UVexplorer Server 2.0 Documentation

Version 118, March 2022

- UVexplorer Server Overview
- Concepts and Terminology
  - Information Structure
  - Networks
  - Agents
  - Discoveries
  - Discovery Runs
  - Discovery Data
    - Device Details
    - Network Maps
    - Reports
    - Events
  - Rollups
  - Users
    - Network Sharing
    - User Types
    - User Groups
    - Account Types
  - API Keys
- Tasks
  - Logging in to UVexplorer Server
  - Navigation
    - Navigating with List Views
    - Navigating with the Nav Bar
    - Navigating with Bread Crumbs
  - Managing Network Sharing
  - Configuring Networks
    - Network Settings Tab
    - Agents Tab
    - Protocols/Credentials Tab
    - Email Settings Tab
    - Saving Network Changes
  - Configuring Agents
    - Agent Settings Tab
    - Discoveries Tab
    - Saving Agent Changes
  - Configuring Discoveries

- Discovery Settings Tab
- Protocols/Credentials Tab
- Include/Exclude Scopes Tab
- Advanced Settings Tab
- Schedule Tab
- Event Settings Tab
- Saving Discovery Changes

Discovery Status

Device Filters

Viewing Discovery Data

- Devices / Maps Tab
  - Device List View
    - Exporting Device Data to CSV Files
  - Map View
    - Editing Map Settings
    - Editing Map Drawing Settings
    - Exporting Maps to Lucidchart
    - Exporting Maps to Visio/PDF/SVG Files
  - Editing Device Groups
  - Custom Device Groups
- Reports Tab
  - Exporting Reports to CSV Files
- Events Tab

Manual Links

Capturing, Viewing, and Exporting Device Configurations

Monitoring Your Network

- Adding, Configuring, and Deleting Monitors
  - Configuring Monitors
    - Schedule Tab
  - Events Tab
    - Log Events
    - Email Events
    - Ping Monitor Settings Tab
    - Ping Monitor Devices Tab
  - Configuring SNMP Interface Monitors
    - SNMP Monitor Settings Tab
    - SNMP Interface Monitor Devices Tab
- Controlling Monitor Execution
  - Disabling Monitors

        - Running Monitors On-Demand
    - Monitor Events
    - Viewing Monitor Status
        - Overall Monitor Status
        - Detailed Monitor Status
        - Overall Device Status
        - Detailed Device Status
        - Monitor Status on Network Maps
    - Viewing Monitor History
        - Monitor Policy History
    - Clearing Monitor Policy History
    - Clearing Device Monitor History
    - Updating Monitored Devices
    - Deleting Monitored Devices
- Exporting to PRTG Network Monitor
    - Configuring PRTG Exports
    - On-Demand Execution of PRTG Exports
    - Configuring Active Directory and Google Workspace Integration
- Managing User Accounts
    - Changing Passwords
    - Creating, Editing, and Deleting Users
        - UVexplorer Users
        - Active Directory Users
        - Google Workspace Users
- Managing User Groups
    - Creating, Editing, and Deleting Groups
        - UVexplorer Groups
        - Active Directory Groups
        - Google Workspace Groups
    - Syncing Active Directory and Google Workspace Group Data
- Managing Web API Keys
- Managing Your UVexplorer Server License
    - Product Information
    - Software Update
- Start Menu Items
    - Open Logs
    - Open UvxAdmin Window
    - Open Web Console
    - Stop UVexplorer Server

Start UVexplorer Server
Uninstall UVexplorer Server

UVexplorer Server Overview

UVexplorer Server is a platform for discovering, mapping, and monitoring computer networks. If you are responsible for building, managing, and troubleshooting networks, UVexplorer Server can help you do it more effectively.

The major features of UVexplorer Server include:

- ➔ Detailed Network Discovery - Discovery and reporting of detailed device inventory data for the devices on your network using protocols such as SNMP, WMI, and SSH/Telnet
- ➔ Physical Network Connectivity - Discovery of physical and logical connections between the devices on your network, including both Layer-2 and Layer-3
- ➔ Wireless Infrastructure Discovery - Discovery of wireless network infrastructure, including wireless access points, wireless controllers, and wireless clients
- ➔ Virtual Infrastructure Discovery - Discovery of VMware and Hyper-V virtual infrastructure, including virtual machines, virtual hosts, and virtual switches
- ➔ Network Maps - Network maps that let you visualize the devices and connections on your network (or interesting subsets thereof)
- ➔ Configuration Backup - Automated backup and viewing of network device configurations using SSH and Telnet, including tracking how configurations change over time
- ➔ Network Change Notifications - Notifications about interesting changes to the devices and connections on your network
- ➔ Data Export - Exporting discovery data to CSV files for external processing and reporting
- ➔ Map Export - Exporting of network maps to Visio, PDF, and SVG file formats, and to Lucidchart, a cloud-based diagramming application
- ➔ Distributed Discovery - Agent-based discovery from multiple points on the network, with results from all agents merged to create a single, comprehensive view of your network
- ➔ Web Console - Browser-based interface for configuring UVexplorer Server and viewing discovery results
- ➔ Basic Network Monitoring - Network monitoring with Ping monitors and SNMP Interface monitors
- ➔ PRTG Network Monitor Integration - For advanced network monitoring, use UVexplorer Server to automatically configure devices and sensors in Paessler's PRTG Network Monitor networking monitoring platform

UVexplorer Server scales from small networks to large networks using its agent-based discovery architecture. Discovery is performed by "discovery agents" deployed on one or more network nodes. Small networks often require only a single discovery agent, while large networks typically benefit from having multiple discovery agents deployed at different locations on the network. Each agent discovers a specific part of the network, and then posts its discovery results up to UVexplorer Server where results from all agents are merged to create one comprehensive model of your network. Device inventory data and network maps are viewed through UVexplorer Server's web browser interface. While UVexplorer Server can be used on any size network, its agent-based discovery architecture supports each of the following scenarios that require distributed discovery:

- ➔ Networks for organizations with multiple buildings, sites, or campuses
- ➔ Networks where firewalls prevent discovery of the entire network from a single point on the network
- ➔ Managed Service Providers (MSPs) who manage multiple different customer networks

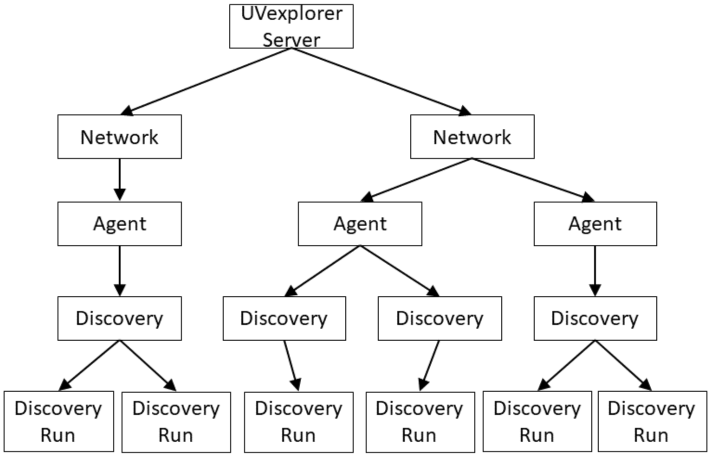
UVexplorer Server can also notify you of changes that occur to the devices and connections in your network (e.g., when devices are added to or removed from the network, or when links between devices go down). UVexplorer Server also provides basic network monitoring with Ping monitors and SNMP Interface monitors. For more advanced monitoring capabilities, UVexplorer Server integrates with PRTG Network Monitor, a powerful monitoring platform from Paessler. UVexplorer Server automatically exports device inventory data and network maps into the PRTG platform, and can automatically configure device sensors within PRTG. In this way, UVexplorer Server makes PRTG more intelligent and easier to set up and configure.

Concepts and Terminology

This section describes concepts and terms that are necessary for understanding UVexplorer Server and using it effectively.

Information Structure

UVexplorer Server organizes network information into Network, Agent, Discovery, and Discovery Run objects. These objects form a hierarchy, as shown in the following diagram. Within UVexplorer Server you can create any number of Networks to represent the computer networks that you manage. Each Network contains one or more Agents that do the work of discovering the network. Each Agent contains one or more Discovery objects. Each Discovery represents a scheduled network scan that collects information about part of your network. Each Discovery Run contains all the data collected during a particular scan of the network.



Networks - Agents - Discoveries - Discovery Runs

Networks

The top level of organization within UVexplorer Server is the “network”. A “network” contains all of the discovery results, device details, and network maps for an actual computer network you are managing. You can create as many “network” objects as you like. A “network” can represent an entire network, or any subset of one. It all depends on how you prefer to think about and manage your network(s). For example, if you are a Managed Service Provider (MSP) who manages multiple customer networks, you would create a separate “network” object for each of the customer networks that you manage. Or, if you manage a large corporate network, you might create a separate “network” object for each of your organization’s buildings, sites, or campuses.

Agents

The second level of organization within UVexplorer Server is the “agent”. A network contains one or more agents. Each agent represents a point of discovery on the network. An agent discovers all or part of the network, and posts its discovery results up to UVexplorer Server. Some networks are configured so that the entire network is visible from a single location (or node) on the network. In this case, you could have a single agent that performs all of the discovery of the entire network. Other networks are configured in a way that prevents any single node on the network from seeing the entire network. In this case you would want to deploy multiple agents throughout the network so that every part of the network is visible to at least one agent. Each agent would then discover a subset of the network, and publish its discovery results up to UVexplorer Server. The server would then merge (or combine) all of the discovery results from the multiple agents into a single, comprehensive model of the complete network.

An agent consists of two parts: 1) the agent’s configuration and 2) the agent software. To create a new agent, you must:

1. Create and configure a new “agent” object within the UVexplorer Server web console
2. Install the agent software on a computer on your network that will run the agent
3. Bind the agent software to the “agent” configuration created in step 1. (This allows the agent software to download its configuration from UVexplorer Server.)

The process of installing the agent software and binding it to an agent configuration is described in detail in the section named “Installing and Configuring UVexplorer Server Agents”.

Discoveries

The job of an agent is to discover part of the network and publish its results to UVexplorer Server. Therefore, when creating and configuring an agent, you need to create one or more “discoveries” that will be run by that agent. Each “discovery” runs on a schedule that you specify (e.g., daily, hourly, every 15 minutes, etc.). Each “discovery” discovers a specified part of the network, which is typically defined using IP address ranges for “ping sweep” discoveries, or defined by a list of seed devices for “ARP crawl” discoveries. Each “discovery” also has many other configuration settings you can use to control how it executes and does its work.

Many agents will contain only a single “discovery”, because that will be sufficient for the agent to discover its part of the network. However, if you want a single agent to discover different parts of the network on different schedules (at different times of day or at different frequencies, for example), an agent can contain multiple “discovery” configurations, if necessary.

Discovery Runs

Each time an agent runs a discovery, the output of the discovery is called a “discovery run” (or sometimes “discovery result”). A “discovery run” contains all the device inventory data and network connectivity information collected during that discovery run. In essence, a “discovery run” is a snapshot of the network’s state at a particular point in time. Each time a discovery finishes running, the agent posts the “discovery run” to UVexplorer Server. The server stores all of the recent discovery runs from all of the discoveries for all of the agents. As new discovery runs are posted to the server, the server updates its model of the network’s current state, including device details and connectivity. In addition to its model of the network’s current state, UVexplorer Server also keeps a historical record of what the network looked like in the past. This allows UVexplorer Server to detect changes in the network over time.

Discovery Data

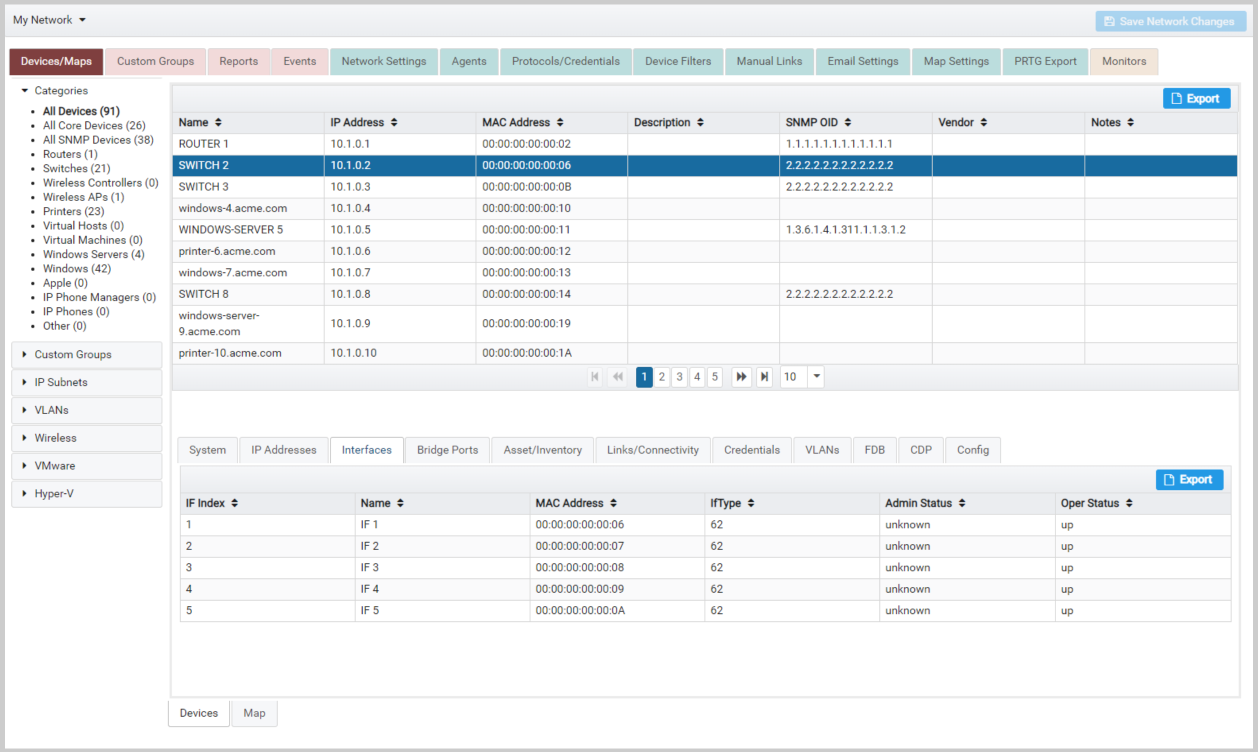
UVexplorer Server collects a lot of data about your network. Here is a summary of the different types of information that can be collected and viewed with UVexplorer Server:

Device Details

Using protocols such as SNMP, WMI, SSH/Telnet, and VMware VIM, detailed information is collected from each device. Here is a list of the information collected by each discovery run. This data can be viewed in UVexplorer Server’s “Devices / Maps” tab which is within the “Devices” sub-tab.

- ❏ MAC & IP Addresses
- ❏ Host Names
- ❏ NetBIOS Name/Domain
- ❏ Vendor, Model, Description
- ❏ SNMP Name/Description/Location/Contact
- ❏ IP Route Table
- ❏ ARP Cache

❑ Forwarding Database
❑ Network Interfaces
❑ Bridge Ports
❑ VLANs
❑ Spanning Tree (STP)
❑ CDP / LLDP
❑ Device Configuration
❑ Asset / Inventory Information
❑ Serial Numbers
❑ Installed Software
❑ Device Connectivity
❑ BIOS
❑ Operating System
❑ Disk Drives
❑ Physical Memory
❑ CPU
❑ Running Processes
❑ Wireless Controller, Access Point, and Client Information
❑ IP Phone and IP Phone Manager Information
❑ VMware Virtual Machine, Virtual Host, Virtual Server, and Virtual Switch Information
❑ Hyper-V Virtual Machine Information



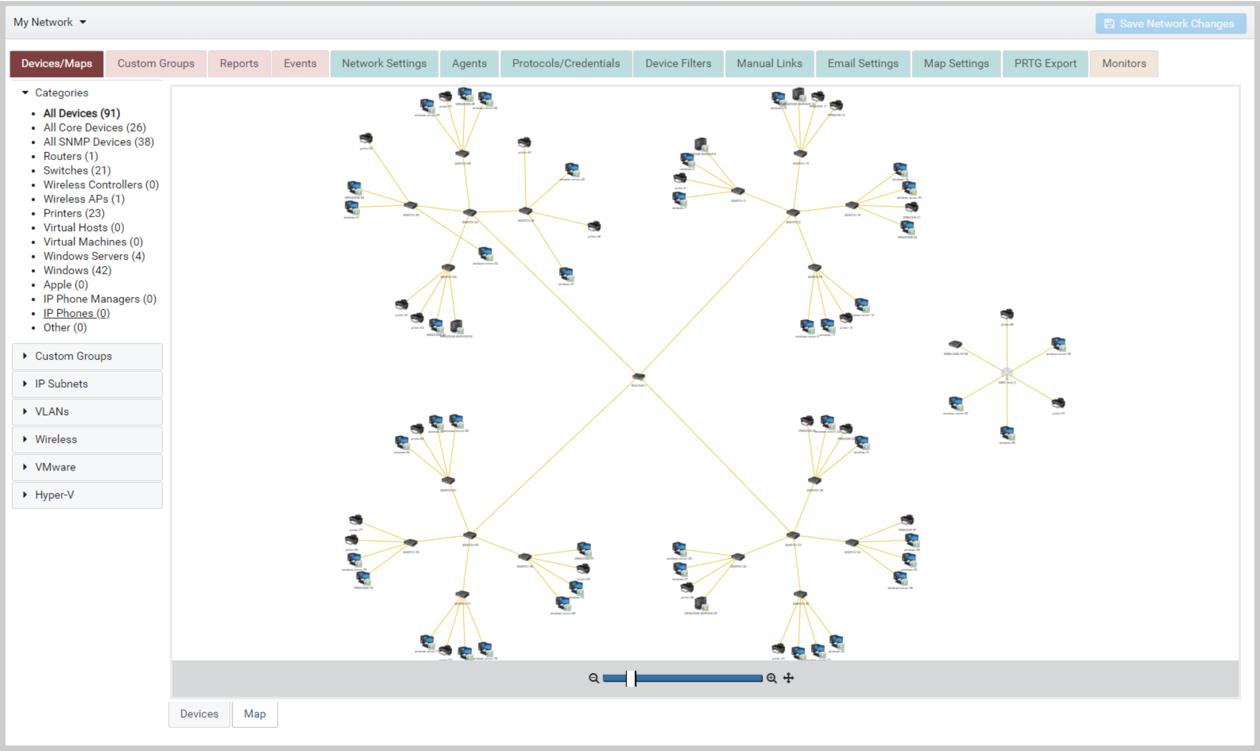
Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
ROUTER 1	10.1.0.1	00:00:00:00:00:02		1.1.1.1.1.1.1.1.1.1.1.1		
SWITCH 2	10.1.0.2	00:00:00:00:00:06		2.2.2.2.2.2.2.2.2.2.2.2		
SWITCH 3	10.1.0.3	00:00:00:00:00:0B		2.2.2.2.2.2.2.2.2.2.2.2		
windows-4.acme.com	10.1.0.4	00:00:00:00:00:10				
WINDOWS-SERVER 5	10.1.0.5	00:00:00:00:00:11		1.3.6.1.4.1.311.1.1.3.1.2		
printer-6.acme.com	10.1.0.6	00:00:00:00:00:12				
windows-7.acme.com	10.1.0.7	00:00:00:00:00:13				
SWITCH 8	10.1.0.8	00:00:00:00:00:14		2.2.2.2.2.2.2.2.2.2.2.2		
windows-server-9.acme.com	10.1.0.9	00:00:00:00:00:19				
printer-10.acme.com	10.1.0.10	00:00:00:00:00:1A				

IF Index	Name	MAC Address	IfType	Admin Status	Oper Status
1	IF 1	00:00:00:00:00:06	62	unknown	up
2	IF 2	00:00:00:00:00:07	62	unknown	up
3	IF 3	00:00:00:00:00:08	62	unknown	up
4	IF 4	00:00:00:00:00:09	62	unknown	up
5	IF 5	00:00:00:00:00:0A	62	unknown	up

Device List - Shows list of discovered devices (select device to see its details)

Network Maps

Using the network interface and link data collected from each device, UVexplorer Server creates a connectivity model of the network that represents how devices are connected to each other at the physical (Layer-2) and logical (Layer-3) levels. Based on this network connectivity model, UVexplorer Server renders visual network maps that display the link structure of the network. You can customize these network maps to look the way you want. Network maps can be viewed in UVexplorer Server's "Devices / Maps" tab within the "Map" sub-tab.



Network Map - Map view of discovered devices (double-click nodes to see device details)

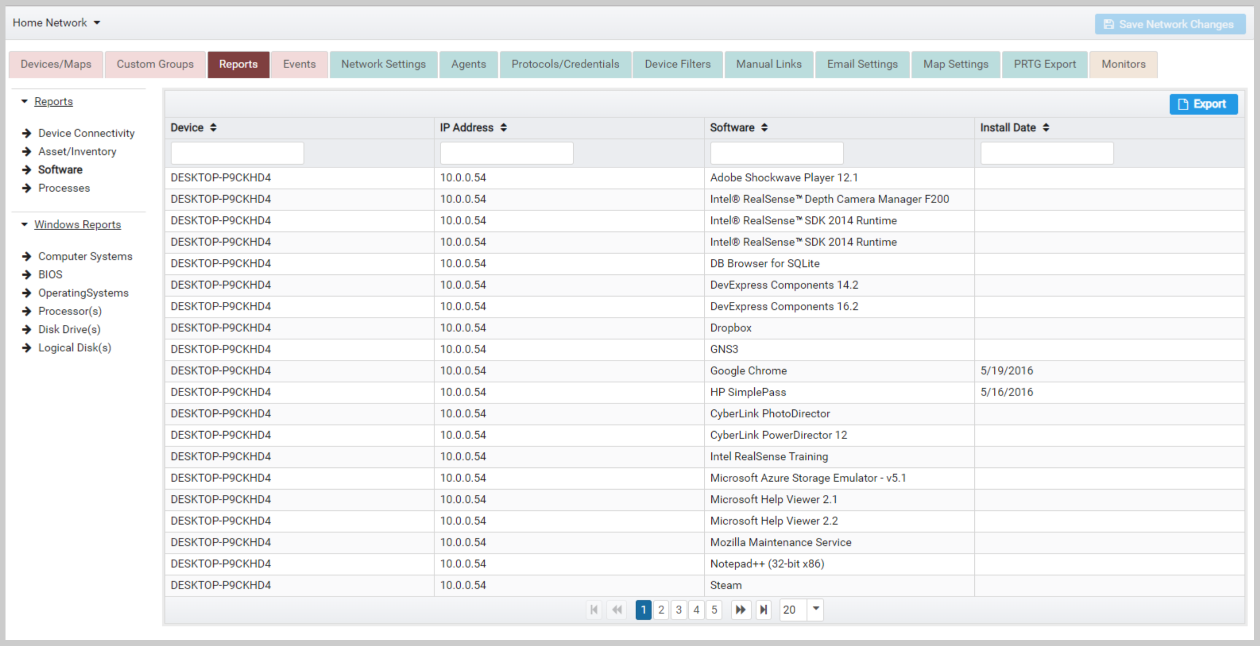
Reports

In addition to providing details about each device, UVexplorer Server also provides a number of useful reports that aggregate data from all devices in the network. For example, on individual devices you can view the "Installed Software" information for ONE device at a time. Or, you can view the "Software" report to see all of the software installed for ALL devices in one view. Reports can be viewed in UVexplorer Server's "Reports" tab.

The reports provided by UVexplorer Server include:

❏ Asset / Inventory
❏ Device Connectivity

❏ Installed Software
❏ Running Processes
❏ Computer Systems (Windows)
❏ BIOS (Windows)
❏ Operating Systems (Windows)
❏ Processors (Windows)
❏ Disk Drives (Windows)
❏ Logical Disks (Windows)

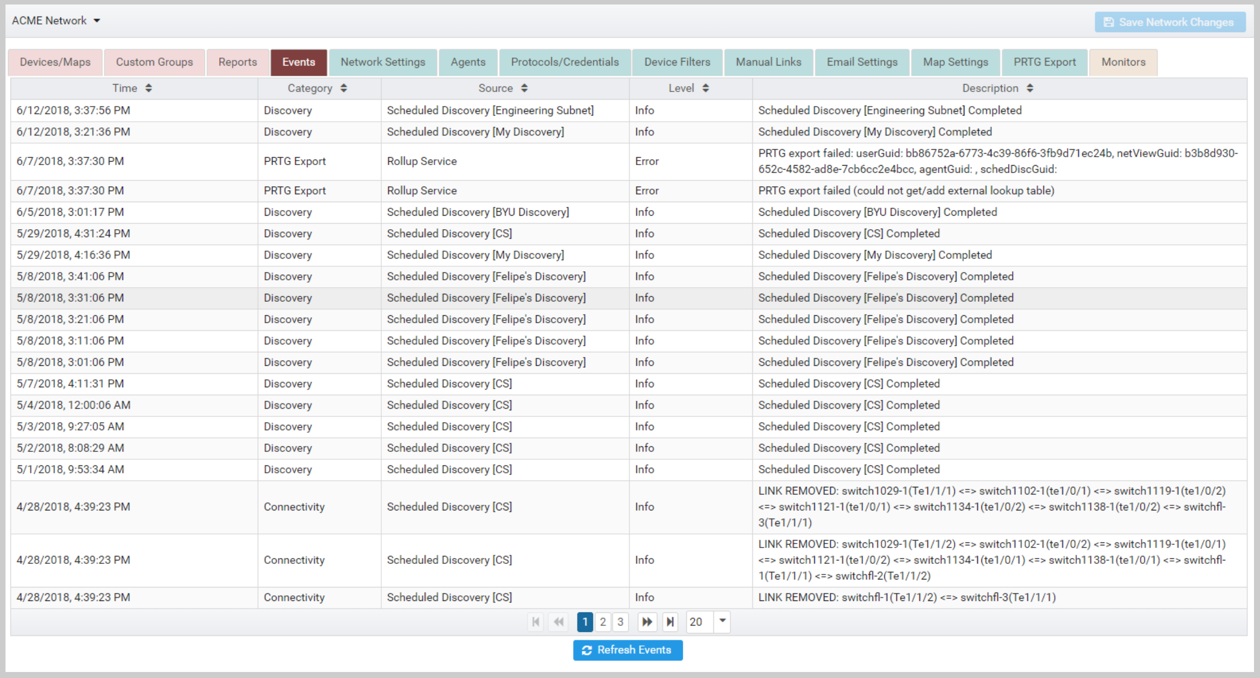


Device	IP Address	Software	Install Date
DESKTOP-P9CKHD4	10.0.0.54	Adobe Shockwave Player 12.1	
DESKTOP-P9CKHD4	10.0.0.54	Intel® RealSense™ Depth Camera Manager F200	
DESKTOP-P9CKHD4	10.0.0.54	Intel® RealSense™ SDK 2014 Runtime	
DESKTOP-P9CKHD4	10.0.0.54	Intel® RealSense™ SDK 2014 Runtime	
DESKTOP-P9CKHD4	10.0.0.54	DB Browser for SQLite	
DESKTOP-P9CKHD4	10.0.0.54	DevExpress Components 14.2	
DESKTOP-P9CKHD4	10.0.0.54	DevExpress Components 16.2	
DESKTOP-P9CKHD4	10.0.0.54	Dropbox	
DESKTOP-P9CKHD4	10.0.0.54	GNS3	
DESKTOP-P9CKHD4	10.0.0.54	Google Chrome	5/19/2016
DESKTOP-P9CKHD4	10.0.0.54	HP SimplePass	5/16/2016
DESKTOP-P9CKHD4	10.0.0.54	CyberLink PhotoDirector	
DESKTOP-P9CKHD4	10.0.0.54	CyberLink PowerDirector 12	
DESKTOP-P9CKHD4	10.0.0.54	Intel RealSense Training	
DESKTOP-P9CKHD4	10.0.0.54	Microsoft Azure Storage Emulator - v5.1	
DESKTOP-P9CKHD4	10.0.0.54	Microsoft Help Viewer 2.1	
DESKTOP-P9CKHD4	10.0.0.54	Microsoft Help Viewer 2.2	
DESKTOP-P9CKHD4	10.0.0.54	Mozilla Maintenance Service	
DESKTOP-P9CKHD4	10.0.0.54	Notepad++ (32-bit x86)	
DESKTOP-P9CKHD4	10.0.0.54	Steam	

Reports Tab

Events

During network discovery and at other times, interesting events will occur in your network and within UVexplorer Server itself. For example, network changes such as devices appearing or disappearing on the network and links going up and down are interesting events. Another interesting event is an error condition detected by UVexplorer Server that might need administrative attention. These and other events are reported within UVexplorer Server’s “Events” tab.



Time	Category	Source	Level	Description
6/12/2018, 3:37:56 PM	Discovery	Scheduled Discovery [Engineering Subnet]	Info	Scheduled Discovery [Engineering Subnet] Completed
6/12/2018, 3:21:36 PM	Discovery	Scheduled Discovery [My Discovery]	Info	Scheduled Discovery [My Discovery] Completed
6/7/2018, 3:37:30 PM	PRTG Export	Rollup Service	Error	PRTG export failed: userGuid: bb86752a-6773-4c39-86f6-3fb9d71ec24b, netViewGuid: b3b8d930-652c-4582-ad8e-7cb6cc2e4bcc, agentGuid: , schedDiscGuid:
6/7/2018, 3:37:30 PM	PRTG Export	Rollup Service	Error	PRTG export failed (could not get/add external lookup table)
6/5/2018, 3:01:17 PM	Discovery	Scheduled Discovery [BYU Discovery]	Info	Scheduled Discovery [BYU Discovery] Completed
5/29/2018, 4:31:24 PM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/29/2018, 4:16:36 PM	Discovery	Scheduled Discovery [My Discovery]	Info	Scheduled Discovery [My Discovery] Completed
5/8/2018, 3:41:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:31:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:21:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:11:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:01:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/7/2018, 4:11:31 PM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/4/2018, 12:00:06 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/3/2018, 9:27:05 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/2/2018, 8:08:29 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/1/2018, 9:53:34 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
4/28/2018, 4:39:23 PM	Connectivity	Scheduled Discovery [CS]	Info	LINK REMOVED: switch1029-1(Te1/1/1) <=> switch1102-1(te1/0/1) <=> switch1119-1(te1/0/2) <=> switch1121-1(te1/0/1) <=> switch1134-1(te1/0/2) <=> switch1138-1(te1/0/2) <=> switchfl-3(Te1/1/1)
4/28/2018, 4:39:23 PM	Connectivity	Scheduled Discovery [CS]	Info	LINK REMOVED: switch1029-1(Te1/1/2) <=> switch1102-1(te1/0/2) <=> switch1119-1(te1/0/1) <=> switch1121-1(te1/0/2) <=> switch1134-1(te1/0/1) <=> switch1138-1(te1/0/1) <=> switchfl-1(Te1/1/1) <=> switchfl-2(Te1/1/2)
4/28/2018, 4:39:23 PM	Connectivity	Scheduled Discovery [CS]	Info	LINK REMOVED: switchfl-1(Te1/1/2) <=> switchfl-3(Te1/1/1)

Events Tab

Rollups

The discovery data described in the previous section can be viewed at four different levels of granularity:

1. Discovery Run - Select a discovery run to view the raw data collected during that discovery run

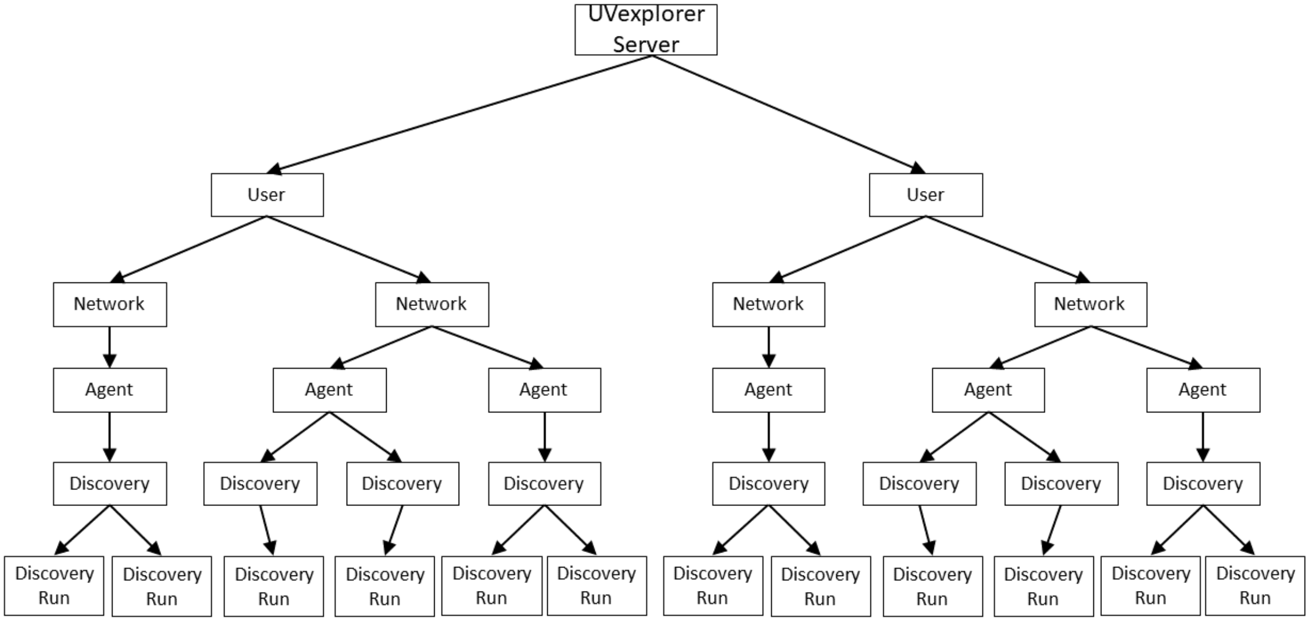
2. Discovery - Select a discovery to see a combined view of the data recently produced by runs of that discovery. Specifically, this view is a merger (or “rollup”) of the most recent runs of the discovery. You can specify how many recent discovery runs to merge, and also how long to remember devices that dynamically come and go, like mobile devices and laptops.

3. Agent - Select an agent to see a combined view of the recent discovery results for the entire agent (from all of its discoveries). This view is a merger (or “rollup”) of the most recent “rollups” for all of the agent’s discoveries (i.e., a rollup of rollups).

4. Network - Select a network to see a combined view of the recent discovery results for the entire network. This view is a merger (or “rollup”) of the most recent “rollups” for all of the network’s agents (i.e., a rollup of rollups).

Users

UVexplorer Server supports multiple user accounts. Each user has their own workspace (networks, agents, discoveries, discovery runs) which is isolated from all other users. The UVexplorer Server installation process requires you to create an initial administrative user account. After that, you can create as many administrative and/or non-administrative user accounts as you want (see the section named Managing Users for details). Because each user has their own isolated workspace, the structure of UVexplorer Server's database is as follows (this diagram adds Users to a similar diagram presented previously):



Users - Networks - Agents - Discoveries - Discovery Runs

Network Sharing

While each user has their own data workspace, being able to share data with other people is important in many organizations. For this reason, UVexplorer Server lets users "share" their network objects with other users, similar to the way a Google Doc can be shared with other people. When a network object is shared with another user, that user will see the shared network in their list of networks, and will be able to view the network's configuration and data. Networks can be shared in either "edit" or "view" mode, depending on whether you want the other person to be able to modify the network's configuration, or just view it.

Networks can be shared with individual users or with user groups. User groups are discussed in a later section.

User Types

There are different types of users that have different capabilities. The different user types are:

1. Observer - these users cannot create their own networks, but can have networks shared with them.
2. Regular - these users can create their own networks, share networks with other users, and have networks shared with them.
3. Administrator - these users can create their own networks, share networks with other users, have networks shared with them, and also perform all administrative functions required to configure the server (e.g., create users, manage the server’s license, etc.).

User Groups

UVexplorer Server also supports user groups. A user group contains zero or more users. User groups are useful for easily configuring permissions for multiple users, and for easily sharing networks with multiple users. Networks can be shared with individual users or with user groups.

There are different types of user groups that have different capabilities. The different group types are:

1. Observer - users in these groups cannot create their own networks, but can have networks shared with them.
2. Regular - users in these groups can create their own networks, share networks with other users, and have networks shared with them.
3. Administrator - users in these groups can create their own networks, share networks with other users, have networks shared with them, and also perform all administrative functions required to configure the server (e.g., create users, manage the server’s license, etc.).

If a user is a member of one or more user groups, they will have the capabilities associated with their user type and the types of all the groups they are members of. For example, if a user is of type Observer and they are a member of a Regular group, the user will have the capabilities of a Regular user.

Account Types

UVexplorer Server natively supports user accounts and user groups. It also provides integrations with Active Directory and Google Workspace user accounts and user groups.

When creating a new user account, the administrator can choose from the following account types:

1. UVexplorer User - a native UVexplorer user account.

2. Active Directory User - a user account that is connected to an Active Directory user account. This type of account allows the user to login using their Active Directory credentials.
3. Google Workspace User - a user account that is connected to a Google Workspace user account. This type of account allows the user to login using their Google Workspace credentials.

Similarly, when creating a new user group, the administrator can choose from the following group types:

1. UVexplorer Group - a native UVexplorer user group.
2. Active Directory Group - a user group that is connected to an Active Directory user group. This type of group allows administrators to leverage user groups they have already created in Active Directory, and to manage group membership through Active Directory.
3. Google Workspace Group - a user group that is connected to a Google Workspace user group. This type of group allows administrators to leverage user groups they have already created in Google Workspace, and to manage group membership through Google Workspace.

API Keys

UVexplorer Server has a Web API that allows external programs to interact with the server. Currently, the Web API is only used by UVexplorer agents to post discovery and monitor data to the server. However, in the future a subset of the Web API will become available to other external programs that need to access the data in the server’s database.

The Web API uses “API keys” to perform authentication of client programs. An API key is merely a string of characters that a client program includes with HTTP requests to authenticate and identify the caller. Currently, there are two tasks related to API keys that you will need to perform:

1. Manage Web API keys (i.e., create, modify, and delete API keys). This can be done in the “Manage API Keys” tab of the “Account” page. Details on how to do this are provided in the “Managing Web API Keys” section of this document.
2. Agent Registration. When registering an agent with UVexplorer Server, you must enter the API key to be used by the agent when calling the server. Details on how to do this are provided in a separate document titled “UVexplorer Server 2.0 Installation”.

Tasks

This section provides detailed instructions on how to perform various tasks within UVexplorer Server.

Logging in to UVexplorer Server

To access the UVexplorer Server web console, enter the URL of your UVexplorer Server in a web browser. The exact URL will depend on three things:

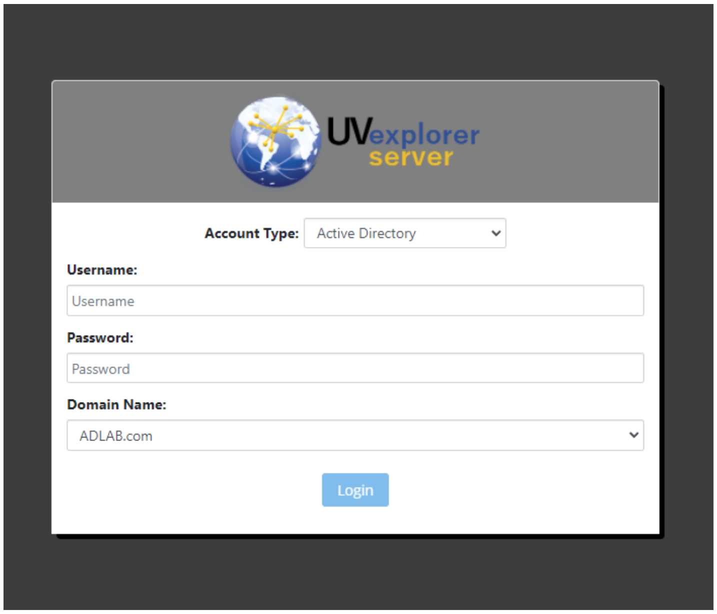
1. Whether you are using HTTP or HTTPS
2. The name of the machine on which you are running the server
3. The port number you configured the server to run on (see the section named "Installing and Configuring UVexplorer Server" for details on how to configure UVexplorer Server)

For example, if you did not enable HTTPS on your server, and it is running on a machine named "manage.acme.com", and it is configured to run on port 5189, your web console URL would be **`http://manage.acme.com:5189/`**

Alternatively, if you did enable HTTPS on your server, and it is running on a machine named "manage.acme.com", and it is configured to run on port 5190, your web console URL would be **`https://manage.acme.com:5190/`**

When you point your browser at your server's URL, if you have not already logged in, your browser will go to the login page before proceeding to the web console. If you are already logged in, your browser will go directly to the web console.

When logging in, you will need to select the type of account you are logging in with (i.e., UVexplorer, Active Directory, or Google Workspace).



Account Type: Active Directory

Domain Name: ADLAB.com

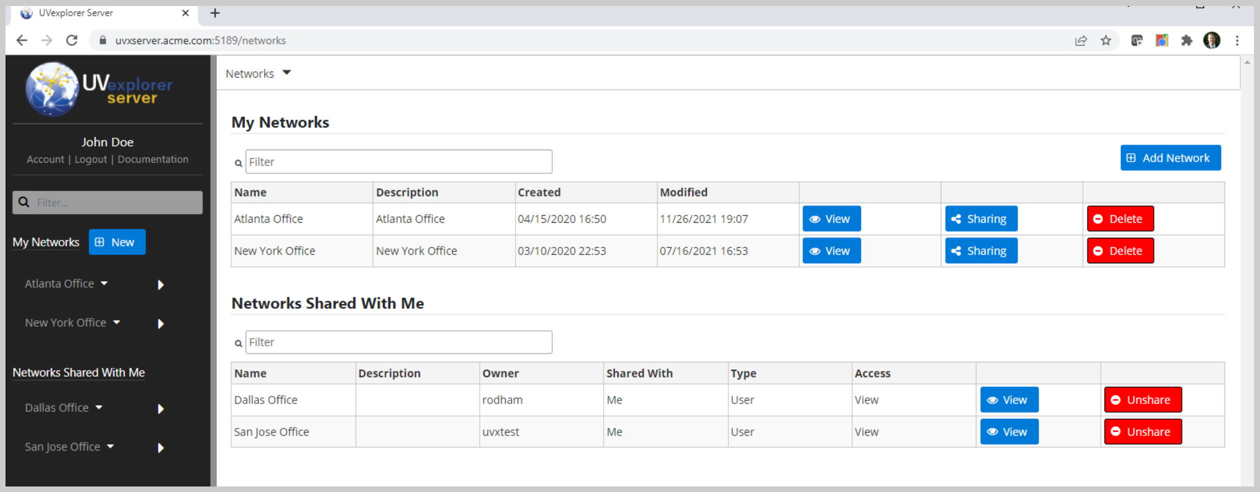
Login

Navigation

As previously described, UVexplorer Server organizes information into network, agent, discovery, and discovery run objects. Learning to navigate between these objects is fundamental to using UVexplorer Server. To configure a network or view its discovery results, you must first navigate to the network by selecting it. The same is true for agent, discovery, and discovery run objects. There are three different ways to navigate between these objects, which are described next.

Navigating with List Views

After logging in, you are taken to the “Network List” view, which displays a list of all your networks. The network list is divided into two sections: “My Networks” and “Networks Shared With Me”. This makes it easy to tell the difference between your own networks versus networks that other people have shared with you. Options are provided for creating, sharing, viewing, and deleting networks.



