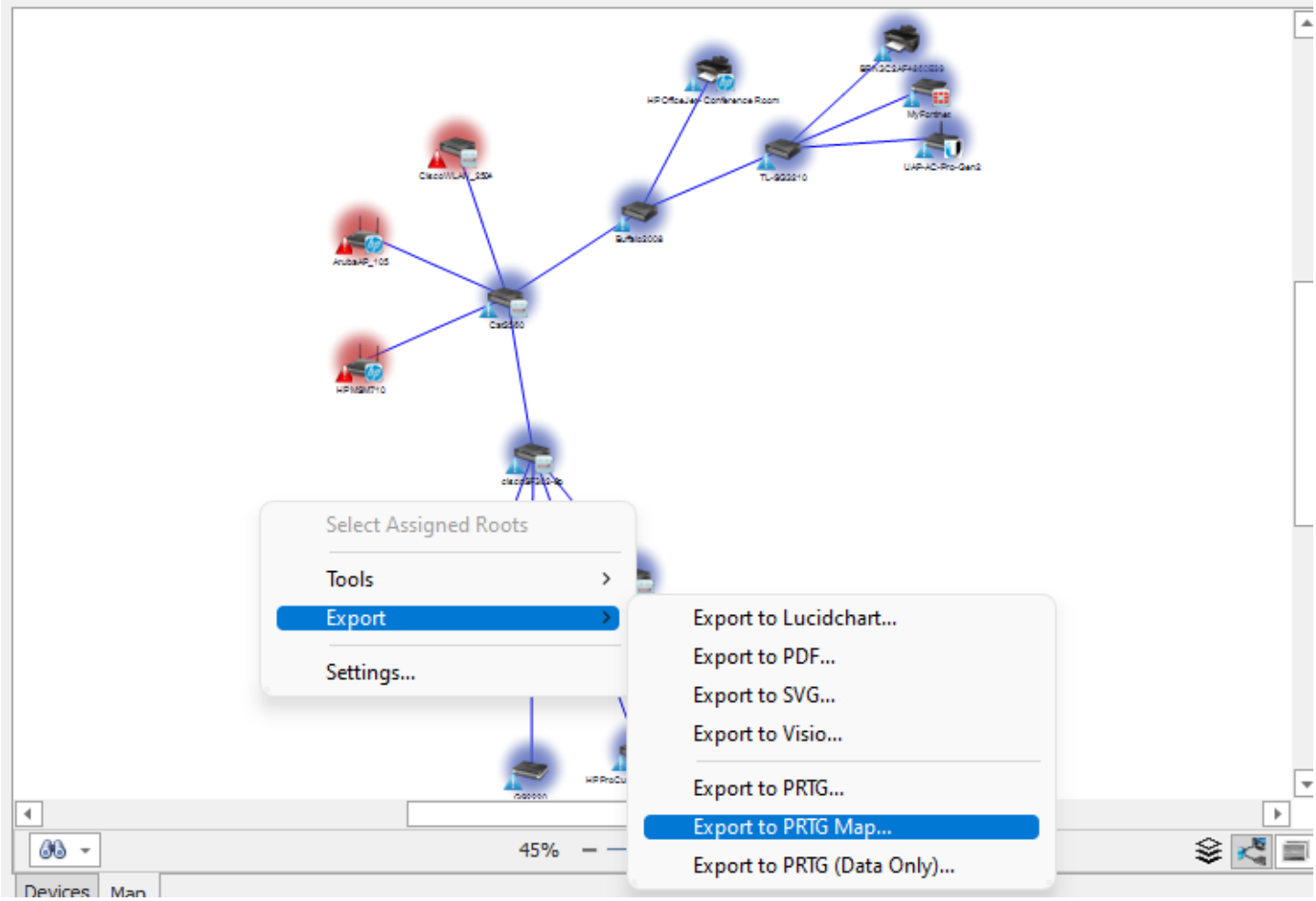
Create Device/Sensors using Template Tags
Exported devices can be configured by cloning an existing PRTG device. Select this option to create devices and sensors by cloning PRTG devices/sensors. Select the 'View/Edit Tag Mappings' button to manage the export template configuration.

See PRTG Export Templates for more information.

Export Maps
In addition to exporting the discovered devices, multiple topology maps can be exported at the completion of a discovery as well. This allows you to keep the topology maps updated on a recurring basis, as changes are detected.

Topology Map PRTG Export

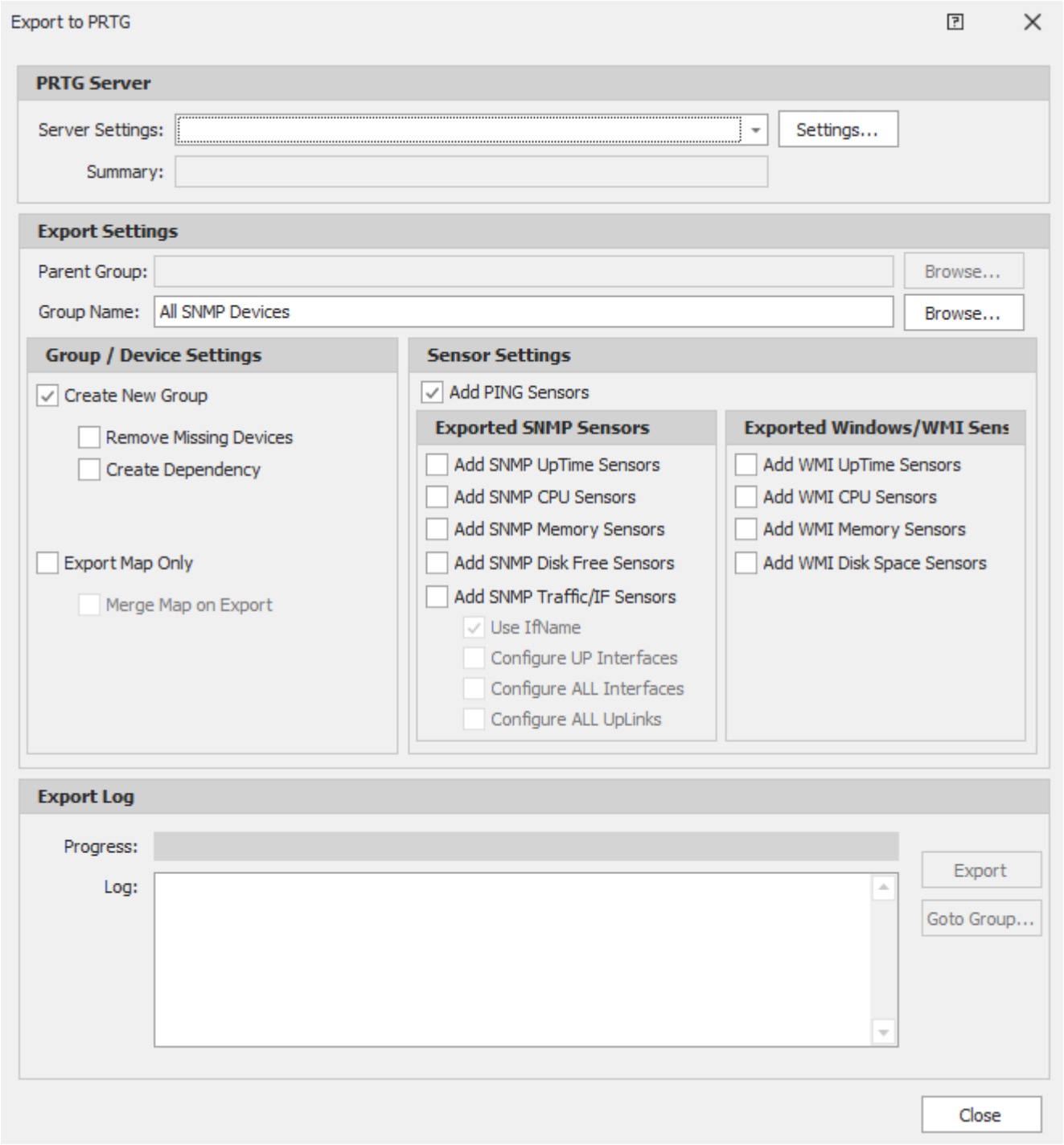
Topology maps can be exported to PRTG using the export dialog, which is accessed from the topology map context menu by right clicking on a topology map and selecting 'Export' then 'Export to PRTG Map...'.