My Networks

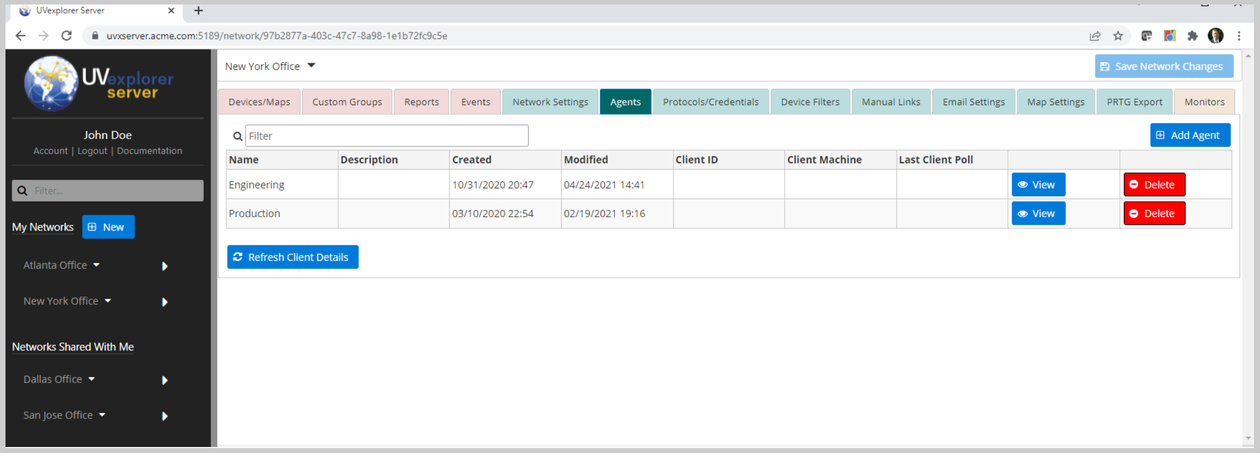
Name	Description	Created	Modified			
Atlanta Office	Atlanta Office	04/15/2020 16:50	11/26/2021 19:07	View	Sharing	Delete
New York Office	New York Office	03/10/2020 22:53	07/16/2021 16:53	View	Sharing	Delete

Networks Shared With Me

Name	Description	Owner	Shared With	Type	Access		
Dallas Office		rodham	Me	User	View	View	Unshare
San Jose Office		uvxtest	Me	User	View	View	Unshare

Network List

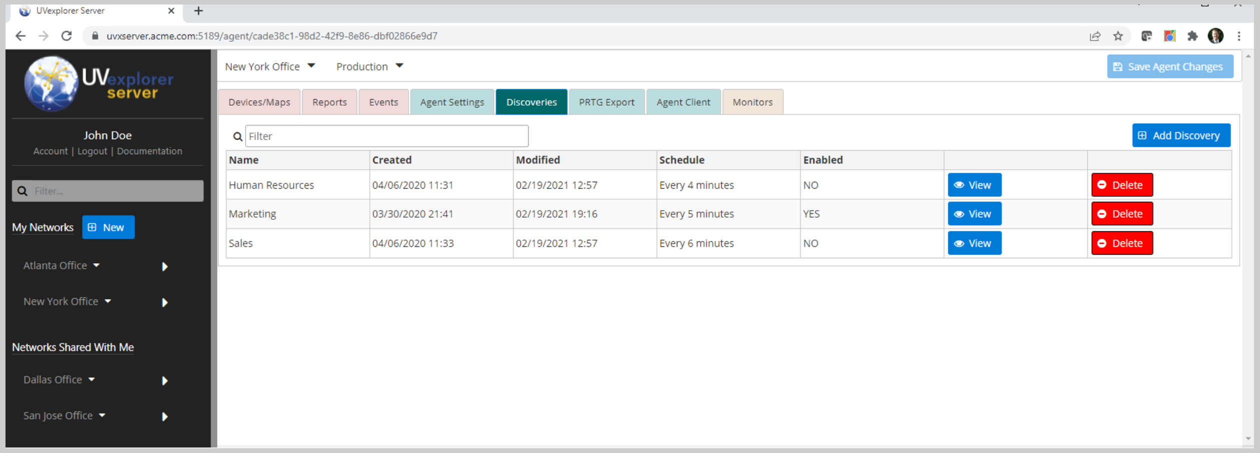
To view the details for a network, you can click the network’s “View” button, which takes you to the “Network” view. This view displays all the details about the selected network. There are many tabs you can select to configure the network and view its discovery results (the contents of these tabs are described later). To view a list of the network’s agents, you can select the “Agents” tab, which displays the “Agent List” view. This view lists all of the network’s agents, and provides options for creating, viewing, and deleting agents.



Name	Description	Created	Modified	Client ID	Client Machine	Last Client Poll
Engineering		10/31/2020 20:47	04/24/2021 14:41			
Production		03/10/2020 22:54	02/19/2021 19:16			

Network's Agent List

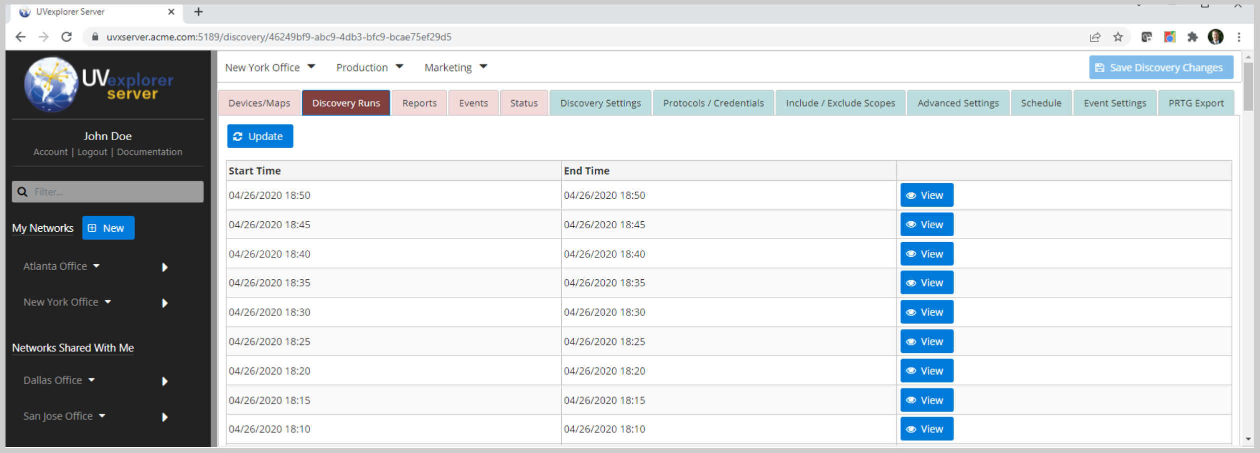
To view the details for an agent, you can click the agent's "View" button, which takes you to the "Agent" view. This view displays all the details about the selected agent. There are many tabs you can select to configure the agent and view its discovery results. To view a list of the agent's discoveries, you can select the "Discoveries" tab, which displays the "Discovery List" view. This view lists all of the agent's discoveries, and provides options for creating, viewing, and deleting discoveries.



Name	Created	Modified	Schedule	Enabled
Human Resources	04/06/2020 11:31	02/19/2021 12:57	Every 4 minutes	NO
Marketing	03/30/2020 21:41	02/19/2021 19:16	Every 5 minutes	YES
Sales	04/06/2020 11:33	02/19/2021 12:57	Every 6 minutes	NO

Agent's Discovery List

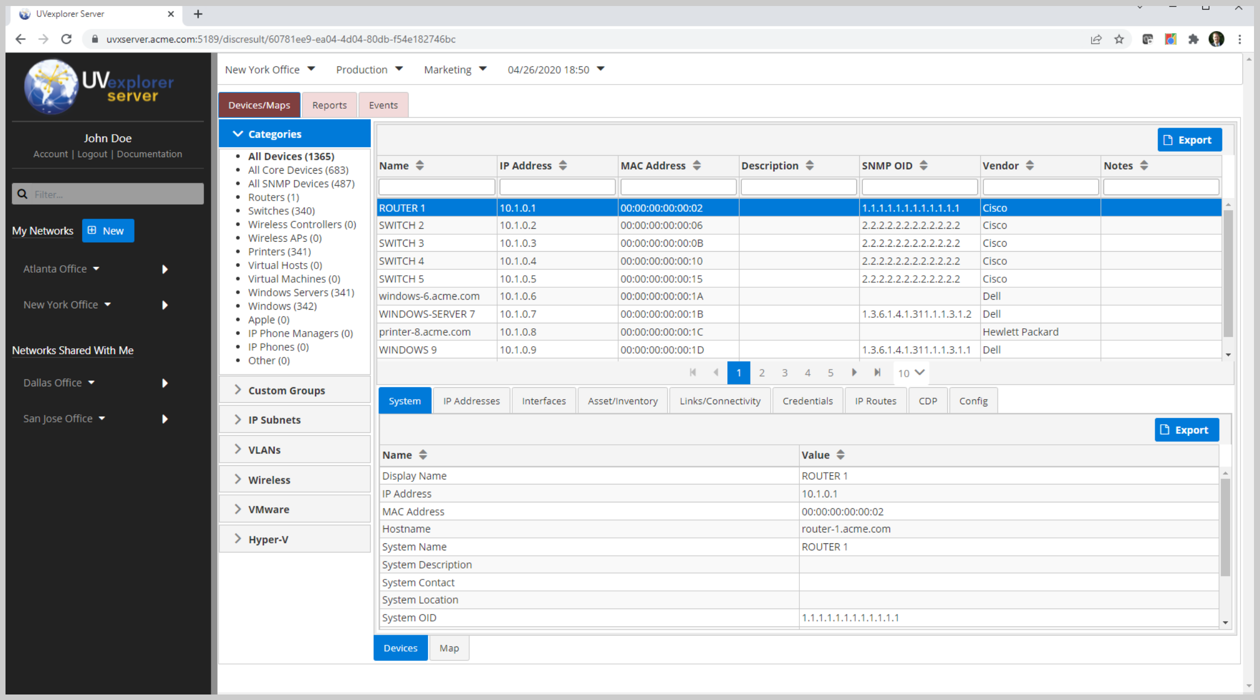
To view the details for one of your discoveries, you can click the discovery's "View" button, which takes you to the "Discovery" view. This view displays all the details about the selected discovery. There are many tabs you can select to configure the discovery and view its discovery results. To view a list of the discovery's "discovery runs", you can select the "Discovery Runs" tab, which displays the "Discovery Run List" view.



Start Time	End Time	
04/26/2020 18:50	04/26/2020 18:50	View
04/26/2020 18:45	04/26/2020 18:45	View
04/26/2020 18:40	04/26/2020 18:40	View
04/26/2020 18:35	04/26/2020 18:35	View
04/26/2020 18:30	04/26/2020 18:30	View
04/26/2020 18:25	04/26/2020 18:25	View
04/26/2020 18:20	04/26/2020 18:20	View
04/26/2020 18:15	04/26/2020 18:15	View
04/26/2020 18:10	04/26/2020 18:10	View

Discovery's "Discovery Run" List

To view the details for a discovery run, you can click the discovery run's "View" button, which takes you to the "Discovery Run" view. This view contains several tabs that display all the details about the discovery run.



Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
ROUTER 1	10.1.0.1	00:00:00:00:00:02		1.1.1.1.1.1.1.1.1.1.1.1	Cisco	
SWITCH 2	10.1.0.2	00:00:00:00:00:06		2.2.2.2.2.2.2.2.2.2.2.2	Cisco	
SWITCH 3	10.1.0.3	00:00:00:00:00:0B		2.2.2.2.2.2.2.2.2.2.2.2	Cisco	
SWITCH 4	10.1.0.4	00:00:00:00:00:10		2.2.2.2.2.2.2.2.2.2.2.2	Cisco	
SWITCH 5	10.1.0.5	00:00:00:00:00:15		2.2.2.2.2.2.2.2.2.2.2.2	Cisco	
windows-6.acme.com	10.1.0.6	00:00:00:00:00:1A			Dell	
WINDOWS-SERVER 7	10.1.0.7	00:00:00:00:00:1B		1.3.6.1.4.1.311.1.1.3.1.2	Dell	
printer-8.acme.com	10.1.0.8	00:00:00:00:00:1C			Hewlett Packard	
WINDOWS 9	10.1.0.9	00:00:00:00:00:1D		1.3.6.1.4.1.311.1.1.3.1.1	Dell	

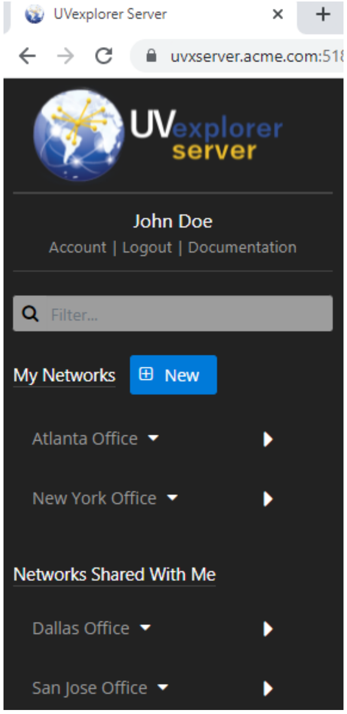
Name	Value
Display Name	ROUTER 1
IP Address	10.1.0.1
MAC Address	00:00:00:00:00:02
Hostname	router-1.acme.com
System Name	ROUTER 1
System Description	
System Contact	
System Location	
System OID	1.1.1.1.1.1.1.1.1.1.1.1

Discovery Run

Navigating with the Nav Bar

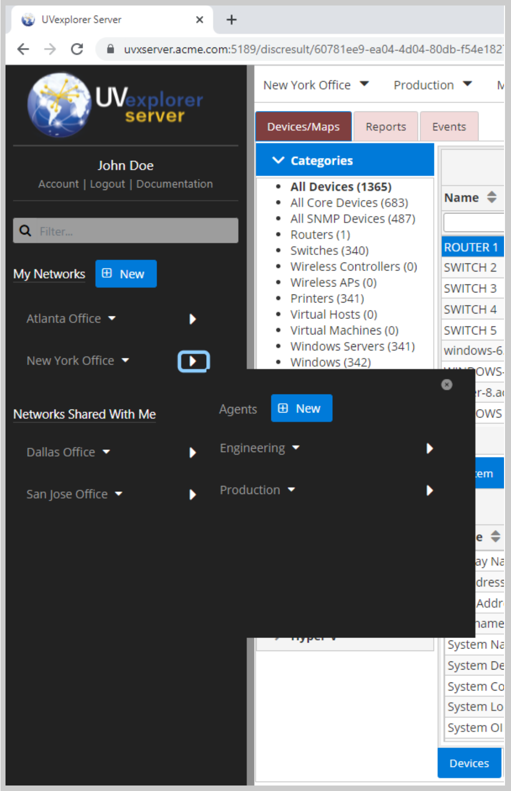
The list views described in the previous section are effective for viewing all of your objects. However, when you have a specific object you are looking for, navigating through the list views can be a bit cumbersome. To make navigating to a specific object more convenient, UVexplorer

Server provides a nav bar on the left side of the screen that lets you quickly navigate to a specific network, agent, discovery, or discovery run.



Nav Bar

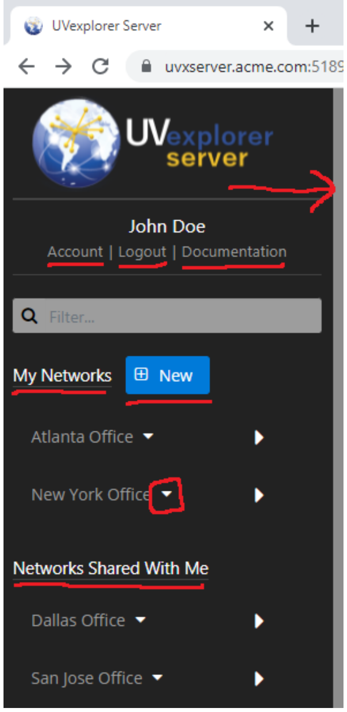
At the bottom of the nav bar there is a list of all your networks. This list is divided into two sections: “My Networks” and “Networks Shared With Me”. This makes it easy to distinguish between networks you own and those that have been shared with you. Clicking on the name of a network will take you directly to the Network view for that network. To navigate to an agent within a network, click on the right-facing triangle next to the network’s name. This will pop up a list of the network’s agents (as shown below). You can either select an agent from the list, which will take you to the Agent view for that agent, or you can click the right-facing triangle next to an agent’s name to see a list of that agent’s discoveries. Using the same technique, you can navigate to any object in the Network - Agent - Discovery - Discovery Run hierarchy.



Using the Nav Bar

The Nav Bar also provides the following features (see picture below):

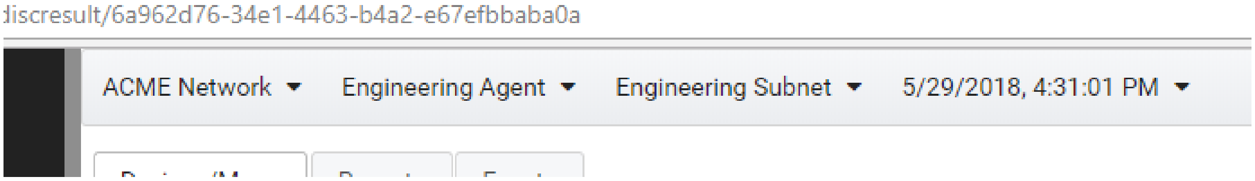
1. Clicking the gray border on the right side of the Navigation Bar will toggle its visibility (make it visible or invisible)
2. Clicking the “Account” link takes you to the “Account” view, which provides user management features (changing passwords, creating/modifying/deleting user accounts and groups, managing your UVexplorer Server license, and managing network sharing)
3. Clicking the “Logout” link will log you out of the web console and take you back to the login page
4. Clicking the “Documentation” link will take you to the UVexplorer user guide
5. Clicking the “My Networks” link takes you to the “Network List” view
6. Clicking the “New” button will let you create a new network object. Similarly, the Nav Bar’s pop-up lists also provide buttons for creating new agent and discovery objects.
7. Clicking the down-facing triangle next to a network name will display a menu that provides options for deleting, sharing, and unsharing networks (be careful when deleting a network, because this operation cannot be undone). Similarly, the Nav Bar’s pop-up lists provide the ability to delete agents and discoveries (again, be careful).
8. Clicking the “Networks Shared With Me” link takes you to the “Network List” view



Nav Bar Features

Navigating with Bread Crumbs

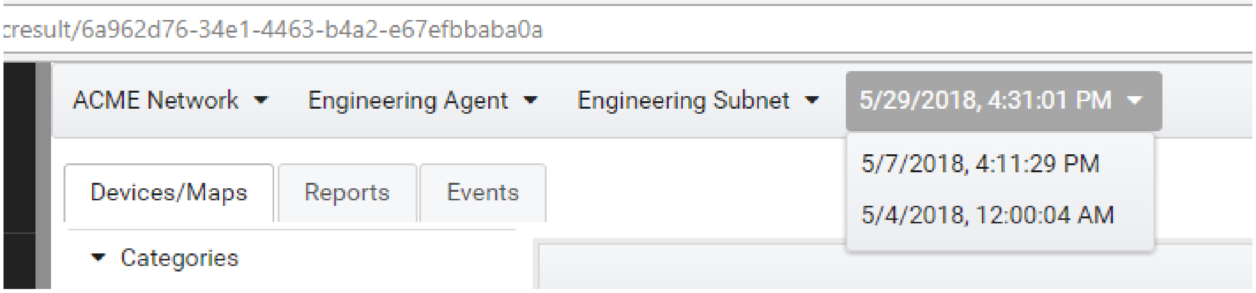
The last way to navigate between objects is the “bread crumbs” control displayed at the top of the web console window (see picture below).



Bread Crumbs Control

The bread crumbs control shows you which object you are currently viewing (network, agent, discovery, discovery run, etc.), and how you got there. For example, in the picture above, the user is viewing a discovery run named “5/29/2018, 4:31:01 PM” that belongs to a discovery named “Engineering Subnet” that is part of an agent named “Engineering Agent” that is part of a network named “ACME Network.

Each entry in the bread crumbs control contains a drop-down list of other objects at its level that you can navigate to. For example, in the picture above, clicking the down-facing triangle next to “ACME Networks” would display a list of other networks you can navigate to. Selecting a network from that list will take you directly to that network. Similarly, the other entries in the bread crumbs control provide lists of agents, discoveries, and discovery runs that you can navigate to (see picture below).



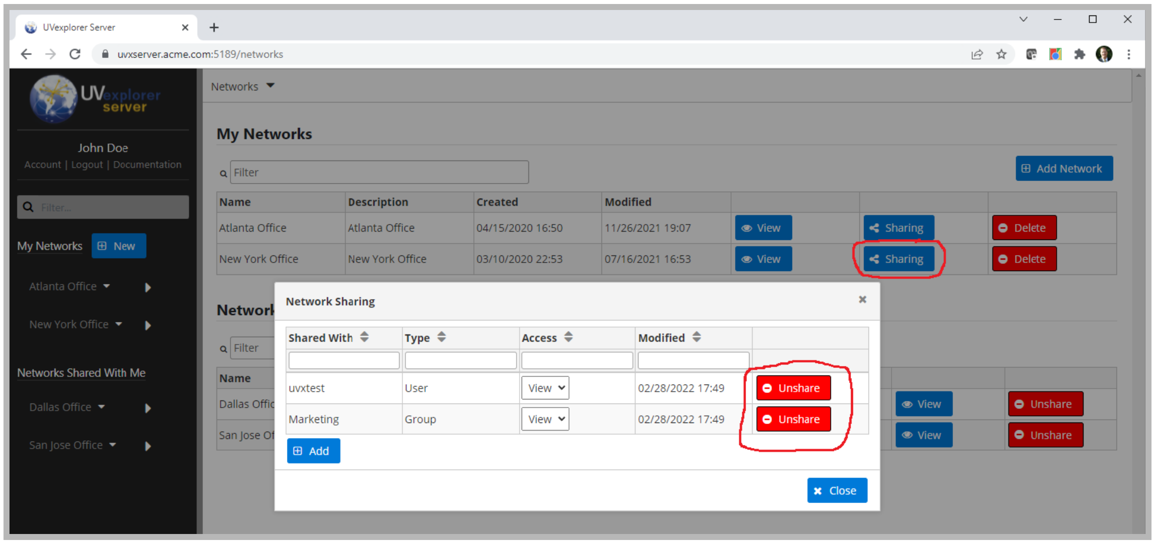
:result/6a962d76-34e1-4463-b4a2-e67efbbaba0a

Navigating with Bread Crumbs Control

Managing Network Sharing

Users can share their networks with other users, similar to the way a Google Doc can be shared with other people. This capability supports scenarios where multiple users are responsible for managing the same network. When a network object is shared with another user, that user will see the shared network in their list of networks, and will be able to view the network's configuration and data (agents, discoveries, etc). Similarly, networks can also be shared with user groups. When a network is shared with a group, all users in that group will see that network in their network list. Networks can be shared in either "edit" or "view" mode, depending on whether you want the other users to be able to modify the network's configuration, or just view it.

In the Network List view, the "My Networks" section lists the networks that belong to you. You can control sharing of your networks by clicking the "Sharing" button. When you click the "Sharing" button, a dialog appears that lets you see who the network has been shared with and whether it was shared in "edit" or "view" mode. You can also "unshare" a network by clicking the "Unshare" button (see picture below).



My Networks

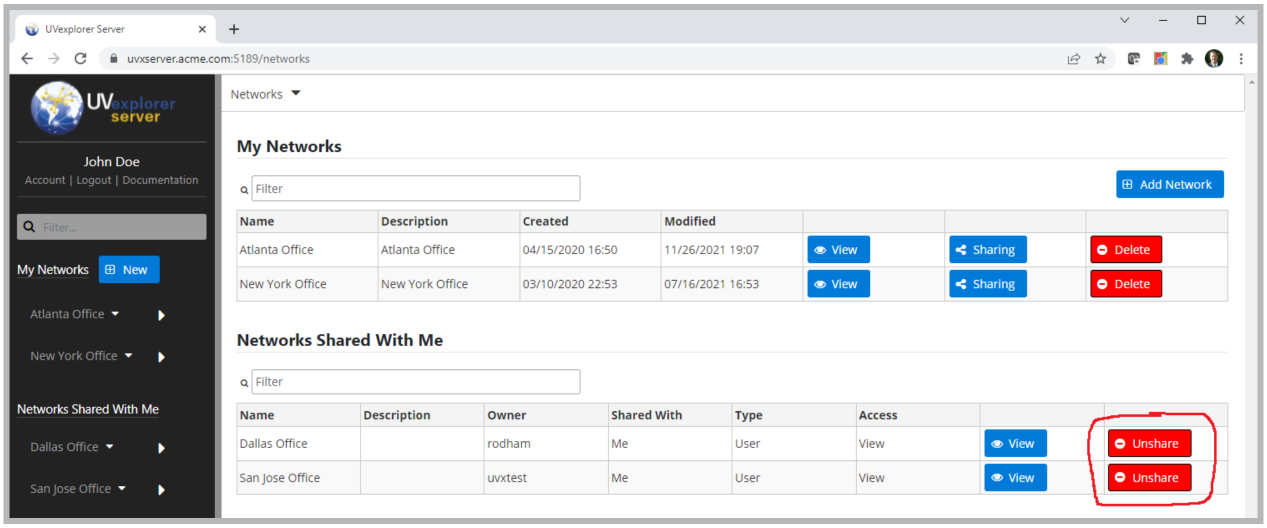
Name	Description	Created	Modified			
Atlanta Office	Atlanta Office	04/15/2020 16:50	11/26/2021 19:07	View	Sharing	Delete
New York Office	New York Office	03/10/2020 22:53	07/16/2021 16:53	View	Sharing	Delete

Network Sharing

Shared With	Type	Access	Modified	
uvxtest	User	View	02/28/2022 17:49	Unshare
Marketing	Group	View	02/28/2022 17:49	Unshare

Sharing in Network List

Also in the Network List view, the “Networks Shared With Me” section lists the networks that others have shared with you, including whether each network was shared in “edit” or “view” mode. You can “unshare” a network that has been shared with you by clicking the “Unshare” button (see picture below). If the network was shared with a group you are a member of, the “Unshare” button will be disabled.



My Networks

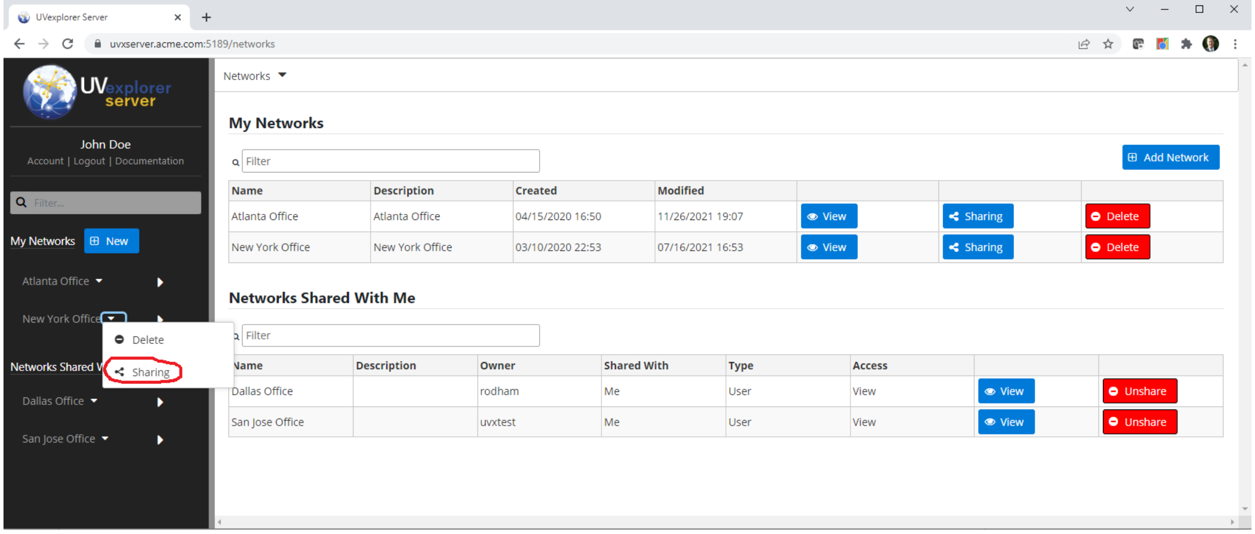
Name	Description	Created	Modified			
Atlanta Office	Atlanta Office	04/15/2020 16:50	11/26/2021 19:07	View	Sharing	Delete
New York Office	New York Office	03/10/2020 22:53	07/16/2021 16:53	View	Sharing	Delete

Networks Shared With Me

Name	Description	Owner	Shared With	Type	Access		
Dallas Office		rodham	Me	User	View	View	Unshare
San Jose Office		uvxtest	Me	User	View	View	Unshare

Unsharing in Network List

Similar options are provided in the Nav Bar. In the “My Networks” section of the Nav Bar, if you click the down-triangle icon next to a network’s name, a menu appears that contains a “Sharing” option that displays a dialog for managing sharing of that network. Similarly, in the “Networks Shared With Me” section of the Nav Bar, if you click the down-triangle icon next to a network’s name, a menu appears that contains an “Unshare” option for unsharing that network (see pictures below).



My Networks

Filter

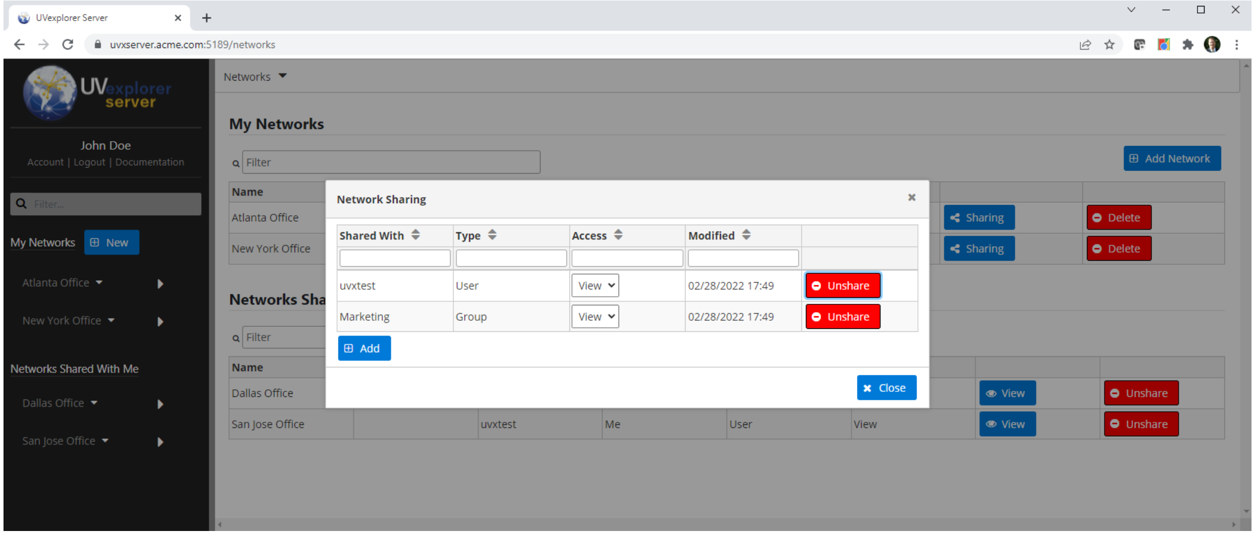
Add Network

Name	Description	Created	Modified			
Atlanta Office	Atlanta Office	04/15/2020 16:50	11/26/2021 19:07	View	Sharing	Delete
New York Office	New York Office	03/10/2020 22:53	07/16/2021 16:53	View	Sharing	Delete

Networks Shared With Me

Filter

Name	Description	Owner	Shared With	Type	Access		
Dallas Office		rodham	Me	User	View	View	Unshare
San Jose Office		uvxtest	Me	User	View	View	Unshare



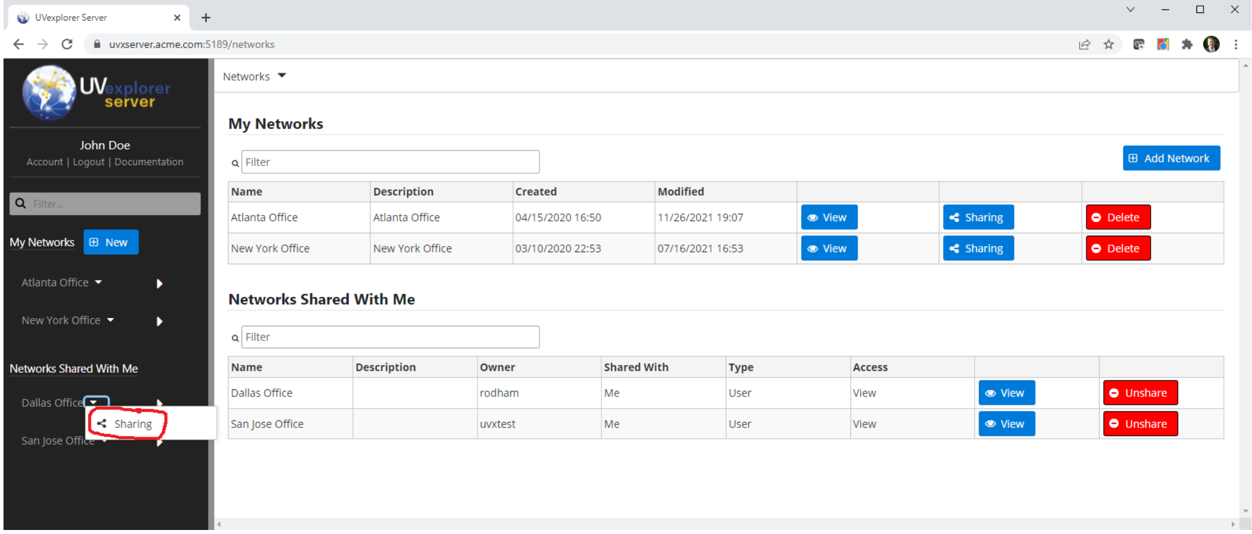
Network Sharing

Shared With	Type	Access	Modified	
uvxtest	User	View	02/28/2022 17:49	Unshare
Marketing	Group	View	02/28/2022 17:49	Unshare

Add

Close

Sharing in Nav Bar

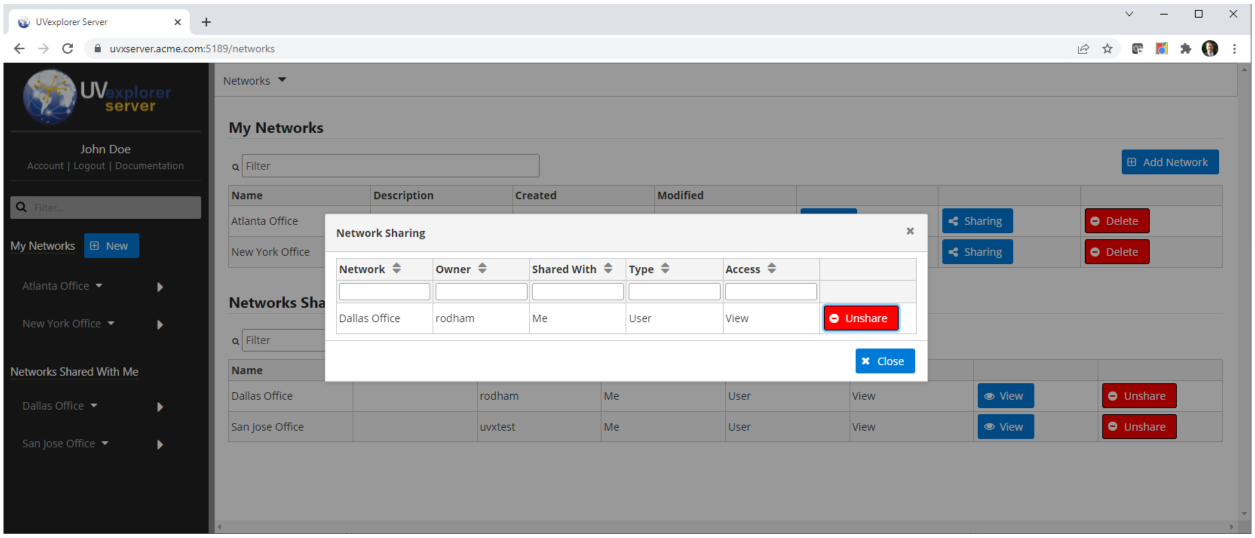


My Networks

Name	Description	Created	Modified			
Atlanta Office	Atlanta Office	04/15/2020 16:50	11/26/2021 19:07	View	Sharing	Delete
New York Office	New York Office	03/10/2020 22:53	07/16/2021 16:53	View	Sharing	Delete

Networks Shared With Me

Name	Description	Owner	Shared With	Type	Access		
Dallas Office		rodham	Me	User	View	View	Unshare
San Jose Office		uvxtest	Me	User	View	View	Unshare

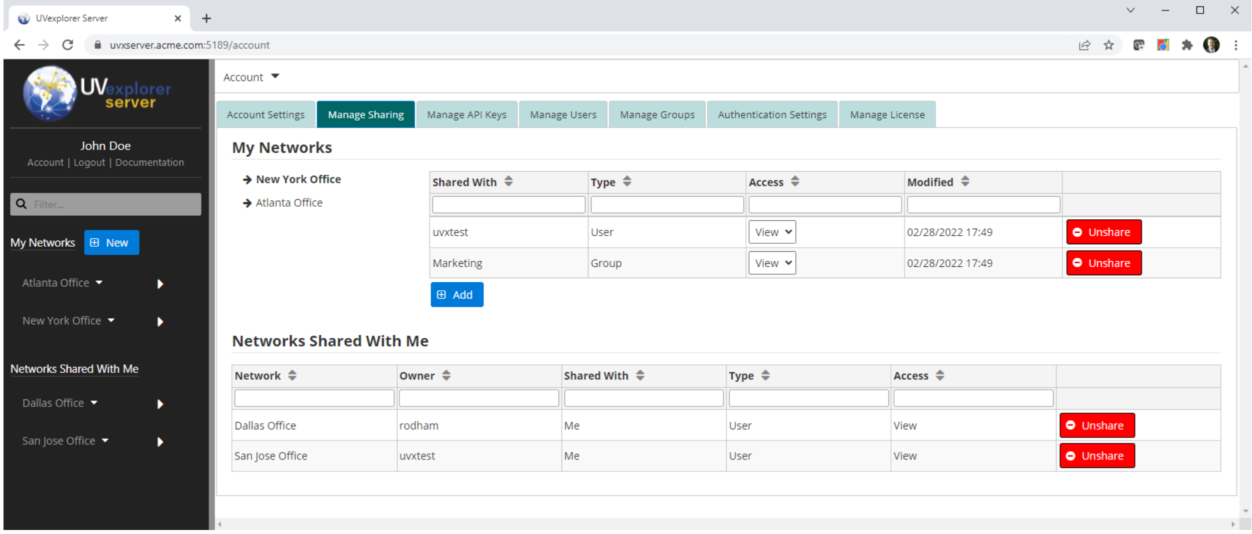


Network Sharing

Network	Owner	Shared With	Type	Access	
Dallas Office	rodham	Me	User	View	Unshare

Unsharing in Nav Bar

For a comprehensive view of network sharing, you can click on the “Account” link at the top of the navigation bar on the left side of the UVexplorer Server window, and select the “Manage Sharing” tab. The “Manage Sharing” tab lets you view and modify the sharing settings for all of your own networks, and also the networks that have been shared with you (see picture below).



My Networks

→ New York Office
→ Atlanta Office

Shared With	Type	Access	Modified	
uvxtest	User	View	02/28/2022 17:49	Unshare
Marketing	Group	View	02/28/2022 17:49	Unshare

Add

Networks Shared With Me

Network	Owner	Shared With	Type	Access	
Dallas Office	rodham	Me	User	View	Unshare
San Jose Office	uvxtest	Me	User	View	Unshare

Manage Sharing Tab

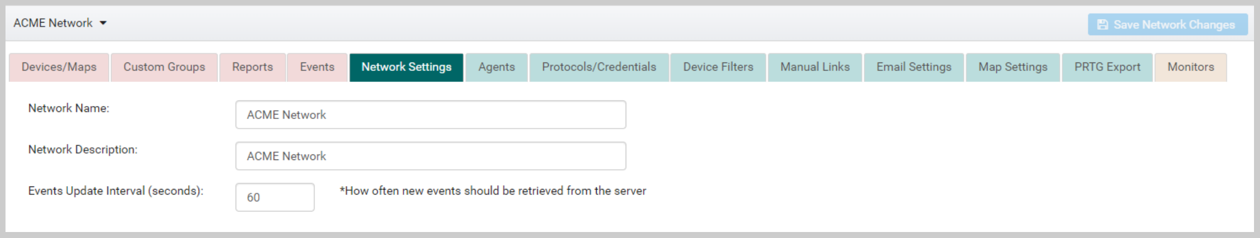
Configuring Networks

As described in the “Navigation” section, you can create, share, and delete network objects either from the Nav Bar or from the Network List. When creating a network, you need to give it a name and, optionally, a description. Once a network has been created, you must configure it.

To configure a network, you must navigate to it using one of the techniques described in the “Navigation” section (Network List, Nav Bar, or Bread Crumbs), which will display the Network view. The Network view contains many tabs that serve a variety of purposes. The following tabs are related to configuring a network:

- ➔ Network Settings Tab
- ➔ Agents Tab
- ➔ Protocols/Credentials Tab
- ➔ Email Settings Tab

Network Settings Tab



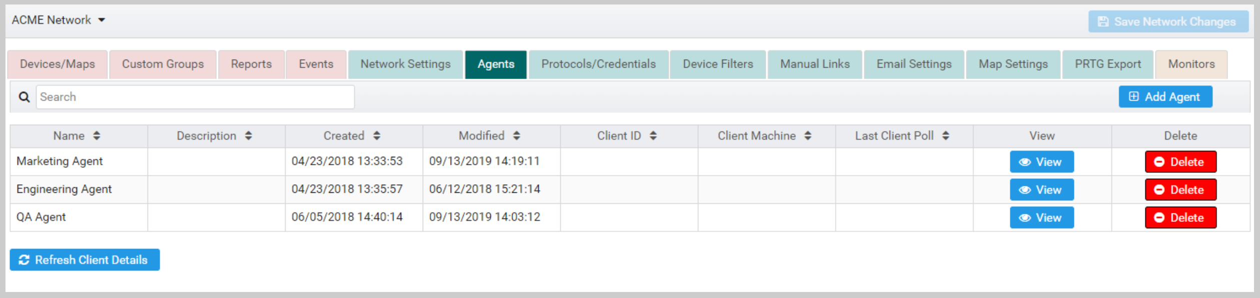
Network Name:	ACME Network
Network Description:	ACME Network
Events Update Interval (seconds):	60 *How often new events should be retrieved from the server

The Network Settings tab lets you modify the following network properties:

- ❏ Network Name - the network’s name
- ❏ Network Description - an optional description of the network

❑ Event Update Interval - specifies how frequently the web console should poll UVexplorer Server to refresh the events displayed in the Events tab, expressed in seconds (applies to refreshing events within the network's agents, discoveries, and discovery runs, as well).

Agents Tab



Name	Description	Created	Modified	Client ID	Client Machine	Last Client Poll	View	Delete
Marketing Agent		04/23/2018 13:33:53	09/13/2019 14:19:11				View	Delete
Engineering Agent		04/23/2018 13:35:57	06/12/2018 15:21:14				View	Delete
QA Agent		06/05/2018 14:40:14	09/13/2019 14:03:12				View	Delete

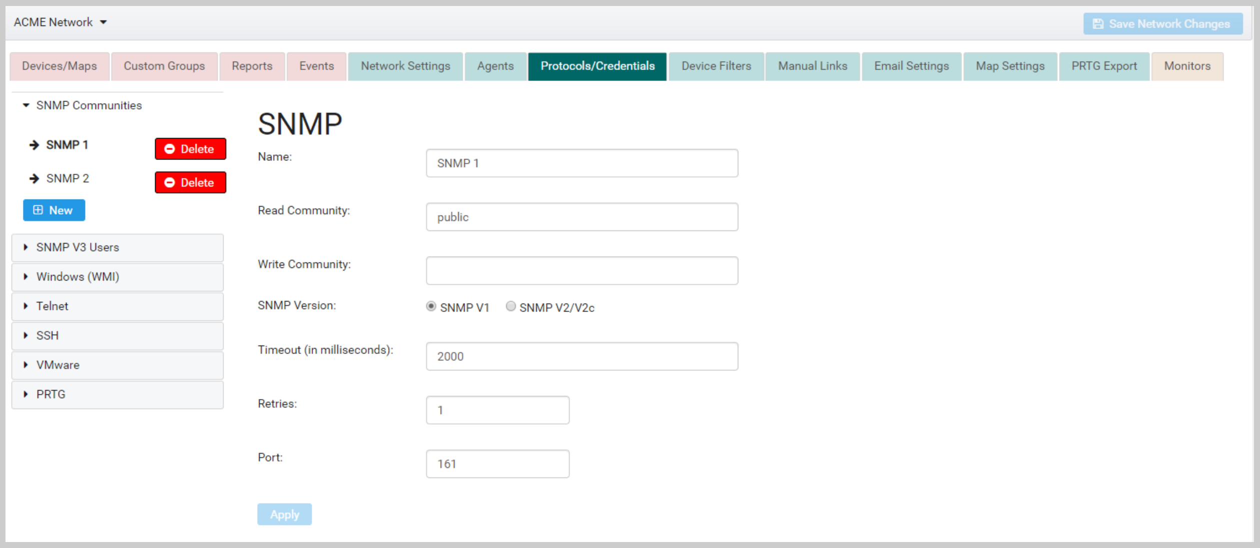
The Agents tab displays the Agent List view described in the "Navigation" section of this document. This view displays a list of all the network's agents.

The "Add Agent" button lets you create a new agent.

The "View" button lets you navigate to the agent in order to configure it or view its discovery data and maps.

The "Delete" button deletes the agent and all discoveries and discovery runs associated with it.

Protocols/Credentials Tab



SNMP

Name: SNMP 1

Read Community: public

Write Community:

SNMP Version: ● SNMP V1 ○ SNMP V2/V2c

Timeout (in milliseconds): 2000

Retries: 1

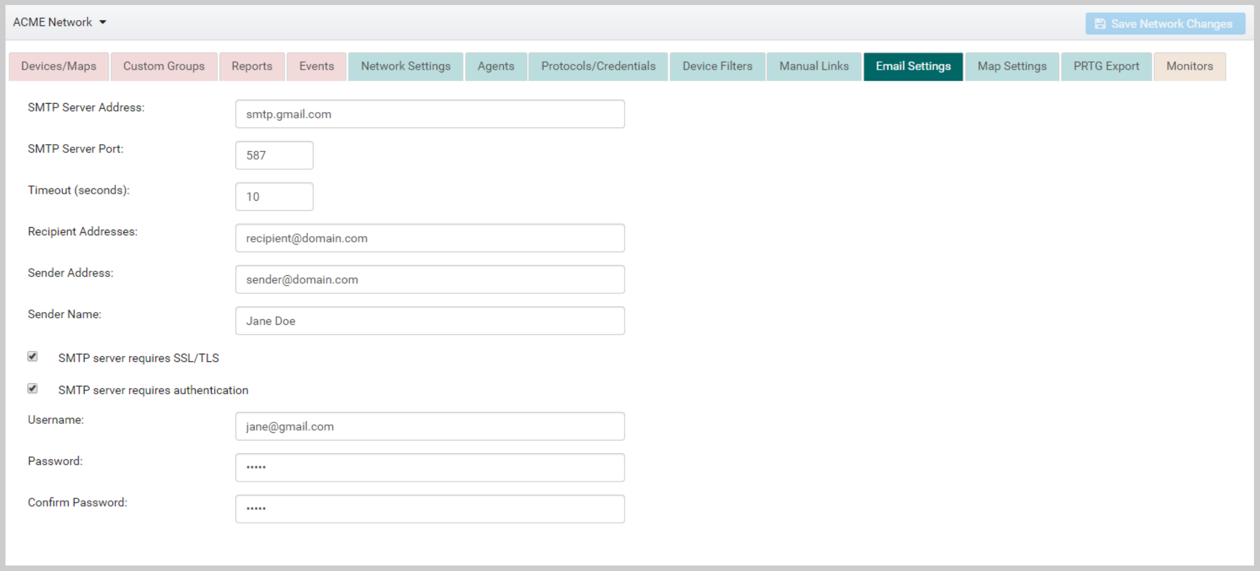
Port: 161

UVexplorer Server uses a variety of protocols to communicate with and learn about the devices on your network. Most of these protocols require some kind of credentials and/or settings in order to operate. The Protocols/Credentials tab lets you specify the credentials for the devices on your network (user names, passwords, etc.), and also other settings that control how the protocols operate (timeouts, retries, etc.).