When a topology map is exported to PRTG you can export the device group, devices in the group, and the map. The export can create a new map or update an existing map.

Configuring PRTG Export

The settings available in the PRTG topology map export dialog is described below.



PRTG Server

To export to PRTG, UVexplorer needs to communicate with your PRTG server.

Server Settings

The server settings drop down list is used to select an available PRTG server to export to. If your server is not shown in the list, you will need to configure the PRTG server settings using the 'Settings' button to the right of the list. See PRTG Server Settings for more information on configuring the server settings.

Summary

The summary provides a brief description of the configuration of the selected PRTG server settings.

Export Settings

Parent Group

Parent Group specifies the parent of the PRTG group the devices will be exported to. The parent

group must be chosen by selecting the 'Browse' button, a list of Groups available on the PRTG server will be presented.

Device Group
Device group specifies the group the devices will be exported to. If you are creating a new group, type the name of the group here and ensure the 'Create New Group' check box is selected. If you are exporting to an existing group, select the group using the 'Browse' button and ensure the 'Create New Group' box is not selected.

Create New Group
Create new group specifies whether the export will be to a new or existing group. If create new is not specified and an existing group is not found under the parent group, then a new group will be created.

Create Topology Map
Create topology map specifies that the topology map associated with the device group being exported, in this case the map used to launch the export dialog, should be exported as a new PRTG map. When a UVexplorer topology map is exported all the devices, background images, and links are exported as a PRTG map.

Overwrite Existing Map
Overwrite existing map specifies that rather than creating a new map, the existing PRTG map associated with the device group being exported should be overwritten.

Note: This will replace the PRTG map and may result in loss of data, including any changes you have made within PRTG to a previously exported map.

Create Devices/Sensors using Template Tags
Exported devices can be configured by cloning an existing PRTG device. Select this option to create devices and sensors by cloning PRTG devices/sensors. Select the 'View/Edit' button to manage the export template configuration.

See PRTG Export Templates for more information.

Create PRTG Status Monitor
UVexplorer is able to report the status of PRTG monitors on devices exported to PRTG. Select this option to create a status monitor for the exported devices.

See PRTG Status Monitor for more information.

Sensor Settings
When devices are exported to PRTG UVexplorer can automatically create monitors for those devices. Monitors are created using detailed knowledge of the devices, such as creating interface monitors only for interfaces that have connections. To create monitors on export, select which monitors you would like to include and UVexplorer will make sure those monitors are only created for devices where it makes sense.

Export Log
UVexplorer will provide an export log including the progress and the devices exported to PRTG.

Export
To begin the export, select the 'Export' button. The export will begin, and details of the export will display in the log. When the export is complete a message will appear in the log.

Go To Group
Go to group will take you to the newly created/updated group in the PRTG browser.

PRTG Export Templates

PRTG provides the ability to create new devices and sensors by cloning existing devices and sensors. Cloning an existing device or sensor provides the ability to easily apply a base configuration to the cloned device. When UVexplorer exports a device to PRTG it can leverage this cloning ability ensuring your PRTG specific configurations are applied to all exported devices of a given type.

To specify a device/sensor to use as a base configuration UVexplorer uses the PRTG tags associated with the device/sensor. Once a PRTG device/sensor has been assigned a tag, that tag can be mapped within UVexplorer to a device type, indicating that all devices of that type should be created by first cloning the PRTG device with the same tag.

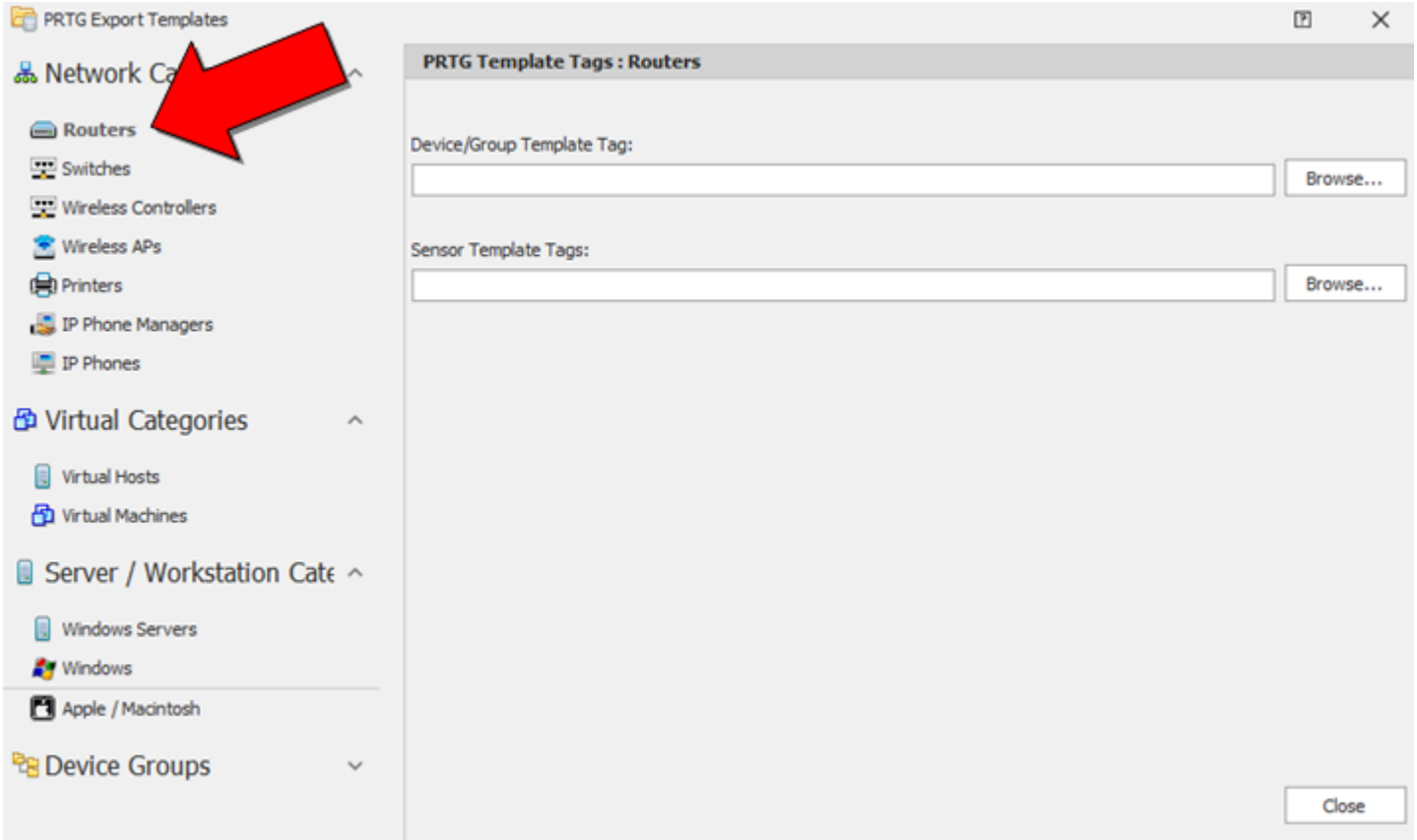
Note: It is recommended you keep tags used with templates unique per device/sensor.

Managing Templates

The templates can be managed in the PRTG export templates dialog. To open the dialog select 'PRTG Export Settings' in the 'Settings' ribbon. The dialog can also be opened from the edit templates button in each of the PRTG export dialogs.

Configuring Templates

Template tags can be specified for each UVexplorer category or device group. To configure the templates for a category/group select it in the navigation pane on the right.



Device/Group Template Tag:
Device/Group template tag specifies the tag on a template PRTG device or a template PRTG group. In the case that the tag matches a PRTG group, a device in the specified category is exported with the same PRTG group structure as the template. For example, the top-level group (or parent group) will be named after the device, and all sub-devices under the group will be configured as PRTG devices with the IP Address/Hostname of the exported device.
If the tag matches a PRTG device, all devices in the specified category will be exported as clones of the template device.

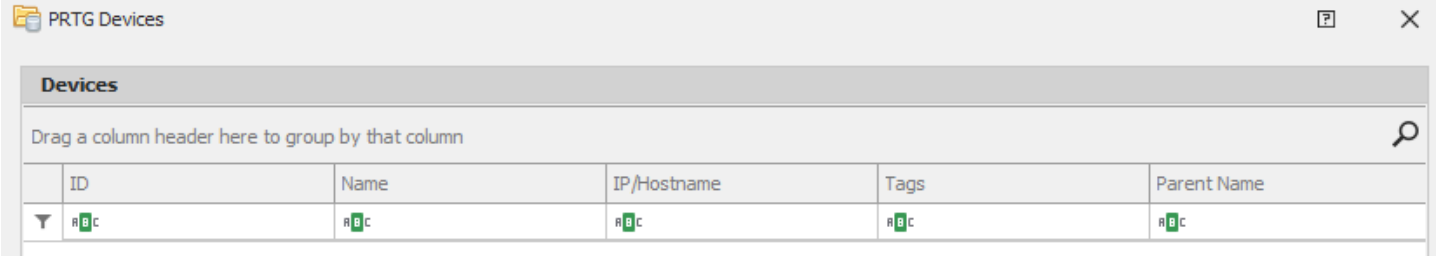
Note: Group tags are given priority over a Device tag and therefore should not be "mixed". Either this template maps to a PRTG group template or to a PRTG device template. Not both. To view the tags available on the PRTG devices select the 'Browse' button.

Sensor Template Tags:
Sensor template tags specifies the tags of the sensors to clone and include. To specify multiple sensor tags for a category tag can be separated by comma or space. To view the tags available on the PRTG sensors select the 'Browse' button.

Example:
If you have specific PRTG settings, you want configured for all devices that support the SNMP protocol. You would start by creating and configuring a device within PRTG with your desired PRTG settings. You would then add a unique PRTG tag to the device such as 'uvexplorer_snmp_template'.

PRTG Devices

The PRTG Devices viewer provides a way to view the devices and their associated tags available from the provided PRTG server. This is primarily a convenience to allow you to view what tags are available on your devices for use in templating configurations for PRTG export.



The following information is available:

ID
The PRTG device identifier.

Name
The PRTG device name.

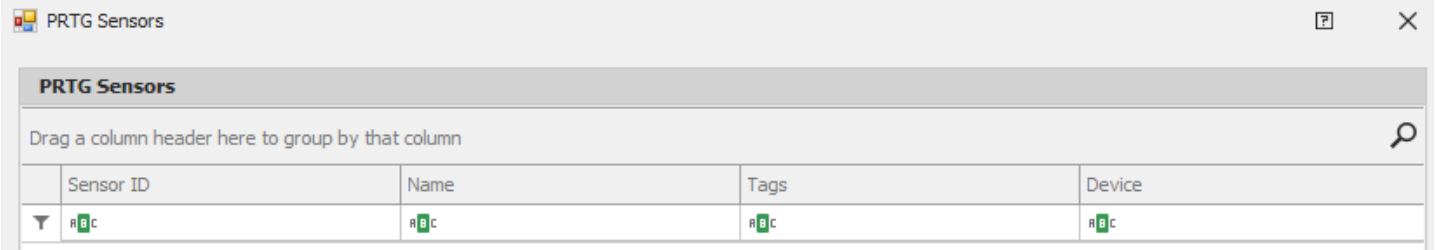
IP/Hostname
The PRTG device IP address or hostname.

Tags
A list of any tags available on the device. These are the values to use when mapping to a device for export.

Parent Name
The name of the PRTG group the PRTG device participates in.

PRTG Sensors

The PRTG Sensors viewer provides a way to view the sensors and their associated tags available from the provided PRTG server. This is primarily a convenience to allow you to view what tags are available on your sensors for use in templating configurations for PRTG export.



The following information is available:

Sensor ID
The PRTG sensor identifier.

Name
The PRTG sensor name.

Tags
A list of any tags available on the sensor. These are the values to use when mapping to a sensor for export.