Along the left side of the Protocols/Credentials tab is an “accordion” control, that lets you access the credentials/settings for the various protocols (SNMP V1/V2, SNMP V3, WMI, Telnet, SSH, VMware, and PRTG). To access the credentials for a particular protocol, click on the heading for the desired protocol, which will expand that section (and contract any others). The section for each protocol displays a list of different credentials that you have previously created for that protocol. You can specify multiple different credentials for each protocol, and UVexplorer Server will try them all (or a subset you specify) when trying to communicate with devices on your network. This means that the more credentials you specify, the longer discoveries will take, because it tries them all for each device (at least until it finds one that works).

Each credential must be given a name. An existing credential may be viewed or modified by clicking on its name in the list, which will cause its properties to appear on the right side.
The “Apply” button causes any changes you’ve made to be applied to the credential.
The “New” button lets you create a new credential.
The “Delete” button lets you delete an existing credential.

Email Settings Tab

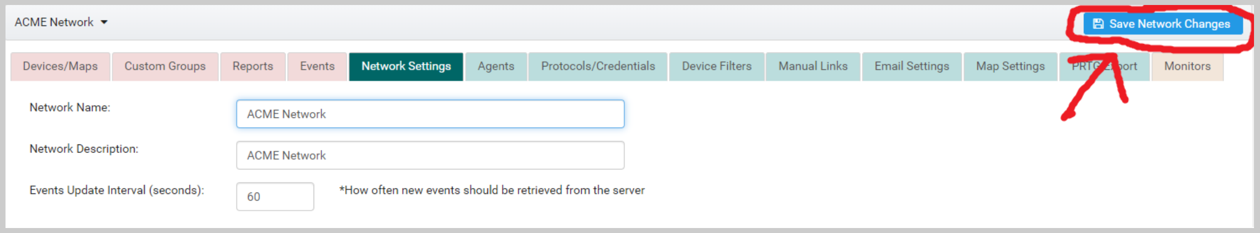


SMTP Server Address: smtp.gmail.com
SMTP Server Port: 587
Timeout (seconds): 10
Recipient Addresses: recipient@domain.com
Sender Address: sender@domain.com
Sender Name: Jane Doe
☑ SMTP server requires SSL/TLS
☑ SMTP server requires authentication
Username: jane@gmail.com
Password: •••••
Confirm Password: •••••

UVexplorer Server can send notification emails to specified addresses about interesting events that occur in the system. For example, if you request it, UVexplorer Server will send you an email that summarizes the results of a discovery run when it completes. Or, you can request notification emails about error conditions that might occur in the system. In order to send emails, UVexplorer Server needs the configuration of the email (SMTP) server it should use to send the emails. The Email Settings tab is where you can specify your email server settings. Of course, if you do not provide these settings, no emails will be sent.

It is important to note that emails may be sent from either the UVexplorer Server, or from one of the network's agents. Therefore, it is important that the specified email server be accessible from the machine running UVexplorer Server, as well as from the machines running UVexplorer Server agents.

Saving Network Changes



Network Name: ACME Network

Network Description: ACME Network

Events Update Interval (seconds): 60 *How often new events should be retrieved from the server

As you move between the various tabs making changes to the network's configuration, none of your changes are permanent until they are "saved" to the UVexplorer Server server. You can manually save your changes by clicking the "Save Network Changes" button in the upper-right corner of the Network view. Prior to clicking "Save Network Changes", your changes are local to your web browser and unknown to the server.

If you navigate away from the network without saving your changes, the web console will automatically save your changes to the server (as if you had manually clicked "Save Network Changes"). This way your changes will not be lost if you forget to save them. However, if you close your web browser without manually saving or navigating away from the network, your changes will be lost.

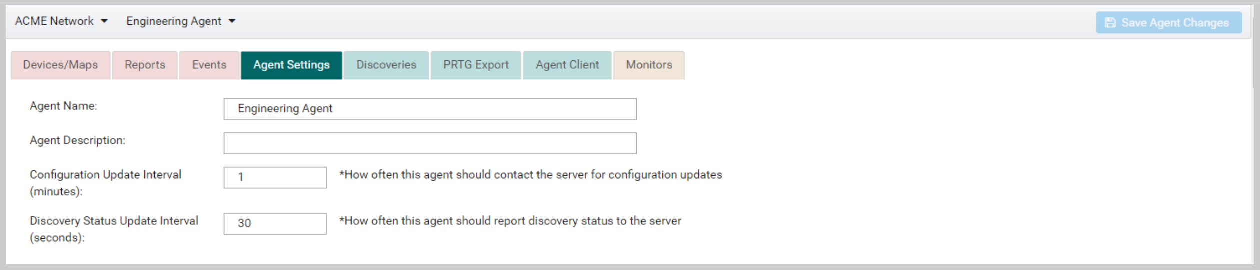
Configuring Agents

As described in the "Navigation" section of this document, you can create and delete agent objects either from the Nav Bar or from the Agent List in a network's "Agents" tab. When creating an agent, you need to give it a name and, optionally, a description. Once an agent has been created, you must configure it.

To configure an agent, you must navigate to it using one of the techniques described in the "Navigation" section (Network List, Nav Bar, or Bread Crumbs), which will display the Agent view. The Agent view contains several tabs that serve a variety of purposes. The following tabs are related to configuring an agent:

- ➔ Agent Settings Tab
- ➔ Discoveries Tab

Agent Settings Tab

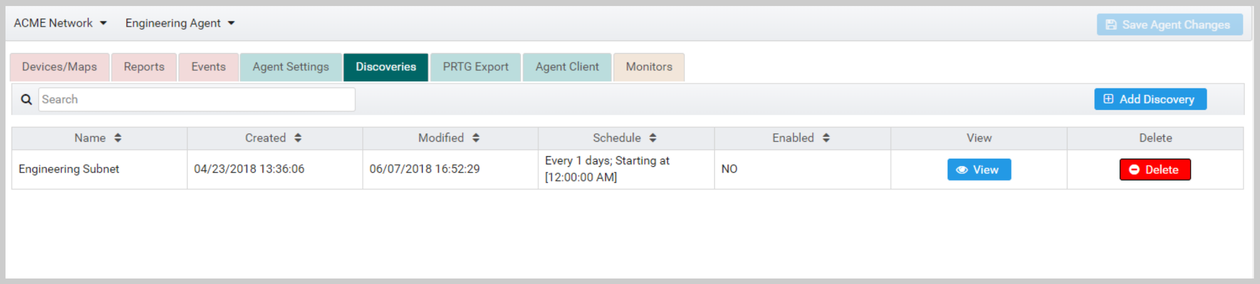


Agent Name:	Engineering Agent	
Agent Description:		
Configuration Update Interval (minutes):	1	*How often this agent should contact the server for configuration updates
Discovery Status Update Interval (seconds):	30	*How often this agent should report discovery status to the server

The Agent Settings tab lets you modify the following agent properties:

- ❏ Agent Name - the agent's name
- ❏ Agent Description - an optional description of the agent
- ❏ Configuration Update Interval - specifies how frequently this agent should poll UVexplorer Server for changes to its configuration, expressed in minutes (the more frequently agents poll for configuration changes, the faster the changes you make will take effect at the agent, and the more load it will put on the server)
- ❏ Discovery Status Update Interval - specifies how frequently this agent should send discovery status updates to the server during discovery runs, expressed in seconds (the more frequently agents send discovery status updates to the server, the more up-to-date the status displayed in a discovery's Status tab will be, and the more load it will put on the server)

Discoveries Tab



Name	Created	Modified	Schedule	Enabled	View	Delete
Engineering Subnet	04/23/2018 13:36:06	06/07/2018 16:52:29	Every 1 days; Starting at [12:00:00 AM]	NO	View	Delete

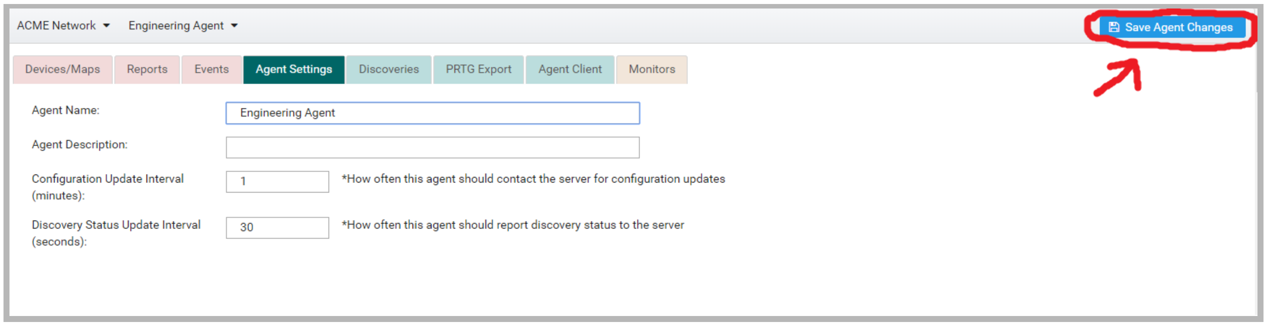
The Discoveries tab displays the Discovery List view described in the "Navigation" section. This view displays a list of all the agent's discoveries.

The "Add Discovery" button lets you create a new discovery.

The "View" button lets you navigate to the discovery in order to configure it or view its discovery data and maps.

The "Delete" button deletes the discovery and all discovery runs and other data associated with it.

Saving Agent Changes



Agent Name: Engineering Agent

Agent Description:

Configuration Update Interval (minutes): 1 *How often this agent should contact the server for configuration updates

Discovery Status Update Interval (seconds): 30 *How often this agent should report discovery status to the server

As you move between the various tabs making changes to the agent's configuration, none of your changes are permanent until they are "saved" to UVexplorer Server. You can manually save your changes by clicking the "Save Agent Changes" button in the upper-right corner of the Agent view. Prior to clicking "Save Agent Changes", your changes are local to your web browser and unknown to the server.

If you navigate away from the agent without saving your changes, the web console will automatically save your changes to the server (as if you had manually clicked "Save Agent Changes"). This way your changes will not be lost if you forget to save them. However, if you close your web browser without manually saving or navigating away from the agent, your changes will be lost.

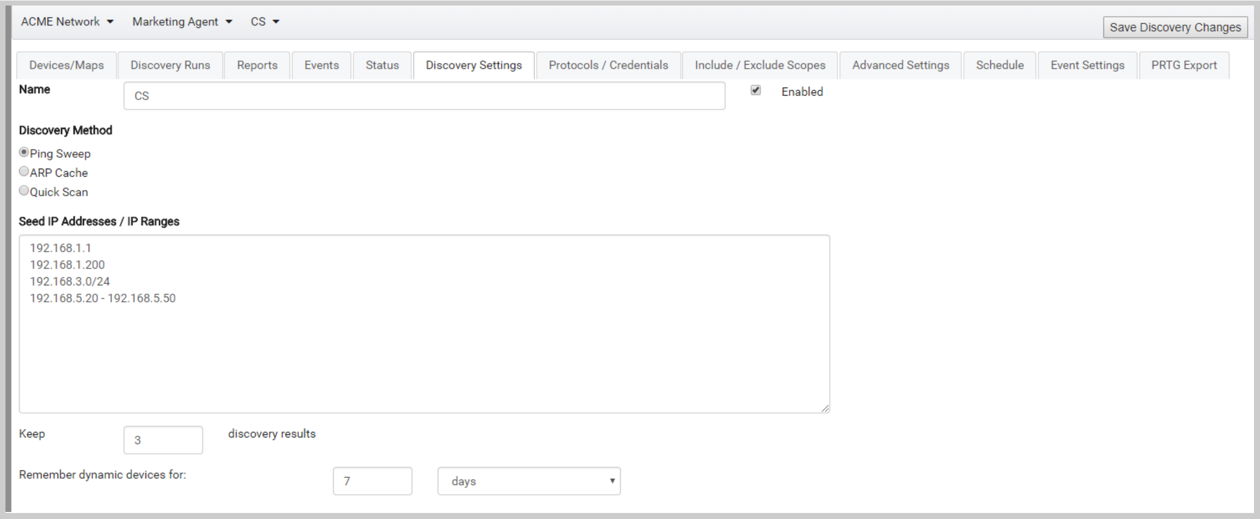
Configuring Discoveries

As described in the "Navigation" section of this document, you can create and delete discovery objects either from the Nav Bar or from the Discovery List in an agent's "Discoveries" tab. When creating a discovery, you need to give it a name. Once a discovery has been created, you must configure it.

To configure a discovery, you must navigate to it using one of the techniques described in the "Navigation" section (Network List, Nav Bar, or Bread Crumbs), which will display the Discovery view. The Discovery view contains several tabs that serve a variety of purposes. The following tabs are related to configuring a discovery:

- ➔ Discovery Settings Tab
- ➔ Protocols/Credentials Tab
- ➔ Include/Exclude Scopes Tab
- ➔ Advanced Settings Tab
- ➔ Schedule Tab
- ➔ Event Settings Tab

Discovery Settings Tab



Name CS ☑ Enabled

Discovery Method

● Ping Sweep
○ ARP Cache
○ Quick Scan

Seed IP Addresses / IP Ranges

```
192.168.1.1
192.168.1.200
192.168.3.0/24
192.168.5.20 - 192.168.5.50
```

Keep 3 discovery results

Remember dynamic devices for: 7 days ▾

The Discovery Settings tab lets you modify the following discovery properties:

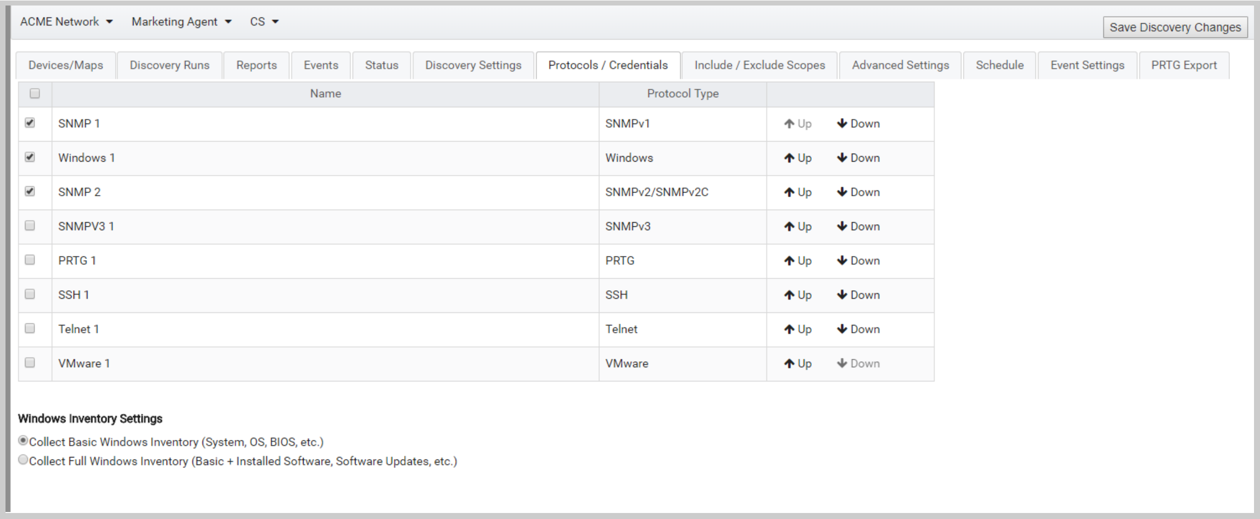
- Discovery Name - the discovery’s name
- Enabled - if a discovery is enabled, it will run at the times defined by its schedule; if a discovery is not enabled, it will not run at all (this is useful for turning a discovery off when you don’t want it to run for some reason)
- Discovery Method - defines what kind of discovery you want to run
    - Ping Sweep - Only devices with the IP addresses listed in the “Seed IP Addresses / IP Ranges” field will be discovered.
    - ARP Cache - This method “crawls” your network by querying the ARP caches on your network devices using the SNMP protocol. The IP addresses found in the ARP caches tell the agent running this discovery what IP addresses it should discover (as opposed to a Ping Sweep, where you tell the agent exactly which IP addresses to discover). ARP Cache discoveries only work well if you specify valid SNMP credentials for your core network devices (switches, routers, etc.). Without SNMP credentials, it won’t be able to read the ARP caches from your devices, and won’t be able to crawl your network.
    - Quick Scan - Ping Sweep and ARP Cache discoveries do a full, detailed discovery of your network, which can take awhile. If you want to do a faster, lighter-weight scan of your network that focuses only on your core network infrastructure (switches, routers, firewalls, etc.), you can do a Quick Scan discovery. Like ARP Cache, Quick Scan discovery will “crawl” your network, but it will do so faster and with a more narrow focus than ARP Cache discovery. This is done primarily using CDP and LLDP information. Quick Scan discovery also requires valid SNMP credentials for your core network devices in order to work properly.
- Seed IP Addresses / IP Ranges - In this text field you should provide the IP addresses the agent running this discovery will use to do the discovery. For Ping Sweep

discoveries, this should include all IP addresses that you want the agent to discover. For ARP Cache and Quick Scan discoveries, you only need to specify the IP addresses of the “seed” (or initial) devices at which the “crawl” of the network will begin. The agent will query the seed devices to find other IP addresses it needs to discover. IP addresses can be specified in one of three ways:

- IP Address: A single IP address; for example 192.168.1.1
- IP Range: A range of IP addresses; two IP addresses separated by a hyphen; for example 192.168.5.20 - 192.168.5.50
- IP Subnet: An IPv4 subnet; subnet IP followed by netmask length in bits separated by forward slash; for example 192.168.3.0/24

- Keep ‘N’ Discovery Results - The number of most recent discovery results (or runs) that UVexplorer Server will keep in its database. Discovery runs older than this will be discarded. Typical values for this would be between 1 and 10.
- Remember Dynamic Devices for ‘X’ Days/Hours/Minutes - Some devices remain on the network all the time (switches, routers, etc.), while other devices dynamically come and go (mobile devices, laptops, etc.). This setting specifies how long UVexplorer Server should “remember” devices that dynamically appear and disappear on the network. Since UVexplorer Server can notify you when devices appear and disappear on the network, this setting helps it avoid notifying you about uninteresting devices that are expected to come and go and should not cause notifications.

Protocols/Credentials Tab



☐	Name	Protocol Type		
☑	SNMP 1	SNMPv1	↑ Up	↓ Down
☑	Windows 1	Windows	↑ Up	↓ Down
☑	SNMP 2	SNMPv2/SNMPv2C	↑ Up	↓ Down
☐	SNMPV3 1	SNMPv3	↑ Up	↓ Down
☐	PRTG 1	PRTG	↑ Up	↓ Down
☐	SSH 1	SSH	↑ Up	↓ Down
☐	Telnet 1	Telnet	↑ Up	↓ Down
☐	VMware 1	VMware	↑ Up	↓ Down

Windows Inventory Settings

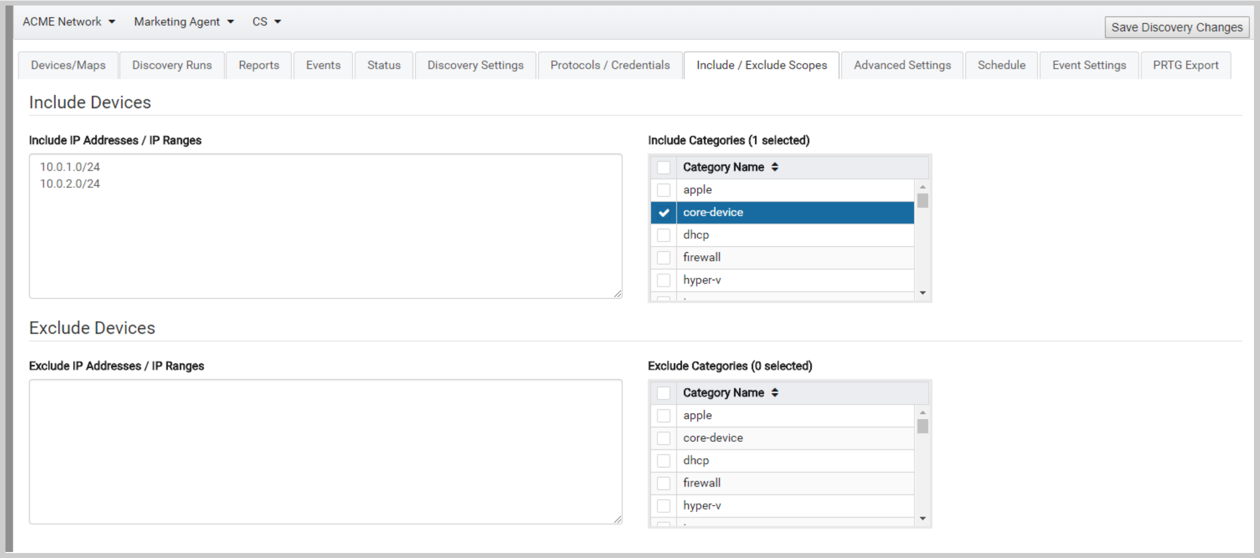
● Collect Basic Windows Inventory (System, OS, BIOS, etc.)
○ Collect Full Windows Inventory (Basic + Installed Software, Software Updates, etc.)

The Protocols/Credentials tab lets you select the protocol credentials/settings you want the agent to use for this discovery. The listed credentials are the ones you created in the network’s Protocols/Credentials tab. As previously stated, if the discovery is ARP Cache or Quick Scan, you must specify valid SNMP credentials for your core network devices (routers, switches, etc.) in order for the discovery to work well.

Only the credentials that you select will be used for the discovery. They will be tried in the order that you specify. You can use the “Up” and “Down” buttons to modify the order. Typically, you should place the credentials that are most likely to work for most devices at the top. This will speed up discovery.

In the “Windows Inventory Settings” section, you can specify what kind of Windows (or WMI) discovery you want the agent to do. “Full Windows Inventory” will take longer than “Basic Windows Inventory” because it collects more information. You can decide whether the additional information (primarily installed software information) is valuable to you. The agent will perform WMI discovery only if you have selected valid Windows credentials for your Windows devices.

Include/Exclude Scopes Tab



Include Devices

Include IP Addresses / IP Ranges

```
10.0.1.0/24
10.0.2.0/24
```

Include Categories (1 selected)

	Category Name
□	apple
☑	core-device
□	dhcp
□	firewall
□	hyper-v

Exclude Devices

Exclude IP Addresses / IP Ranges

Exclude Categories (0 selected)

	Category Name
□	apple
□	core-device
□	dhcp
□	firewall
□	hyper-v

There are times when you might not be interested in all of the devices that the agent can discover. For example, you might only be interested in seeing core network devices in your discovery results, and would like to omit everything else. Or, you might want to make sure that the discovery stays within a certain part of your network and doesn’t venture into other areas of the network. For this purpose, the Include/Exclude Scopes tab lets you specify exactly which devices and what parts of your network should be included in the discovery.

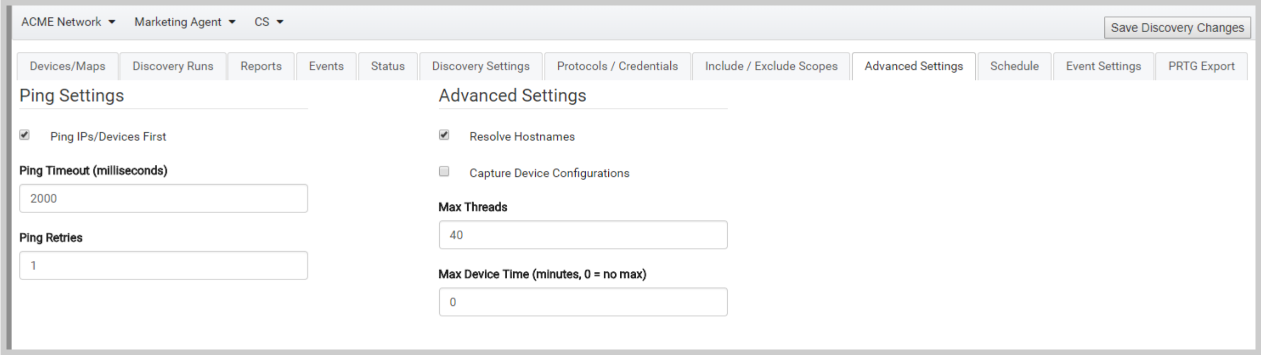
Using the “Include IP Addresses / IP Ranges” field and the “Include Categories” list, you can specify exactly which IP addresses and what types of devices to include in the discovery results. In this case, the discovery results will include only the devices that you specify, and nothing else. Only devices with IP addresses and categories that match your specification will be included.

Using the “Exclude IP Addresses / IP Ranges” field and the “Exclude Categories” list, you can specify which IP addresses and device types to exclude from the discovery results. In this case, the discovery results will include all devices discovered by the agent except the ones that you specify. Devices with IP addresses or categories that match your specification will be excluded.

For both including and excluding, IP addresses can be specified in one of three ways:

- IP Address: A single IP address; for example 192.168.1.1
- IP Range: A range of IP addresses; two IP addresses separated by a hyphen; for example 192.168.5.20 - 192.168.5.50
- IP Subnet: An IPv4 subnet; subnet IP followed by netmask length in bits separated by forward slash; for example 192.168.3.0/24

Advanced Settings Tab



Ping Settings

☑ Ping IPs/Devices First

Ping Timeout (milliseconds): 2000

Ping Retries: 1

Advanced Settings

☑ Resolve Hostnames

☐ Capture Device Configurations

Max Threads: 40

Max Device Time (minutes, 0 = no max): 0

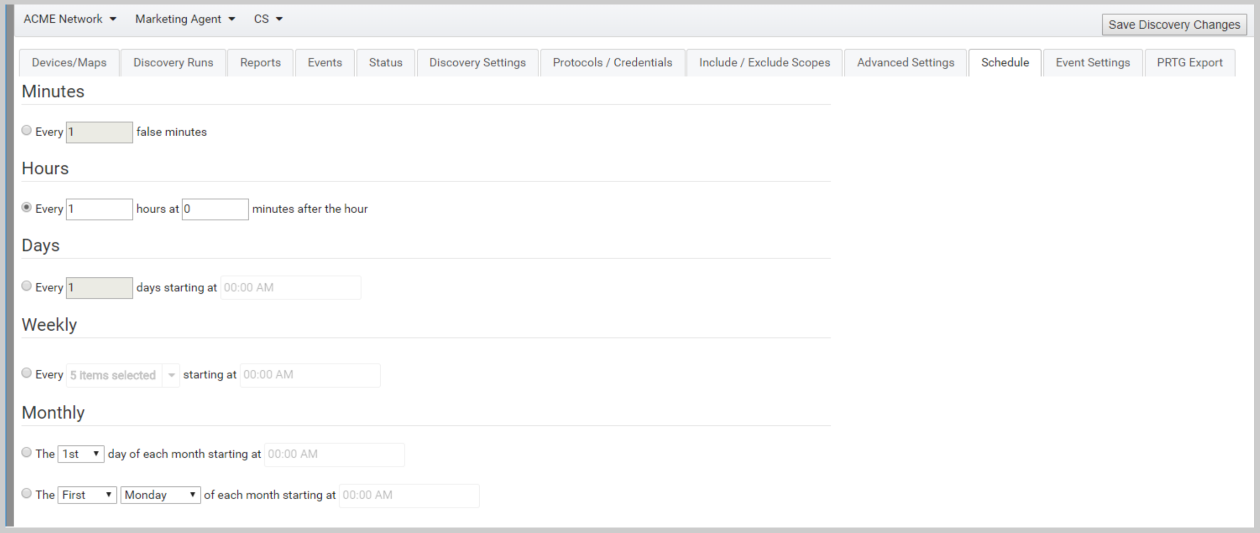
Advanced discovery settings can be specified in the Advanced Settings tab. These settings, which control various aspects of discovery, include the following:

- Ping Settings
  - Ping IPs/Devices First - This setting can be used to restrict discovery to only devices that respond to Ping (ICMP) requests. If this feature is enabled, before trying to discover an IP address, the agent running the discovery will first send a Ping request to ensure a device is communicating on that address. If the Ping fails, the agent will not make further attempts to communicate with that device, which results in a faster scan of the network (i.e., it “fails fast”). However, if Ping is not enabled on your network, you will want to disable this feature, because otherwise all Ping requests will fail, and nothing will be discovered.
  - Ping Timeout - how long the agent running this discovery should wait for a Ping response before it considers the Ping to have failed, expressed in milliseconds
  - Ping Retries - the number of times the agent running this discovery should retry failed Pings
- Other Advanced Settings
  - Resolve Hostnames - whether or not the agent running this discovery should use DNS to do hostname lookups on discovered IP addresses
  - Capture Device Configurations - Whether or not the agent running this discovery should capture network device configurations using SSH and/or Telnet protocols.

If this feature is enabled, it only works if you have specified valid SSH or Telnet credentials for the devices you want to capture configurations for.

- Max Threads - Maximum number of threads the agent running this discovery should use when running the discovery. This lets you control how many devices on your network the agent will communicate with at the same time. A higher number of threads will often speed up discovery, but may also put more burden on your network. A lower number of threads will often slow down discovery, but may put less burden on your network.
- Max Device Time - Maximum number of minutes the agent running this discovery should spend discovering any particular device. Sometimes there are devices that take an inordinately long time to discover, either because they are misconfigured or have unusually large amounts of data. This setting lets you specify how long the agent should work on any device before giving up and moving on.

Schedule Tab



Minutes

○ Every 1 false minutes

Hours

● Every 1 hours at 0 minutes after the hour

Days

○ Every 1 days starting at 00:00 AM

Weekly

○ Every 5 items selected starting at 00:00 AM

Monthly

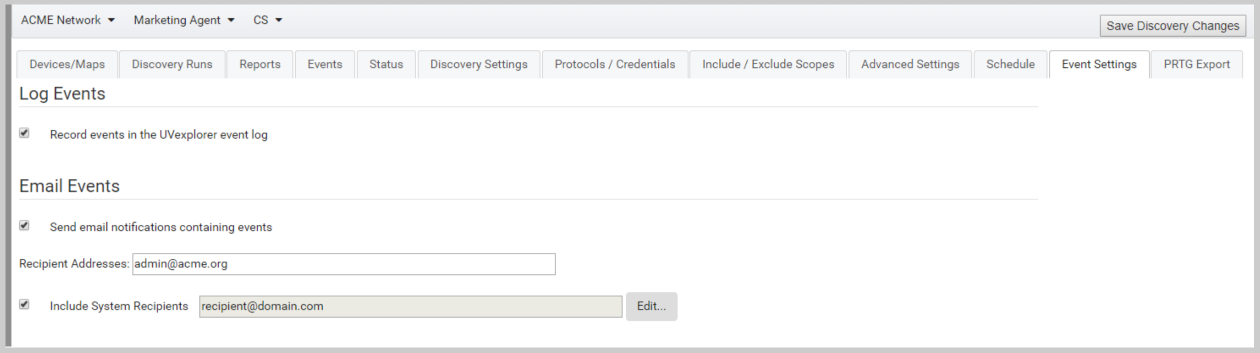
○ The 1st ▾ day of each month starting at 00:00 AM

○ The First ▾ Monday ▾ of each month starting at 00:00 AM

Discoveries run on a scheduled basis. The Schedule tab lets you specify the execution schedule for the discovery. For example, you can specify schedules like “Run every 60 minutes” or “Run every 2 days at Noon”. There are several scheduling options, all of which are self-explanatory.

Please note that the discovery will run only if it is enabled. The “Enabled” setting in the Discovery Settings tab controls whether or not the discovery will run according to its schedule. If a discovery is not running as you expect, you should first check to make sure it is enabled.

Event Settings Tab



Log Events

☑ Record events in the UVexplorer event log

Email Events

☑ Send email notifications containing events

Recipient Addresses: admin@acme.org

☑ Include System Recipients recipient@domain.com

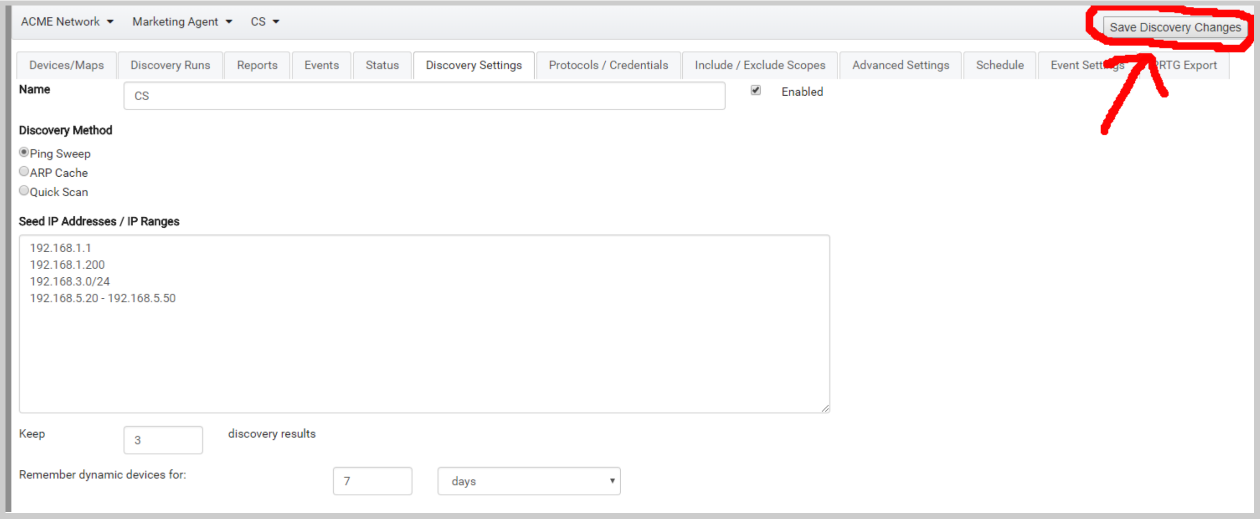
When a discovery executes there are interesting events that may occur. Here are some examples of events:

- Discovery completed
- Discovery encountered an error
- A new device was detected on the network
- A critical device disappeared from the network
- A new network link appeared on the network
- A critical network link went down

The Event Settings tab lets you specify settings that control how events should be reported. These settings include the following:

- Record Events in the UVexplorer Server Event Log - specifies whether or not events produced by the discovery will appear in the Events tab for the discovery, and also in the Events tabs for its agent and network.
- Send Email Notifications Containing Events - If this setting is enabled, each time a discovery run completes, UVexplorer Server will send an email summarizing the discovery results collected and also interesting events that occurred during the discovery run.
    - Recipient Addresses - specifies what email addresses you want discovery summary emails sent to
    - Include System Recipients - specifies whether or not the email recipients listed in the network’s Email Settings tab should also receive discovery summary emails

Saving Discovery Changes



Name CS ☑ Enabled

Discovery Method

● Ping Sweep
○ ARP Cache
○ Quick Scan

Seed IP Addresses / IP Ranges

```
192.168.1.1
192.168.1.200
192.168.3.0/24
192.168.5.20 - 192.168.5.50
```

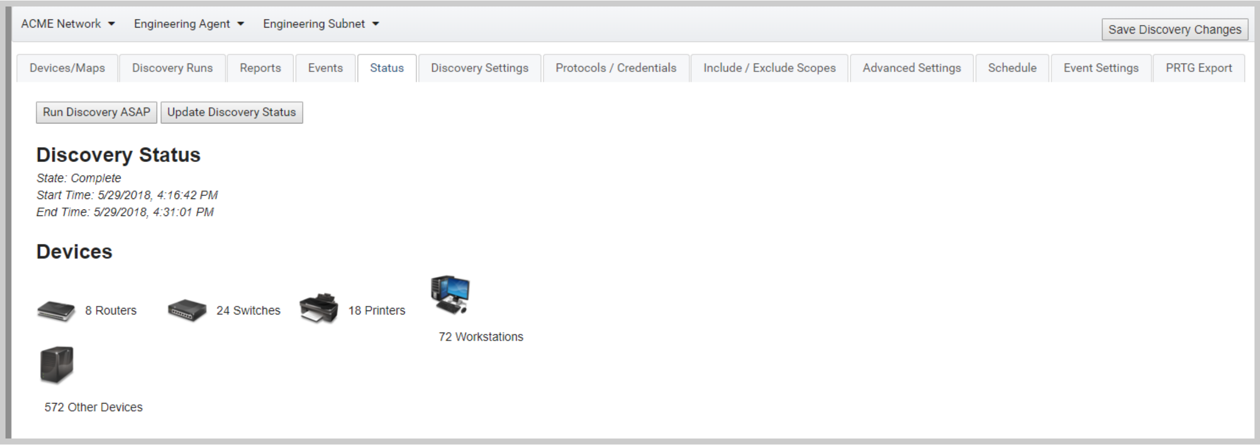
Keep 3 discovery results

Remember dynamic devices for: 7 days

As you move between the various tabs making changes to the discovery's configuration, none of your changes are permanent until they are "saved" to UVexplorer Server. You can manually save your changes by clicking the "Save Discovery Changes" button in the upper-right corner of the Discovery view. Prior to clicking "Save Discovery Changes", your changes are local to your web browser and unknown to the server.

If you navigate away from the discovery without saving your changes, the web console will automatically save your changes to the server (as if you had manually clicked "Save Discovery Changes"). This way your changes will not be lost if you forget to save them. However, if you close your web browser without manually saving or navigating away from the discovery, your changes will be lost.

Discovery Status



Discovery Status

State: Complete
Start Time: 5/29/2018, 4:16:42 PM
End Time: 5/29/2018, 4:31:01 PM

Devices

8 Routers
24 Switches
18 Printers
72 Workstations
572 Other Devices

The Status tab lets you see the most recent status for this discovery reported by the discovery's agent. If the agent is currently running the discovery, it will show the progress of the current discovery run. If the discovery is not currently running, it will show the progress reported by the agent the last time the discovery completed. If the discovery has never run before, the status will be empty.

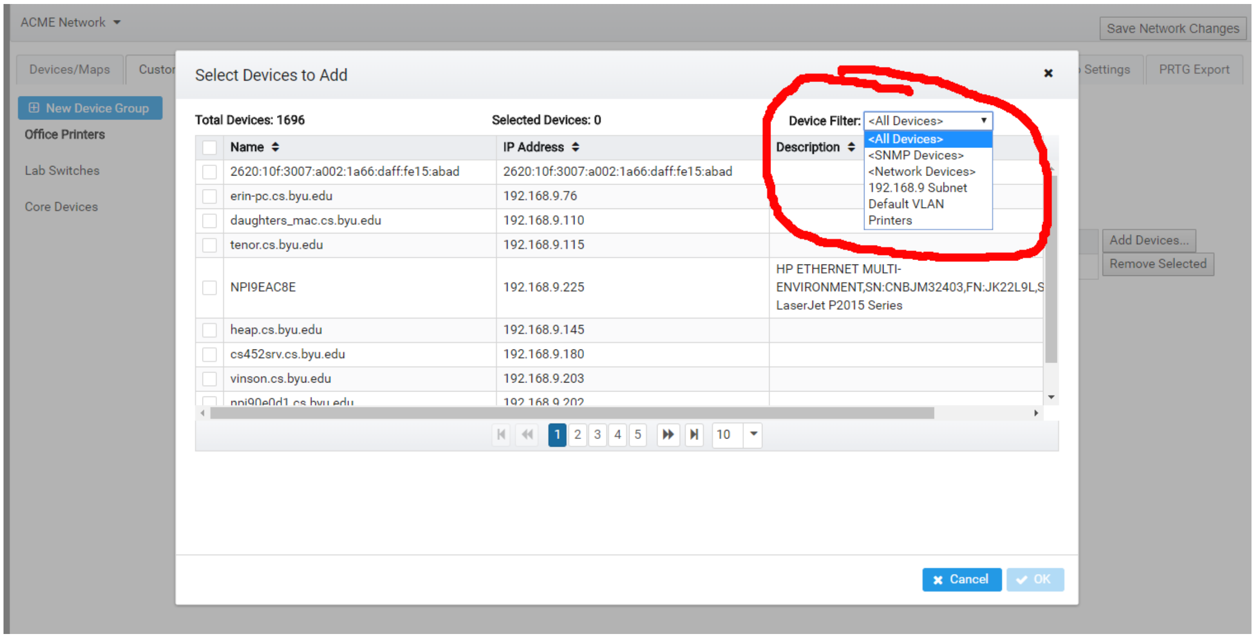
The discovery status is updated automatically according to the Discovery Status Update Interval you set in the agent's Agent Settings tab. This interval controls both how often the agent reports discovery status to UVexplorer Server, and how often the Status tab queries the server for the latest status.

Update Discovery Status - You can click the "Update Discovery Status" button to tell the Status tab to immediately query the server for the latest discovery status. This will ensure that you have the latest available information.

Run Discovery ASAP - Normally, discoveries run automatically according to the schedule you specify. However, sometimes it is convenient to run a discovery on demand (for example, when you are testing the discovery's configuration). Clicking the "Run Discovery ASAP" button will cause UVexplorer Server to run the discovery "as soon as possible". This tells UVexplorer Server that you would like to run the discovery ASAP. The next time the discovery's agent queries the server for configuration changes, it will notice that you have requested the discovery to run ASAP, and will start running the discovery right away. The length of time it will take for the agent to run the discovery depends on the Configuration Update Interval you specified in the agent's Agent Settings tab. This setting tells the agent software how often it should query UVexplorer Server for configuration changes. For example, if this setting has a value of 60 seconds, it will take up to 60 seconds for the agent to start running the discovery. Or, if this setting has a value of 3600 seconds (one hour), it will take up to one hour for the agent to start running the discovery. If you have access to the machine running the agent, you can also click the "Get Config" button in the top-right corner of the agent's main window, which will cause the agent to immediately query the server for configuration updates. This will cause the discovery to start running immediately.

Device Filters

In several places the UVexplorer Server web console displays lists of devices that you can select from. For large networks these lists can become very long, so it is often useful to "filter" a device list to show a smaller subset of devices. For example, rather than viewing "all devices", you might want to view only "printers" or only "SNMP devices" or only "core devices". Device filters let you pare down device lists to show only the devices you are interested in (see the picture below).



Select Devices to Add

Total Devices: 1696

Selected Devices: 0

Device Filter: <All Devices>

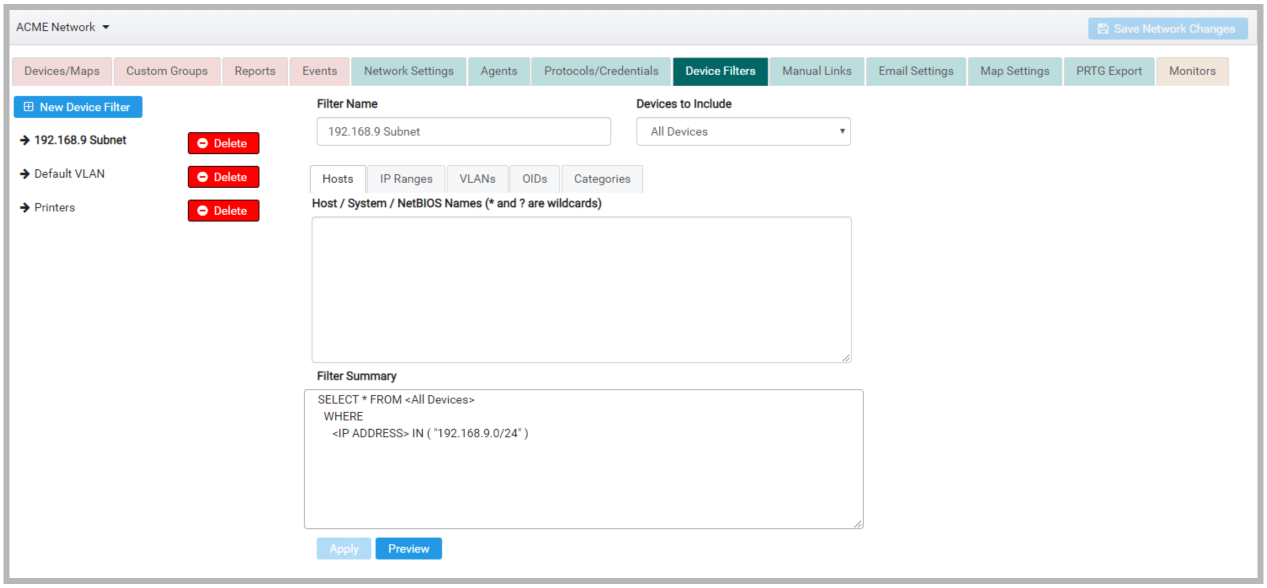
□	Name	IP Address	Description
□	2620:10f:3007:a002:1a66:daff:fe15:abad	2620:10f:3007:a002:1a66:daff:fe15:abad	
□	erin-pc.cs.byu.edu	192.168.9.76	
□	daughters_mac.cs.byu.edu	192.168.9.110	
□	tenor.cs.byu.edu	192.168.9.115	
□	NPI9EAC8E	192.168.9.225	HP ETHERNET MULTI-ENVIRONMENT,SN:CNBJM32403,FN:JK22L9L,S LaserJet P2015 Series
□	heap.cs.byu.edu	192.168.9.145	
□	cs452srv.cs.byu.edu	192.168.9.180	
□	vinson.cs.byu.edu	192.168.9.203	
□	npi90e0d1.cs.byu.edu	192.168.9.202	

UVexplorer Server has three built-in device filters that are always available:

- ➔ All Devices - Show all devices
- ➔ SNMP Devices - Only show devices that support the SNMP protocol.
- ➔ Network Devices - Only show devices that are part of the networking infrastructure (switches, routers, etc.)