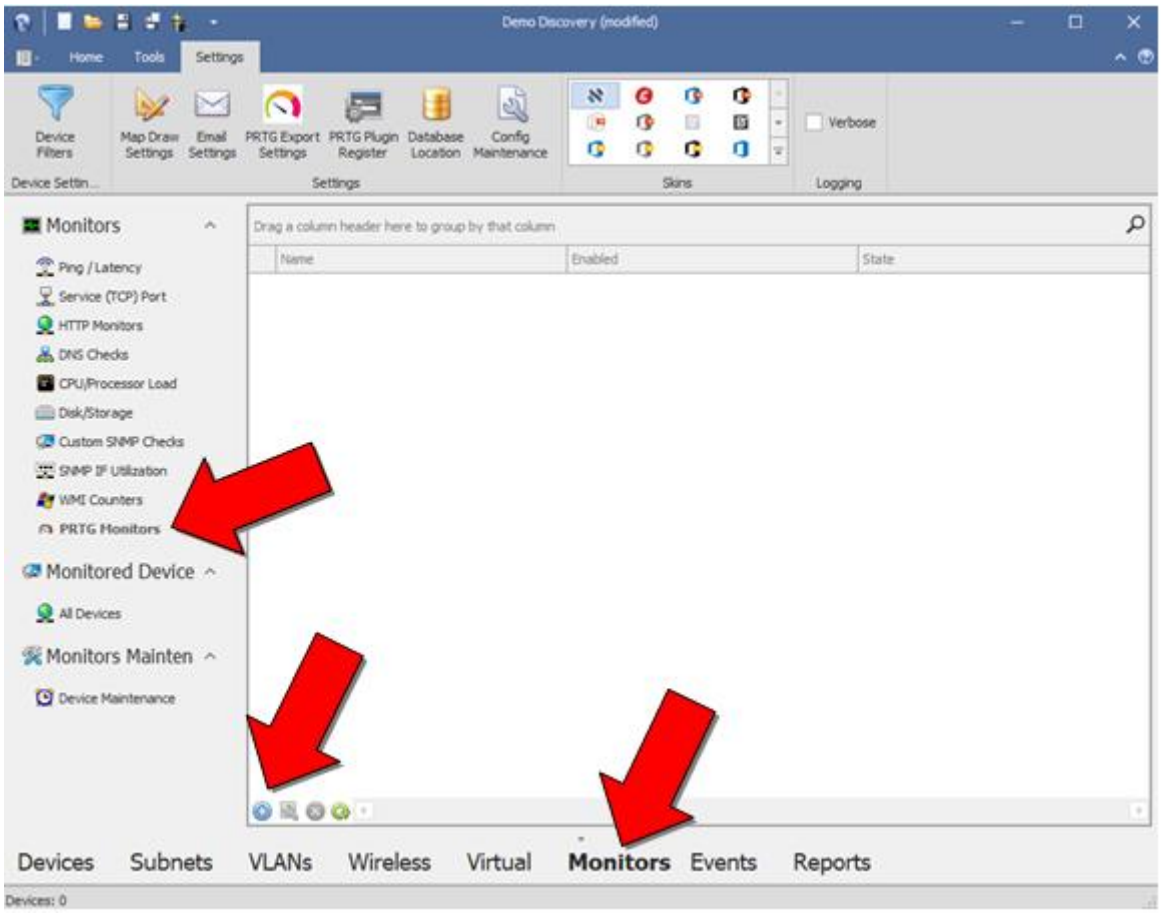
Device
The name of the PRTG device the PRTG sensor is assigned to.

PRTG Status Monitor

The PRTG Status monitor is used to display the status of PRTG monitors within UVexplorer. When enabled UVexplorer will poll the status of the PRTG device state and display that state within UVexplorer. UVexplorer can also alert on changes to the state of a PRTG monitor.

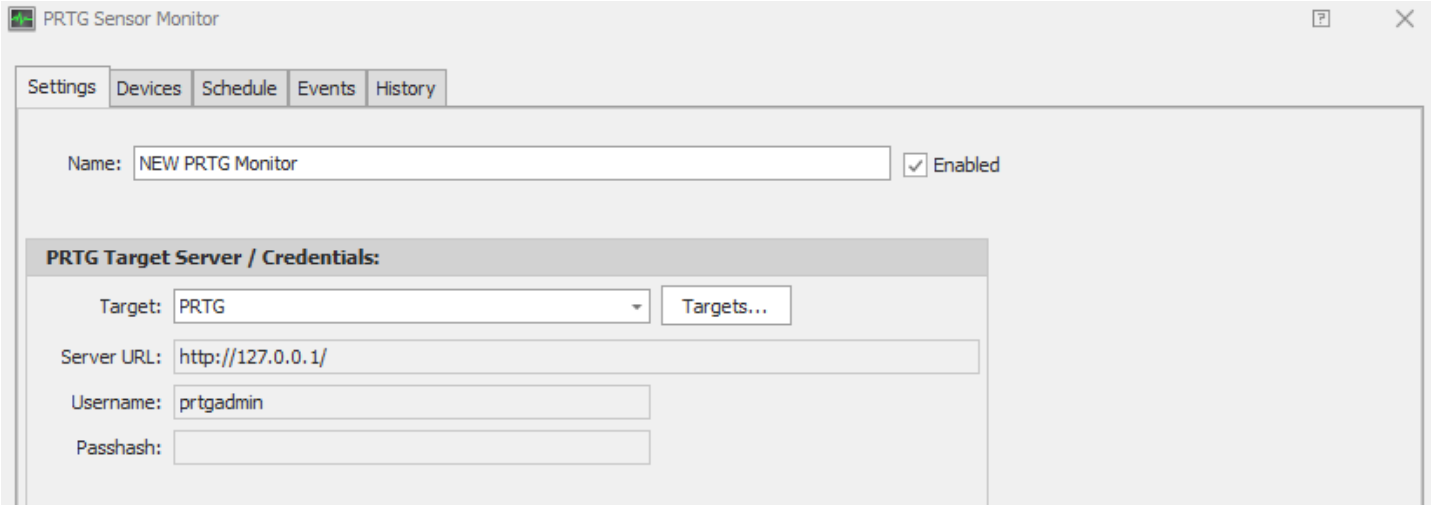
Creating a PRTG monitor

A PRTG monitor can be created automatically when devices are exported to PRTG by selecting the 'Create PRTG status monitor' option. PRTG monitors can also be created in the UVexplorer monitor section by selecting 'PRTG Monitors' in the left pane and pressing the '+' button in the bottom left corner of the center pane. Created monitors can be edited by selecting the wrench button in the bottom left of the center pane.



Configuring a PRTG monitor

Settings



Name

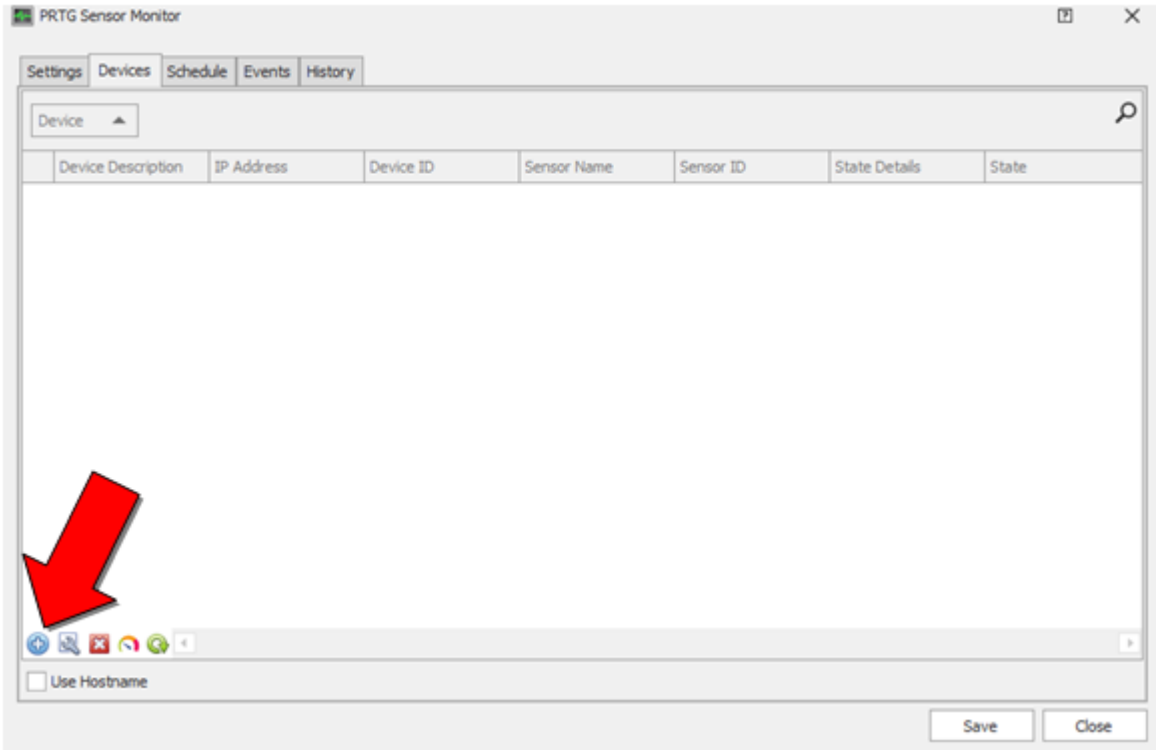
The monitor's name is used to reference the monitor within the application and when monitor notifications are created.

PRTG Target Server

The PRTG target is the PRTG server whose devices states will be monitored. See PRTG Server Settings for more information on configuring PRTG server settings.

Devices

The devices tab shows the devices monitored by the current monitor. The monitor state of the device will be displayed here as well.



Adding Devices

Devices can be added to the monitor by pressing the '+' button in the lower left corner of the device list. A device picker will be presented containing the devices available to monitor. See Monitor Device Picker for more information on adding devices to monitors.

Removing Devices

Devices can be removed from the monitor by selecting them in the device list and pressing the 'x' button.

Device Sensors

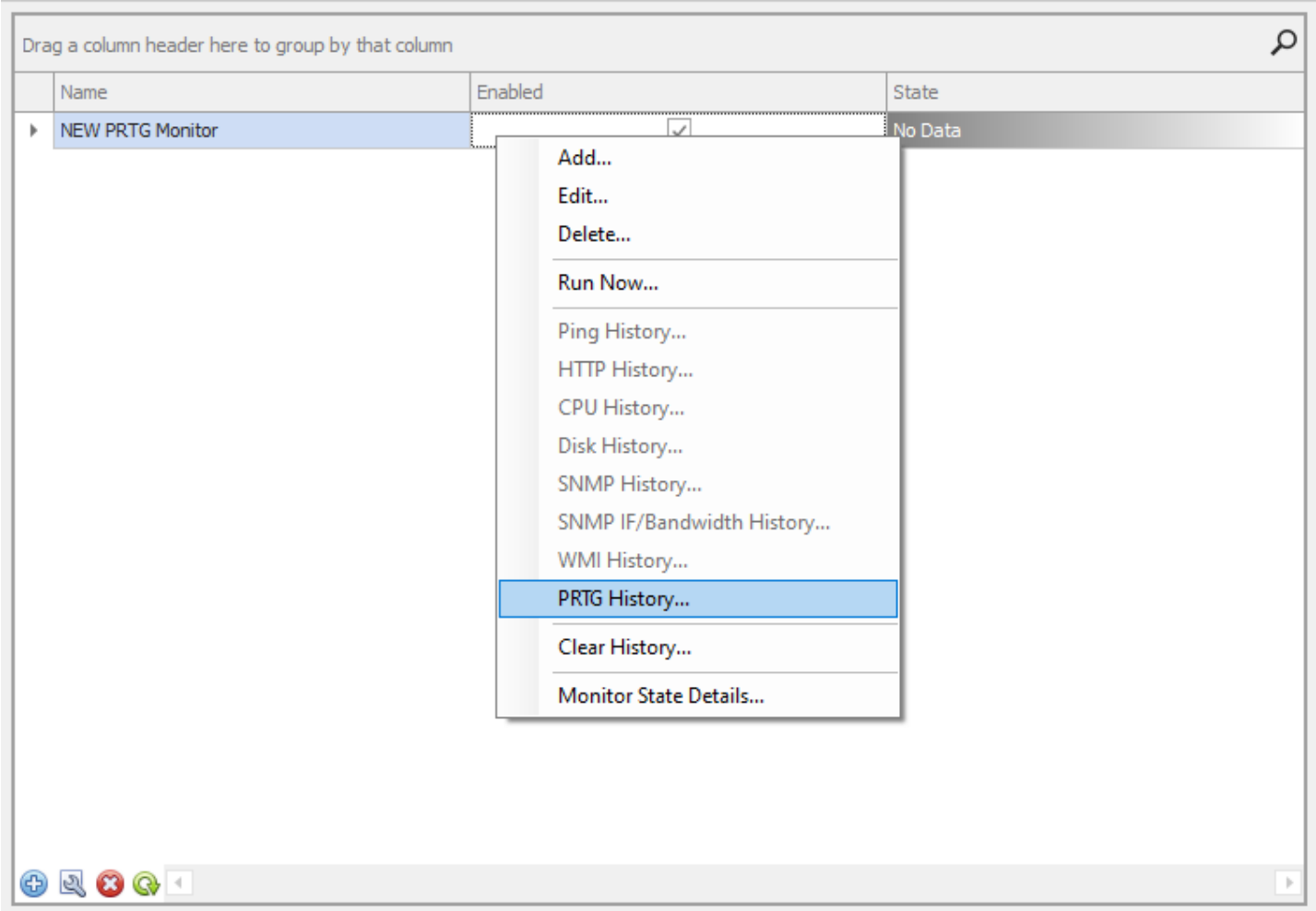
UVexplorer allows you to specify which PRTG sensors to monitor within the PRTG Monitor. When a PRTG Monitor is created by exporting devices and groups to PRTG the sensors selected at export will be added to the Monitor. To add or change sensors from the PRTG monitor editor either double select a device in the list or select the device in the list and press the 'wrench' button in the lower left corner of the list. An editor containing the available monitors will be presented.

Schedule / Events / History

See Configuring Monitors for information about configuring the schedule, events, and history of a monitor.

PRTG Status Monitor History

The PRTG Status Monitor History contains a historical view of the state of a PRTG sensor monitored by UVexplorer. To open the PRTG History dialog right click a PRTG monitor and select the 'PRTG History...' item in the context menu.