In addition to these built-in filters, you can also define your own custom device filter that match the way you want to view your devices. For example, you could create a device filter named "Printers" that only shows printer devices, or a filter named "Default VLAN" that only shows devices on the network's default VLAN, or a filter named "192.168.9.0 Subnet" that only shows devices on the 192.168.9 subnet.

Each network object has its own set of custom device filters. To manage a network's custom device filters, navigate to the network View and select the Device Filters tab.



Filter Name: 192.168.9 Subnet

Devices to Include: All Devices

Host / System / NetBIOS Names (* and ? are wildcards)

Filter Summary

```
SELECT * FROM <All Devices>
  WHERE
    <IP ADDRESS> IN ( "192.168.9.0/24" )
```

In the Device Filters tab you can create, modify, and delete custom device filters. The custom filters you create will appear everywhere that UVexplorer Server allows device filtering.

Click the “New Device Filter” button to create a new device filter.

To delete a device filter, click the “Delete” button next to its name.

To edit a device filter, select the filter from the list on the left by clicking on its name. This will cause the filter’s properties to be displayed in the area on the right. Give your filter a meaningful name, and also define which devices should be included by the filter. This is done by modifying the following properties:

- ❑ Filter Name - your filter’s name
- ❑ Devices to Include - Select a base set of devices for your filter (All Devices, SNMP Devices, Network Devices). This is just a starting point. You can refine your filter further with the following properties.
- ❑ Hosts - The Hosts tab lets you filter devices based on their names (DNS host names, SNMP system names, and NetBIOS names). In the text field you can specify as many name strings as you like, with one name per line. You can also use * and ? wildcards in your name strings (* matches zero or more of any character, and ? matches exactly one of any character) . Example: switch*.acme.org
  Leave this blank if you do not want to filter devices by name.
- ❑ IP Ranges - The IP Ranges tab lets you filter devices based on their IP addresses. IP addresses can be specified in one of three ways:
  - ❑ IP Address: A single IP address; for example 192.168.1.1
  - ❑ IP Range: A range of IP addresses; two IP addresses separated by a hyphen; for example 192.168.5.20 - 192.168.5.50

    - ❏ IP Subnet: An IPv4 subnet; subnet IP followed by netmask length in bits separated by forward slash; for example 192.168.3.0/24

  Leave this blank if you do not want to filter devices by IP address.
- ❏ VLANs - The VLANs tab lets you filter devices based by VLAN. In the text field you can specify VLAN names or indexes, with one name or index per line. You can also use * and ? wildcards in your VLAN name strings (* matches zero or more of any character, and ? matches exactly one of any character) . Example: default
  Leave this blank if you do not want to filter devices by VLAN.
- ❏ OIDs - The OIDs tab lets you filter devices based by SNMP OID. In the text field you can specify any number of OIDs, with one OID per line. You can also use * and ? wildcards in your OIDs (* matches zero or more of any character, and ? matches exactly one of any character) . Example: 1.3.6.1.4.1.9.*
  Leave this blank if you do not want to filter devices by OID.
- ❏ Categories - The Categories tab lets you filter devices by type. Select the device types you want included in your filter.
  Leave this blank if you do not want to filter devices by type.

The “Filter Summary” field summarizes your device filter as a SQL-like query string.
The “Preview” button displays a list of devices that match your filter criteria.
The “Apply” button is used to save your changes to the filter.

Viewing Discovery Data

This section explains how you can view the device information and network maps discovered and created by UVexplorer Server.

You can view discovery results, including device details and maps, by navigating to any of the following objects:

- ❏ Discovery Run - View the raw results of a particular discovery run.
- ❏ Discovery - View a rollup (or merge) of the most recent several runs of this discovery. (You can specify how many runs should be remembered and merged using the Keep setting in the discovery’s Discovery Settings tab.)
- ❏ Agent - View a rollup (or merge) of the most recent discovery results produced by all of the agent’s discoveries. This provides a single comprehensive view of all the data and maps for the entire agent.
- ❏ Network - Displays a rollup (or merge) of the most recent discovery results for all of the network’s agents. This provides a single comprehensive view of all the data and maps for the entire network.

All of these views (network, agent, discovery, discovery run) have the following tabs for viewing your device data and maps:

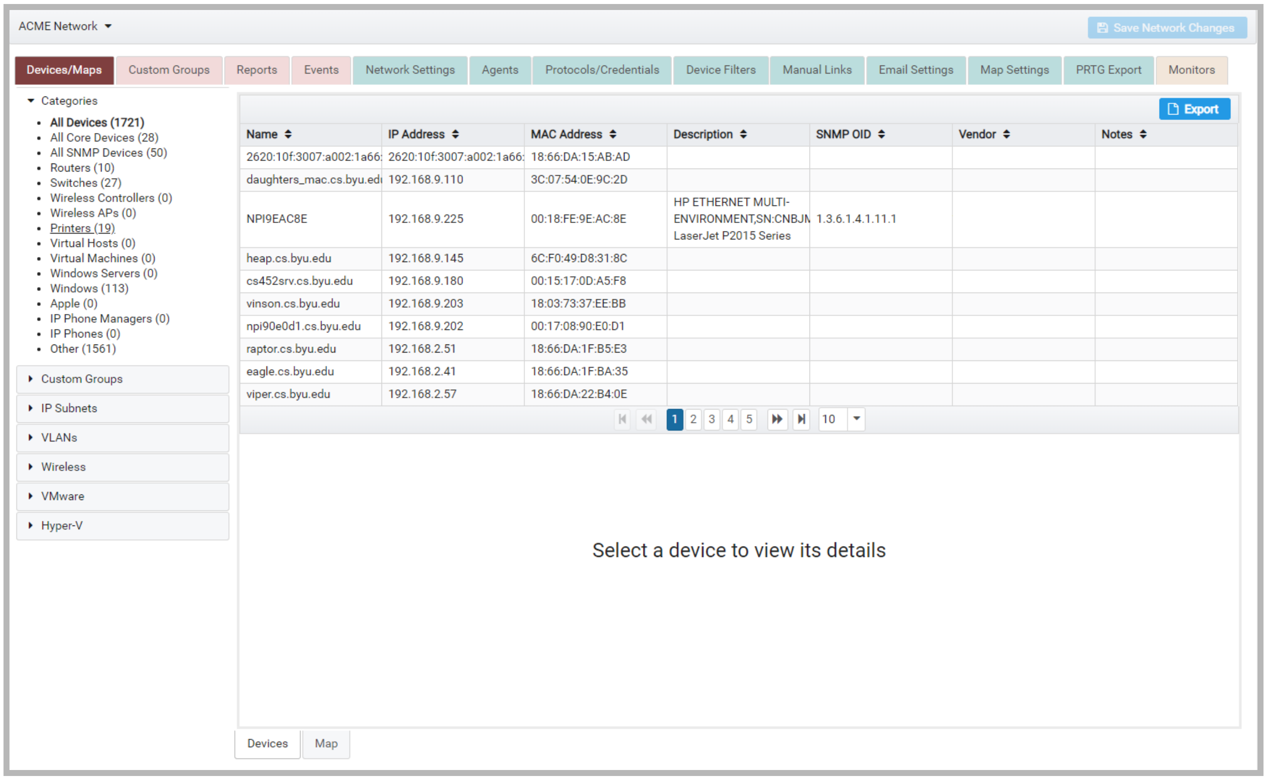
- ❏ Devices/Maps - In this tab you can view device details and network maps.
- ❏ Reports - This tab provides several aggregate reports of your data.

- ❑ Events - This tab displays a log of events that were produced during the discovery process.

These tabs are described in detail in the following subsections.

Devices / Maps Tab

The Devices / Maps tab lets you view device details and network maps. This tab organizes devices into “device groups”. A device group is a collection of devices that have something in common. For example, the “All SNMP Devices” group contains all devices that have valid SNMP credentials; the “Switches” group contains all devices that are network switches; the “Printers” group contains all devices that are printers; etc. On the left side there is an “accordion” control that lists the names of all available “device groups”. To view the devices in a device group, select the group by clicking on its name in the accordion control. Selecting a group causes the data and maps for that group to be loaded (see picture below).



Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
2620:10f:3007:a002:1a66:	2620:10f:3007:a002:1a66:	18:66:DA:15:AB:AD				
daughters_mac.cs.byu.edu	192.168.9.110	3C:07:54:0E:9C:2D				
NPI9EAC8E	192.168.9.225	00:18:FE:9E:AC:8E	HP ETHERNET MULTI-ENVIRONMENT,SN:CNBJN LaserJet P2015 Series	1.3.6.1.4.1.11.1		
heap.cs.byu.edu	192.168.9.145	6C:F0:49:D8:31:8C				
cs452srv.cs.byu.edu	192.168.9.180	00:15:17:0D:A5:F8				
vinson.cs.byu.edu	192.168.9.203	18:03:73:37:EE:BB				
npi90e0d1.cs.byu.edu	192.168.9.202	00:17:08:90:E0:D1				
raptor.cs.byu.edu	192.168.2.51	18:66:DA:1F:B5:E3				
eagle.cs.byu.edu	192.168.2.41	18:66:DA:1F:BA:35				
viper.cs.byu.edu	192.168.2.57	18:66:DA:22:B4:0E				

Select a device to view its details

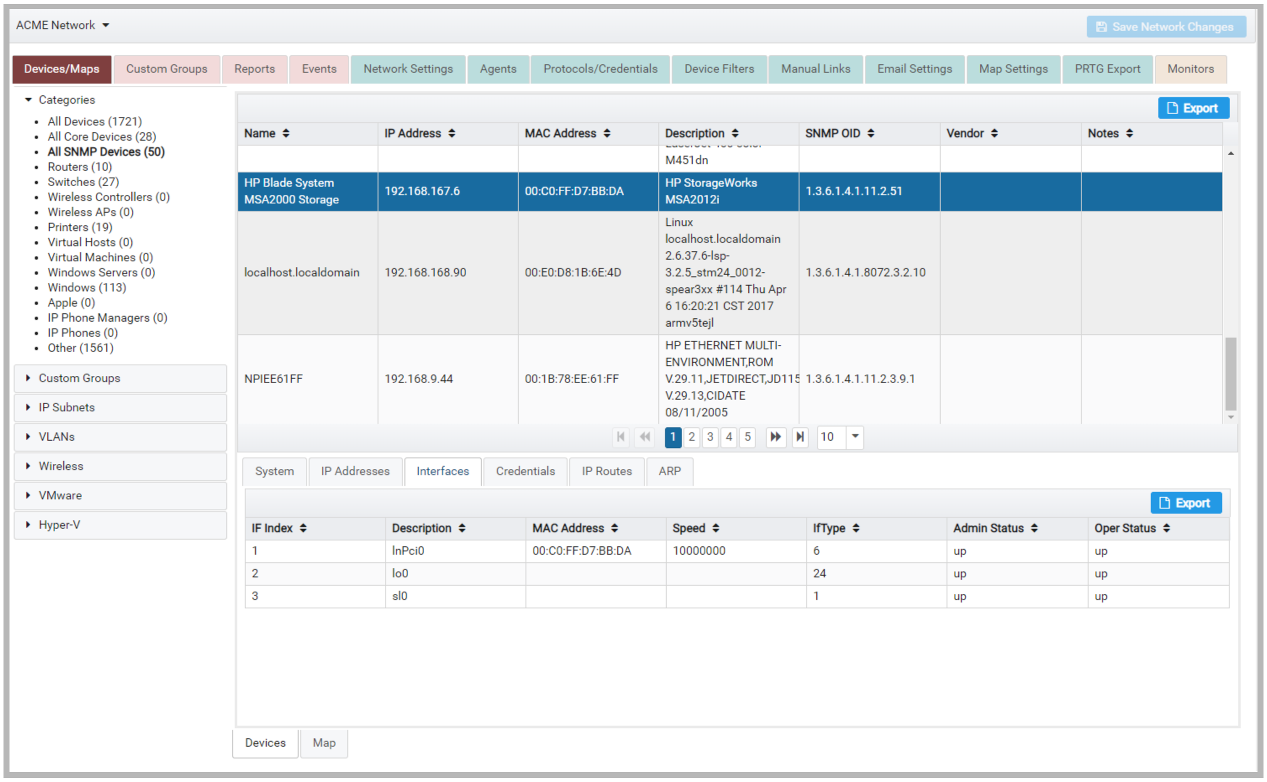
In the accordion control, devices groups are organized into the following collections:

- ❑ Categories - These are groups that organize devices by device type (or category); examples of these groups are router, switch, printer, wireless AP, server, workstation, Windows, Apple, etc.
- ❑ Custom Groups - These are custom device groups created by the user (see the section named “Custom Groups” for details)

- ❏ IP Subnets - These are groups that organize devices by their IP subnets
- ❏ VLANS - These are groups that organize devices by their VLANs
- ❏ Wireless - These are groups containing different kinds of wireless devices (controller, access point, etc.)
- ❏ VMware - These are groups containing different kinds of VMware virtual devices
- ❏ Hyper-V - These are groups containing different kinds of Hyper-V virtual devices

At the bottom of the Devices / Maps tab, you can select between two different views of the devices in the current group. Selecting “Devices” at the bottom displays a list view of the devices. Alternatively, selecting “Map” at the bottom displays a map view of the devices.

Device List View



Categories

- All Devices (1721)
- All Core Devices (28)
- **All SNMP Devices (50)**
- Routers (10)
- Switches (27)
- Wireless Controllers (0)
- Wireless APs (0)
- Printers (19)
- Virtual Hosts (0)
- Virtual Machines (0)
- Windows Servers (0)
- Windows (113)
- Apple (0)
- IP Phone Managers (0)
- IP Phones (0)
- Other (1561)

Custom Groups

IP Subnets

VLANs

Wireless

VMware

Hyper-V

Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
			M451dn			
HP Blade System MSA2000 Storage	192.168.167.6	00:C0:FF:D7:BB:DA	HP StorageWorks MSA2012i	1.3.6.1.4.1.11.2.51		
localhost.localdomain	192.168.168.90	00:E0:D8:1B:6E:4D	Linux localhost.localdomain 2.6.37.6-lsp-3.2.5_stm24_0012-spear3xx #114 Thu Apr 6 16:20:21 CST 2017 armv5tejl	1.3.6.1.4.1.8072.3.2.10		
NPIEE61FF	192.168.9.44	00:1B:78:EE:61:FF	HP ETHERNET MULTI-ENVIRONMENT,ROM V.29.11,JETDIRECT,JD115 V.29.13,CIDATE 08/11/2005	1.3.6.1.4.1.11.2.3.9.1		

IF Index	Description	MAC Address	Speed	IfType	Admin Status	Oper Status
1	lnPci0	00:C0:FF:D7:BB:DA	10000000	6	up	up
2	lo0			24	up	up
3	sl0			1	up	up

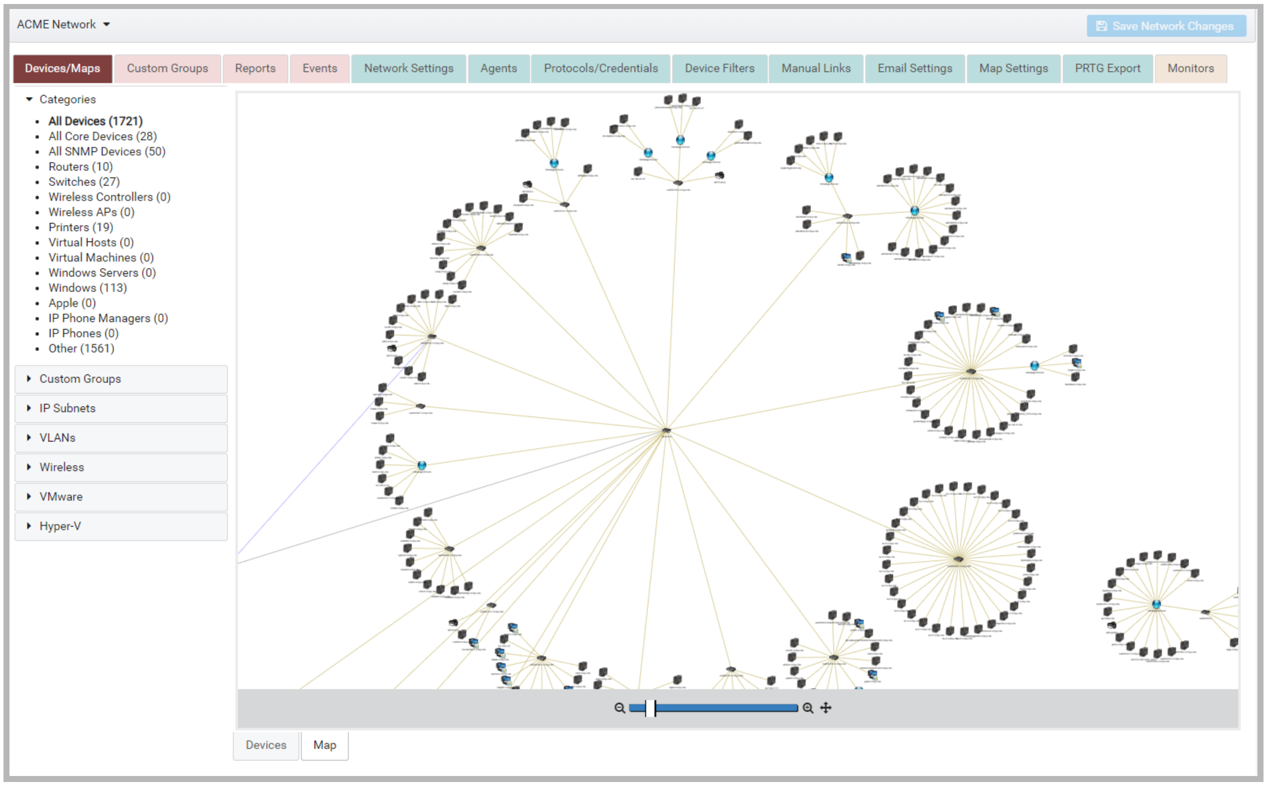
When the “Devices” view is selected, the area on the right displays a list of the devices in the current group. You can scroll through the list to see all of the devices in the group. To see detailed inventory data for a device, select the device in the list by clicking on it. Device details are displayed in the area under the device list. The device details are displayed in a tab control. Each tab contains a specific kind of data about the device. For example, the System tab displays basic device information, such as IP address, MAC address, hostname, vendor, and model; the Interfaces tab displays information about all of the device’s network interfaces; the IP Routes tab displays the IP route table for the device; etc. There are many different tabs, and you should look through them to see what kinds of information are available.

Exporting Device Data to CSV Files

The contents of the device list can be exported to a CSV file by clicking the “Export” button in the top-right corner above the device list.

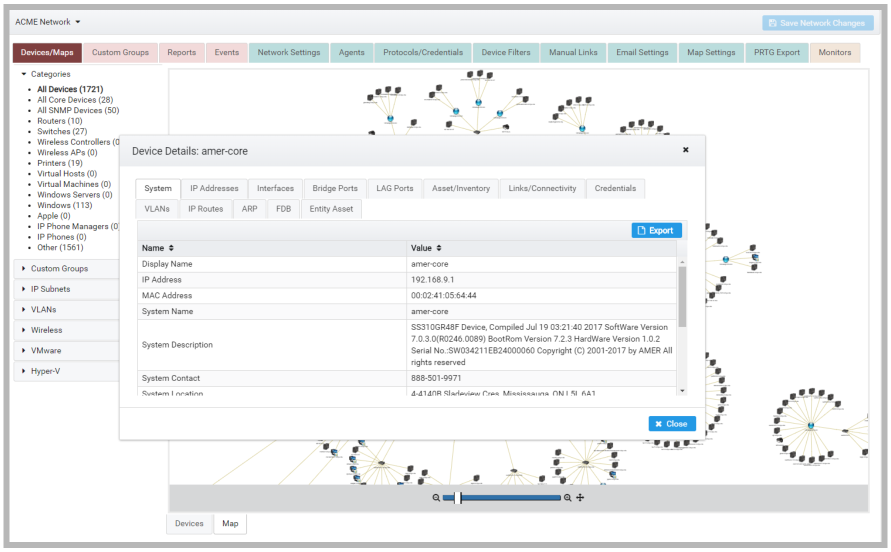
The contents of the device details area can be exported to a CSV file by clicking the “Export” button in the top-right corner of the device details area.

Map View



The Map view displays a map of the current group’s devices and the connections between them. Maps have the following features:

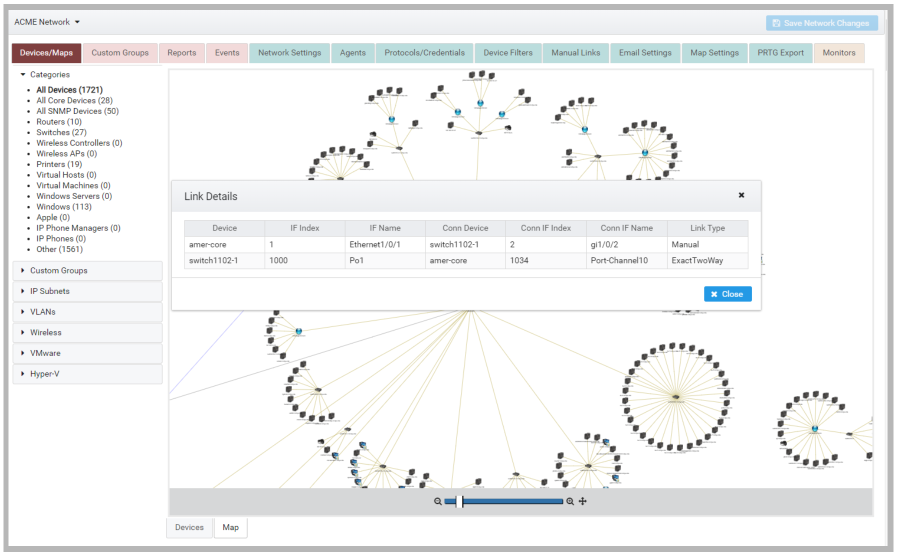
- ❑ Panning - Pan (or scroll) the map by clicking and dragging the mouse.
- ❑ Zooming - Zoom the map in and out by doing the following:
    - ❑ Use the zooming slider below the map
    - ❑ Use the mouse scroll wheel while pressing the CTRL key
    - ❑ Click the “zoom to fit” button to the right of the zooming slider below the map
- ❑ Device Details - View device details by double-clicking the device’s icon
    - ❑ Device details can be exported to a CSV file by clicking the “Export” button



Device Details: amer-core

Name	Value
Display Name	amer-core
IP Address	192.168.9.1
MAC Address	00:02:41:05:64:44
System Name	amer-core
System Description	SS310GR48F Device, Compiled Jul 19 03:21:40 2017 SoftWare Version 7.0.3.0(R0246.0089) BootRom Version 7.2.3 HardWare Version 1.0.2 Serial No.:SW034211EB24000060 Copyright (C) 2001-2017 by AMER All rights reserved
System Contact	888-501-9971
System Location	4-4140B Sladeview Cres, Mississauga, ON L5L 6A1

- ❑ Link Details - View link details by doing the following:
  - ❑ Double-click a link to view its details
  - ❑ Hover the mouse over a link to pop-up the names of the ports connected to each end of the link



Link Details

Device	IF Index	IF Name	Conn Device	Conn IF Index	Conn IF Name	Link Type
amer-core	1	Ethernet1/0/1	switch1102-1	2	gi1/0/2	Manual
switch1102-1	1000	Po1	amer-core	1034	Port-Channel10	ExactTwoWay

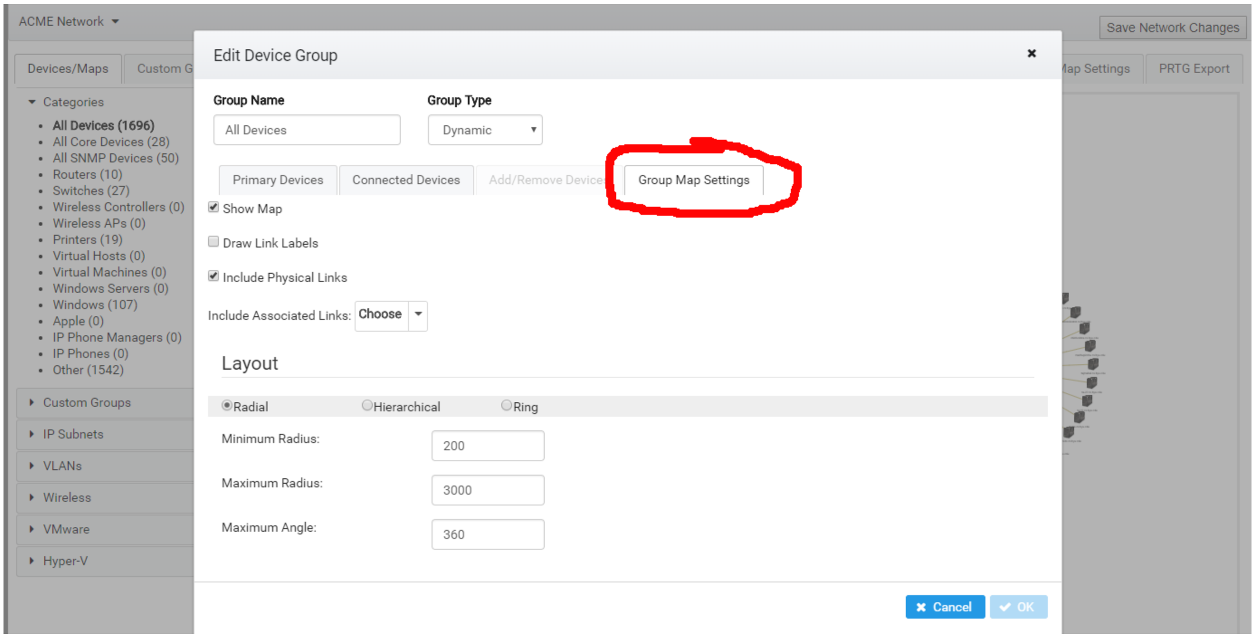
Editing Map Settings

UVexplorer Server automatically arranges the layout of devices on network maps in either a Radial or Hierarchical fashion. For each device group, you can specify whether you want the group's map to be laid out using the Radial or Hierarchical approach. You can also specify a number of other settings that affect the layout or visual appearance of the map. You can even specify that a device group should have no map at all, which hides the "Map" view for the group altogether.

To edit a device group's map settings, you must open the device group editor dialog. This can be done in any of the following ways:

- ➔ Double-click inside the group's map
- ➔ Right-click on the group's map, and select "Edit Device Group…" from the context menu
- ➔ Double-click on the group's name in the device group accordion control
- ➔ Right-click on the group's name in the device group accordion control, and select "Edit Device Group…" from the context menu

After opening the device group editor dialog, select the Group Map Settings tab, as shown below.



Edit Device Group

Group Name: All Devices

Group Type: Dynamic

☑ Show Map

□ Draw Link Labels

☑ Include Physical Links

Include Associated Links: Choose

Layout

● Radial ○ Hierarchical ○ Ring

Minimum Radius: 200

Maximum Radius: 3000

Maximum Angle: 360

In the Group Map Settings tab, you will find the following settings:

- ❑ Show Map - controls whether or not the map for this device group is visible

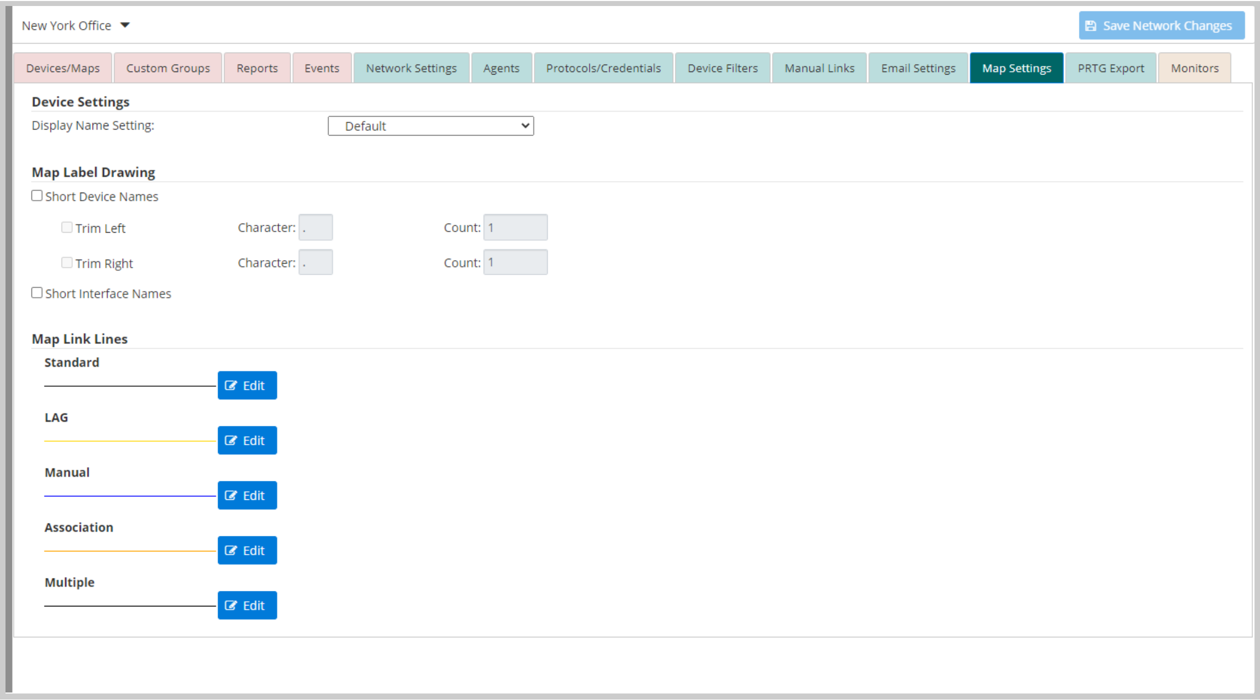
- ❑ Draw Link Labels - controls whether or not link details (port names, etc.) are drawn on the group's map; these details can always be seen by hovering the mouse over the link, independent of this setting
- ❑ Include Physical Links - controls whether or not physical links are drawn on the map; this is useful when you prefer that a map display only "associated" links and not physical links (associated links are explained next)
- ❑ Include Associated Links - controls which types of associated links are drawn on the group's map. Most links on network maps represent physical connections between devices on your network. However, UVexplorer Server can also draw "associated" links between devices that are associated with (or related to) each other, independent of physical connectivity. Specifically, UVexplorer Server knows how to draw the following types of "associated" links:
  - ❑ Virtual Associations - Links between virtual machines and the physical machines that hosts them
  - ❑ Wireless Associations - Links between wireless access points and the wireless controllers that control them
  - ❑ IP Phone Associations - Links between IP phones and the IP phone managers that manage them
- ❑ Radial Layout Settings - if you select "Radial" layout for the group's map, the map will be laid out in a circular fashion. 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. The following settings control the radial layout algorithm.
  - ❑ Minimum Radius - 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 - the maximum length in pixels between a node and its children. When the nodes are laid out, they have to stay within an angle. If the nodes won't fit within the angle at the radius distance, then the distance is expanded until 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 in an attempt 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 Settings - if you select "Hierarchical" layout for the group's map, the map will be laid out in a hierarchical fashion. 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. The following settings control the hierarchical layout algorithm.

- Level Spacing - 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.

Editing Map Drawing Settings

In addition to the map settings described in the previous section, you can also control the way that labels and links are drawn on a group's map. 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. These map drawing settings are managed at the network level instead of the device group level, so that all maps within a network share the same map drawing settings. To edit the map drawing settings for a network, navigate to the network and select the Map Settings tab (see picture below).



Device Settings

Display Name Setting: Default

Map Label Drawing

☐ Short Device Names

☐ Trim Left Character: . Count: 1

☐ Trim Right Character: . Count: 1

☐ Short Interface Names

Map Link Lines

Standard Edit

LAG Edit

Manual Edit

Association Edit

Multiple Edit

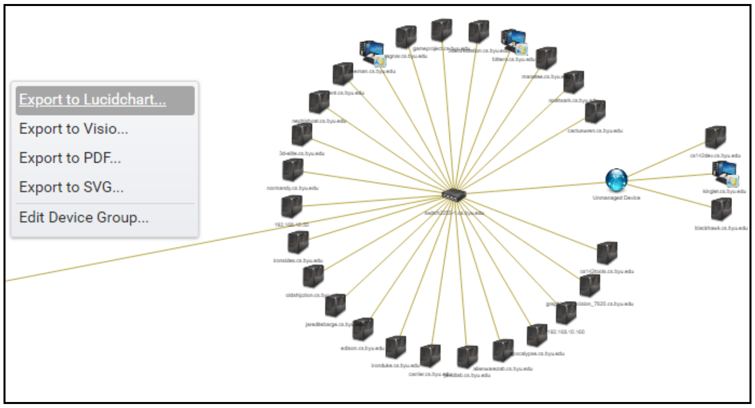
The following map drawing settings are available:

- Device Settings

    - ❏ Display Name Setting - This setting controls how device names are displayed throughout the application. “Default” means to use the default algorithm for displaying device names. “Host Name” means to use hostnames when displaying device names. “IP Address” means to use IP addresses when displaying device names.
- ❏ Map Label Drawing
    - ❏ 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 - Maps support displaying five link types. By default all link types will be drawn with a simple black line. The map drawing settings allow you to draw links of different types with different colors or patterns. To edit the link line color or pattern for a particular link type, click the “Edit” button next to the link type. The following link types are supported:
    - ❏ Standard - Standard link lines represent a physical 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.

Exporting Maps to Lucidchart

Network maps can be exported to Lucidchart. Lucidchart is a cloud-based diagramming tool that lets you create diagrams of any kind, similar to Microsoft Visio. To export a map to Lucidchart, open the map, right-click on the map, and select “Export to Lucidchart…” from the context menu. A dialog will appear containing export configuration settings. Once the settings are configured, click the “Export” button to initiate the export. When the export is complete, a dialog will appear giving you the option of opening the exported Lucidchart document. You can then view and edit your map in Lucidchart.

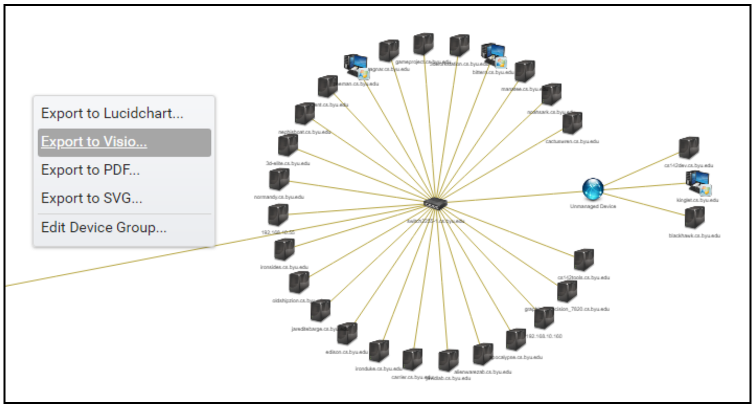


The following settings are available when exporting a map to Lucidchart.

- ❏ Include Device Labels and Include Link Labels - these options determine whether to include the device and link labels in the exported map. Occasionally the device and link labels make the map look cluttered; this setting allows you to export the map without them.
- ❏ Sheets Across and Sheets Down - the number of pages wide and high the exported document should be
- ❏ Include Device Properties and Include Link Properties - UVexplorer Server can attach detailed device and link information to the device and link shapes in the Lucidchart document.

Exporting Maps to Visio/PDF/SVG Files

Network maps can be exported to Visio, PDF and SVG files. To export a map, open the map, right-click on the map, and select either “Export to Visio…” or “Export to PDF…” or “Export to SVG…” from the context menu. A dialog will appear containing export configuration settings. Once the settings are configured, click the “Export” button to initiate the export. The exported file will be generated by the UVexplorer Server server and returned to your web browser. Your browser will then let you save or open the exported file (the exact behavior will depend on what browser and operating system you are using).

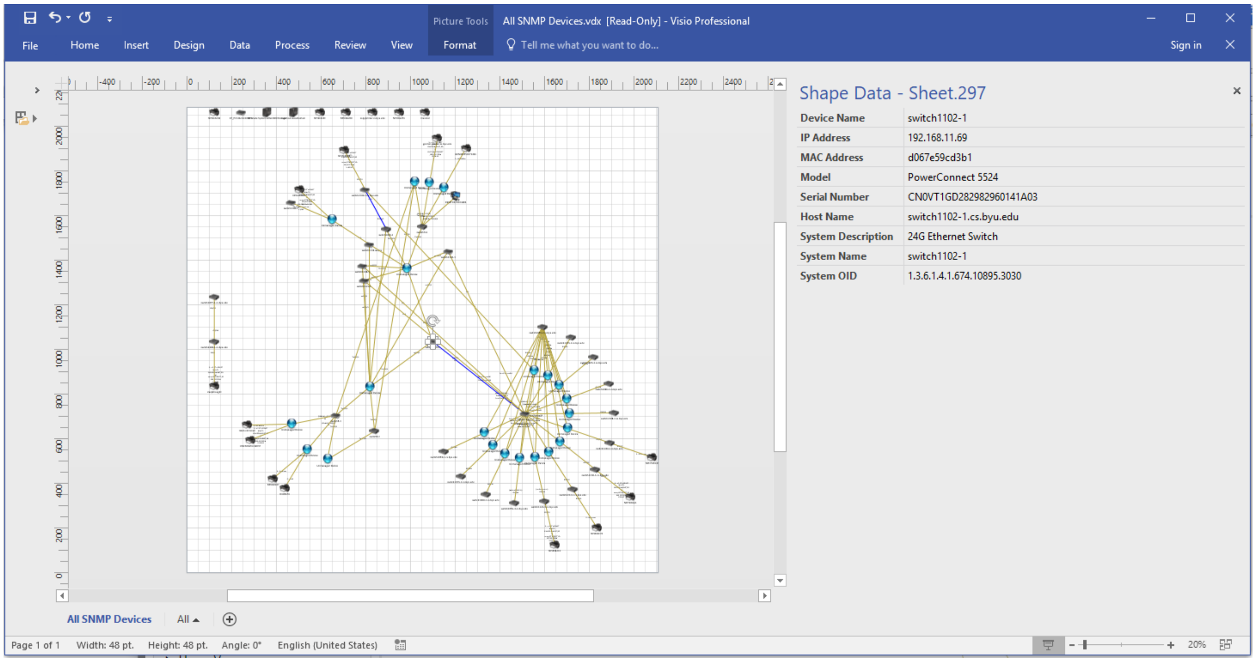


The following settings are available for all types of exports.

- ❏ Include Device Labels and Include Link Labels - these options determine whether to include the device and link labels in the exported map. Occasionally the device and link labels make the map look cluttered; this setting allows you to export the map without them.

The following settings are available only for Visio exports.

- ❏ Sheets Across and Sheets Down - the number of pages wide and high the exported document should be
- ❏ Include Device Properties and Include Link Properties - UVexplorer Server can attach detailed device and link information to the device and link shapes in the Visio document. When viewing the map in Visio, the detailed device and link information can be viewed by opening the Shape Data Window. To open the Shape Data Window, go to the Data menu and check the Shape Data Window checkbox. (See the picture below.)



Shape Data - Sheet.297

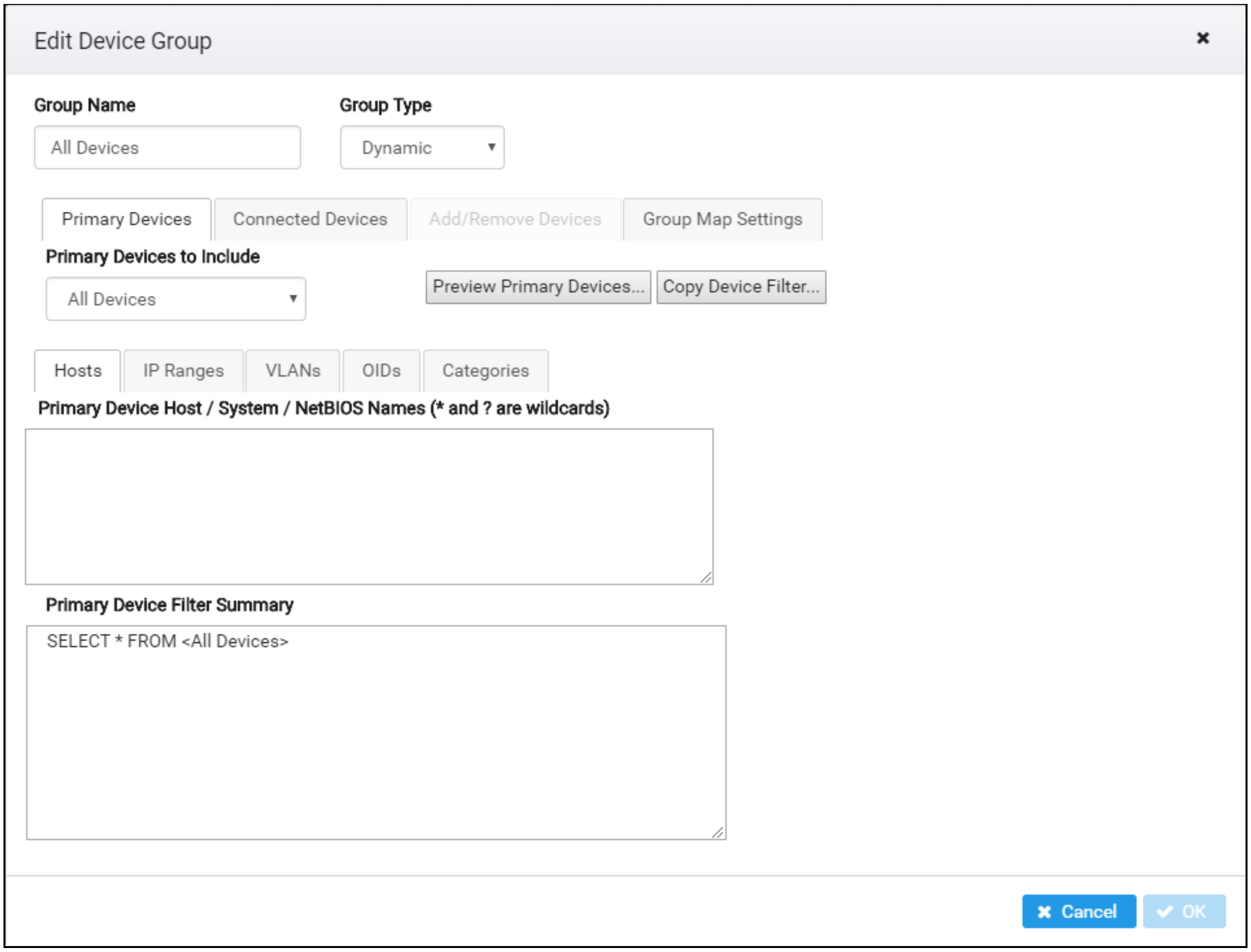
Device Name	switch1102-1
IP Address	192.168.11.69
MAC Address	d067e59cd3b1
Model	PowerConnect 5524
Serial Number	CN0VT1GD282982960141A03
Host Name	switch1102-1.cs.byu.edu
System Description	24G Ethernet Switch
System Name	switch1102-1
System OID	1.3.6.1.4.1.674.10895.3030

Editing Device Groups

A device group is a collection of devices that have common properties. Therefore, a device group is defined by the properties devices must have to be in the group. For example, a group named “Office Printers” might be defined as any device that is a “printer” and has an IP address in the 192.168.9.0/24 subnet. Another example would be a group named “Cisco Switches” that is defined as any device with a hostname of the form “switch-*.acme.com” and an SNMP OID of the form “1.3.6.1.4.1.9.*”.

You can edit the properties of a device group in order to change the devices that are in it. To edit a device group's properties, you must open the device group editor dialog. This can be done in any of the following ways:

- ➔ Double-click on the group's name in the device group accordion control
- ➔ Right-click on the group's name in the device group accordion control, and select "Edit Device Group…" from the context menu
- ➔ Double-click inside the group's map
- ➔ Right-click on the group's map, and select "Edit Device Group…" from the context menu



Edit Device Group

Group Name: All Devices

Group Type: Dynamic

Primary Devices to Include: All Devices

Primary Device Host / System / NetBIOS Names (* and ? are wildcards)

Primary Device Filter Summary

```
SELECT * FROM <All Devices>
```

There are two kinds of device groups: Static and Dynamic.

- ➔ For Static groups, you manually select the devices that you want to be in the group.

- ➔ For Dynamic device groups, UVexplorer Server will dynamically and automatically determine which devices are in the group based on criteria you specify. These criteria can filter devices based on device type, hostname, IP address, VLAN, and SNMP OID. A Dynamic group can be defined in terms of two sets of devices: Primary devices and Connected devices. Primary devices are the base devices you want in the group.

Connected devices are additional devices that are physically connected to the Primary devices that you also want in the group. For example, suppose you want to create a device group that contains several network switches, and all servers connected to those switches. In this case, the Primary devices would be the network switches, and the Connected devices would be the servers connected to them. Many device groups can be defined using only Primary devices; in this case you don't need to specify Connected devices. Specifying Primary devices is required, but specifying Connected devices is optional, and only done when necessary.

Device group properties include the following:

- Group Name - the group's name
- Group Type - the group's type: Dynamic or Static
- Primary Devices (dynamic groups only) - the criteria that define the group's primary devices
- Connected Devices (dynamic groups only) - the criteria that define the group's connected devices
- Add/Remove Devices (static groups only) - manually select the devices in the group
- Group Map Settings - settings that control the group's map contents and layout (described previously in the section named "Editing Map Settings")

The filtering criteria for the Primary and Connected devices are defined using the following properties:

- Devices to Include - Select a base set of devices for your group (No Devices, All Devices, SNMP Devices, Network Devices). This is just a starting point. You can refine your filter further with the following properties.
- Hosts - The Hosts tab lets you filter devices based on their names (DNS host names, SNMP system names, and NetBIOS names). In the text field you can specify as many name strings as you like, with one name per line. You can also use * and ? wildcards in your name strings (* matches zero or more of any character, and ? matches exactly one of any character) . Example: switch*.acme.org
  Leave this blank if you do not want to filter devices by name.
- IP Ranges - The IP Ranges tab lets you filter devices based on their IP addresses. IP addresses can be specified in one of three ways:
    - IP Address: A single IP address; for example 192.168.1.1
    - IP Range: A range of IP addresses; two IP addresses separated by a hyphen; for example 192.168.5.20 - 192.168.5.50
    - IP Subnet: An IPv4 subnet; subnet IP followed by netmask length in bits separated by forward slash; for example 192.168.3.0/24

  Leave this blank if you do not want to filter devices by IP address.
- VLANs - The VLANs tab lets you filter devices based by VLAN. In the text field you can specify VLAN names or indexes, with one name or index per line. You can also use *

and ? wildcards in your VLAN name strings (* matches zero or more of any character, and ? matches exactly one of any character) . Example: default
Leave this blank if you do not want to filter devices by VLAN.

❏ <u>OIDs</u> - The OIDs tab lets you filter devices based by SNMP OID. In the text field you can specify any number of OIDs, with one OID per line. You can also use * and ? wildcards in your OIDs (* matches zero or more of any character, and ? matches exactly one of any character) . Example: 1.3.6.1.4.1.9.*
Leave this blank if you do not want to filter devices by OID.

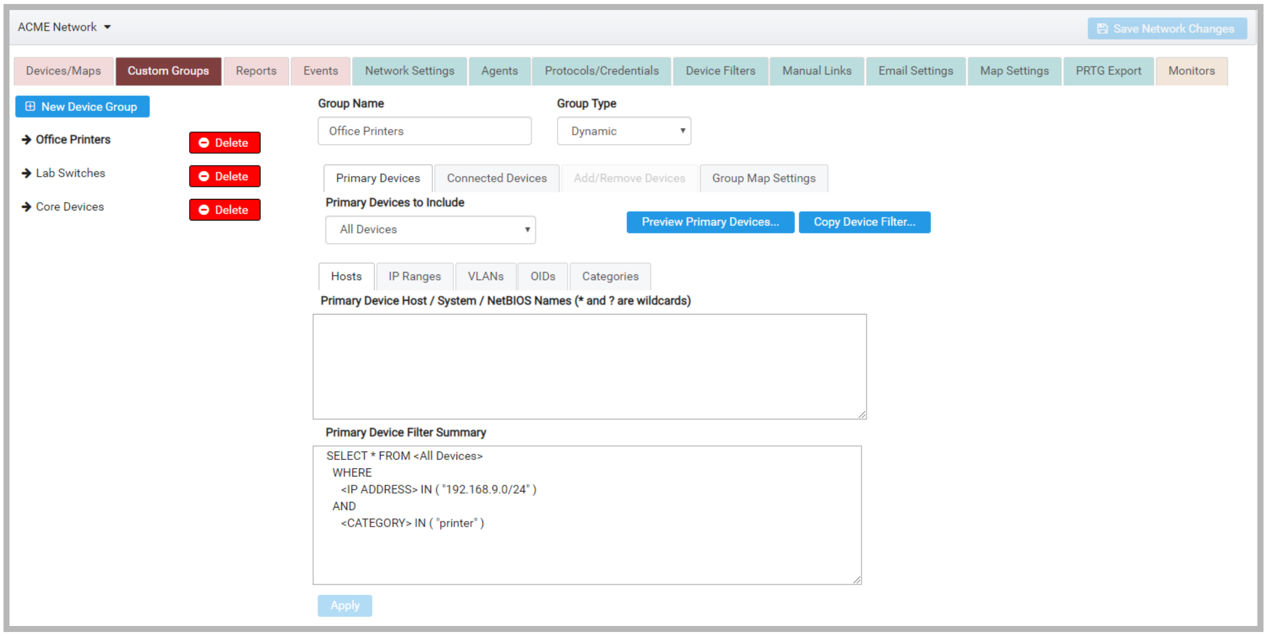
❏ <u>Categories</u> - The Categories tab lets you filter devices by type. Select the device types you want included in your filter.
Leave this blank if you do not want to filter devices by type.

The “Filter Summary” field summarizes your device selection criteria as a SQL-like query string.
The “Preview Devices...” button displays a list of devices that match your criteria.
The “Copy Device Filter…” button lets you copy filtering criteria from an existing device filter definition.

After making changes to the group definition, you can click the “Apply” button to save your changes.

Custom Device Groups

UVexplorer Server pre-defines a wide variety of device groups that are commonly useful. However, you will probably want to create custom device groups that precisely match the way you want to view and manage your network. Each network object contains its own set of custom device groups. You can manage a network’s custom device groups by navigating to the network and selecting the Custom Groups tab (see picture below).



Group Name: Office Printers

Group Type: Dynamic

Primary Devices to Include: All Devices

Primary Device Host / System / NetBIOS Names (* and ? are wildcards)

Primary Device Filter Summary

```
SELECT * FROM <All Devices>
  WHERE
    <IP ADDRESS> IN ( "192.168.9.0/24" )
  AND
    <CATEGORY> IN ( "printer" )
```

In the Custom Groups tab you can create, modify, and delete custom device groups. The custom groups you create will appear in the “Custom Groups” section of the device group accordion control (on the left side of the Devices/Maps tab).

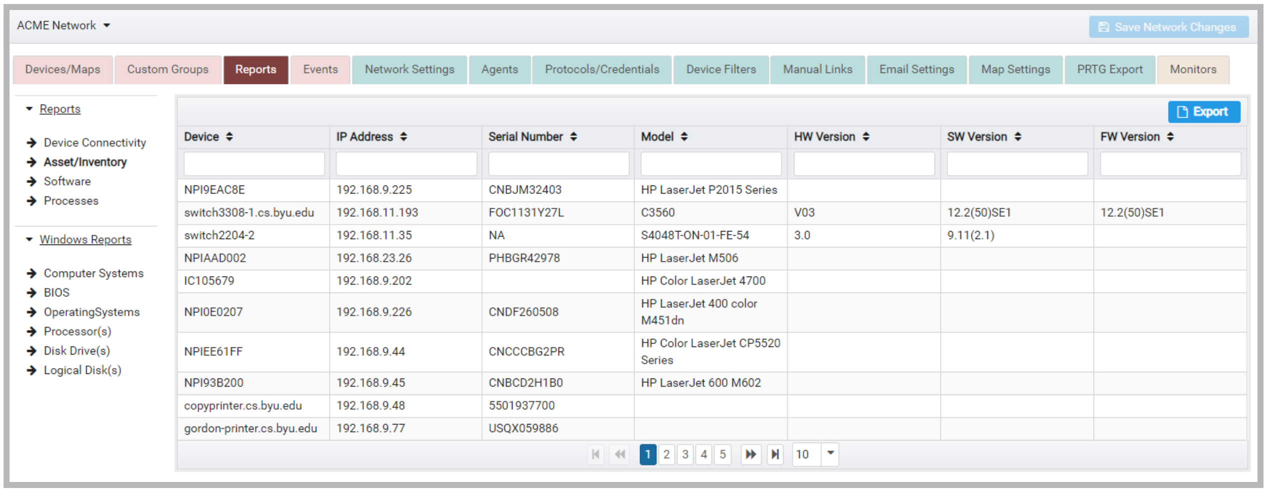
Click the “New Device Group” button to create a new device group.

To delete a device group, click the “Delete” button next to its name.

To edit a device group, select the group from the list on the left by clicking on its name. This will cause the group’s properties to be displayed in the area on the right. Give your group a meaningful name, and also define which devices should be included in the group. This is done as described in the previous section, “Editing Device Groups”.

Reports Tab

While the Devices/Maps tab lets you view detailed information for individual devices, the Reports tab let you view information for all devices in the data set combined together in a set of useful reports.



Device	IP Address	Serial Number	Model	HW Version	SW Version	FW Version
NPI9EAC8E	192.168.9.225	CNBJM32403	HP LaserJet P2015 Series			
switch3308-1.cs.byu.edu	192.168.11.193	FOC1131Y27L	C3560	V03	12.2(50)SE1	12.2(50)SE1
switch2204-2	192.168.11.35	NA	S4048T-ON-01-FE-54	3.0	9.11(2.1)	
NPIAAD002	192.168.23.26	PHBGR42978	HP LaserJet M506			
IC105679	192.168.9.202		HP Color LaserJet 4700			
NPI0E0207	192.168.9.226	CNDF260508	HP LaserJet 400 color M451dn			
NPIEE61FF	192.168.9.44	CNCCCBG2PR	HP Color LaserJet CP5520 Series			
NPI93B200	192.168.9.45	CNBCD2H1B0	HP LaserJet 600 M602			
copyprinter.cs.byu.edu	192.168.9.48	5501937700				
gordon-printer.cs.byu.edu	192.168.9.77	USQX059886				

In order for these reports to contain meaningful data, you must provide valid SNMP and/or Windows credentials for your devices to be used during discovery. Without such credentials, UVexplorer Server will be unable to collect the data in the reports.

The following reports are available.

- General Reports
  - Asset / Inventory - SNMP asset / inventory information, including device name, IP address, serial number, model, hardware version, software version, and firmware version.
  - Device Connectivity - detailed information about the physical links between devices in the network
  - Installed Software - software packages installed on each device
  - Processes - the processes (or programs) running on each device at the time discovery occurred
- Windows Reports - the following reports are available for Windows devices
  - Computer Systems - detailed description of each Windows device, including device name, IP address, description, model, manufacturer, and total memory
  - BIOS - detailed BIOS information for each Windows device
  - Operating Systems - detailed operating system information for each Windows device
  - Processor(s) - detailed description of each Windows device’s CPU(s)
  - Disk Drive(s) - detailed description of each Windows device’s physical disk drive(s)
  - Logical Drive(s) - detailed description of each Windows device’s logical disk drive(s)

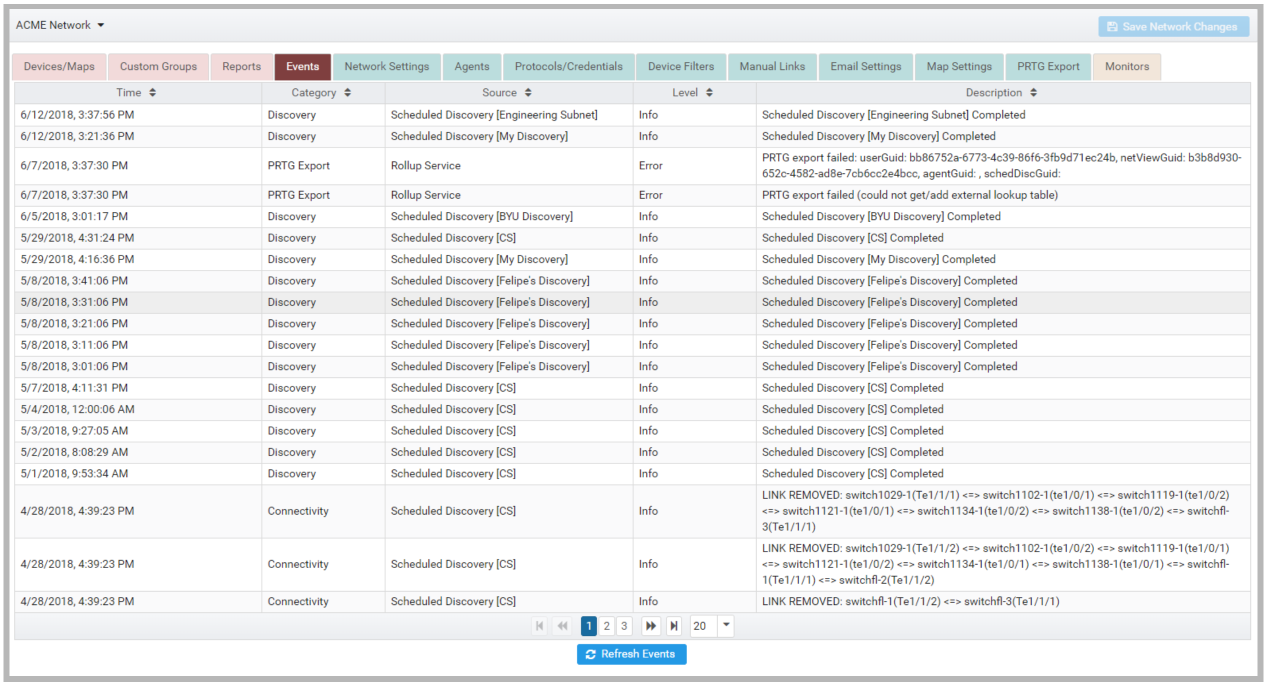
The content of each report can be filtered by entering search values in the filter fields at the top of each column. Only rows that contain the filter values you specify will appear in the report.

Exporting Reports to CSV Files

You can also export the contents of a report to a CSV file by clicking the “Export” button. When this button is clicked, the CSV file will be generated by UVexplorer Server and returned to your web browser. Your browser will then let you view or save the CSV file.

Events Tab

The Events tab lets you view interesting events that occurred during network discovery, and also error conditions you need to be aware of.



Time	Category	Source	Level	Description
6/12/2018, 3:37:56 PM	Discovery	Scheduled Discovery [Engineering Subnet]	Info	Scheduled Discovery [Engineering Subnet] Completed
6/12/2018, 3:21:36 PM	Discovery	Scheduled Discovery [My Discovery]	Info	Scheduled Discovery [My Discovery] Completed
6/7/2018, 3:37:30 PM	PRTG Export	Rollup Service	Error	PRTG export failed: userGuid: bb86752a-6773-4c39-86f6-3fb9d71ec24b, netViewGuid: b3b8d930-652c-4582-ad8e-7cb6cc2e4bcc, agentGuid: , schedDiscGuid:
6/7/2018, 3:37:30 PM	PRTG Export	Rollup Service	Error	PRTG export failed (could not get/add external lookup table)
6/5/2018, 3:01:17 PM	Discovery	Scheduled Discovery [BYU Discovery]	Info	Scheduled Discovery [BYU Discovery] Completed
5/29/2018, 4:31:24 PM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/29/2018, 4:16:36 PM	Discovery	Scheduled Discovery [My Discovery]	Info	Scheduled Discovery [My Discovery] Completed
5/8/2018, 3:41:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:31:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:21:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:11:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/8/2018, 3:01:06 PM	Discovery	Scheduled Discovery [Felipe's Discovery]	Info	Scheduled Discovery [Felipe's Discovery] Completed
5/7/2018, 4:11:31 PM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/4/2018, 12:00:06 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/3/2018, 9:27:05 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/2/2018, 8:08:29 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
5/1/2018, 9:53:34 AM	Discovery	Scheduled Discovery [CS]	Info	Scheduled Discovery [CS] Completed
4/28/2018, 4:39:23 PM	Connectivity	Scheduled Discovery [CS]	Info	LINK REMOVED: switch1029-1(Te1/1/1) <=> switch1102-1(te1/0/1) <=> switch1119-1(te1/0/2) <=> switch1121-1(te1/0/1) <=> switch1134-1(te1/0/2) <=> switch1138-1(te1/0/2) <=> switchfl-3(Te1/1/1)
4/28/2018, 4:39:23 PM	Connectivity	Scheduled Discovery [CS]	Info	LINK REMOVED: switch1029-1(Te1/1/2) <=> switch1102-1(te1/0/2) <=> switch1119-1(te1/0/1) <=> switch1121-1(te1/0/2) <=> switch1134-1(te1/0/1) <=> switch1138-1(te1/0/1) <=> switchfl-1(Te1/1/1) <=> switchfl-2(Te1/1/2)
4/28/2018, 4:39:23 PM	Connectivity	Scheduled Discovery [CS]	Info	LINK REMOVED: switchfl-1(Te1/1/2) <=> switchfl-3(Te1/1/1)

Common types of events include the following:

- Discovery run completed
- New device appeared on the network
- Device disappeared from the network
- New link appeared on the network
- Link disappeared from the network
- Error or warning condition was detected

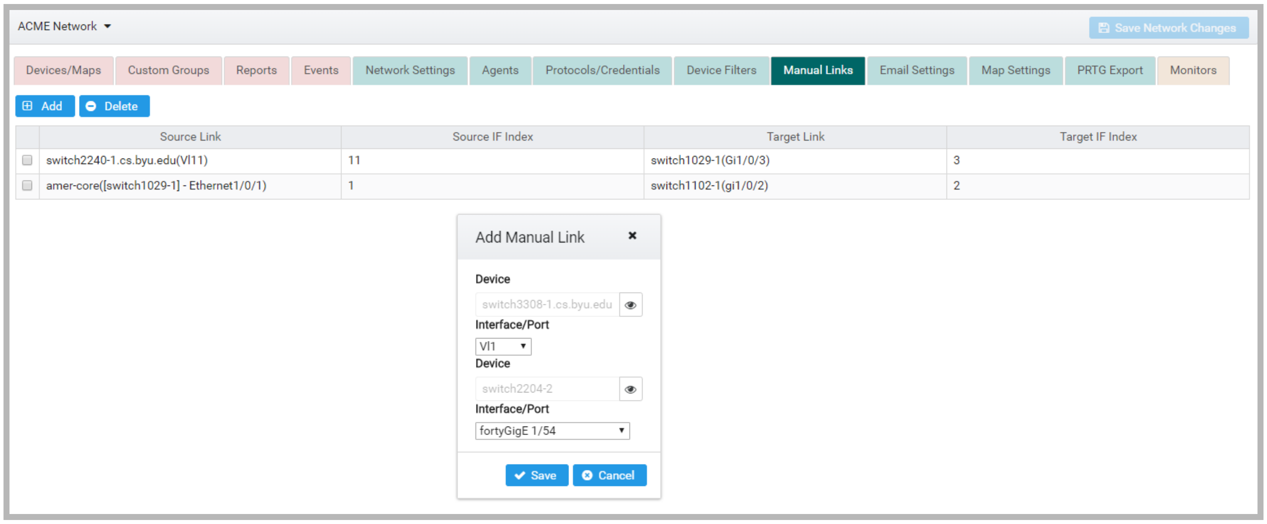
When viewing a discovery run, the Events tab displays events only for that discovery run.
When viewing a discovery, the Events tab displays events only for that discovery and its discovery runs.
When viewing an agent, the Events tab displays events only for that agent and its discoveries and discovery runs.

When viewing a network, the Events tab displays events for the entire network, including all agents, discoveries, and discovery runs.

Manual Links

Occasionally, there might be a link in your network that is not discovered automatically by UVexplorer Server. In this case you can add the link by hand by creating a “manual link”. A manual link is created by selecting the two devices connected by the links, as well as the network interfaces on each device that participate in the link. Once a manual link has been created, UVexplorer Server will automatically add the link to all network maps and other connectivity views.

Manual links are managed at the network level. To create or delete manual links, navigate to the network, and select the “Manual Links” tab (see picture below).



	Source Link	Source IF Index	Target Link	Target IF Index
□	switch2240-1.cs.byu.edu(Vl11)	11	switch1029-1(Gi1/0/3)	3
□	amer-core([switch1029-1] - Ethernet1/0/1)	1	switch1102-1(gi1/0/2)	2

Add Manual Link ×

Device: switch3308-1.cs.byu.edu

Interface/Port: Vl1

Device: switch2204-2

Interface/Port: fortyGigE 1/54

The Manual Links tab displays all of the manual links that have been previously created.

To create a new manual link, click the “Add” button, which will display a dialog where you can select the devices and network interfaces involved in the new link.

To delete a manual link, select it by checking the checkbox in its row, and click the “Delete” button.

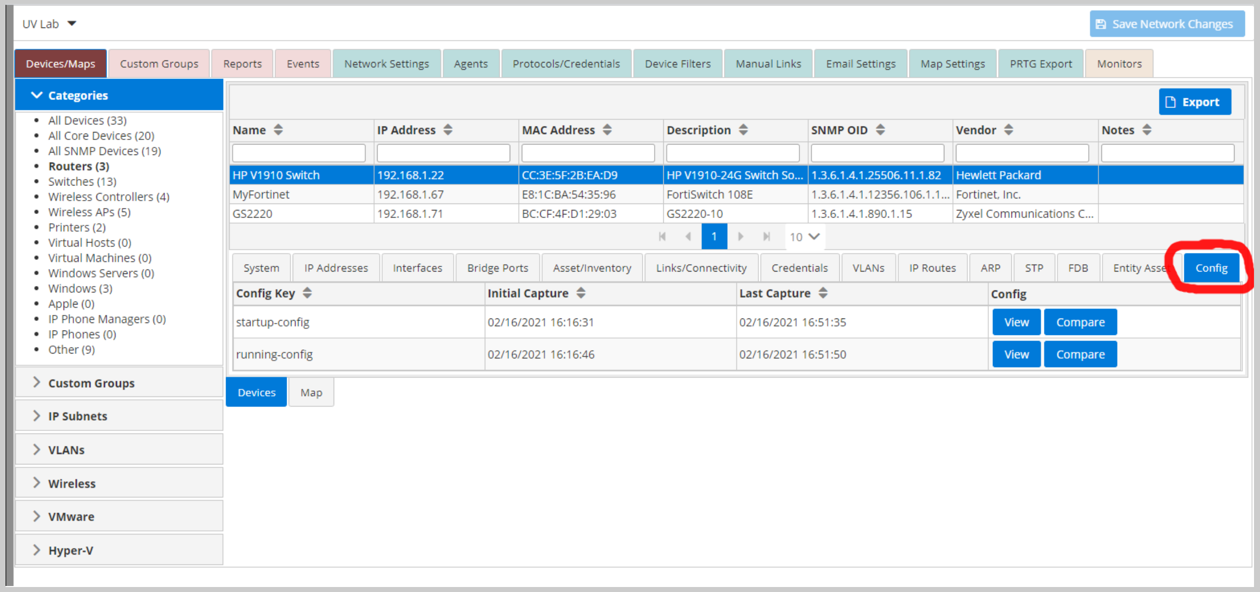
Capturing, Viewing, and Exporting Device Configurations

UVexplorer Server can capture device configurations for many network devices (switches, routers, firewalls, etc.). It does so using the SSH and Telnet protocols. Once connected, a script is run against the device to capture its configuration. Therefore, in order for device configuration capture to work, you must provide valid SSH or Telnet credentials for devices you want to capture configurations for.

To enable configuration capture, you must do the following:

1. Enable "Capture Device Configurations" in the discovery's Advanced Settings tab.
2. In the discovery's Protocols/Credentials tab, provide valid SSH or Telnet credentials for devices you want to capture configurations for.

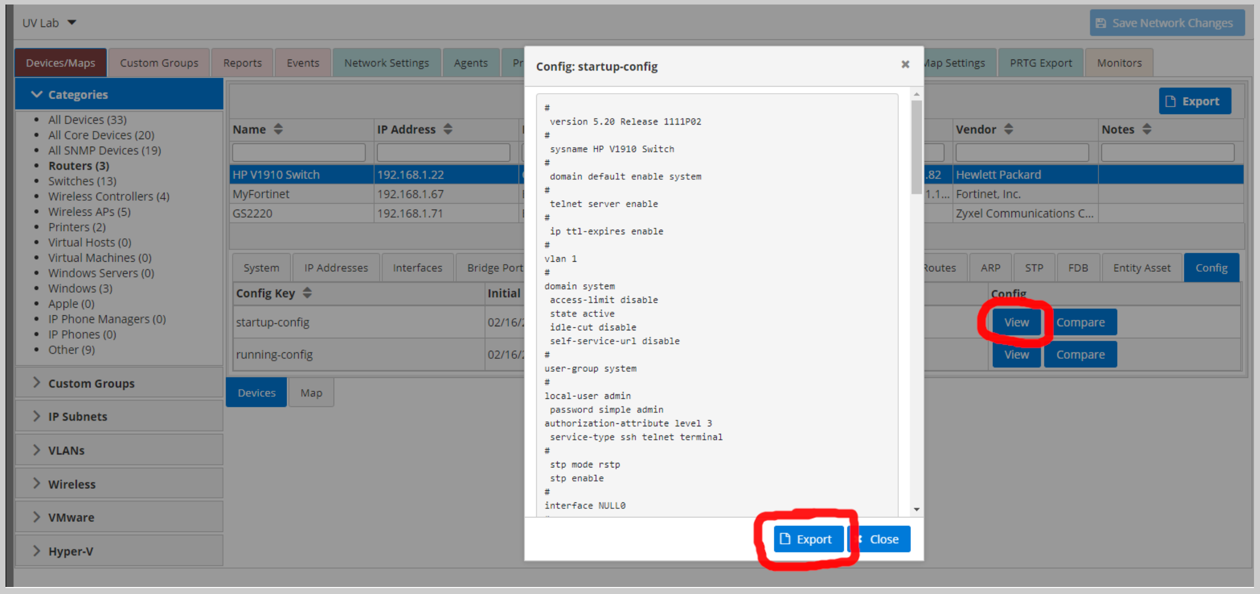
After the discovery runs, the device configurations can be viewed in the device details view. To view device details, go to the Devices/Maps tab, and select the device of interest. You can also double-click a device on a network map to see its details. In the device details, select the Config tab. The Config tab displays a list of captured configurations, which may include the device's "startup configuration" and/or the device's "running configuration".



Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
HP V1910 Switch	192.168.1.22	CC:3E:5F:2B:EA:D9	HP V1910-24G Switch So...	1.3.6.1.4.1.25506.11.1.82	Hewlett Packard	
MyFortinet	192.168.1.67	E8:1C:BA:54:35:96	FortiSwitch 108E	1.3.6.1.4.1.12356.106.1.1...	Fortinet, Inc.	
GS2220	192.168.1.71	BC:CF:4F:D1:29:03	GS2220-10	1.3.6.1.4.1.890.1.15	Zyxel Communications C...	

Config Key	Initial Capture	Last Capture	Config
startup-config	02/16/2021 16:16:31	02/16/2021 16:51:35	View Compare
running-config	02/16/2021 16:16:46	02/16/2021 16:51:50	View Compare

To view a device configuration, click the "View" button. This will display the text for the device configuration in a dialog. In this dialog, you can export the configuration text by clicking the "Export" button, which will cause the UVexplorer Server server to download the configuration text file to your web browser. Your browser will let you view or save the file.

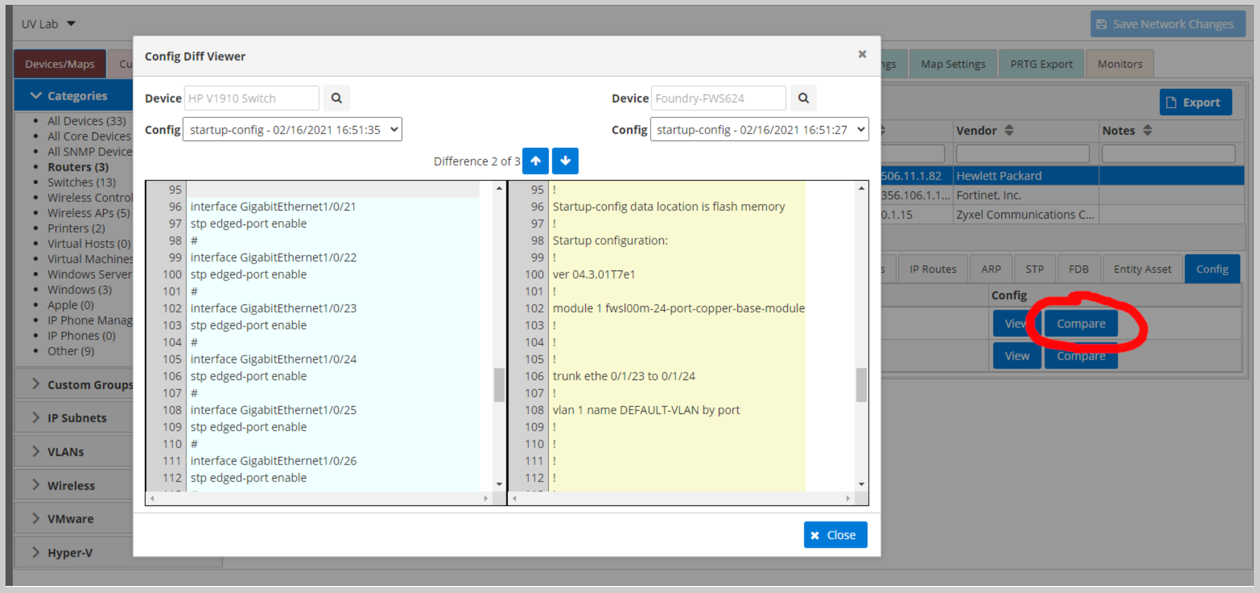


```
#
 version 5.20 Release 1111P02
#
 sysname HP V1910 Switch
#
 domain default enable system
#
 telnet server enable
#
 ip ttl-expires enable
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
#
local-user admin
 password simple admin
authorization-attribute level 3
 service-type ssh telnet terminal
#
 stp mode rstp
 stp enable
#
interface NULL0
```

It is often useful to view the differences between different device configurations. Some common uses for this are:

1. Seeing how the configuration of a device has changed over time
2. Seeing the differences between a device's startup and running configurations
3. Seeing the differences between the configurations of two different devices

To view the differences between device configurations, click the "Compare" button. Doing so displays a dialog that lets you select the configurations you want to compare, and browse the differences between them. The configurations being compared could come from the same device or from two different devices (see picture below).



Device HP V1910 Switch
Config startup-config - 02/16/2021 16:51:35

Device Foundry-FWS624
Config startup-config - 02/16/2021 16:51:27

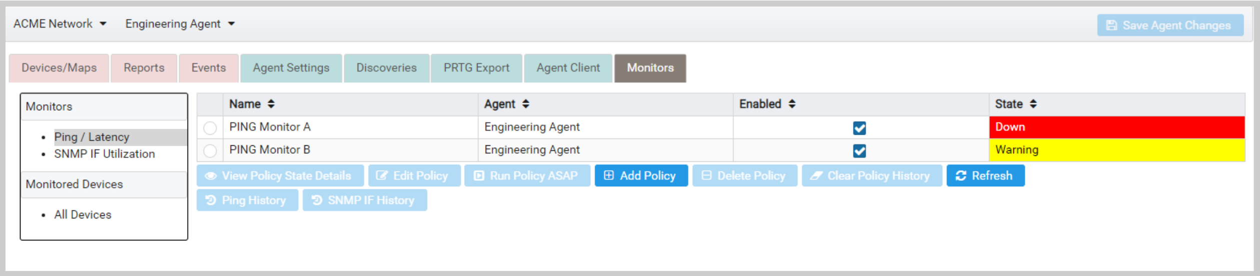
```

interface GigabitEthernet1/0/21
stp edged-port enable
#
interface GigabitEthernet1/0/22
stp edged-port enable
#
interface GigabitEthernet1/0/23
stp edged-port enable
#
interface GigabitEthernet1/0/24
stp edged-port enable
#
interface GigabitEthernet1/0/25
stp edged-port enable
#
interface GigabitEthernet1/0/26
stp edged-port enable
```

```
!
Startup-config data location is flash memory
!
Startup configuration:
!
ver 04.3.01T7e1
!
module 1 fwsl00m-24-port-copper-base-module
!
!
!
trunk ethe 0/1/23 to 0/1/24
!
vlan 1 name DEFAULT-VLAN by port
!
!
!
!
```

Monitoring Your Network

UVexplorer Server lets you monitor your network using Ping monitors and SNMP Interface monitors. Monitors are executed by agents. Monitors are created and configured on an agent by navigating to the relevant agent and selecting the Monitors tab.

The Monitors tab on a network shows a “rollup” (or “union”) of all the monitors for all of the network’s agents. At the network level, monitor status can be viewed, but monitors cannot be configured. Monitor configuration must be done at the agent level. Therefore, the network Monitors tab contains a subset of the agent functionality. This section describes the agent Monitors tab.



	Name ⇕	Agent ⇕	Enabled ⇕	State ⇕
○	PING Monitor A	Engineering Agent	☑	Down
○	PING Monitor B	Engineering Agent	☑	Warning

Agent Monitors Tab

On the left side of the agent Monitors tab, select “Ping / Latency” to view your Ping monitors, or select “SNMP IF Utilization” to view your SNMP network interface monitors. You can also select “All Devices” to see a device-centric view that shows the status of all monitor elements on each device that is being monitored.

Adding, Configuring, and Deleting Monitors

To create a new monitor policy, select the appropriate monitor type, and then click the “Add Policy” button. This will create a new monitor policy.

To delete a monitor policy, select the monitor policy in the list by clicking the radio button to the left of the monitor’s name, and then click the “Delete Policy” button.

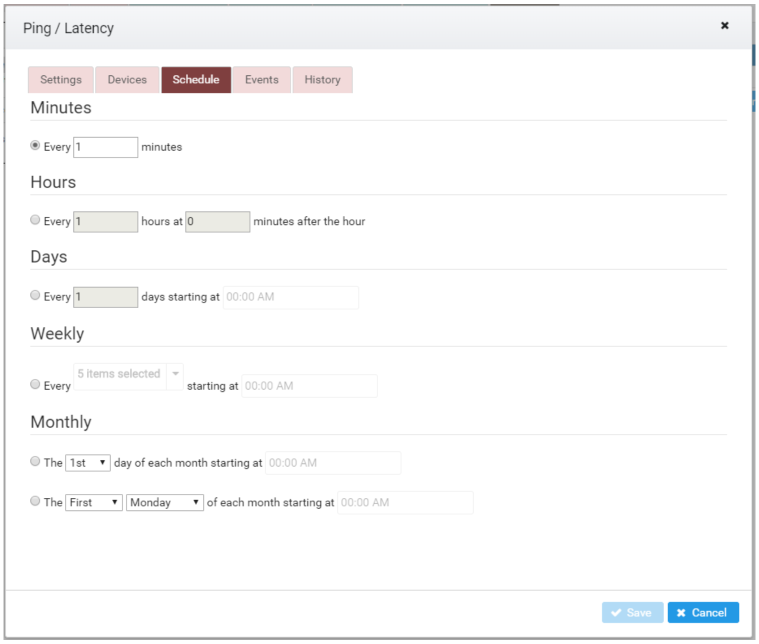
To edit a monitor policy, select the monitor policy in the list by clicking the radio button to the left of the monitor’s name, and then click the “Edit Policy” button. This will bring up an editor that lets you view and modify the policy’s settings.

Configuring Monitors

Each monitor policy consists of settings specific to that monitor along with schedule settings, event notification settings, and monitor result history settings.

Schedule Tab

In the Schedule Tab you can specify the schedule on which the monitor policy should run. Monitors can be scheduled to run on a specified interval allowing you to monitor the state of a device over time. For example, you could configure a monitor to “run every 15 minutes”.



Ping / Latency

Minutes

● Every 1 minutes

Hours

○ Every 1 hours at 0 minutes after the hour

Days

○ Every 1 days starting at 00:00 AM

Weekly

○ Every 5 items selected starting at 00:00 AM

Monthly

○ The 1st day of each month starting at 00:00 AM

○ The First Monday of each month starting at 00:00 AM

Monitor Schedule Tab

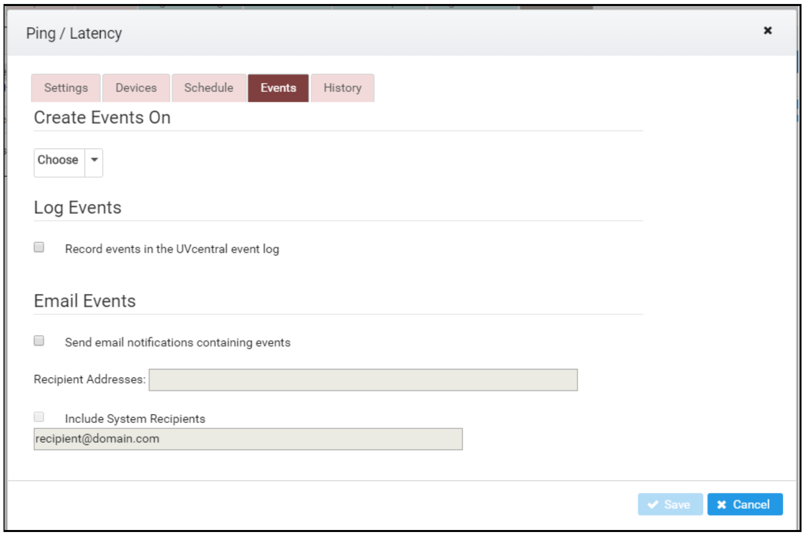
The following schedule types are available:

<u>Minutes</u>
This schedule will run the monitor every N minutes. For example, ‘Run every 30 minutes’.
<u>Hours</u>
This schedule will run the monitor every N hours at a specified minute during the hour. For example, ‘Run every 6 hours’.
<u>Days</u>
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’.
<u>Weekly</u>
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’.

Events Tab

Each monitor has a current state associated with it. If desired, UVexplorer Server can notify you about monitor state change events. UVexplorer Server can log events and also send notification emails.



Create Events On

Choose

Log Events

□ Record events in the UVcentral event log

Email Events

□ Send email notifications containing events

Recipient Addresses:

□ Include System Recipients

recipient@domain.com

Monitor Events Tab

Create Events On
In the dropdown list, select which monitor states should cause events to be generated. The following states are available:

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 monitor's 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.

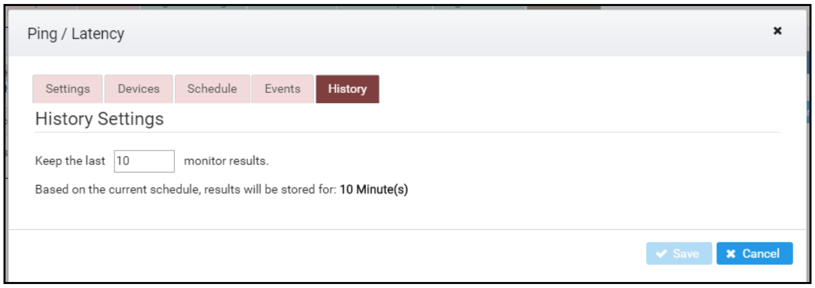
Log Events

This check box can be used to indicate whether events should be recorded in the UVexplorer Server event view.

Email Events

UVexplorer Server can be configured to send email notifications containing details about monitor state changes. To enable emails on monitor state changes, select the “Send email notifications 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 network’s email server settings are configured.

History Tab



Ping / Latency

History Settings

Keep the last 10 monitor results.

Based on the current schedule, results will be stored for: **10 Minute(s)**

Monitor History Tab

Each time a monitor is run, the results of the monitor queries are stored. Over time, 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 limit the number of results to keep. As a convenience, the time duration the monitor results will be stored is displayed. This is based on the number of results and the current monitor schedule. This value will change as the number of results and/or 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.

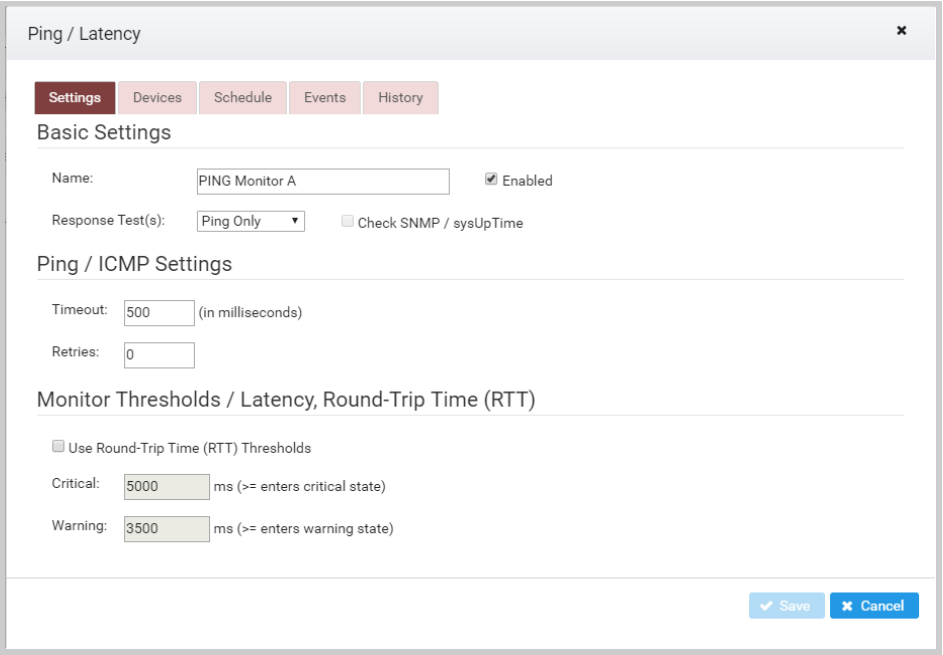
In an attempt to maintain system stability, the maximum number of stored monitor results is limited to 1000.

Configuring Ping Monitors

Ping monitors allow 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 monitor's specified thresholds. The Ping monitor editor lets you select the device IP addresses to be monitored, and also configure other settings that control the monitor's operation. The Schedule, Events and History tabs are the same for all monitor types. See the section called "Configuring Monitors" for more information about these tabs. The Ping-specific tabs are described below.

Ping Monitor Settings Tab

The Settings tab lets you specify a variety of settings that define the behavior of the Ping monitor.



Basic Settings

Name: PING Monitor A ☑ Enabled

Response Test(s): Ping Only ▾ □ Check SNMP / sysUpTime

Ping / ICMP Settings

Timeout: 500 (in milliseconds)

Retries: 0

Monitor Thresholds / Latency, Round-Trip Time (RTT)

□ Use Round-Trip Time (RTT) Thresholds

Critical: 5000 ms (>= enters critical state)

Warning: 3500 ms (>= enters warning state)

Ping Monitor Settings Tab

Name
Specify a name that will be used to refer to the monitor. Monitor names do not have to 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, SNMP, 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 device will go into the “Information” state (meant not to alarm, but to provide information that can be used for troubling shooting).

Note: SNMP requests require the device to have valid SNMP credentials associated with it.

Ping /ICMP Settings

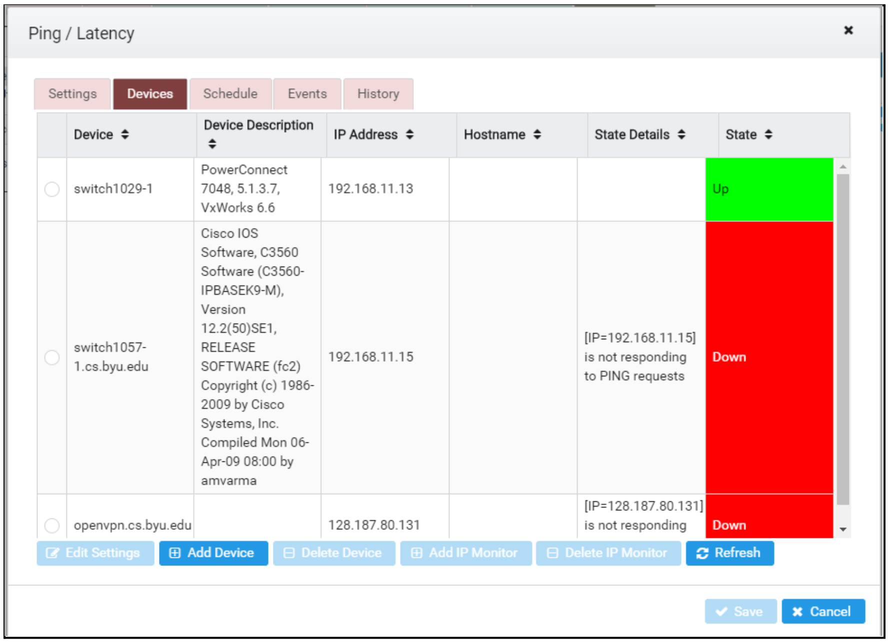
The Ping/ICMP settings specify the timeout in milliseconds and the number of retries to be performed for each ping request. If the device responds to the ping request within the specified timeout and retries the request will be considered valid.

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.