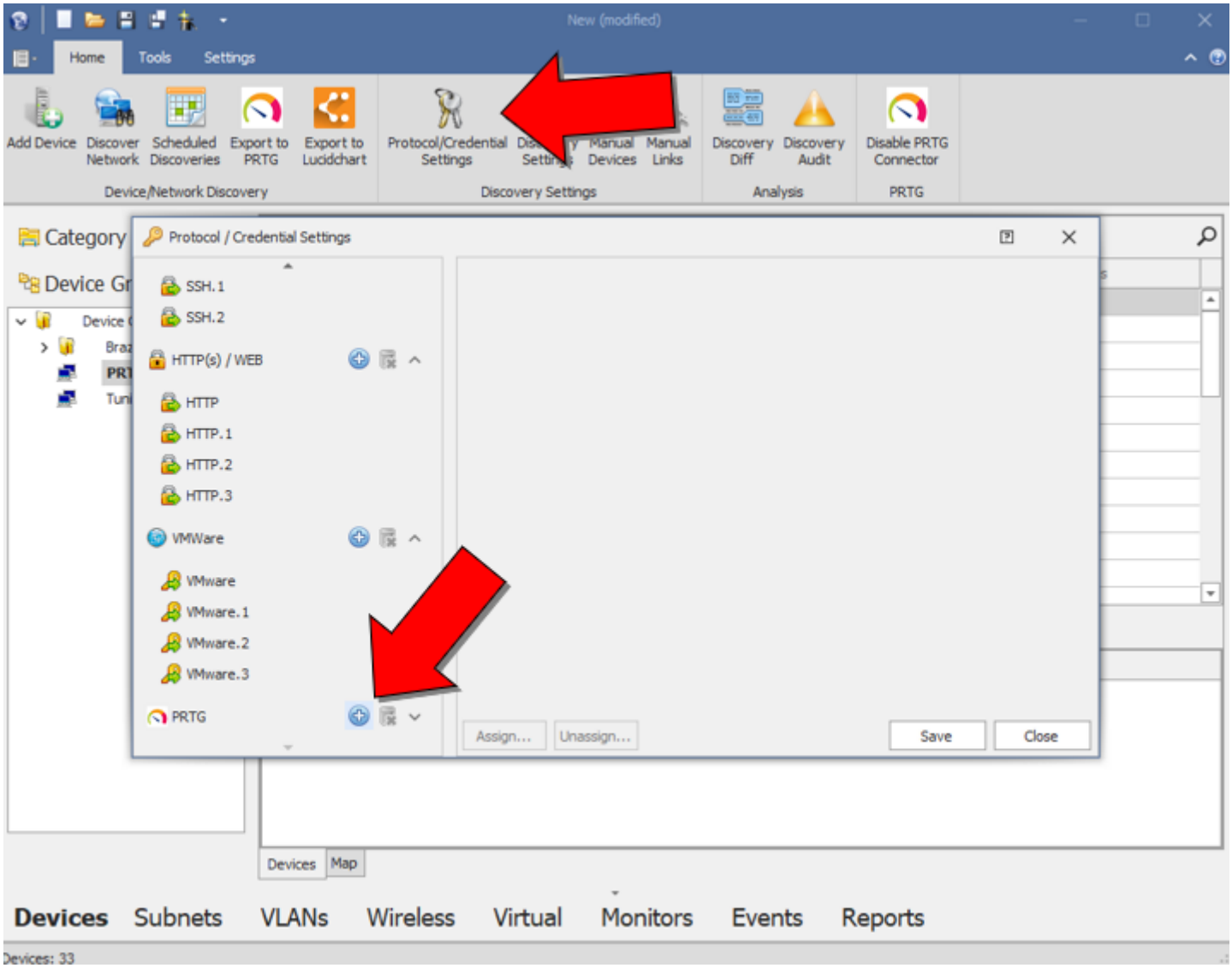


The history dialog contains a list of all the devices and sensors participating in the monitor. The columns display the time the sensor state was polled and the state of the sensor at that time.

PRTG Server Settings

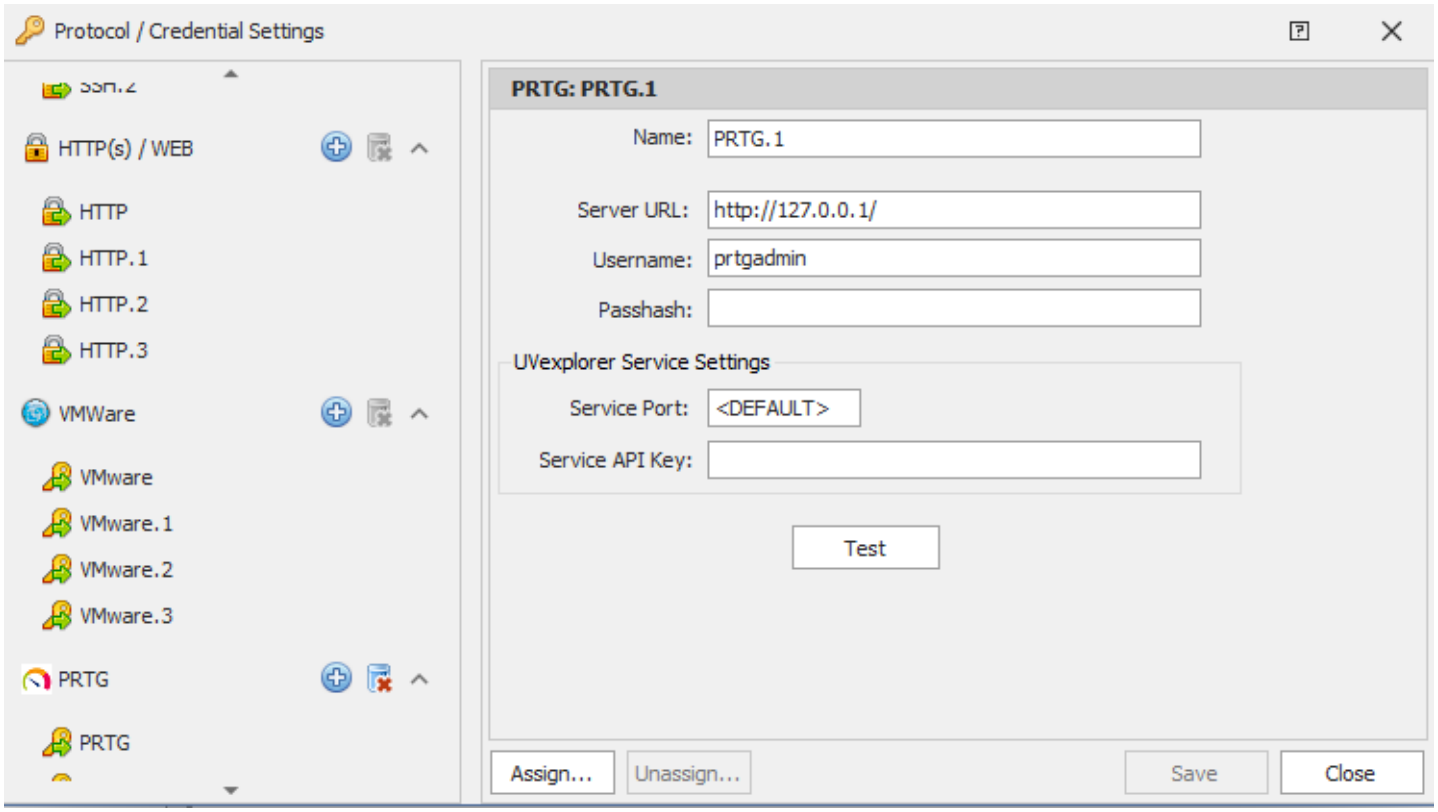
To export to PRTG, UVexplorer needs to communicate with your PRTG server. The PRTG server connection settings are stored as a PRTG credential within UVexplorer and can be accessed using the Credential Manager available in the PRTG export wizard and the export dialog.

To create new PRTG server settings select the '+' button within the credential manager and new PRTG settings will be created.



Configuration

The Protocol / Credential Settings dialog box will request the following information to connect to the PRTG server:



Name

The settings name is the name you choose to identify a particular PRTG server; this is especially useful if you are exporting to multiple servers.

Server URL

The server URL is the address of your PRTG server. If the server is on the same machine as UVexplorer you can use the local address, for example: "http://127.0.0.1/". If the server is available on your local network, you can use the IP address of the machine the server is installed on, for example: "http://192.168.1.15". If the server is available on a remote network the address or domain name for the server should be used. If PRTG is running on a port other than 80 the port should be specified: "http://127.0.0.1:8080/".

Username

Username is the account name for your PRTG system. The default is 'admin'.