Ping Monitor Devices Tab

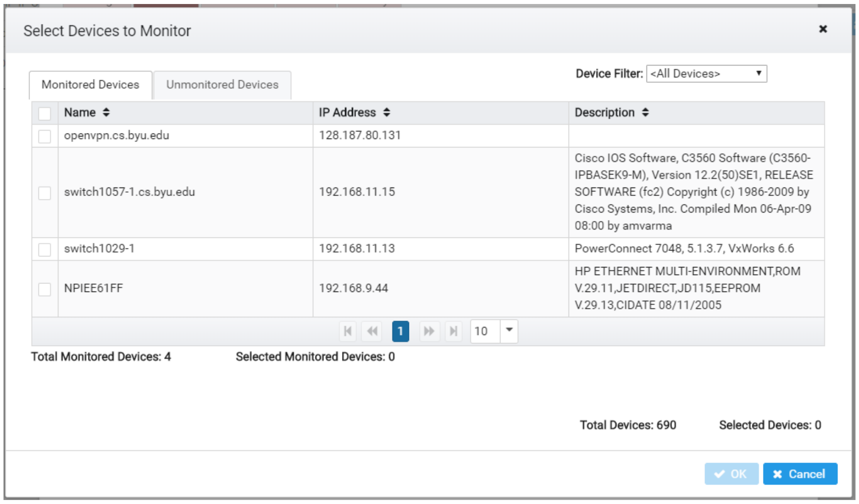
The Devices tab lists all of the IP addresses that are being monitored by this Ping monitor. It also displays the current status of each IP address (UP, DOWN, etc.). To update the status information, click the “Refresh” button.



	Device	Device Description	IP Address	Hostname	State Details	State
○	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13			Up
○	switch1057-1.cs.byu.edu	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(50)SE1, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Mon 06-Apr-09 08:00 by amvarma	192.168.11.15		[IP=192.168.11.15] is not responding to PING requests	Down
○	openvpn.cs.byu.edu		128.187.80.131		[IP=128.187.80.131] is not responding	Down

Ping Monitor Devices Tab

To add IP addresses to a Ping monitor, click the “Add Device” button. This will display a dialog that lets you select devices to be added. The “Monitored Devices” tab lists all devices that currently have at least one monitor on them. The “Unmonitored Devices” tab lists all devices that currently have no monitors on them. After selecting devices in one or both tabs, click the “OK” button. This will add the primary IP address for each selected device to the Ping monitor.



Device Filter: <All Devices>

□	Name ⬍	IP Address ⬍	Description ⬍
□	openvpn.cs.byu.edu	128.187.80.131	
□	switch1057-1.cs.byu.edu	192.168.11.15	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(50)SE1, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Mon 06-Apr-09 08:00 by amvarma
□	switch1029-1	192.168.11.13	PowerConnect 7048, 5.1.3.7, VxWorks 6.6
□	NPIEE61FF	192.168.9.44	HP ETHERNET MULTI-ENVIRONMENT,ROM V.29.11,JETDIRECT,JD115,EEPROM V.29.13,CIDATE 08/11/2005

Total Monitored Devices: 4 Selected Monitored Devices: 0

Total Devices: 690 Selected Devices: 0

Ping Monitor Device Selector

To add one or more of a device’s secondary IP addresses to a Ping monitor, select one of the device’s IP addresses in the Devices tab, and click the “Add IP Monitor” button. This will display a dialog that lets you select any or all of the device’s secondary IP addresses.

To edit the settings for an IP address, select the IP address in the Devices tab, and click the “Edit Settings” button. If desired, you can configure the IP address to resolve a defined "Hostname" before sending the ping requests.

To remove an IP address from a Ping monitor, select the IP address in the Devices tab, and click the “Delete IP Monitor” button.

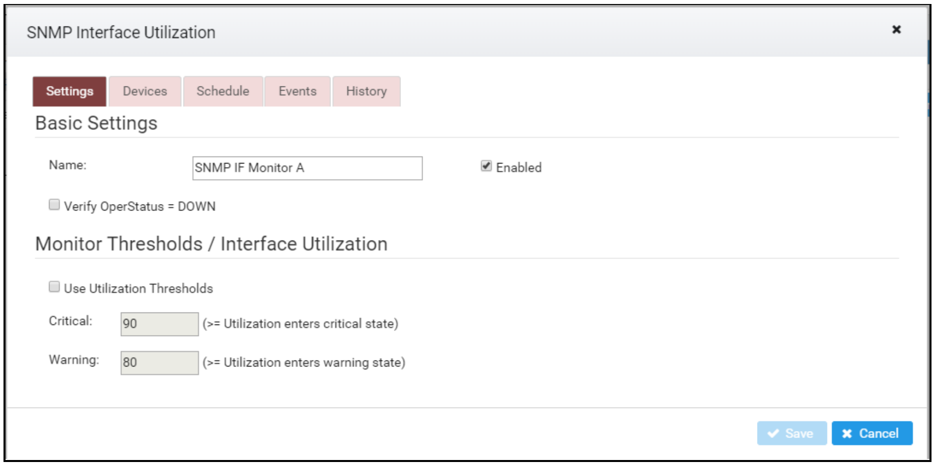
To remove ALL of a device’s IP addresses from a Ping monitor, select one of the device’s IP addresses in the Devices tab, and click the “Delete Device” button.

Configuring SNMP Interface Monitors

SNMP interface monitors let you monitor the Up/Down status of network interfaces on SNMP-enabled devices. You can also monitor network interface utilization. The SNMP interface monitor editor lets you select the device network interfaces to be monitored, and also configure many other settings that control the monitor’s operation. The Schedule, Events and History tabs are the same for all monitor types. See the section called “Configuring Monitors” for more information about those tabs. The SNMP interface monitor-specific tabs are described below.

SNMP Monitor Settings Tab

The Settings tab lets you specify a variety of settings that define the behavior of the SNMP interface monitor.



Basic Settings

Name: SNMP IF Monitor A ☑ Enabled

☐ Verify OperStatus = DOWN

Monitor Thresholds / Interface Utilization

☐ Use Utilization Thresholds

Critical: 90 (>= Utilization enters critical state)

Warning: 80 (>= Utilization enters warning state)

SNMP Interface Monitor Settings Tab

Name
Specify a name that will be used to refer to the monitor. Monitor names do not have to be unique, but it is recommended you use unique names to differentiate them.

Verify OperStatus = Down
By default, an SNMP interface monitor will check to ensure the interface is Up. Checking this box will cause the monitor to check to ensure that the interface is Down.

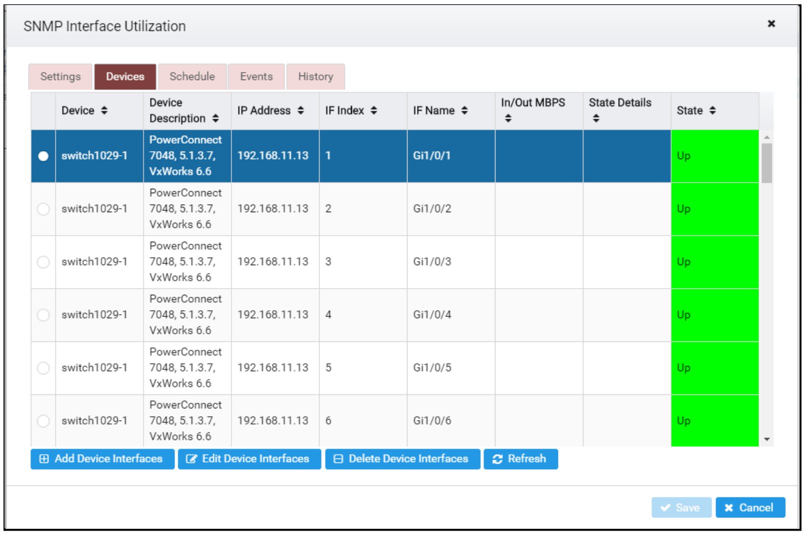
Use Utilization Thresholds
Checking this box will cause the monitor to check the interface utilization thresholds (Critical and Warning).

Critical
If the interface’s utilization exceeds this value, the monitor will go into the Down state.

Warning
If the interface’s utilization exceeds this value, the monitor will go into the Warning state.

SNMP Interface Monitor Devices Tab

The Devices tab lists all of the network interfaces that are being monitored by this SNMP interface monitor. It also displays the current status of each interface (UP, DOWN, etc.). To update the status information, click the “Refresh” button.

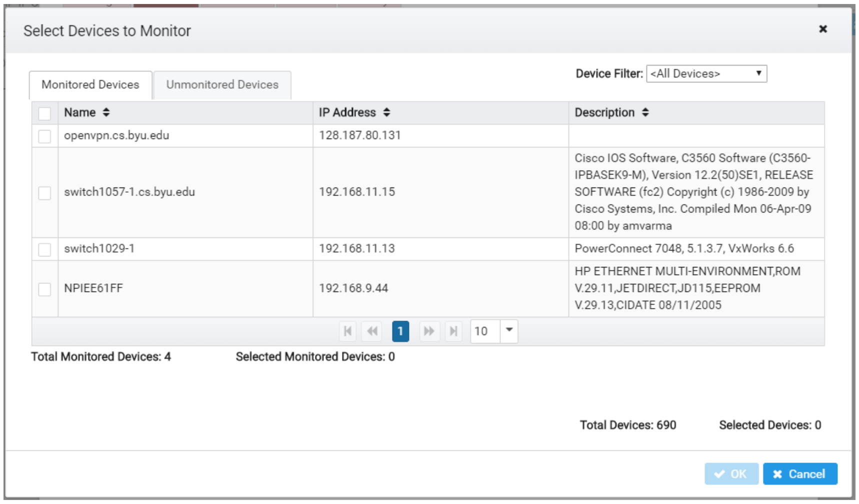


SNMP Interface Utilization ×

	Device ⬍	Device Description ⬍	IP Address ⬍	IF Index ⬍	IF Name ⬍	In/Out MBPS ⬍	State Details ⬍	State ⬍
●	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13	1	Gi1/0/1			Up
○	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13	2	Gi1/0/2			Up
○	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13	3	Gi1/0/3			Up
○	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13	4	Gi1/0/4			Up
○	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13	5	Gi1/0/5			Up
○	switch1029-1	PowerConnect 7048, 5.1.3.7, VxWorks 6.6	192.168.11.13	6	Gi1/0/6			Up

SNMP Interface Monitor Devices Tab

To add network interfaces to an SNMP interface monitor, click the “Add Device” button. This will display a dialog that lets you select devices to be added. The “Monitored Devices” tab lists all devices that currently have at least one monitor on them. The “Unmonitored Devices” tab lists all devices that currently have no monitors on them. After selecting devices in one or both tabs, click the “OK” button. This will add all of the Up interfaces on the selected devices to the SNMP Interface monitor.



Select Devices to Monitor ×

Device Filter: <All Devices>

□	Name ⬍	IP Address ⬍	Description ⬍
□	openvpn.cs.byu.edu	128.187.80.131	
□	switch1057-1.cs.byu.edu	192.168.11.15	Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(50)SE1, RELEASE SOFTWARE (fc2) Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Mon 06-Apr-09 08:00 by amvarma
□	switch1029-1	192.168.11.13	PowerConnect 7048, 5.1.3.7, VxWorks 6.6
□	NPIEE61FF	192.168.9.44	HP ETHERNET MULTI-ENVIRONMENT,ROM V.29.11,JETDIRECT,JD115,EEPROM V.29.13,CIDATE 08/11/2005

Total Monitored Devices: 4 Selected Monitored Devices: 0

Total Devices: 690 Selected Devices: 0

SNMP Interface Monitor Device Selector

For fine-grained control over which of a device’s network interfaces are monitored, select one of the device’s interfaces in the Devices tab, and click the “Edit Device Interfaces” button. This will display a dialog that lets you select exactly which of the device’s interfaces should be monitored.

To remove ALL of a device's network interfaces from an SNMP interface monitor, select one of the device's interfaces in the Devices tab, and click the "Delete Device Interfaces" button.

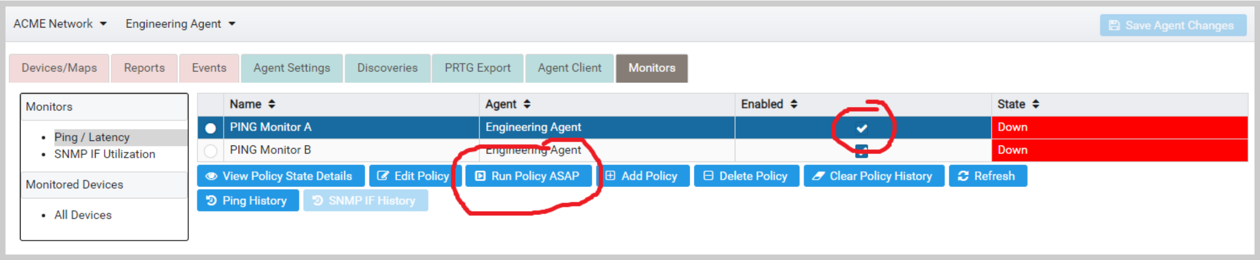
Controlling Monitor Execution

Disabling Monitors

Monitor policies will run according to their defined schedules. However, sometimes it is necessary to disable a monitor to prevent it from running (for example, when devices are down for maintenance). There are two ways to disable a monitor policy:

1. Uncheck the policy's "Enabled" check box in the agent Monitors tab
2. Uncheck the "Enabled" check box in the policy editor

Of course, to re-enable a policy, simply re-check the "Enabled" check box.



	Name	Agent	Enabled	State
●	PING Monitor A	Engineering Agent	✓	Down
○	PING Monitor B	Engineering Agent	✓	Down

Agent Monitors Tab

Running Monitors On-Demand

Monitor policies will run according to their defined schedules. However, sometimes it is desirable to run a monitor policy on-demand. This can be especially useful when tuning a monitor policy's settings, or debugging a policy that is not working as expected.

To run a monitor policy on demand, select the policy in the agent's Monitors tab, and click the "Run Policy ASAP" button. This will cause the policy to run the next time the agent polls the UVexplorer Server server for its updated configuration. How long this takes is determined by the agent's "Configuration Update Interval" setting (in the agent's Agent Settings tab), which controls how frequently the agent polls the server for configuration updates.

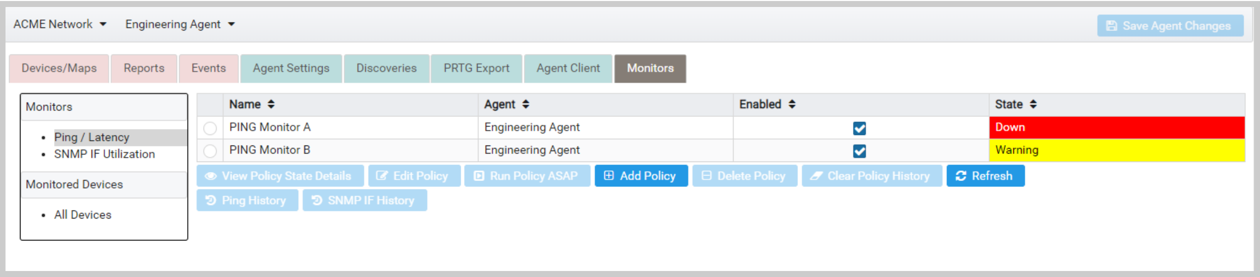
Monitor Events

As previously discussed, a monitor policy can be configured to generate events when monitor elements (IP addresses, network interfaces, devices, etc.) change state. These events appear in the agent's Events tab.

Viewing Monitor Status

Overall Monitor Status

In the Monitors tab, the “State” column displays the overall status of each monitor. This status is automatically refreshed according to the “Events Update Interval” setting on the agent’s network. You can also update the state information immediately by clicking the “Refresh” button.

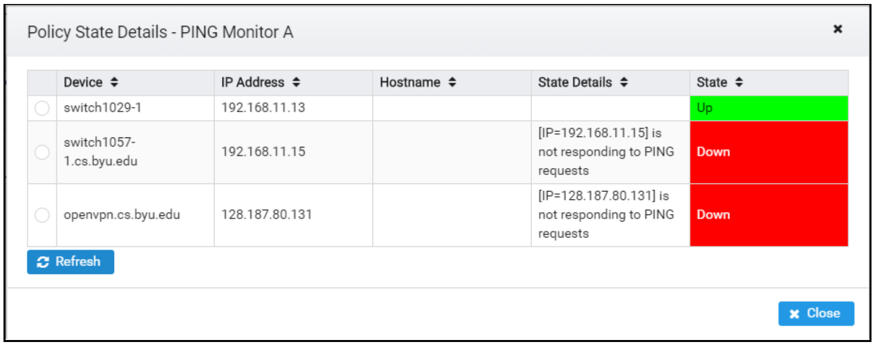


	Name	Agent	Enabled	State
○	PING Monitor A	Engineering Agent	☑	Down
○	PING Monitor B	Engineering Agent	☑	Warning

Agent Monitors Tab

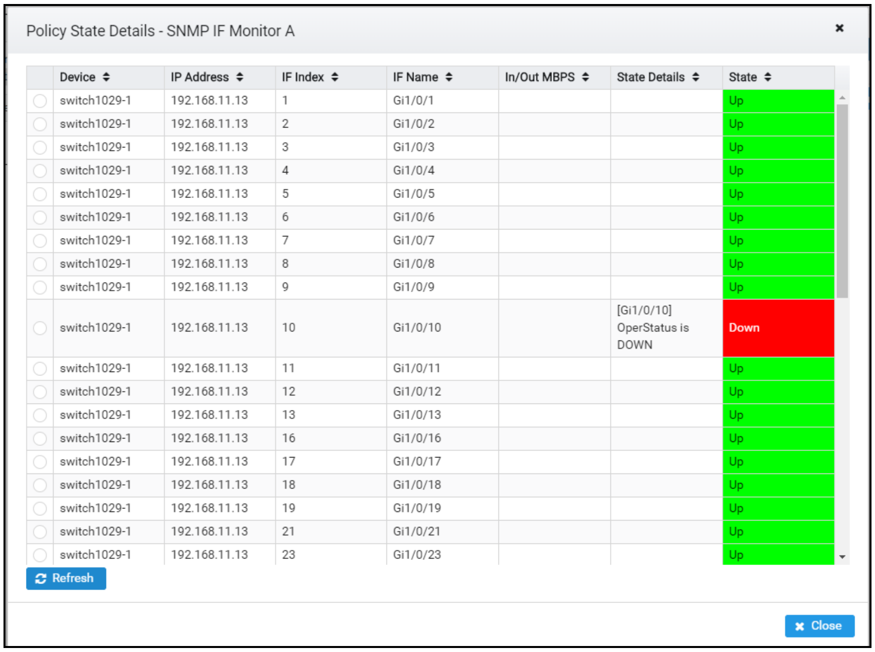
Detailed Monitor Status

For detailed monitor status information (per IP-address or per network interface), double-click the monitor in the monitor list, or select the monitor of interest and click the “View Policy State Details” button. Both of these actions will display a dialog showing status information for each IP address or network interface being monitored by the policy. This status is automatically refreshed according to the “Events Update Interval” setting on the agent’s network. You can also update the state information immediately by clicking the “Refresh” button.



	Device	IP Address	Hostname	State Details	State
○	switch1029-1	192.168.11.13			Up
○	switch1057-1.cs.byu.edu	192.168.11.15		[IP=192.168.11.15] is not responding to PING requests	Down
○	openvpn.cs.byu.edu	128.187.80.131		[IP=128.187.80.131] is not responding to PING requests	Down

Ping Policy State Details



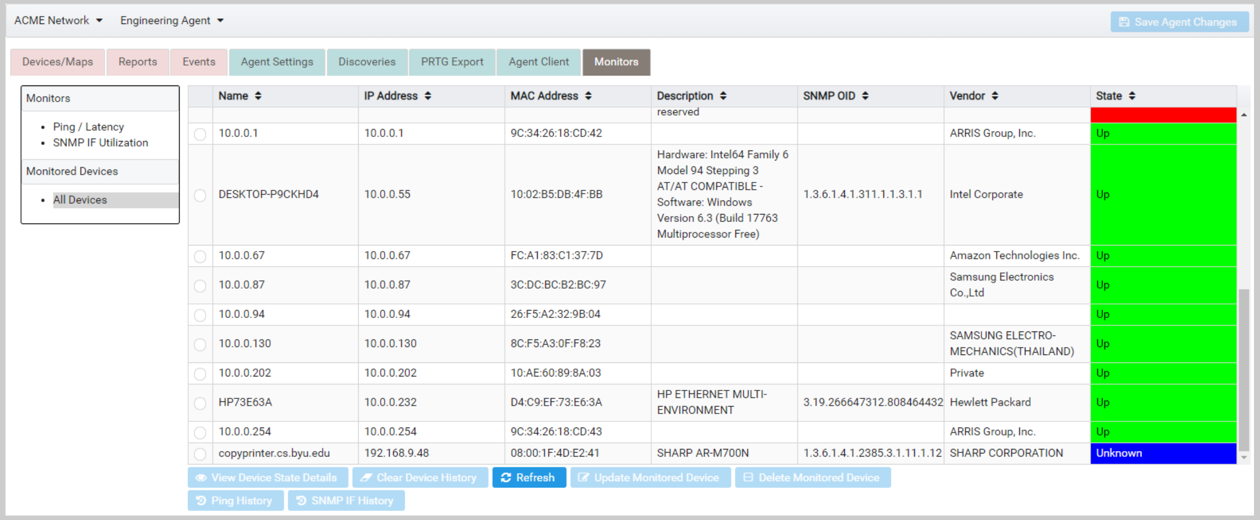
Policy State Details - SNMP IF Monitor A

	Device	IP Address	IF Index	IF Name	In/Out MBPS	State Details	State
○	switch1029-1	192.168.11.13	1	Gi1/0/1			Up
○	switch1029-1	192.168.11.13	2	Gi1/0/2			Up
○	switch1029-1	192.168.11.13	3	Gi1/0/3			Up
○	switch1029-1	192.168.11.13	4	Gi1/0/4			Up
○	switch1029-1	192.168.11.13	5	Gi1/0/5			Up
○	switch1029-1	192.168.11.13	6	Gi1/0/6			Up
○	switch1029-1	192.168.11.13	7	Gi1/0/7			Up
○	switch1029-1	192.168.11.13	8	Gi1/0/8			Up
○	switch1029-1	192.168.11.13	9	Gi1/0/9			Up
○	switch1029-1	192.168.11.13	10	Gi1/0/10		[Gi1/0/10] OperStatus is DOWN	Down
○	switch1029-1	192.168.11.13	11	Gi1/0/11			Up
○	switch1029-1	192.168.11.13	12	Gi1/0/12			Up
○	switch1029-1	192.168.11.13	13	Gi1/0/13			Up
○	switch1029-1	192.168.11.13	16	Gi1/0/16			Up
○	switch1029-1	192.168.11.13	17	Gi1/0/17			Up
○	switch1029-1	192.168.11.13	18	Gi1/0/18			Up
○	switch1029-1	192.168.11.13	19	Gi1/0/19			Up
○	switch1029-1	192.168.11.13	21	Gi1/0/21			Up
○	switch1029-1	192.168.11.13	23	Gi1/0/23			Up

SNMP Interface Policy State Details

Overall Device Status

For a device-centric status view, go to the Monitors tab, and select “All Devices” on the left side. This will display a list of all devices that are currently being monitored (i.e., have at least one monitor defined on them), and each device’s current overall status (Up, Down, etc.). This status is automatically refreshed according to the “Events Update Interval” setting on the agent’s network. You can also update the state information immediately by clicking the “Refresh” button.

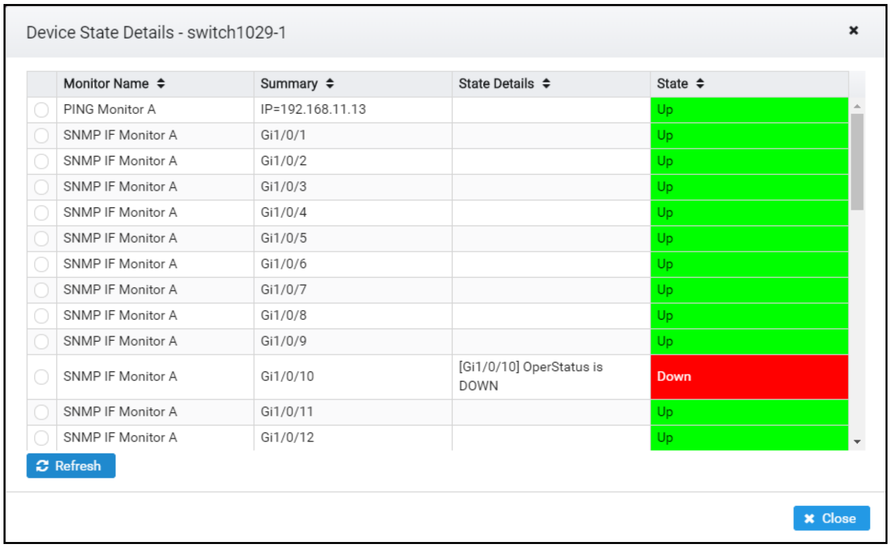


	Name	IP Address	MAC Address	Description	SNMP OID	Vendor	State
				reserved			
○	10.0.0.1	10.0.0.1	9C:34:26:18:CD:42			ARRIS Group, Inc.	Up
○	DESKTOP-P9CKHD4	10.0.0.55	10:02:B5:DB:4F:BB	Hardware: Intel64 Family 6 Model 94 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)	1.3.6.1.4.1.311.1.1.3.1.1	Intel Corporate	Up
○	10.0.0.67	10.0.0.67	FC:A1:83:C1:37:7D			Amazon Technologies Inc.	Up
○	10.0.0.87	10.0.0.87	3C:DC:BC:B2:BC:97			Samsung Electronics Co.,Ltd	Up
○	10.0.0.94	10.0.0.94	26:F5:A2:32:9B:04				Up
○	10.0.0.130	10.0.0.130	8C:F5:A3:0F:F8:23			SAMSUNG ELECTRO-MECHANICS(THAILAND)	Up
○	10.0.0.202	10.0.0.202	10:AE:60:89:8A:03			Private	Up
○	HP73E63A	10.0.0.232	D4:C9:EF:73:E6:3A	HP ETHERNET MULTI-ENVIRONMENT	3.19.266647312.808464432	Hewlett Packard	Up
○	10.0.0.254	10.0.0.254	9C:34:26:18:CD:43			ARRIS Group, Inc.	Up
○	copyprinter.cs.byu.edu	192.168.9.48	08:00:1F:4D:E2:41	SHARP AR-M700N	1.3.6.1.4.1.2385.3.1.11.1.12	SHARP CORPORATION	Unknown

Overall Device Status

Detailed Device Status

For detailed device status information (per IP address and per network interface), double-click the device in the device list, or select the device of interest and click the “View Device State Details” button. Both of these actions will display a dialog showing status information for each IP address or network interface being monitored on the device. This status is automatically refreshed according to the “Events Update Interval” setting on the agent’s network. You can also update the state information immediately by clicking the “Refresh” button.



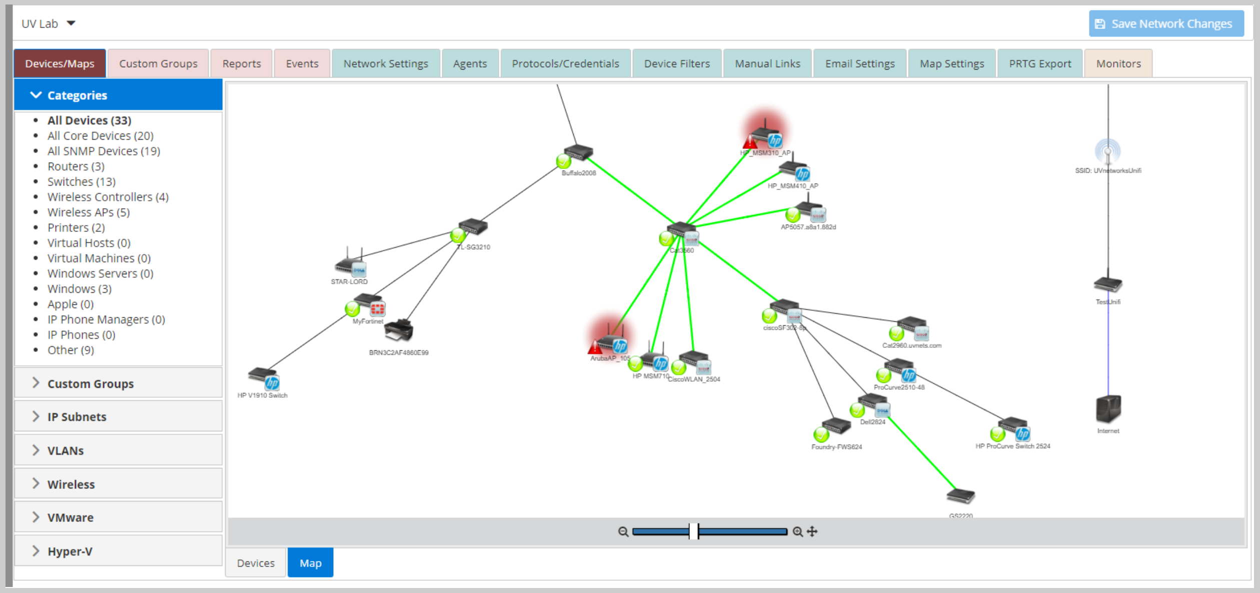
Device State Details - switch1029-1

	Monitor Name	Summary	State Details	State
○	PING Monitor A	IP=192.168.11.13		Up
○	SNMP IF Monitor A	Gi1/0/1		Up
○	SNMP IF Monitor A	Gi1/0/2		Up
○	SNMP IF Monitor A	Gi1/0/3		Up
○	SNMP IF Monitor A	Gi1/0/4		Up
○	SNMP IF Monitor A	Gi1/0/5		Up
○	SNMP IF Monitor A	Gi1/0/6		Up
○	SNMP IF Monitor A	Gi1/0/7		Up
○	SNMP IF Monitor A	Gi1/0/8		Up
○	SNMP IF Monitor A	Gi1/0/9		Up
○	SNMP IF Monitor A	Gi1/0/10	[Gi1/0/10] OperStatus is DOWN	Down
○	SNMP IF Monitor A	Gi1/0/11		Up
○	SNMP IF Monitor A	Gi1/0/12		Up

Detailed Device Status

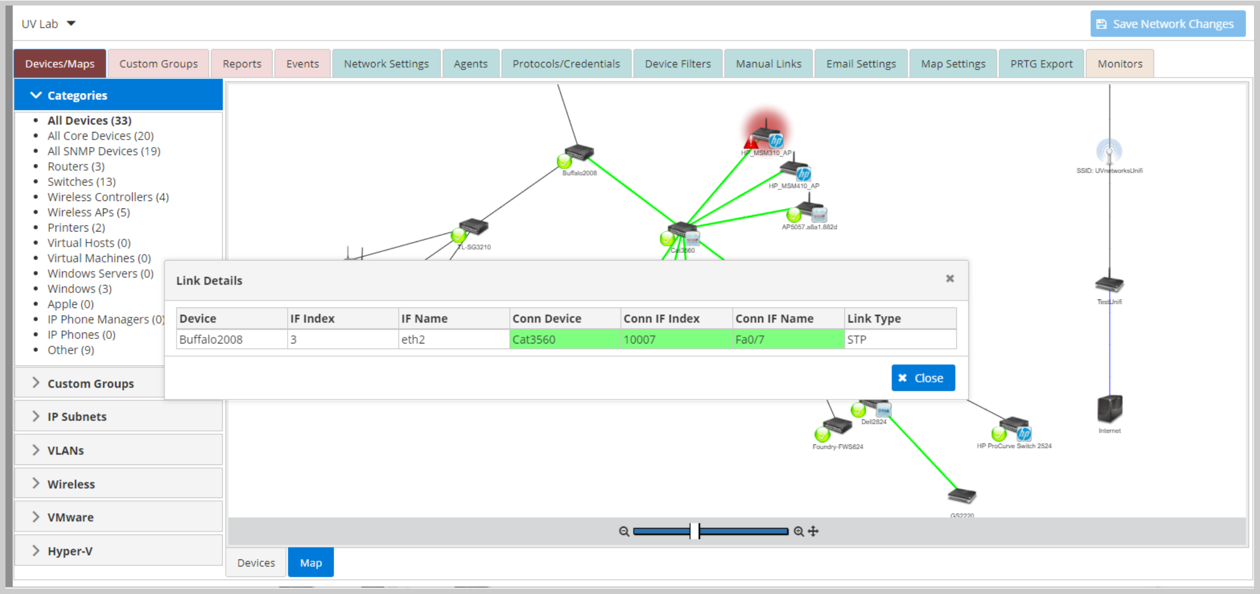
Monitor Status on Network Maps

Monitor status is also reflected on network maps. Specifically, a device’s overall monitor status is displayed on all network maps including that device, and the status of SNMP Interface monitors is displayed on all network maps including links connected to that interface (see picture below).



Monitor Status on Network Maps

SNMP Interface monitor status is also displayed in the “Link Details” dialog that is displayed when you double-click a link on a network map (see picture below).



Link Details

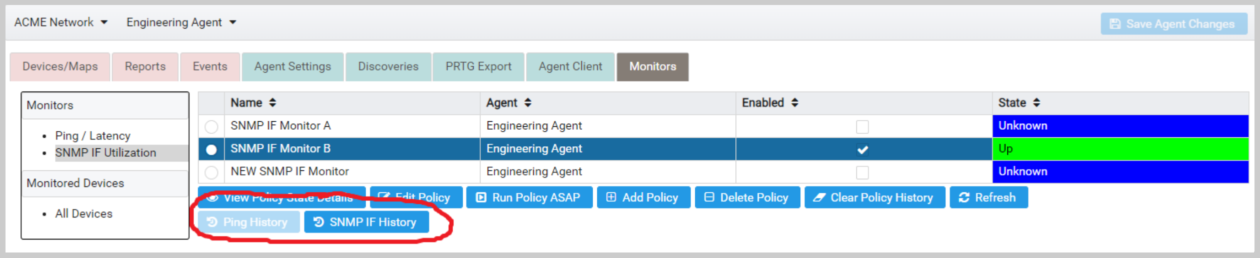
Device	IF Index	IF Name	Conn Device	Conn IF Index	Conn IF Name	Link Type
Buffalo2008	3	eth2	Cat3560	10007	Fa0/7	STP

Interface Status in Link Details

Viewing Monitor History

To view historical data for Ping and SNMP Interface monitors, go to the Monitors Tab. Historical data can be viewed at both policy and device levels.

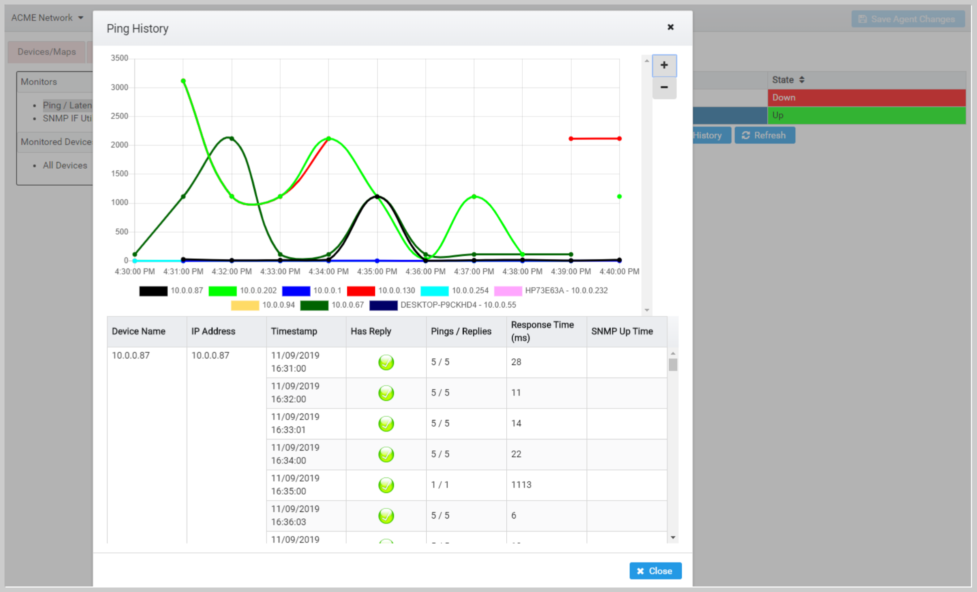
Monitor Policy History



	Name	Agent	Enabled	State
○	SNMP IF Monitor A	Engineering Agent	□	Unknown
●	SNMP IF Monitor B	Engineering Agent	✓	Up
○	NEW SNMP IF Monitor	Engineering Agent	□	Unknown

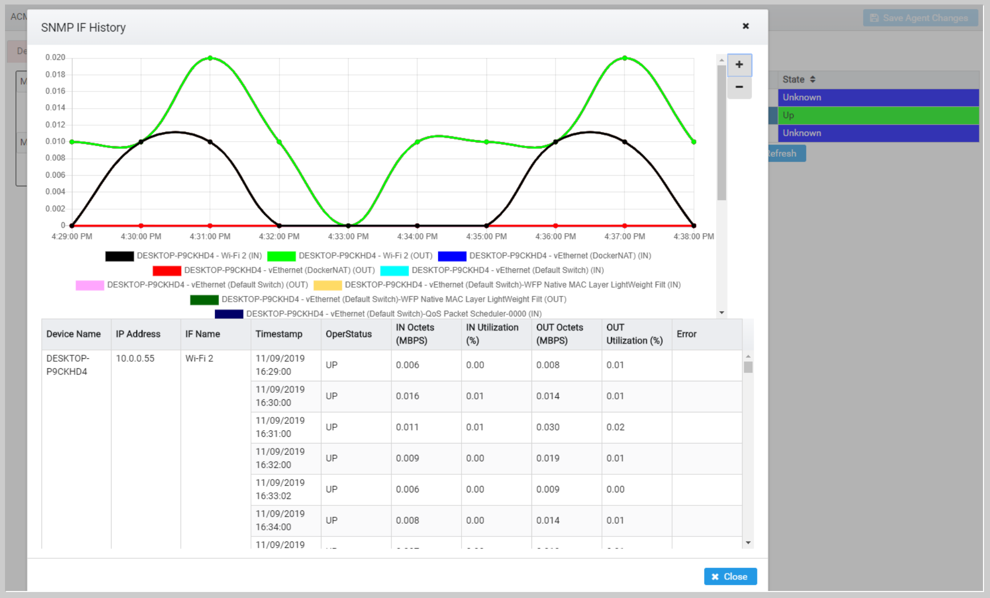
Select Policy in Agent Monitors Tab

To view history for a monitor policy, go to the Monitors tab, and select either “Ping / Latency” or “SNMP IF Utilization” on the left side. Next, select the policy of interest in the table. If you selected a Ping monitor policy, click the “Ping History” button. If you selected an SNMP Interface monitor policy, click the “SNMP IF History” button. This will display historical data for the policy in both graphical and tabular forms (see below). This data is automatically refreshed according to the “Events Update Interval” setting on the agent’s network.



Device Name	IP Address	Timestamp	Has Reply	Pings / Replies	Response Time (ms)	SNMP Up Time
10.0.0.87	10.0.0.87	11/09/2019 16:31:00	✓	5 / 5	28	
		11/09/2019 16:32:00	✓	5 / 5	11	
		11/09/2019 16:33:01	✓	5 / 5	14	
		11/09/2019 16:34:00	✓	5 / 5	22	
		11/09/2019 16:35:00	✓	1 / 1	1113	
		11/09/2019 16:36:03	✓	5 / 5	6	
		11/09/2019				

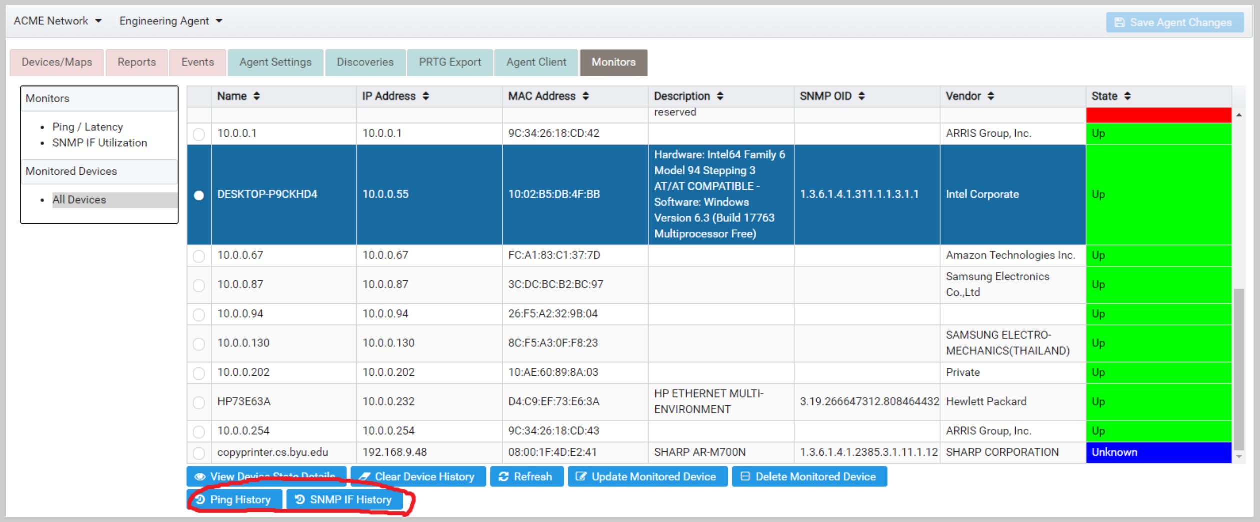
Policy Ping History


SNMP IF History
×
0.020
0.018
0.016
0.014
0.012
0.010
0.008
0.006
0.004
0.002
0
4:29:00 PM
4:30:00 PM
4:31:00 PM
4:32:00 PM
4:33:00 PM
4:34:00 PM
4:35:00 PM
4:36:00 PM
4:37:00 PM
4:38:00 PM
+
−
DESKTOP-P9CKHD4 - Wi-Fi 2 (IN)
DESKTOP-P9CKHD4 - Wi-Fi 2 (OUT)
DESKTOP-P9CKHD4 - vEthernet (DockerNAT) (IN)
DESKTOP-P9CKHD4 - vEthernet (DockerNAT) (OUT)
DESKTOP-P9CKHD4 - vEthernet (Default Switch) (IN)
DESKTOP-P9CKHD4 - vEthernet (Default Switch) (OUT)
DESKTOP-P9CKHD4 - vEthernet (Default Switch)-WFP Native MAC Layer LightWeight Filt (IN)
DESKTOP-P9CKHD4 - vEthernet (Default Switch)-WFP Native MAC Layer LightWeight Filt (OUT)
DESKTOP-P9CKHD4 - vEthernet (Default Switch)-QoS Packet Scheduler-0000 (IN)
State
Unknown
Up
Unknown
Save Agent Changes
✖ Close

Device Name	IP Address	IF Name	Timestamp	OperStatus	IN Octets (MBPS)	IN Utilization (%)	OUT Octets (MBPS)	OUT Utilization (%)	Error
DESKTOP-P9CKHD4	10.0.0.55	Wi-Fi 2	11/09/2019 16:29:00	UP	0.006	0.00	0.008	0.01	
			11/09/2019 16:30:00	UP	0.016	0.01	0.014	0.01	
			11/09/2019 16:31:00	UP	0.011	0.01	0.030	0.02	
			11/09/2019 16:32:00	UP	0.009	0.00	0.019	0.01	
			11/09/2019 16:33:02	UP	0.006	0.00	0.009	0.00	
			11/09/2019 16:34:00	UP	0.008	0.00	0.014	0.01	
			11/09/2019						

Policy SNMP Interface History

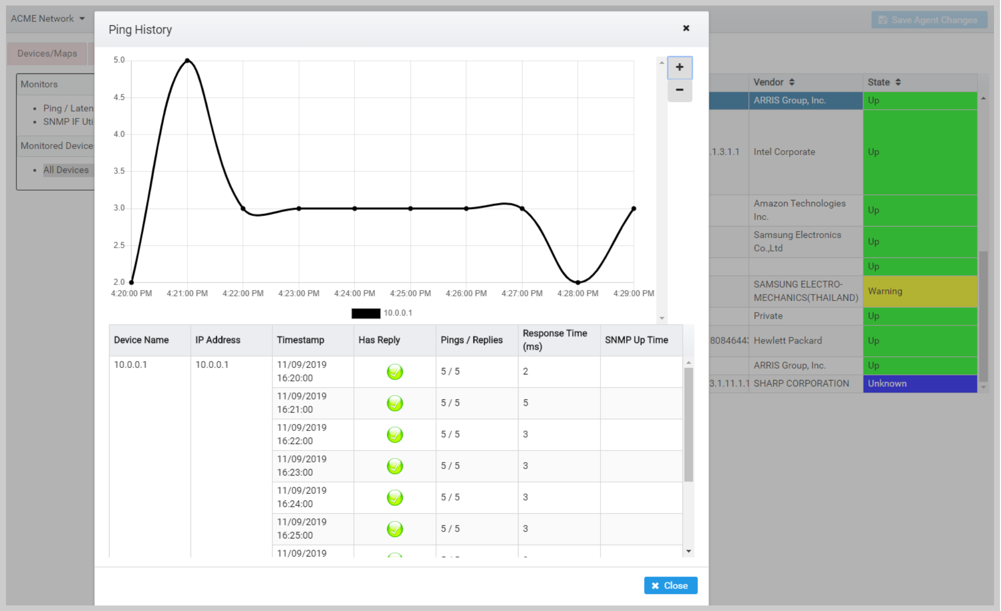
Device Monitor History



	Name	IP Address	MAC Address	Description	SNMP OID	Vendor	State
				reserved			
○	10.0.0.1	10.0.0.1	9C:34:26:18:CD:42			ARRIS Group, Inc.	Up
●	DESKTOP-P9CKHD4	10.0.0.55	10:02:B5:DB:4F:BB	Hardware: Intel64 Family 6 Model 94 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)	1.3.6.1.4.1.311.1.1.3.1.1	Intel Corporate	Up
○	10.0.0.67	10.0.0.67	FC:A1:83:C1:37:7D			Amazon Technologies Inc.	Up
○	10.0.0.87	10.0.0.87	3C:DC:BC:B2:BC:97			Samsung Electronics Co.,Ltd	Up
○	10.0.0.94	10.0.0.94	26:F5:A2:32:9B:04				Up
○	10.0.0.130	10.0.0.130	8C:F5:A3:0F:F8:23			SAMSUNG ELECTRO-MECHANICS(THAILAND)	Up
○	10.0.0.202	10.0.0.202	10:AE:60:89:8A:03			Private	Up
○	HP73E63A	10.0.0.232	D4:C9:EF:73:E6:3A	HP ETHERNET MULTI-ENVIRONMENT	3.19.266647312.808464432	Hewlett Packard	Up
○	10.0.0.254	10.0.0.254	9C:34:26:18:CD:43			ARRIS Group, Inc.	Up
○	copyprinter.cs.byu.edu	192.168.9.48	08:00:1F:4D:E2:41	SHARP AR-M700N	1.3.6.1.4.1.2385.3.1.11.1.12	SHARP CORPORATION	Unknown

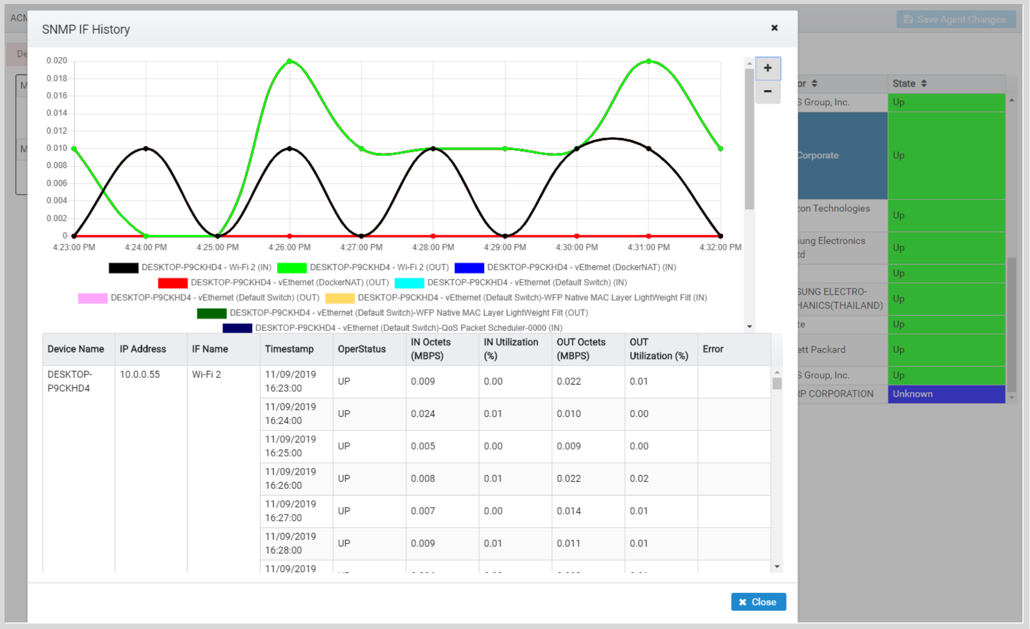
Select Device in Agent Monitors Tab

To view monitor history for a specific device, go to the Monitors tab, and select “All Devices” on the left side. Next, select the device of interest in the table. To view Ping history for the selected device, click the “Ping History” button. To view SNMP Interface history for the selected device, click the “SNMP IF History” button. This will display historical data for the device in both graphical and tabular forms (see below). This data is automatically refreshed according to the “Events Update Interval” setting on the agent’s network.



Device Name	IP Address	Timestamp	Has Reply	Pings / Replies	Response Time (ms)	SNMP Up Time
10.0.0.1	10.0.0.1	11/09/2019 16:20:00	✓	5 / 5	2	
		11/09/2019 16:21:00	✓	5 / 5	5	
		11/09/2019 16:22:00	✓	5 / 5	3	
		11/09/2019 16:23:00	✓	5 / 5	3	
		11/09/2019 16:24:00	✓	5 / 5	3	
		11/09/2019 16:25:00	✓	5 / 5	3	
		11/09/2019				

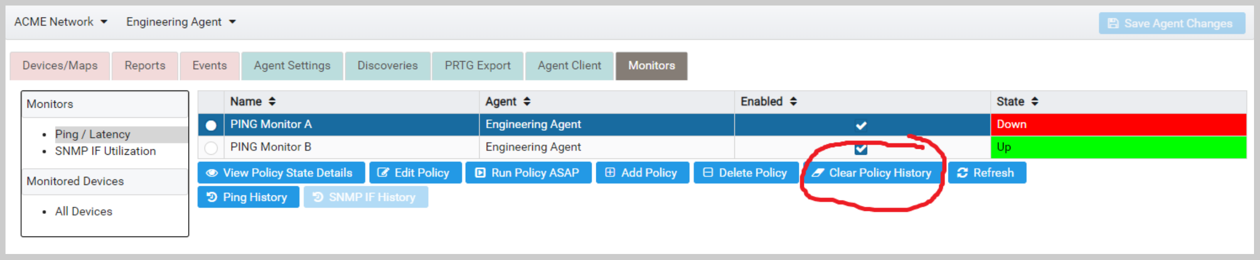
Device Ping History


ACM
De
M
M
Save Agent Changes
or
State
S Group, Inc.
Up
Corporate
Up
zon Technologies
Up
sung Electronics
td
Up
Up
SUNG ELECTRO-
HANICS(THAILAND)
Up
te
Up
ett Packard
Up
S Group, Inc.
Up
IP CORPORATION
Unknown
SNMP IF History
×
+
−
0.020
0.018
0.016
0.014
0.012
0.010
0.008
0.006
0.004
0.002
0
4:23:00 PM
4:24:00 PM
4:25:00 PM
4:26:00 PM
4:27:00 PM
4:28:00 PM
4:29:00 PM
4:30:00 PM
4:31:00 PM
4:32:00 PM
■ DESKTOP-P9CKHD4 - Wi-Fi 2 (IN)
■ DESKTOP-P9CKHD4 - Wi-Fi 2 (OUT)
■ DESKTOP-P9CKHD4 - vEthernet (DockerNAT) (IN)
■ DESKTOP-P9CKHD4 - vEthernet (DockerNAT) (OUT)
■ DESKTOP-P9CKHD4 - vEthernet (Default Switch) (IN)
■ DESKTOP-P9CKHD4 - vEthernet (Default Switch) (OUT)
■ DESKTOP-P9CKHD4 - vEthernet (Default Switch)-WFP Native MAC Layer LightWeight Filt (IN)
■ DESKTOP-P9CKHD4 - vEthernet (Default Switch)-WFP Native MAC Layer LightWeight Filt (OUT)
■ DESKTOP-P9CKHD4 - vEthernet (Default Switch)-QoS Packet Scheduler-0000 (IN)
✖ Close

Device Name	IP Address	IF Name	Timestamp	OperStatus	IN Octets (MBPS)	IN Utilization (%)	OUT Octets (MBPS)	OUT Utilization (%)	Error
DESKTOP-P9CKHD4	10.0.0.55	Wi-Fi 2	11/09/2019 16:23:00	UP	0.009	0.00	0.022	0.01	
			11/09/2019 16:24:00	UP	0.024	0.01	0.010	0.00	
			11/09/2019 16:25:00	UP	0.005	0.00	0.009	0.00	
			11/09/2019 16:26:00	UP	0.008	0.01	0.022	0.02	
			11/09/2019 16:27:00	UP	0.007	0.00	0.014	0.01	
			11/09/2019 16:28:00	UP	0.009	0.01	0.011	0.01	
			11/09/2019						

Device SNMP Interface History

Clearing Monitor Policy History

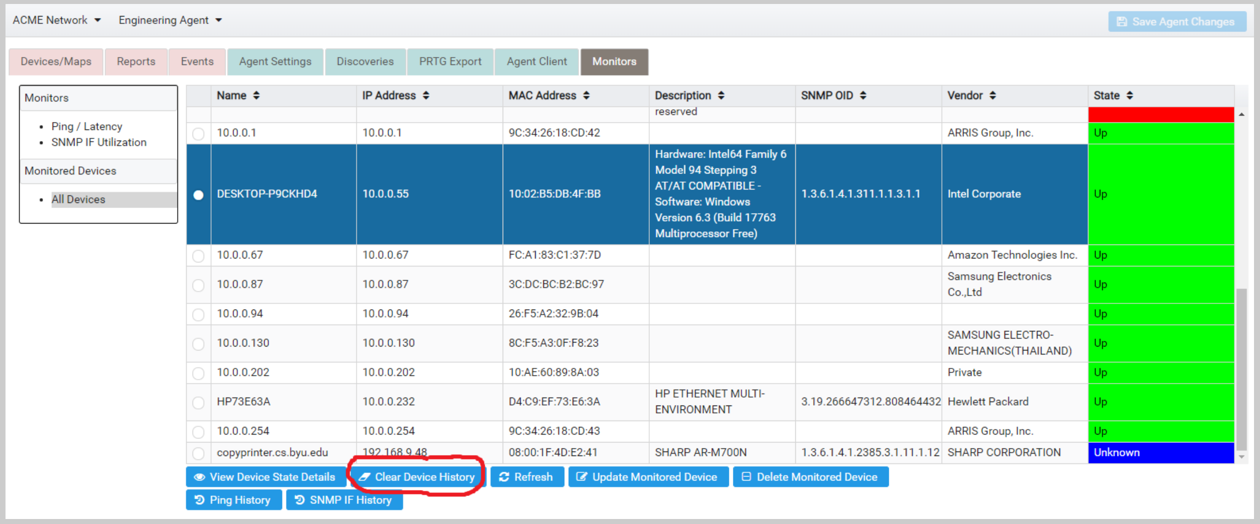


	Name	Agent	Enabled	State
●	PING Monitor A	Engineering Agent	✓	Down
○	PING Monitor B	Engineering Agent	☑	Up

Clear Monitor Policy History

Sometimes it is desirable to delete the historical data associated with a monitor policy. To do this, go to the Monitors tab, and select either “Ping / Latency” or “SNMP IF Utilization” on the left side. Next, select the policy of interest in the table, and click the “Clear Policy History” button.

Clearing Device Monitor History



	Name	IP Address	MAC Address	Description	SNMP OID	Vendor	State
				reserved			
○	10.0.0.1	10.0.0.1	9C:34:26:18:CD:42			ARRIS Group, Inc.	Up
●	DESKTOP-P9CKHD4	10.0.0.55	10:02:B5:DB:4F:BB	Hardware: Intel64 Family 6 Model 94 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)	1.3.6.1.4.1.311.1.1.3.1.1	Intel Corporate	Up
○	10.0.0.67	10.0.0.67	FC:A1:83:C1:37:7D			Amazon Technologies Inc.	Up
○	10.0.0.87	10.0.0.87	3C:DC:BC:B2:BC:97			Samsung Electronics Co.,Ltd	Up
○	10.0.0.94	10.0.0.94	26:F5:A2:32:9B:04				Up
○	10.0.0.130	10.0.0.130	8C:F5:A3:0F:F8:23			SAMSUNG ELECTRO-MECHANICS(THAILAND)	Up
○	10.0.0.202	10.0.0.202	10:AE:60:89:8A:03			Private	Up
○	HP73E63A	10.0.0.232	D4:C9:EF:73:E6:3A	HP ETHERNET MULTI-ENVIRONMENT	3.19.266647312.808464432	Hewlett Packard	Up
○	10.0.0.254	10.0.0.254	9C:34:26:18:CD:43			ARRIS Group, Inc.	Up
○	copyprinter.cs.byu.edu	192.168.9.48	08:00:1F:4D:E2:41	SHARP AR-M700N	1.3.6.1.4.1.2385.3.1.11.1.12	SHARP CORPORATION	Unknown

Clear Device Monitor History

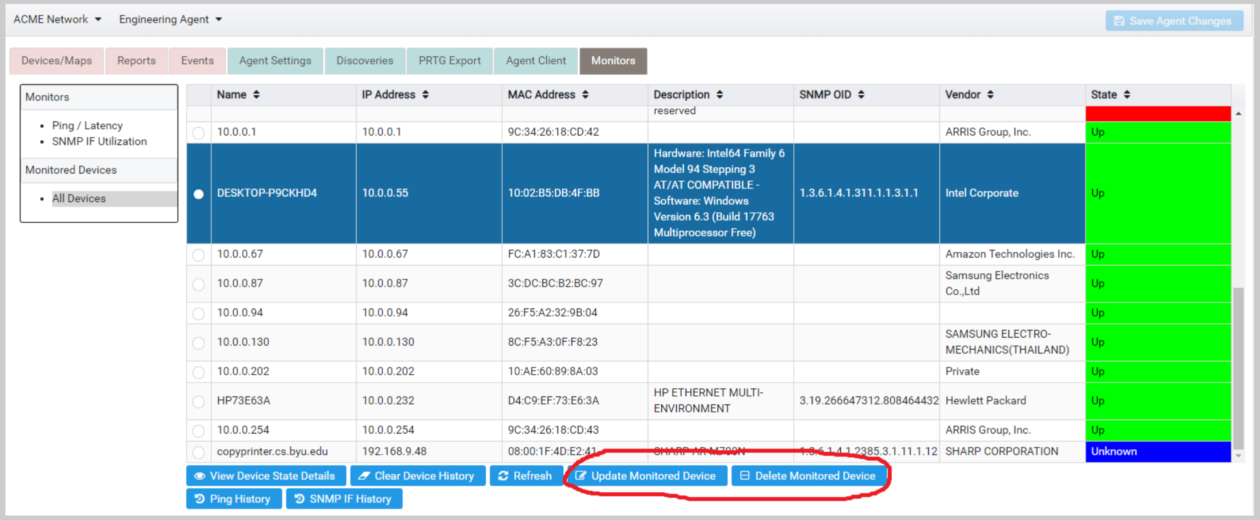
Sometimes it is desirable to delete the historical monitor data associated with a specific device. To do this, go to the Monitors tab, and select “All Devices” on the left side. Next, select the device of interest in the table, and click the “Clear Device History” button. This will delete all of the monitor history for the selected device across all monitor policies it participates in.

Updating Monitored Devices

When the first monitor is created on a device, UVexplorer Server makes a copy of the device’s information in its database. As subsequent discoveries are run, the monitored device’s information is not automatically updated using the latest discovery results. However, if you want to update a monitored device's information from the latest discovery result, do the following:

1. Navigate to the agent's Monitor tab
2. Select "All Devices" on the left side, which will display all monitored devices and their current statuses.
3. Select the device you want to update in the device list
4. Click the "Update Monitored Device" button

This will cause the latest device information to be copied from the most recent discovery result into the monitored device.



	Name	IP Address	MAC Address	Description	SNMP OID	Vendor	State
				reserved			
○	10.0.0.1	10.0.0.1	9C:34:26:18:CD:42			ARRIS Group, Inc.	Up
●	DESKTOP-P9CKHD4	10.0.0.55	10:02:B5:DB:4F:BB	Hardware: Intel64 Family 6 Model 94 Stepping 3 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 17763 Multiprocessor Free)	1.3.6.1.4.1.311.1.1.3.1.1	Intel Corporate	Up
○	10.0.0.67	10.0.0.67	FC:A1:83:C1:37:7D			Amazon Technologies Inc.	Up
○	10.0.0.87	10.0.0.87	3C:DC:BC:B2:BC:97			Samsung Electronics Co.,Ltd	Up
○	10.0.0.94	10.0.0.94	26:F5:A2:32:9B:04				Up
○	10.0.0.130	10.0.0.130	8C:F5:A3:0F:F8:23			SAMSUNG ELECTRO-MECHANICS(THAILAND)	Up
○	10.0.0.202	10.0.0.202	10:AE:60:89:8A:03			Private	Up
○	HP73E63A	10.0.0.232	D4:C9:EF:73:E6:3A	HP ETHERNET MULTI-ENVIRONMENT	3.19.266647312.808464432	Hewlett Packard	Up
○	10.0.0.254	10.0.0.254	9C:34:26:18:CD:43			ARRIS Group, Inc.	Up
○	copyprinter.cs.byu.edu	192.168.9.48	08:00:1F:4D:E2:41	SHARP AR-M700N	1.3.6.1.4.1.2385.3.1.11.1.12	SHARP CORPORATION	Unknown

Updating and Deleting Monitored Devices

Deleting Monitored Devices

If you want to delete all monitors currently defined on a particular device, do the following:

1. Navigate to the agent's Monitors tab
2. Select "All Devices" on the left side, which will display all monitored devices and their current statuses.
3. Select the device you want to delete in the device list
4. Click the "Delete Monitored Device" button

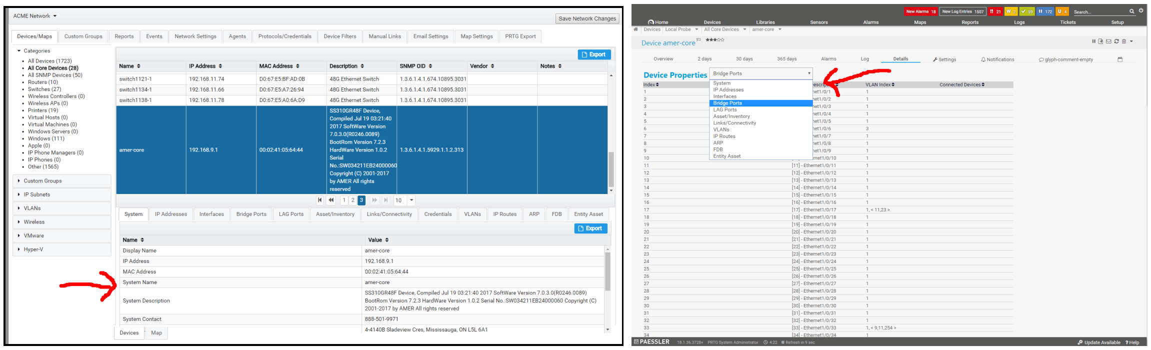
This will cause all monitors that are defined on the selected device to be removed.

Exporting to PRTG Network Monitor

PRTG Network Monitor is a popular network monitoring platform with advanced monitoring capabilities. UVexplorer Server's core strengths of fast and accurate network discovery, detailed device inventory, and automatic network mapping are a powerful complement to PRTG's monitoring features. To give you powerful network monitoring capabilities, UVexplorer Server integrates tightly with PRTG to bring fast and accurate network discovery, detailed device inventory, and automatic network mapping to the PRTG platform. Here's how:

When a discovery run completes, UVexplorer Server automatically exports discovery results into PRTG. There are two types of exports you can choose from:

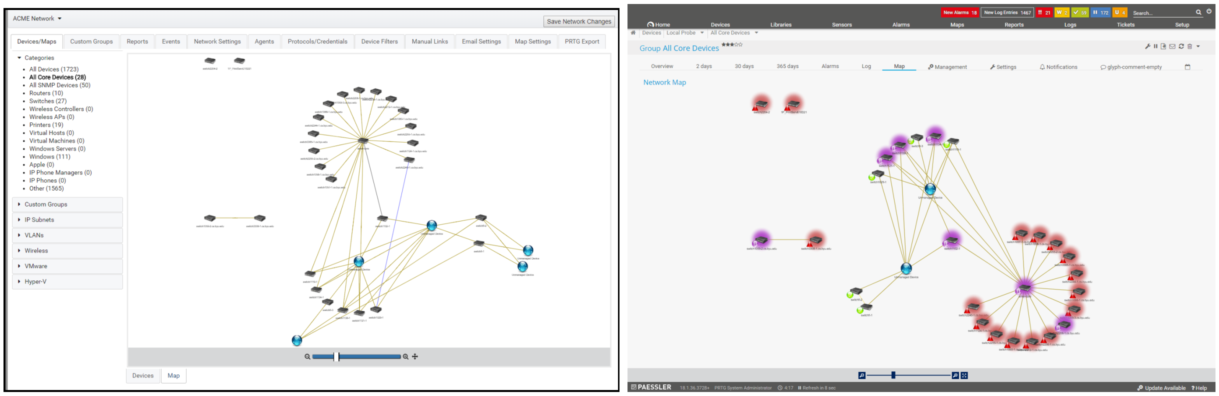
1. Export Data Only - This type of export is targeted at PRTG users who have already configured their PRTG server, and just want to add the data discovered by UVexplorer Server to their existing devices and groups. A data-only export overlays device details and network maps onto the devices and device groups you have created in your PRTG server. UVexplorer Server's device details and network maps appear automatically within PRTG's web console. Exported data and maps are updated each time the discovery runs so it is always current.



Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
switch1121-1	192.168.11.74	D0:67:E5:BF:AD:0B	48G Ethernet Switch	1.3.6.1.4.1.674.10895.3031		
switch1134-1	192.168.11.66	D0:67:E5:A7:26:94	48G Ethernet Switch	1.3.6.1.4.1.674.10895.3031		
switch1138-1	192.168.11.78	D0:67:E5:A0:6A:D9	48G Ethernet Switch	1.3.6.1.4.1.674.10895.3031		
amer-core	192.168.9.1	00:02:41:05:64:44	SS310GR48F Device, Compiled Jul 19 03:21:40 2017 SoftWare Version 7.0.3.0(R0246.0089) BootRom Version 7.2.3 HardWare Version 1.0.2 Serial No.:SW034211EB24000060 Copyright (C) 2001-2017 by AMER All rights reserved	1.3.6.1.4.1.5929.1.1.2.313		

Name	Value
Display Name	amer-core
IP Address	192.168.9.1
MAC Address	00:02:41:05:64:44
System Name	amer-core
System Description	SS310GR48F Device, Compiled Jul 19 03:21:40 2017 SoftWare Version 7.0.3.0(R0246.0089) BootRom Version 7.2.3 HardWare Version 1.0.2 Serial No.:SW034211EB24000060 Copyright (C) 2001-2017 by AMER All rights reserved
System Contact	888-501-9971
	4-4140B Sladeview Cres, Mississauga, ON L5L 6A1

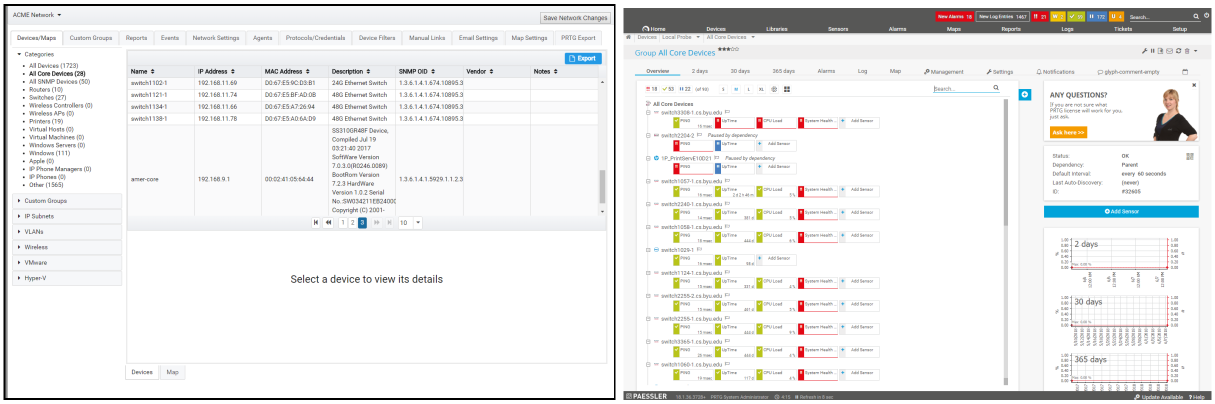
Device Details Exported into PRTG



Network Map Exported into PRTG

2. Export Groups/Devices - This type of export is targeted at PRTG users who want UVexplorer Server to help them configure their PRTG server, as well as add additional data not provided by PRTG. A groups/devices export uses discovery results to automatically create PRTG devices, device groups, and network maps. And, if you request it, UVexplorer Server automatically creates sensors on devices that are exported into PRTG. You can specify what sensor types you want UVexplorer Server to create on

the exported devices, and it does so automatically. This is great for creating sensors in bulk (e.g., Ping sensors), and you only get the sensors that you specifically ask for. And, UVexplorer Server automatically keeps your PRTG devices and sensors up-to-date as your network changes (e.g., when new devices are added to the network). In this way, UVexplorer Server helps you configure your PRTG server and keep its configuration up-to-date as your network changes.



Name	IP Address	MAC Address	Description	SNMP OID	Vendor	Notes
switch1102-1	192.168.11.69	D0:67:E5:9C:D3:B1	24G Ethernet Switch	1.3.6.1.4.1.674.10895.3		
switch1121-1	192.168.11.74	D0:67:E5:BF:AD:0B	48G Ethernet Switch	1.3.6.1.4.1.674.10895.3		
switch1134-1	192.168.11.66	D0:67:E5:A7:26:94	48G Ethernet Switch	1.3.6.1.4.1.674.10895.3		
switch1138-1	192.168.11.78	D0:67:E5:A0:6A:D9	48G Ethernet Switch	1.3.6.1.4.1.674.10895.3		
amer-core	192.168.9.1	00:02:41:05:64:44	SS310GR48F Device, Compiled Jul 19 03:21:40 2017 SoftWare Version 7.0.3.0(R0246.0089) BootRom Version 7.2.3 HardWare Version 1.0.2 Serial No.:SW034211EB24000 Copyright (C) 2001-	1.3.6.1.4.1.5929.1.1.2.3		

Select a device to view its details

All Core Devices
switch3308-1.cs.byu.edu
switch2204-2 Paused by dependency
1P_PrintServE10D21 Paused by dependency
switch1057-1.cs.byu.edu
switch2240-1.cs.byu.edu
switch1058-1.cs.byu.edu
switch1029-1
switch1124-1.cs.byu.edu
switch2255-2.cs.byu.edu
switch2255-1.cs.byu.edu
switch3365-1.cs.byu.edu
switch1060-1.cs.byu.edu

Status: OK
Dependency: Parent
Default Interval: every 60 seconds
Last Auto-Discovery: (never)
ID: #32605

Device Group Exported into PRTG

Configuring PRTG Exports

PRTG exports can be configured at any of three levels: discovery, agent, and network. These represent three different levels of visibility within your network. At the discovery level, you can see only the discovery data produced by that discovery. At the agent level, you can see the discovery data produced by all of the agent's discoveries. At the network level, you can see all of the discovery data for the entire network. You can configure PRTG exports at whichever level makes the most sense for you. (PRTG exports are disabled by default, so you must explicitly enable them if you want them.) Regardless of which level you choose, PRTG exports run automatically whenever a discovery run completes that affects the exported data. This keeps your PRTG server configuration constantly up-to-date as new discovery data becomes available.

To configure PRTG export, do the following:

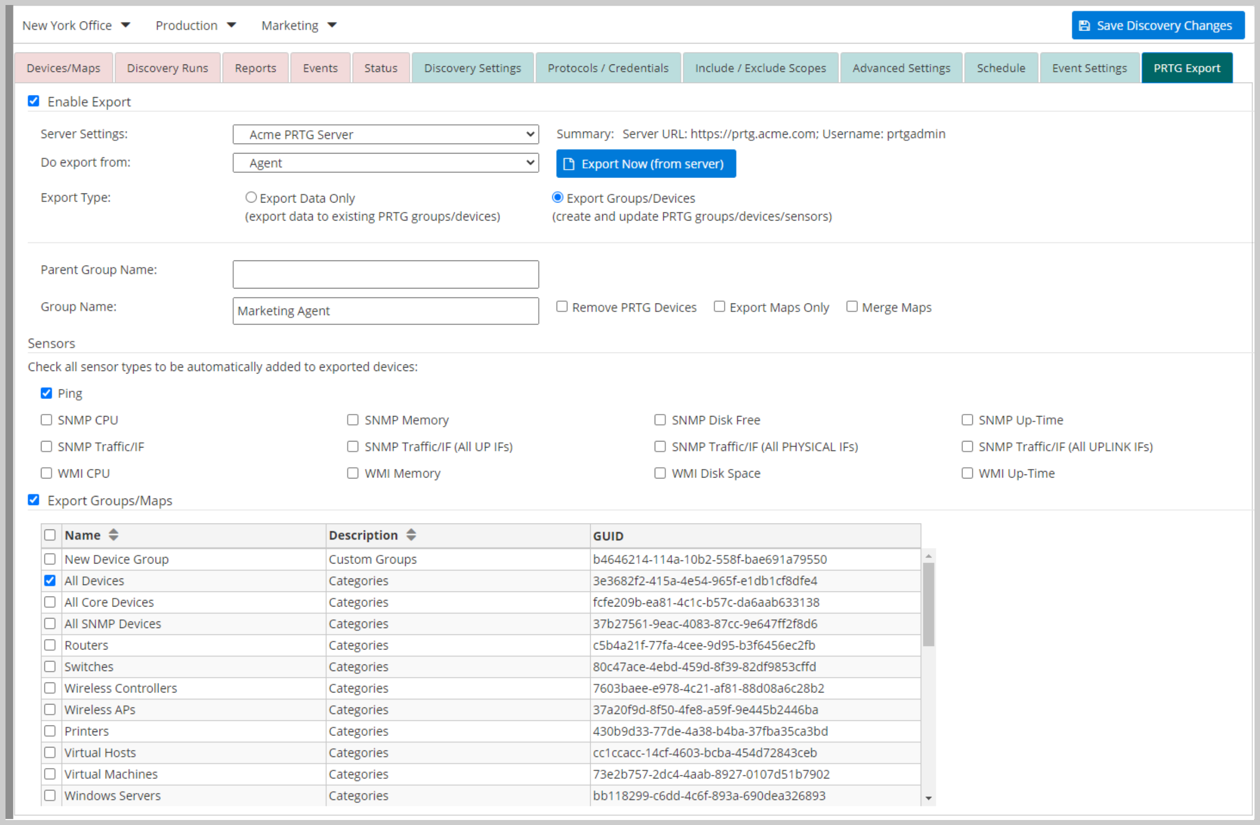
1. Create a PRTG credential UVexplorer Server can use to communicate with your PRTG server. To do this, navigate to the relevant network object, and open the Protocols/Credentials tab. Open the PRTG section in the accordion control, and create a new PRTG credential. Configure the following properties of the credential:
    a. Server URL - your PRTG server's URL. Make sure the URL you enter starts with "http://" if your PRTG server is not using HTTPS, and starts with "https://" if your PRTG server is using HTTPS. Also, be sure to include the correct port number in your URL. Example: https://prtg.acme.com:4000/

b. Username - admin user name for your PRTG server. Example: prtgadmin

c. Passhash - the “passhash” value for your PRTG admin account. To obtain this value, go to the PRTG web console, go to the “Setup” menu, select “Account Settings”, select “My Account”. In the “My Account” page, you will see a field named “Passhash”. Select “Show passhash”, which will display your account’s passhash value. Copy the passhash value into the PRTG credential within the UVexplorer Server console.

d. Be sure to save your changes by clicking the “Save Network Changes” button.

2. After creating your PRTG credential, navigate to any network, agent, or discovery object and open the PRTG Export tab (see the picture below).



☑ Enable Export

Server Settings: Acme PRTG Server

Summary: Server URL: https://prtg.acme.com; Username: prtgadmin

Do export from: Agent

Export Type: ○ Export Data Only (export data to existing PRTG groups/devices) ● Export Groups/Devices (create and update PRTG groups/devices/sensors)

Parent Group Name:

Group Name: Marketing Agent

□ Remove PRTG Devices □ Export Maps Only □ Merge Maps

Sensors

Check all sensor types to be automatically added to exported devices:

☑ Ping

□ SNMP CPU □ SNMP Memory □ SNMP Disk Free □ SNMP Up-Time

□ SNMP Traffic/IF □ SNMP Traffic/IF (All UP IFs) □ SNMP Traffic/IF (All PHYSICAL IFs) □ SNMP Traffic/IF (All UPLINK IFs)

□ WMI CPU □ WMI Memory □ WMI Disk Space □ WMI Up-Time

☑ Export Groups/Maps

□	Name	Description	GUID
□	New Device Group	Custom Groups	b4646214-114a-10b2-558f-bae691a79550
☑	All Devices	Categories	3e3682f2-415a-4e54-965f-e1db1cf8dfe4
□	All Core Devices	Categories	fcfe209b-ea81-4c1c-b57c-da6aab633138
□	All SNMP Devices	Categories	37b27561-9eac-4083-87cc-9e647ff2f8d6
□	Routers	Categories	c5b4a21f-77fa-4cee-9d95-b3f6456ec2fb
□	Switches	Categories	80c47ace-4ebd-459d-8f39-82df9853cffd
□	Wireless Controllers	Categories	7603baee-e978-4c21-af81-88d08a6c28b2
□	Wireless APs	Categories	37a20f9d-8f50-4fe8-a59f-9e445b2446ba
□	Printers	Categories	430b9d33-77de-4a38-b4ba-37fba35ca3bd
□	Virtual Hosts	Categories	cc1ccacc-14cf-4603-bcba-454d72843ceb
□	Virtual Machines	Categories	73e2b757-2dc4-4aab-8927-0107d51b7902
□	Windows Servers	Categories	bb118299-c6dd-4c6f-893a-690dea326893

Configure the following properties:

- ❑ Server Settings - select the PRTG credential you want the export to use when communicating with your PRTG server
- ❑ Do export from - the location from which the PRTG export will be done: UVexplorer Server agent or UVexplorer Server server. Discovery-level exports can be done either from the agent or from the server - it’s your choice. Network and agent-level exports must be done from the server, so this choice is disabled for them.
- ❑ Export Type - select the type of export you want to do. Select “Export Data Only” if you want device details and network maps overlaid on top of your existing PRTG devices

and groups. Select “Export Groups/Devices” if you want UVexplorer Server to create new devices, sensors, and groups in PRTG, in addition to providing device details and network maps.

- Parent Group Name / ID (optional) - the name of an existing PRTG device group that the exported device groups will be placed in. If you want to place the exported device group(s) in a parent group, enter the parent group’s name here. Alternatively, you can enter the PRTG ID of the parent group. This is useful if your PRTG group names are not unique (i.e., used in multiple places). If no parent group is specified, exported groups will be placed within the “Local Probe” PRTG group.
- Group Name (optional) - the name of the exported device group. If this value is provided, the export will create (or update) a PRTG device group with this name that contains ALL of the devices in the network, agent, or discovery. If the network, agent, or discovery contains a lot of devices, this will create a lot of devices in PRTG and it could take a long time, so please be careful when using this option. If you would rather export only a subset of the devices, use the “Export Groups/Maps” feature instead, which is described next. If a Parent Group Name has been specified, the exported device group will be created within the specified parent group.
- Export Groups/Maps (optional) - Select the UVexplorer Server device groups you would like to export into PRTG. This lets you export a subset rather than all devices. If a Parent Group Name has been specified, the exported device groups will be created within the specified parent group.
- Remove PRTG Devices - controls whether PRTG devices that are no longer in the exported device group should be automatically deleted from PRTG, or should be left in PRTG even though they no longer exist on the UVexplorer Server side (thus making the export additive and never subtractive).
- Export Maps Only - export maps to PRTG, but do not create PRTG devices or sensors. This can be used to add UVexplorer Server maps to existing PRTG device groups.
- Merge Maps - when exporting maps, if a previous version of a map already exists in PRTG, merge the new map with the old map rather than replacing the old map.
- Sensors (optional) - select which type of PRTG sensors you want UVexplorer Server to create on exported devices.

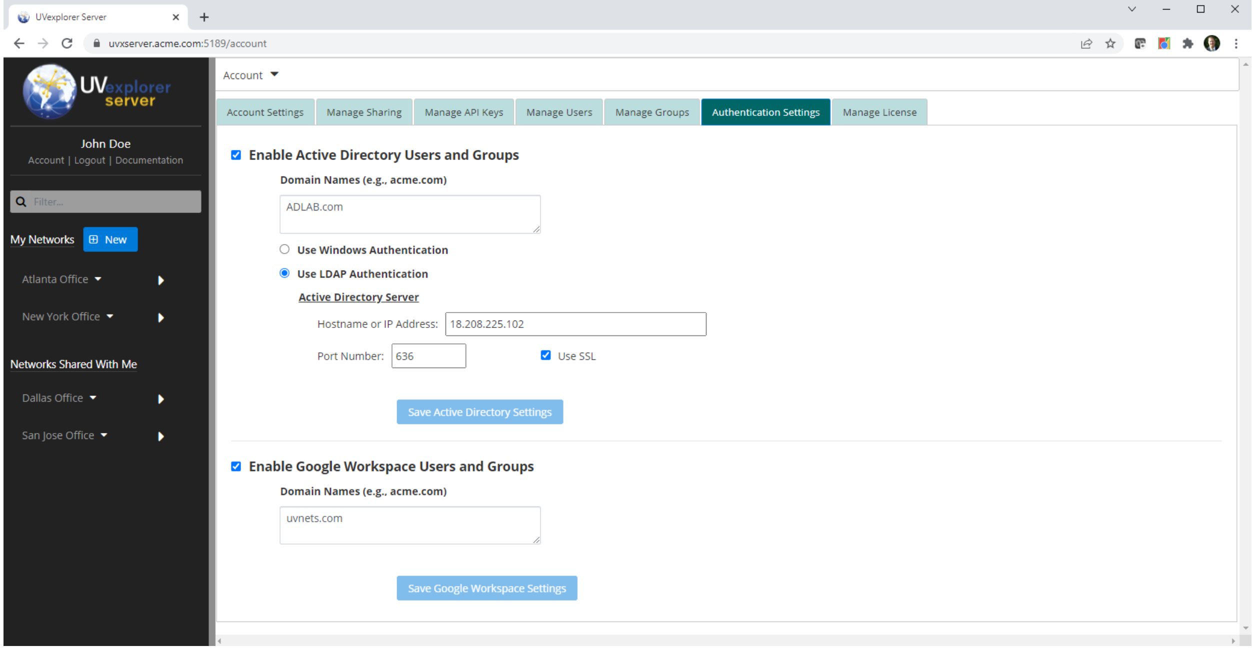
On-Demand Execution of PRTG Exports

As described previously, PRTG exports occur automatically whenever discovery runs complete execution. This automatic, scheduled execution of exports is usually what you want. However, sometimes you will probably want to run a PRTG export immediately rather than waiting for its next scheduled execution. For example, when you configure an export’s settings, you will probably want to test the modified configuration to make sure it works the way you want. To support immediate, on-demand execution of exports, the PRTG Export tab provides a button named “Export Now”. Clicking this button causes the export to be performed immediately.

This is similar to the “Run ASAP” button provided by the Discovery view’s Status tab. For exports that are configured to be run by the agent instead of the server, the discovery “Run ASAP” button is another way to test your PRTG export configuration on-demand. Of course, “Run ASAP” will test both the discovery itself and the PRTG export, while the “Export Now” button will test only the PRTG export. For technical reasons, the “Export Now” feature always performs the export from the UVexplorer Server server, even if the export is configured to normally run on the agent. To test an export performed from the agent, use the discovery “Run ASAP” feature.

Configuring Active Directory and Google Workspace Integration

In addition to its own native user accounts and user groups, UVexplorer Server can also use existing Active Directory and Google Workspace user accounts and groups. By default, Active Directory and Google Workspace integration is disabled. To enable Active Directory and/or Google Workspace integration, select the “Authentication Settings” tab (see picture below).



☑ Enable Active Directory Users and Groups

Domain Names (e.g., acme.com)

ADLAB.com

○ Use Windows Authentication

● Use LDAP Authentication

Active Directory Server

Hostname or IP Address: 18.208.225.102

Port Number: 636 ☑ Use SSL

☑ Enable Google Workspace Users and Groups

Domain Names (e.g., acme.com)

uvnets.com

To configure Active Directory integration, specify the follow properties:

- Domain Names - a list of allowed Active Directory domain names.
- Authentication Type - select the type of authentication that should be used when connecting to Active Directory (Windows Authentication or LDAP Authentication).
- Active Directory Server Hostname or IP Address
- Active Directory Server TCP Port Number
- SSL - indicate whether SSL should be used when communicating with Active Directory.

To configure Google Workspace integration, specify the follow properties:

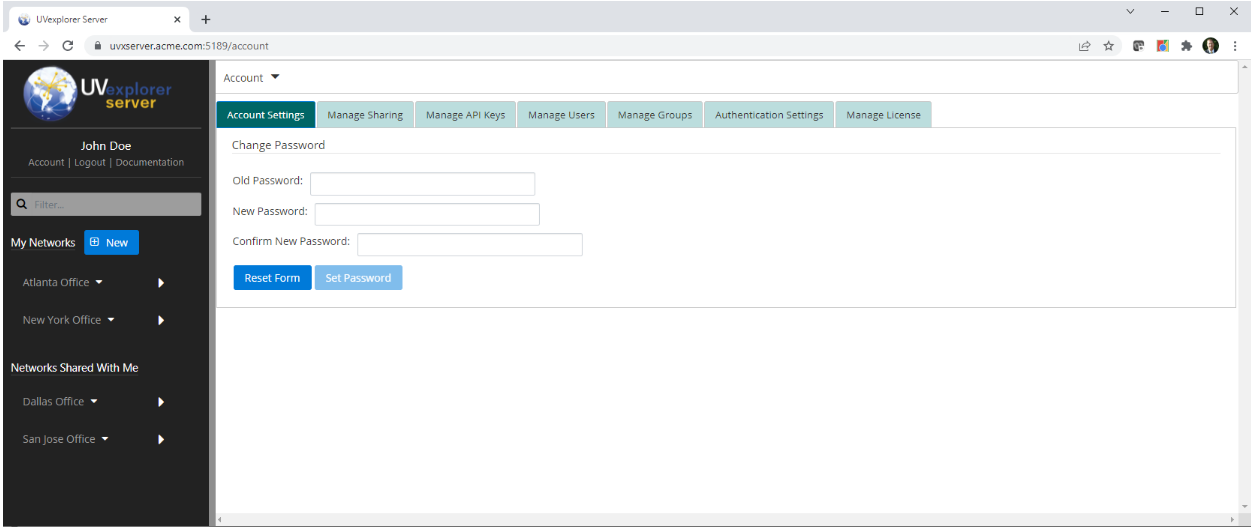
❏ Domain Names - a list of allowed Google Workspace domain names.

Managing User Accounts

When first installed, the UVexplorer Server server has one administrative user account that was created during installation. You can create any number of additional user accounts.

Changing Passwords

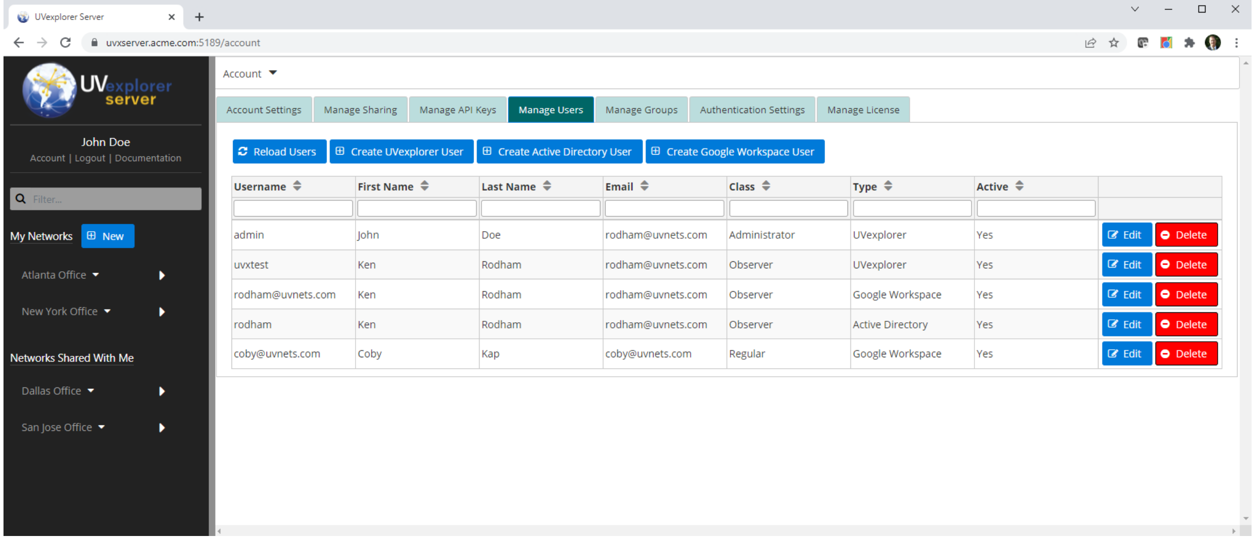
The “Account Settings” tab lets the current user change their own password (see picture below).



Active Directory and Google Workspace users cannot change their passwords through UVexplorer Server. Instead, they should change their passwords through Active Directory or Google Workspace.

Creating, Editing, and Deleting Users

If you are an admin user, you will also see a tab named “Manage Users”. This tab lets you manage user accounts. It lists all existing users, and provides options for creating, editing, and deleting users (see picture below).