Passhash

Passhash is a hash of your password PRTG provides for authenticating with their server. The hash is available within PRTG in Account Settings page accessed using the 'Setup - Account Settings - My Account' link.

Testing Configuration

PRTG server configuration can be tested within the PRTG export wizard by selecting the 'Test' button. UVexplorer will attempt to communicate with the PRTG server using the URL, username and passhash provided. If the server is available a message displaying the PRTG version will be displayed.

Support Tools

Support tools are provided as advanced features for troubleshooting and maintaining your UVexplorer application. As these tools are not necessary for regular use of UVexplorer, they are disabled by default to simplify the UVexplorer application.

Enabling Support Tools

Support tools are enabled using the 'SupportToolsEnabled' flag in the UVexplorer.cfg file located in the application's installation directory. To enable the support tools, edit the config file in a text editor such as notepad and set the value of the 'SupportToolsEnabled' entry to 'True' (i.e. <value>True</value>). To disable the support tools set the value to 'False'. UVexplorer must be restarted for the changes to take effect.

Available Support Tools

Master Network
Network Cleaner

Master Network

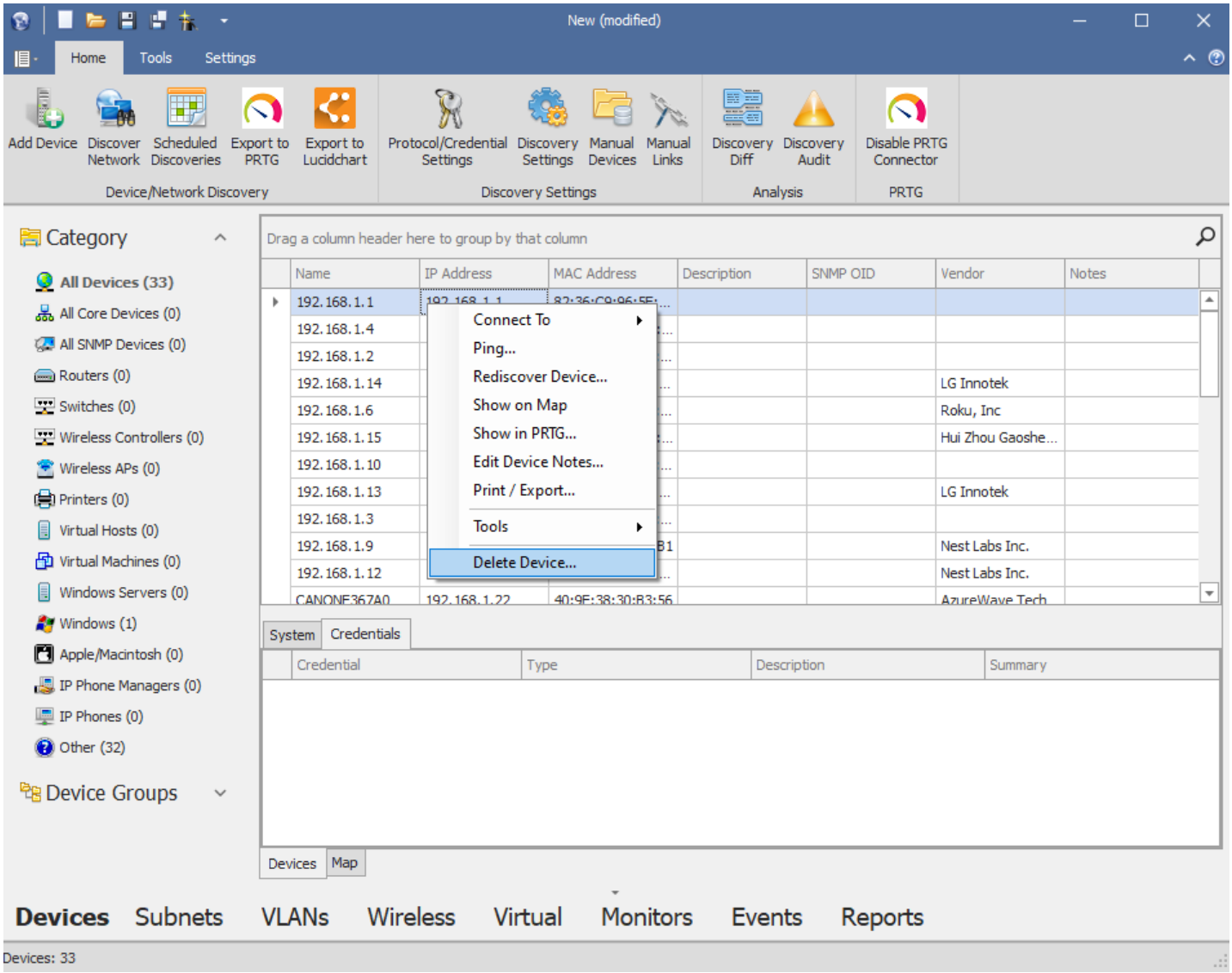
UVexplorer can discover multiple networks and subnetworks and isolate the results of those discoveries to networks referred to as 'Discovery Results' within UVexplorer. Discovery results provide a snapshot of a network at a given time and can be opened and viewed independent of other discoveries.

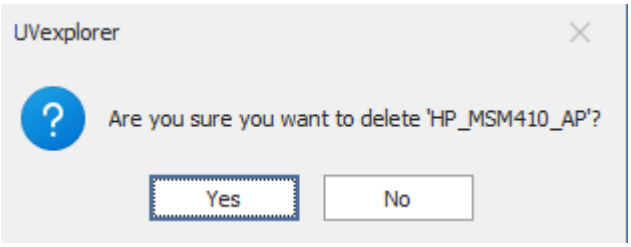
UVexplorer is also able to track devices from multiple Discovery Results over time. This unique feature allows UVexplorer to monitor as devices come and go on the network and as changes are made. To support this feature UVexplorer must contain a master network which tracks the identity of all devices ever discovered.

Typically, the management of the master network will take care of itself and configuring the master network will not be necessary. If you have run discoveries containing devices, you no longer want tracked you can manually remove them from the master network. This is especially useful if you discovered a large network containing devices you are no longer interested in.

Deleting Devices

To delete devices from the master network, select them in the list and right click and select 'Delete Device…'. The selected devices will be removed from the master network.





If the deleted devices are re-discovered by a scheduled or manual discovery, they will be re-added to the network. Devices which are currently being monitored may not be deleted from the master network. To delete them they must first be removed from any monitors. See Monitors for more information.

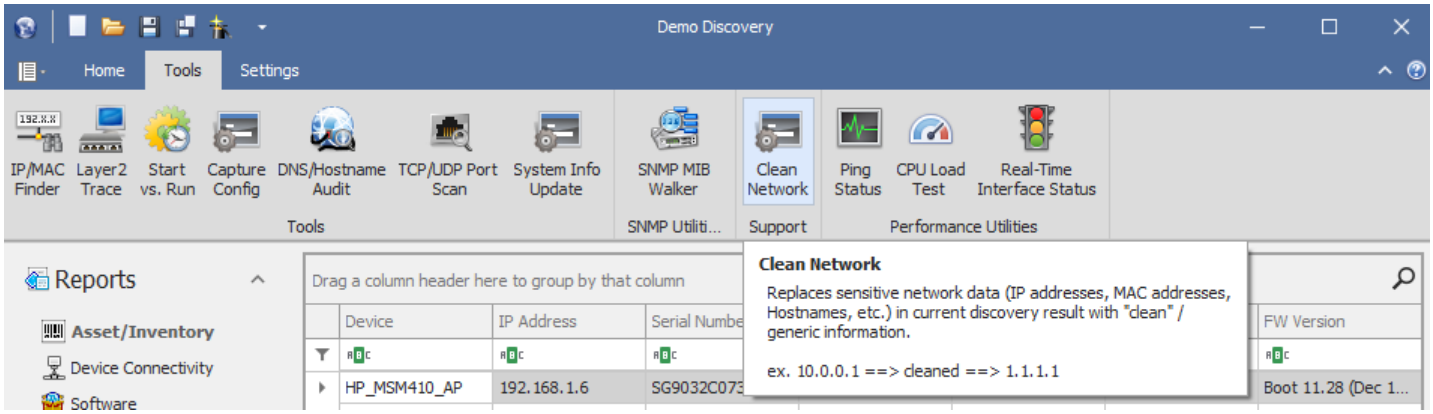
Network Cleaner

The network cleaner is a utility which enables removing any confidential or identifying information from a discovery result. This is primarily useful in creating an anonymous discovery result for sharing with UVexplorer support for troubleshooting discovery and connectivity issues.

A cleaned network file will randomize all IP and MAC addresses, replace identifying system information, and remove any references to device credentials.

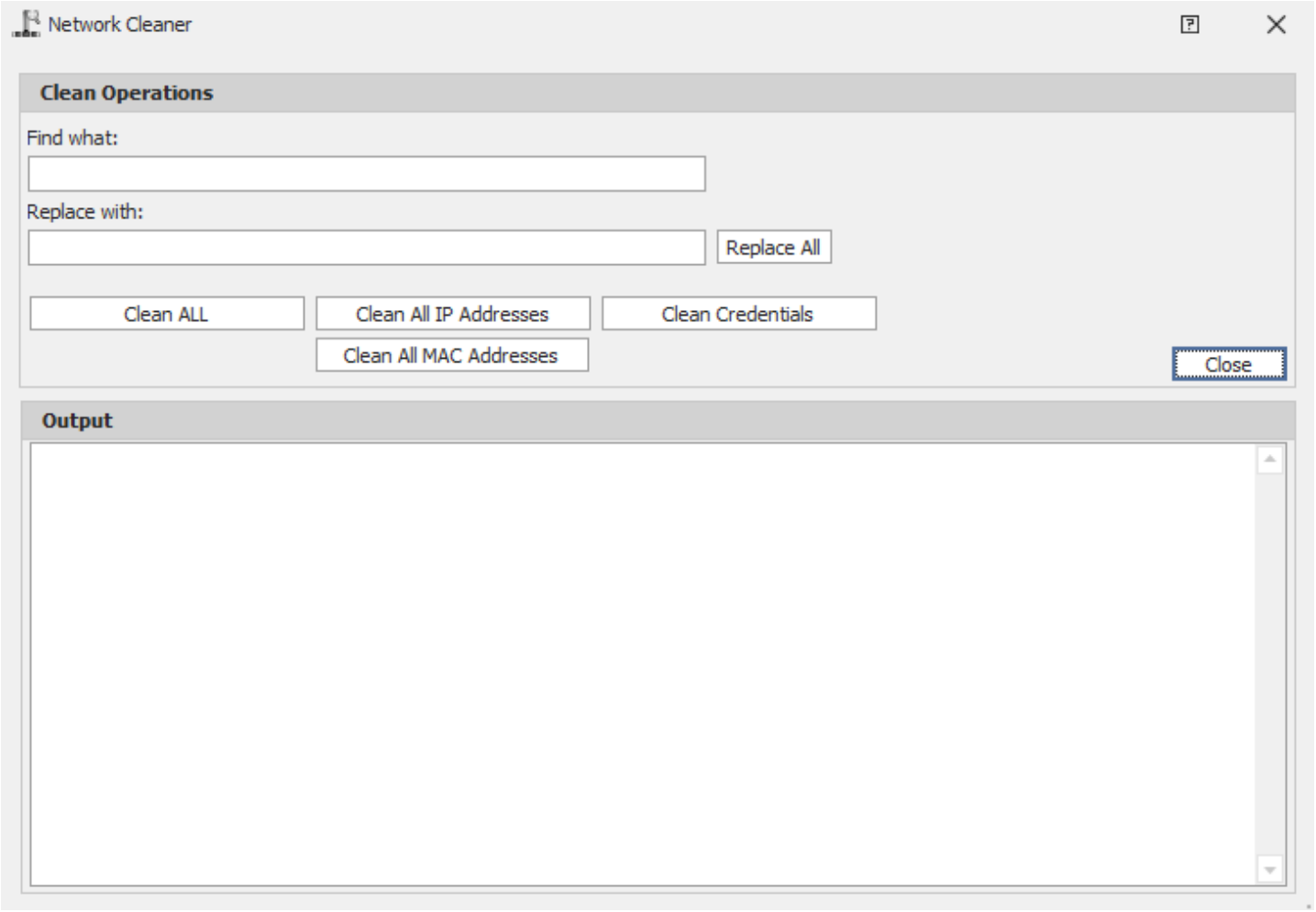
Running the Network Cleaner

The network cleaner is available in the 'Tools' ribbon. To run the cleaner open the discovery result you would like to clean and launch the cleaner.



As the cleaner performs its operations the discovery result will be modified. When you have completed all the desired clean operations the result can be saved, and the clean discovery result can be viewed within UVexplorer.

Discovery results, clean or otherwise, can be imported and exported from the getting started page of the application.



Find and Replace
Find and replace will replace text in the system information, such as host name, which matches the find text with the replace text. To replace text, enter the find and replace texts and press 'Replace All'.

Clean All
Clean all will run all the clean operations at once.

Clean All IP Addresses
Most network engineers consider the IP addresses and structure of their network to be secure information. When cleaning a network, the IP addresses should be replaced with random IP addresses. When IP addresses are cleaned the IP address will be replaced with a random address. All IP addresses of a particular subnet will be mapped to the same new random subnet. This is necessary to maintain the connectivity of the network which is the primary goal of sharing a discovery result.

When IP addresses are randomized any instance of a particular IP address on the network will be randomize to the same address. This allows any references to a particular IP address to be maintained.

Clean All MAC Addresses
MAC addresses are designed to be unique for each device and asset within a device. When cleaning a network, the MAC addresses should be replaced with random MAC addresses. The first portion of a MAC address contains information about the vendor/provider of the device. This information is required by UVexplorer to determine the provider and role of a device. When MAC addresses are cleaned the first portion is maintained while the last portion is randomized. This means that anyone with access to your clean discovery results could determine who the vendor of a device is but could

not determine the unique identity of your devices.

When MAC addresses are randomized any instance of a particular MAC address on the network will be randomized to the same address. This allows references to an entity by MAC address to be maintained.

Clean Credentials
UVexplorer discovery results maintain references to the credentials used to discover the information of a given device. When cleaning the network for sharing the credential references should be removed to protect the credential information. When clean credentials run all references to credentials and settings will be removed.

Congratulations! You have made it to the end of the 291-page User Guide. If you'd like additional assistance, please reach out to our friendly, Utah Support Team at Support@UVnets.com or +1.801.871.5071.

Copyright © 2022