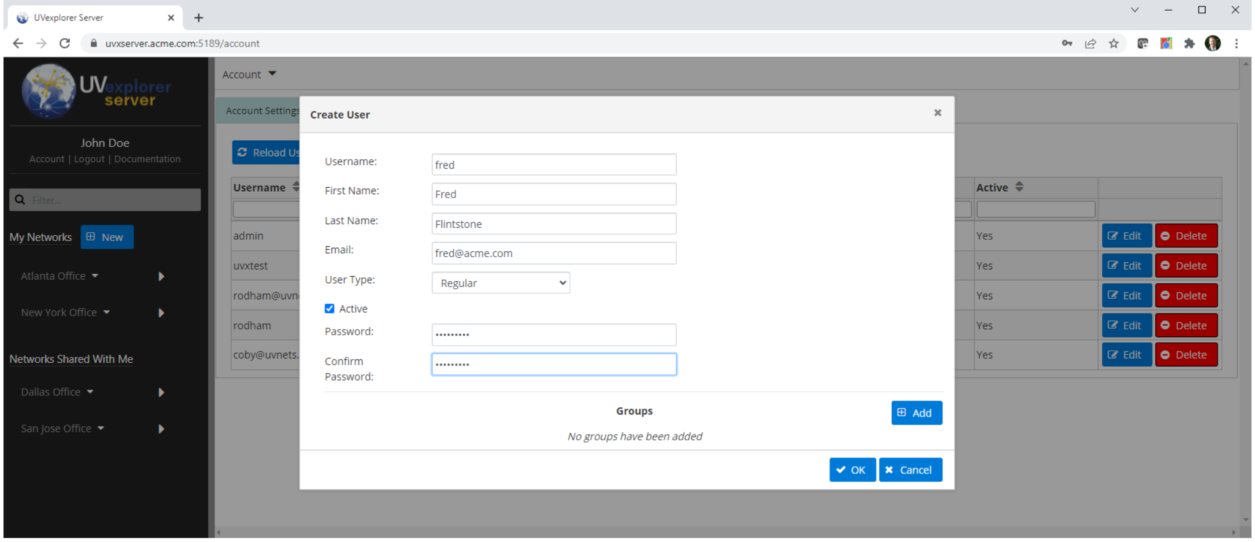
Username	First Name	Last Name	Email	Class	Type	Active	
admin	John	Doe	rodham@uvnets.com	Administrator	UVexplorer	Yes	Edit Delete
uvxtest	Ken	Rodham	rodham@uvnets.com	Observer	UVexplorer	Yes	Edit Delete
rodham@uvnets.com	Ken	Rodham	rodham@uvnets.com	Observer	Google Workspace	Yes	Edit Delete
rodham	Ken	Rodham	rodham@uvnets.com	Observer	Active Directory	Yes	Edit Delete
coby@uvnets.com	Coby	Kap	coby@uvnets.com	Regular	Google Workspace	Yes	Edit Delete

When creating a new user account, the administrator can choose from the following account types:

1. UVexplorer User - a native UVexplorer user account.
2. Active Directory User - a user account that is connected to an Active Directory user account. This type of account allows the user to login using their Active Directory credentials.
3. Google Workspace User - a user account that is connected to a Google Workspace user account. This type of account allows the user to login using their Google Workspace credentials.

UVexplorer Users

To create a new UVexplorer user, click the “Create UVexplorer User” button. This will open a dialog that lets you edit the properties of the new user (see picture below).



Create User

Username: fred

First Name: Fred

Last Name: Flintstone

Email: fred@acme.com

User Type: Regular

☑ Active

Password: •••••••••

Confirm Password: •••••••••

Groups

No groups have been added

User properties include the following:

- Username - the username the user will enter when logging in
- First Name - the user’s first name
- Last Name - the user’s last name
- Email - the user’s email address
- User Type- specifies the type of this user: Observer, Regular, or Administrator.
- Active - whether or not the user is active. A user can login only if their account is active. This setting can be used to temporarily disable a user account.
- Password / Confirm Password - the password the user will enter when logging in
- Groups - by clicking the “Add” button, you can add the new user to one or more user groups.

After configuring the new user’s properties, click the “OK” button to create the user.

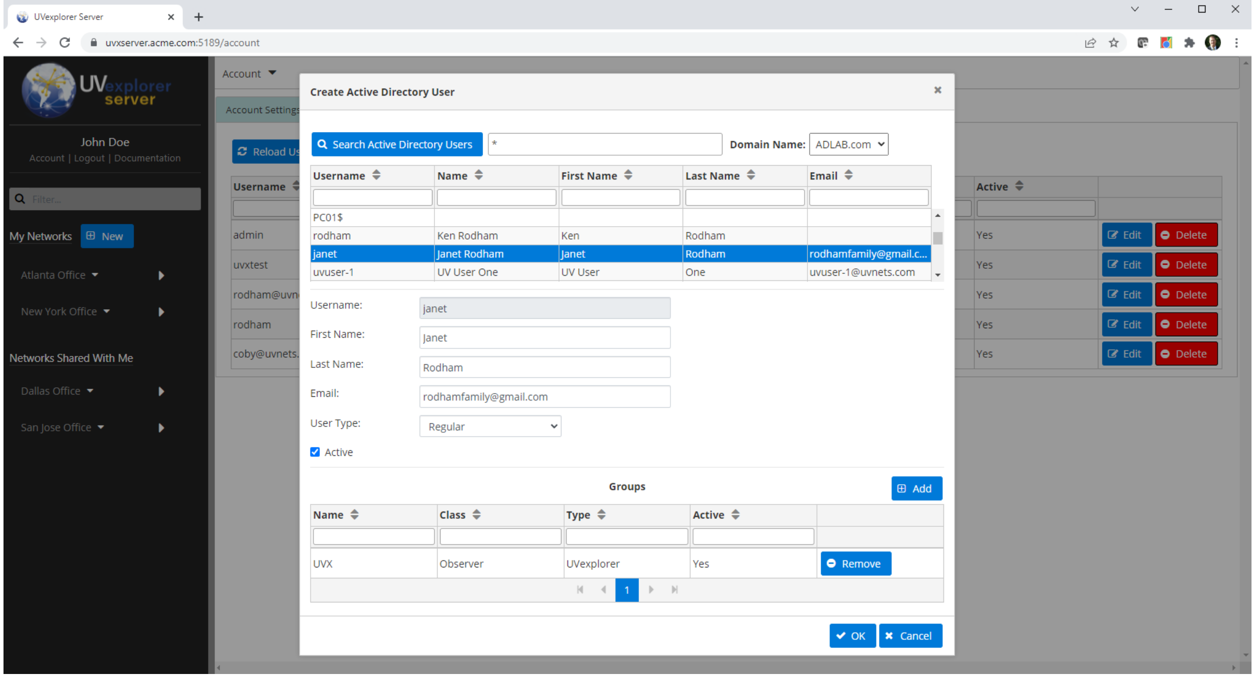
To edit the properties of an existing user, click the user’s “Edit” button. This will display a dialog that lets you modify the user’s properties.

To delete a user, click the user’s “Delete” button.

Active Directory Users

If your organization uses Active Directory, you might prefer to let users access UVexplorer Server using their existing Active Directory accounts. To make this possible, UVexplorer Server is integrated with Active Directory. Specifically, you can create user accounts in UVexplorer that are connected to Active Directory user accounts. This allows users to login to UVexplorer Server using their existing Active Directory credentials.

To create a new Active Directory user, click the “Create Active Directory User” button. You will be asked to enter your Active Directory administrator username and password so UVexplorer Server can read user information from Active Directory. After providing your credentials, a dialog will open that lets you edit the properties of the new user (see picture below).



Create Active Directory User

Search Active Directory Users: * Domain Name: ADLAB.com

Username	Name	First Name	Last Name	Email
PC01$				
rodham	Ken Rodham	Ken	Rodham	
janet	Janet Rodham	Janet	Rodham	rodhamfamily@gmail.c...
uvuser-1	UV User One	UV User	One	uvuser-1@uvnets.com

Username: janet

First Name: Janet

Last Name: Rodham

Email: rodhamfamily@gmail.com

User Type: Regular

☑ Active

Groups

Name	Class	Type	Active	
UVX	Observer	UVexplorer	Yes	Remove

The next step is to search Active Directory for the Active Directory user you want to associate with the new user account. To do this, type in a complete or partial Active Directory username in the search text field, and click the "Search Active Directory Users" button. All Active Directory users that match the search text will be displayed in a list. Next, select a user in the list. This will auto-populate the new user's properties to the extent possible. User properties include the following:

- ❏ Username - the username the user will enter when logging in. This value is read from Active Directory and cannot be edited.
- ❏ First Name - the user's first name. This value is imported from Active Directory, but can be changed if desired.
- ❏ Last Name - the user's last name. This value is imported from Active Directory, but can be changed if desired.
- ❏ Email - the user's email address. This value is imported from Active Directory, but can be changed if desired.
- ❏ User Type- specifies the type of the user: Observer, Regular, or Administrator.
- ❏ Active - whether or not the user is active. A user can login only if their account is active. This setting can be used to temporarily disable a user account.
- ❏ Groups - by clicking the "Add" button, you can add the new user to one or more user groups.

After configuring the new user's properties, click the "OK" button to create the user. Once the user has been created, they will be able to login using their Active Directory credentials.

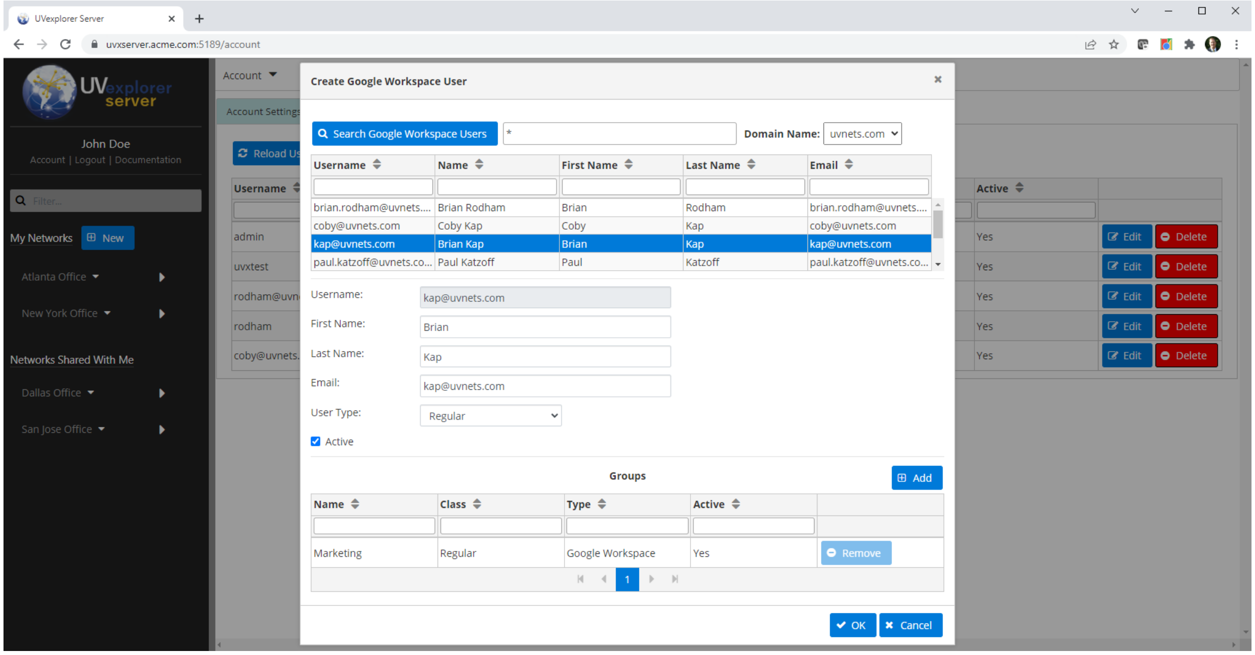
To edit the properties of an Active Directory user, click the user's "Edit" button. This will display a dialog that lets you modify the user's properties. If you change the user's login name in Active Directory, you can sync their login name in UVexplorer by clicking the "Sync User With Active Directory" button in the editing dialog. This will import the new login name from Active Directory into UVexplorer.

To delete an Active Directory user, click the user's "Delete" button.

Google Workspace Users

If your organization uses Google Workspace, you might prefer to let users access UVexplorer Server using their existing Google Workspace accounts. To make this possible, UVexplorer Server is integrated with Google Workspace. Specifically, you can create user accounts in UVexplorer that are connected to Google Workspace user accounts. This allows users to login to UVexplorer Server using their existing Google Workspace credentials.

To create a new Google Workspace user, click the "Create Google Workspace User" button. You will be asked to enter your Google Workspace administrator credentials so UVexplorer Server can read user information from Google Workspace. After providing your credentials, a dialog will open that lets you edit the properties of the new user (see picture below).



Create Google Workspace User

* Domain Name: uvnets.com

Username	Name	First Name	Last Name	Email
brian.rodham@uvnets....	Brian Rodham	Brian	Rodham	brian.rodham@uvnets....
coby@uvnets.com	Coby Kap	Coby	Kap	coby@uvnets.com
kap@uvnets.com	Brian Kap	Brian	Kap	kap@uvnets.com
paul.katzoff@uvnets.co...	Paul Katzoff	Paul	Katzoff	paul.katzoff@uvnets.co...

Username: kap@uvnets.com

First Name: Brian

Last Name: Kap

Email: kap@uvnets.com

User Type: Regular

☑ Active

Groups

Name	Class	Type	Active	
Marketing	Regular	Google Workspace	Yes	Remove

The next step is to search Google Workspace for theGoogle Workspace user you want to associate with the new user account. To do this, type in a complete or partial Google Workspace username in the search text field, and click the "Search Google Workspace Users" button. All Google Workspace users that match the search text will be displayed in a list. Next, select a user in the list. This will auto-populate the new user’s properties to the extent possible. User properties include the following:

- ❏ Username - the username the user will enter when logging in. This value is read from Google Workspace and cannot be edited.
- ❏ First Name - the user’s first name. This value is imported from Google Workspace, but can be changed if desired.
- ❏ Last Name - the user’s last name. This value is imported from Google Workspace, but can be changed if desired.
- ❏ Email - the user’s email address. This value is imported from Google Workspace, but can be changed if desired.
- ❏ User Type- specifies the type of this user: Observer, Regular, or Administrator.
- ❏ Active - whether or not the user is active. A user can login only if their account is active. This setting can be used to temporarily disable a user account.
- ❏ Groups - by clicking the “Add” button, you can add the new user to one or more user groups.

After configuring the new user’s properties, click the “OK” button to create the user. Once the user has been created, they will be able to login using their Google Workspace credentials.

To edit the properties of a Google Workspace user, click the user’s “Edit” button. This will display a dialog that lets you modify the user’s properties. If you change the user’s login name in Google Workspace, you can sync their login name in UVexplorer by clicking the “Sync User With Google Workspace” button in the editing dialog. This will import the new login name from Google Workspace into UVexplorer.

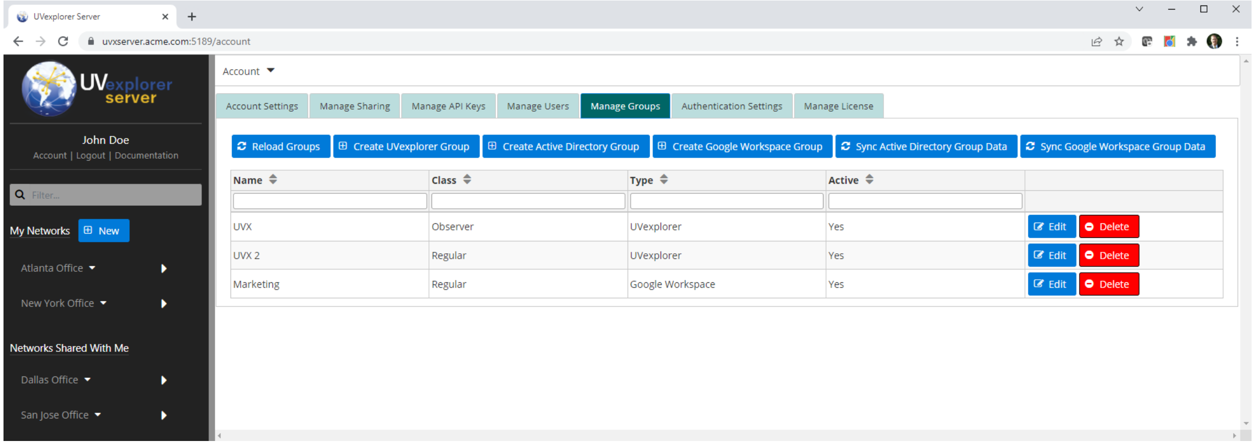
To delete a Google Workspace user, click the user’s “Delete” button.

Managing User Groups

In addition to creating individual user accounts, you can also create user groups to make it easier to manage user capabilities and network sharing on a group basis.

Creating, Editing, and Deleting Groups

If you are an admin user, you will also see a tab named “Manage Groups”. This tab lets you manage user groups. It lists all existing groups, and provides options for creating, editing, and deleting groups (see picture below).



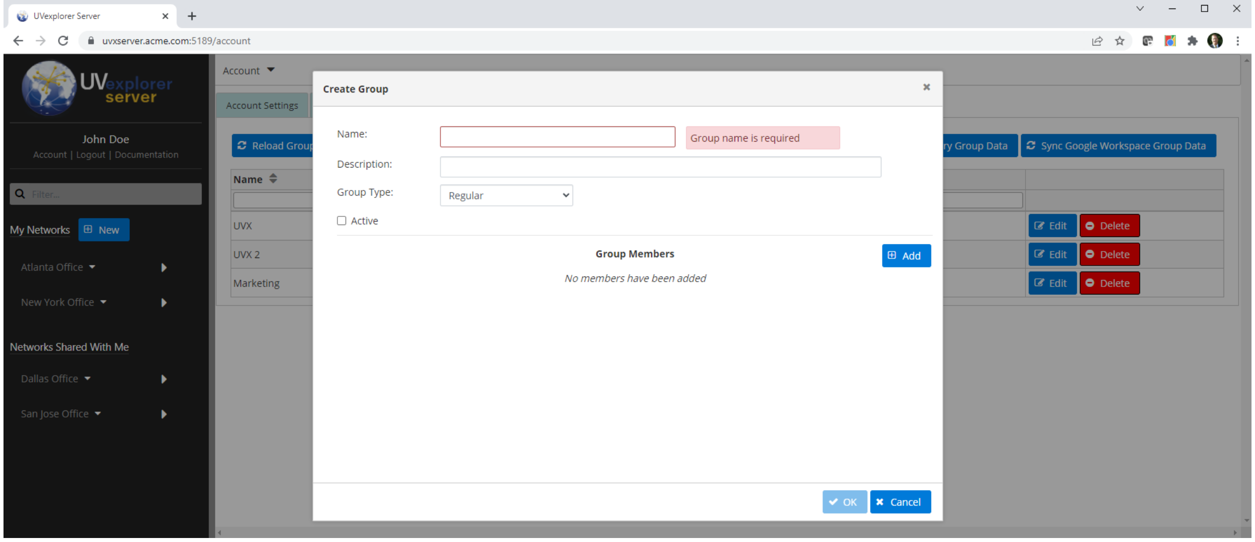
Name	Class	Type	Active	
UVX	Observer	UVexplorer	Yes	Edit Delete
UVX 2	Regular	UVexplorer	Yes	Edit Delete
Marketing	Regular	Google Workspace	Yes	Edit Delete

When creating a new group, the administrator can choose from the following group types:

1. UVexplorer Group - a native UVexplorer group.
2. Active Directory Group- a group that is connected to an Active Directory group. For this type of group, group membership is managed through Active Directory.
3. Google Workspace Group- a group that is connected to a Google Workspace group. For this type of group, group membership is managed through Google Workspace.

UVexplorer Groups

To create a new UVexplorer group, click the “Create UVexplorer Group” button. This will open a dialog that lets you edit the properties of the new group (see picture below).



Create Group

Name: Group name is required

Description:

Group Type: Regular

□ Active

Group Members

No members have been added

User properties include the following:

❑ Name - the group’s name

❑ Description - a description of the group’s purpose

- ❏ Group Type- specifies the type of this group: Observer, Regular, or Administrator. Users that are members of this group inherit this group type (in addition to their own type).
- ❏ Active - whether or not the group is active. If the group is inactive, it is as if it doesn't exist and has no effect on its member users. This setting can be used to temporarily disable a group.
- ❏ Group Members - by clicking the "Add" button, you can add users to the group.

After configuring the new group's properties, click the "OK" button to create the group.

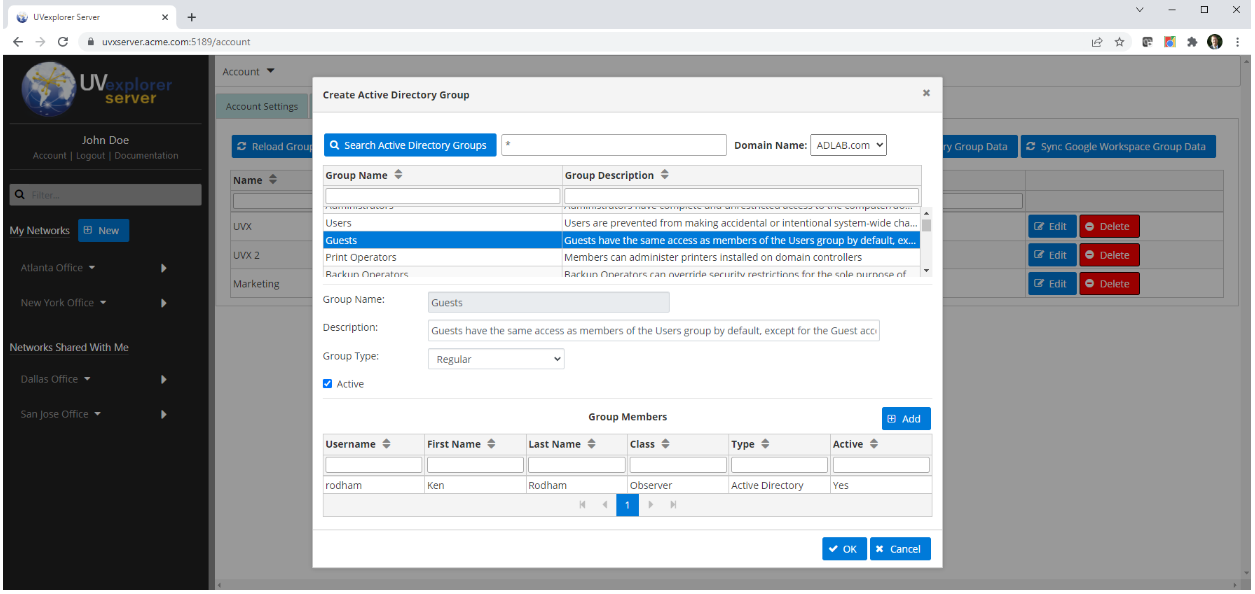
To edit the properties of an existing group, click the group's "Edit" button. This will display a dialog that lets you modify the group's properties.

To delete a group, click the group's "Delete" button.

Active Directory Groups

If your organization uses Active Directory, you might prefer to use groups that already exist in Active Directory. To make this possible, UVexplorer Server is integrated with Active Directory. Specifically, you can create groups in UVexplorer that are connected to Active Directory groups. This allows you to manage group membership through Active Directory.

To create a new Active Directory group, click the "Create Active Directory Group" button. You will be asked to enter your Active Directory administrator credentials so UVexplorer Server can read group information from Active Directory. After providing your credentials, a dialog will open that lets you edit the properties of the new group (see picture below).



Create Active Directory Group ×

Search Active Directory Groups | * | Domain Name: ADLAB.com

Group Name	Group Description
Administrators	Administrators have complete and unrestricted access to the computer/do...
Users	Users are prevented from making accidental or intentional system-wide cha...
Guests	Guests have the same access as members of the Users group by default, ex...
Print Operators	Members can administer printers installed on domain controllers
Backup Operators	Backup Operators can override security restrictions for the sole purpose of

Group Name: Guests

Description: Guests have the same access as members of the Users group by default, except for the Guest acc

Group Type: Regular

☑ Active

Group Members | Add

Username	First Name	Last Name	Class	Type	Active
rodham	Ken	Rodham	Observer	Active Directory	Yes

1

✔ OK | ✖ Cancel

The next step is to search Active Directory for the Active Directory group you want to associate with the new group. To do this, enter a complete or partial Active Directory group name in the search text field, and click the “Search Active Directory Groups” button. All Active Directory groups that match the search text will be displayed in a list. Next, select a group in the list. This will auto-populate the new group’s properties to the extent possible. Group properties include the following:

- ❏ Group Name - the group’s name. This value is read from Active Directory and cannot be edited.
- ❏ Description - a description of the group’s purpose. This value is imported from Active Directory, but can be changed if desired.
- ❏ Group Type- specifies the type of the group: Observer, Regular, or Administrator. Users that are members of this group inherit this group type (in addition to their own type).
- ❏ Active - whether or not the group is active. If the group is inactive, it is as if it doesn’t exist and has no effect on its member users. This setting can be used to temporarily disable a group.
- ❏ Group Members - the group’s member users. An Active Directory group can only include Active Directory users. Because group membership is managed in Active Directory, a new Active Directory group may already have member users (i.e., if Active Directory users that are in the group have already been created in UVexplorer). To add new members to an Active Directory group, click the “Add” button. This will display a dialog that lets you create Active Directory users for the group’s members that do not yet have corresponding users in UVexplorer.

After configuring the new group’s properties, click the “OK” button to create the group.

To edit the properties of an Active Directory group, click the group’s “Edit” button. This will display a dialog that lets you modify the group’s properties. If you change the group’s name in Active Directory, you can sync its name in UVexplorer by clicking the “Sync Group With Active Directory” button in the editing dialog. This will import the new name from Active Directory into UVexplorer.

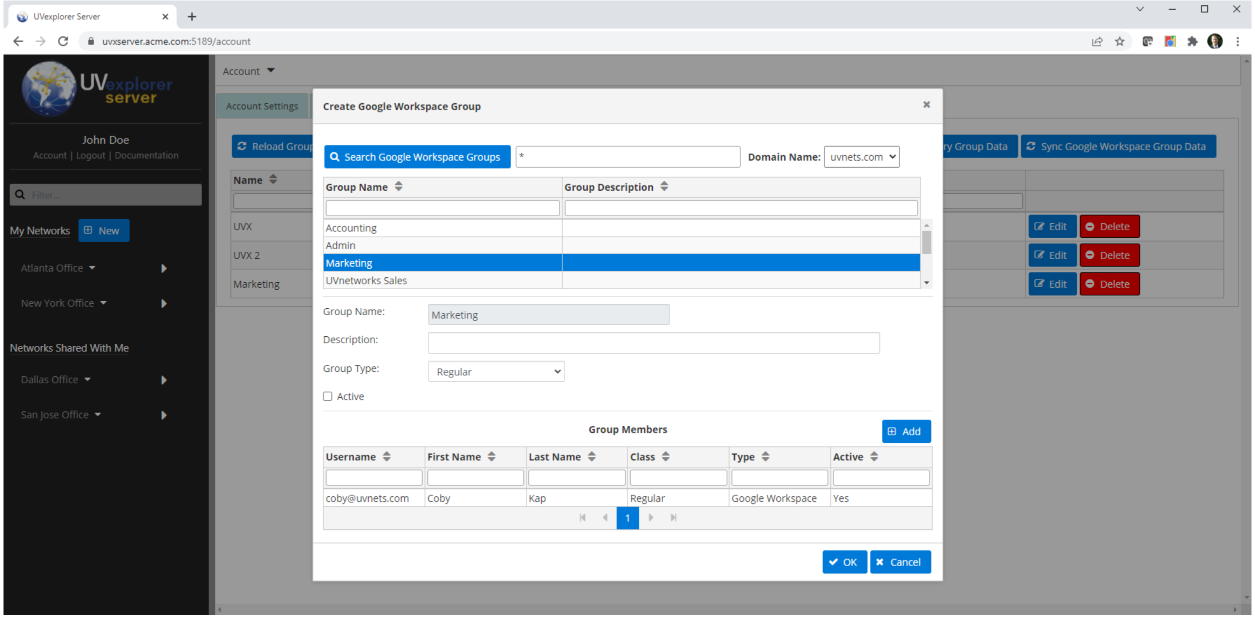
To delete an Active Directory group, click the group’s “Delete” button.

Google Workspace Groups

If your organization uses Google Workspace, you might prefer to use groups that already exist in Google Workspace. To make this possible, UVexplorer Server is integrated with Google Workspace. Specifically, you can create groups in UVexplorer that are connected to Google Workspace groups. This allows you to manage group membership through Google Workspace.

To create a new Google Workspace group, click the “Create Google Workspace Group” button. You will be asked to enter your Google Workspace administrator credentials so UVexplorer

Server can read group information from Google Workspace. After providing your credentials, a dialog will open that lets you edit the properties of the new group (see picture below).



Create Google Workspace Group

*

Domain Name: uvnets.com

Group Name	Group Description
Accounting	
Admin	
Marketing	
UVnetworks Sales	

Group Name: Marketing

Description:

Group Type: Regular

☐ Active

Group Members

Username	First Name	Last Name	Class	Type	Active
coby@uvnets.com	Coby	Kap	Regular	Google Workspace	Yes

The next step is to search Google Workspace for the Google Workspace group you want to associate with the new group. To do this, enter a complete or partial Google Workspace group name in the search text field, and click the “Search Google Workspace Groups” button. All Google Workspace groups that match the search text will be displayed in a list. Next, select a group in the list. This will auto-populate the new group’s properties to the extent possible. Group properties include the following:

❑ Group Name - the group’s name. This value is read from Google Workspace and cannot be edited.

❑ Description - a description of the group’s purpose. This value is imported from Google Workspace, but can be changed if desired.

❑ Group Type- specifies the type of the group: Observer, Regular, or Administrator. Users that are members of this group inherit this group type (in addition to their own type).

❑ Active - whether or not the group is active. If the group is inactive, it is as if it doesn’t exist and has no effect on its member users. This setting can be used to temporarily disable a group.

❑ Group Members - the group’s member users. A Google Workspace group can only include Google Workspace users. Because group membership is managed in Google Workspace, a new Google Workspace group may already have member users (i.e., if Google Workspace users that are in the group have already been created in UVexplorer). To add new members to a Google Workspace group, click the “Add” button. This will display a dialog that lets you create Google Workspace users for the group’s members that do not yet have corresponding users in UVexplorer.

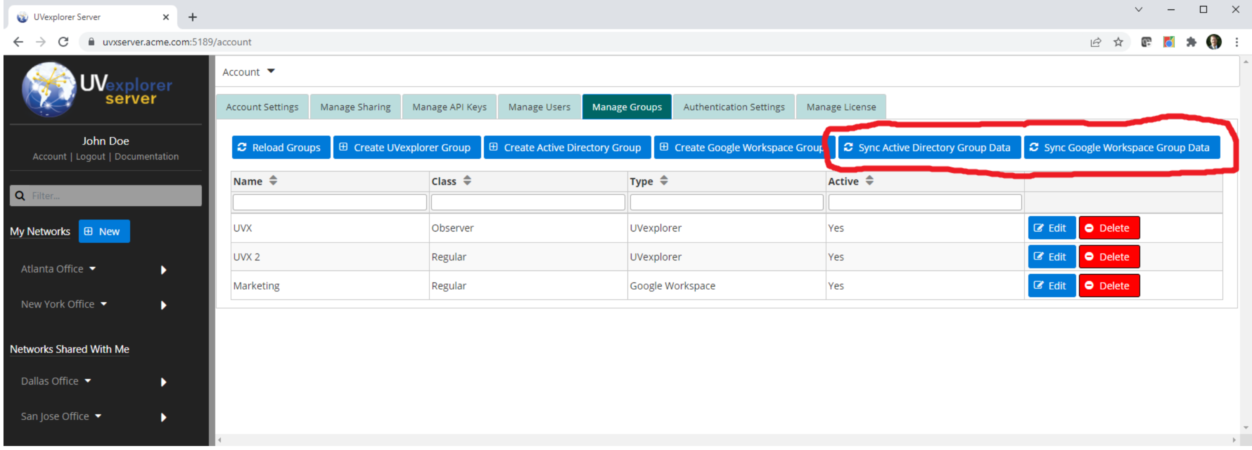
After configuring the new group’s properties, click the “OK” button to create the group.

To edit the properties of a Google Workspace group, click the group’s “Edit” button. This will display a dialog that lets you modify the group’s properties. If you change the group’s name in Google Workspace, you can sync its name in UVexplorer by clicking the “Sync Group With Google Workspace” button in the editing dialog. This will import the new name from Google Workspace into UVexplorer.

To delete a Google Workspace group, click the group’s “Delete” button.

Syncing Active Directory and Google Workspace Group Data

To improve performance, UVexplorer Server caches information about Active Directory and Google Workspace groups in its database. This information is periodically refreshed from Active Directory and Google Workspace to keep it up-to-date. However, when you modify groups and/or group memberships in Active Directory or Google Workspace, UVexplorer’s cached group information will be out-of-date until the next time it refreshes the data. To force UVexplorer to immediately refresh the cached group data, click the “Sync Active Directory Group Data” or “Sync Google Workspace Group Data” button in the “Manage Groups” tab (see picture below).

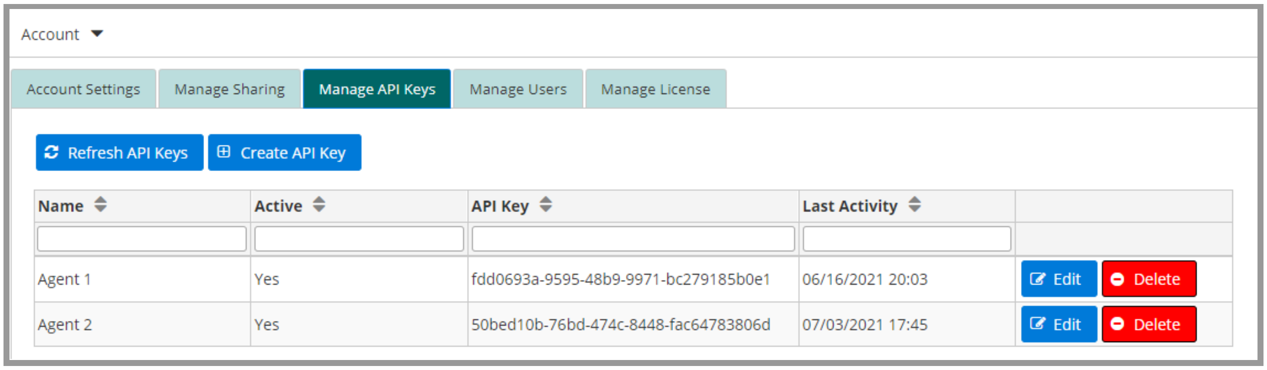


Name	Class	Type	Active	
UVX	Observer	UVexplorer	Yes	Edit Delete
UVX 2	Regular	UVexplorer	Yes	Edit Delete
Marketing	Regular	Google Workspace	Yes	Edit Delete

Managing Web API Keys

A UVexplorer agent uses an API key to authenticate with the server when posting discovery and monitor data to the server. Therefore, when registering an agent with the server you must provide the API key the agent should use when calling the server’s Web API. As described below, within each user account you may create zero or more API keys. Each API key is bound to the user account under which it was created. When an agent calls the server’s Web API, it must provide its API key to identify which user account it belongs to. You can use one API key for all of a user’s agents, or you can assign a unique API key to each agent (recommended).

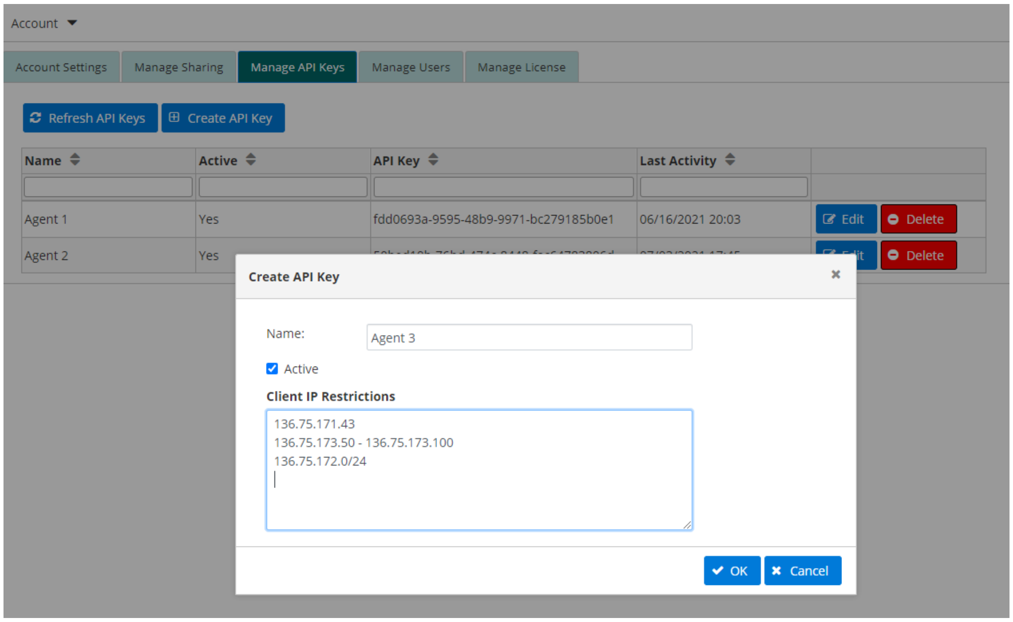
To view the logged-in user’s API keys, click the “Account” link at the top of the navigation bar on the left side of the UVexplorer Server window, and select the “Manage API Keys” tab. This tab lets you view, create, edit, and delete API keys (see picture below).



Name	Active	API Key	Last Activity
Agent 1	Yes	fdd0693a-9595-48b9-9971-bc279185b0e1	06/16/2021 20:03
Agent 2	Yes	50bed10b-76bd-474c-8448-fac64783806d	07/03/2021 17:45

To create a new API key, click the “Create API Key” button. A dialog will appear that lets you configure the following settings on the new API key (see picture below):

- Name - a descriptive name for the API key.
- Active - check this box to activate the API key, or leave it unchecked to leave it inactive. An inactive key will not work, so this property can be used to turn a key’s access on or off.
- Client IP Restrictions - if you want to restrict the client IP addresses from which the API key can be used, enter valid client IP addresses in the Client IP Restrictions field. You can enter single IP addresses, IP address ranges, and/or IP subnets.



Create API Key

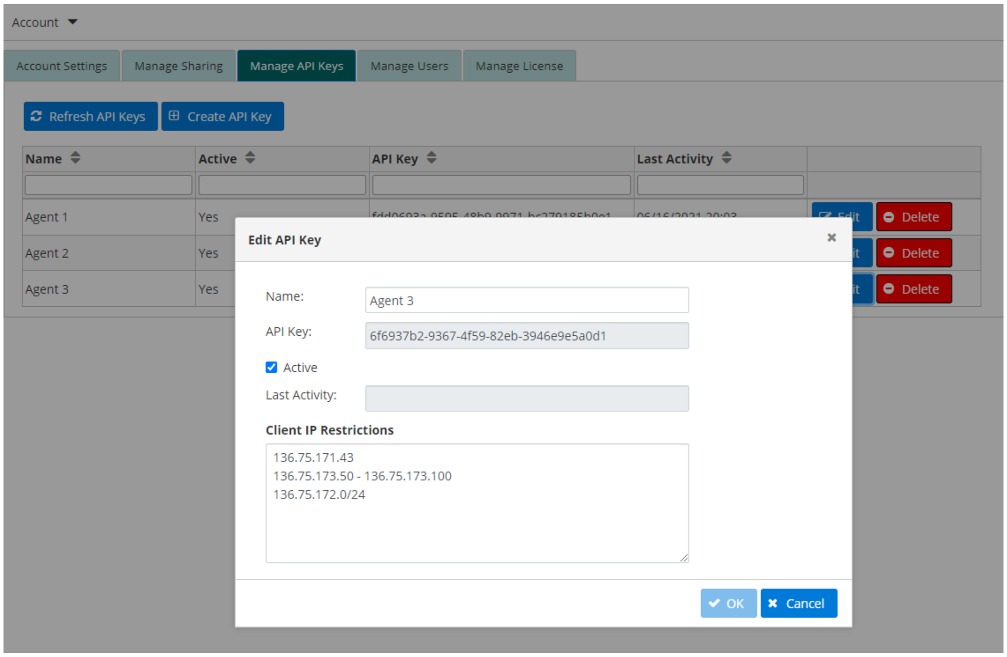
Name: Agent 3

☑ Active

Client IP Restrictions

```
136.75.171.43
136.75.173.50 - 136.75.173.100
136.75.172.0/24
```

To edit an existing API key, click the “Edit” button next to the key in the key list. To delete an existing API key, click the “Delete” button next to the key in the key list. When you click “Edit”, a dialog will appear that lets you edit the properties of the selected key (see picture below). You can change a key’s name, client IP restrictions, and active/inactive status.



Name	Active	API Key	Last Activity
Agent 1	Yes		
Agent 2	Yes		
Agent 3	Yes		

Edit API Key

Name: Agent 3

API Key: 6f6937b2-9367-4f59-82eb-3946e9e5a0d1

☑ Active

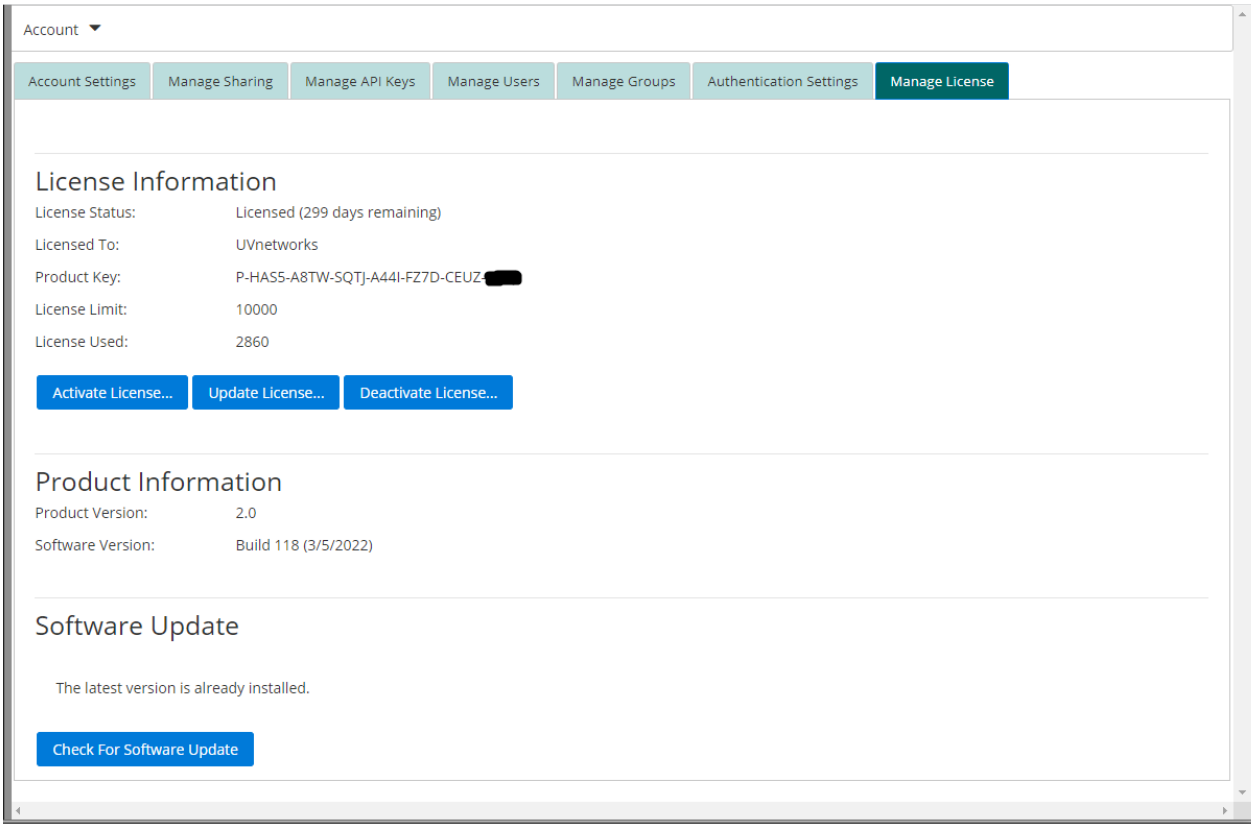
Last Activity:

Client IP Restrictions

136.75.171.43
136.75.173.50 - 136.75.173.100
136.75.172.0/24

Managing Your UVexplorer Server License

In order to use UVexplorer Server, you must activate your UVexplorer Server license by entering the license key you received when you downloaded the product. License management features are accessed by clicking the “Account” link at the top of the navigation bar on the left side of the UVexplorer Server window. The “Manage License” tab displays the current status of your license, and allows you to activate, update, and deactivate your license (see picture below).



License Information

License Status: Licensed (299 days remaining)

Licensed To: UVnetworks

Product Key: P-HAS5-A8TW-SQTJ-A44I-FZ7D-CEUZ-[redacted]

License Limit: 10000

License Used: 2860

Product Information

Product Version: 2.0

Software Version: Build 118 (3/5/2022)

Software Update

The latest version is already installed.

The following license properties are shown:

- License Status- the current status of the license (activation status, days remaining, etc.)
- Licensed To - the name of the person or organization associated with the license
- Product Key - the product key for the license
- License Limit - the maximum number of network interfaces allowed by the license
- License Used - the number of network interfaces currently in the UVexplorer Server database

Clicking the “Activate License” button runs the license activation wizard, which steps you through the process of activating your UVexplorer Server license. This requires that you have the product license key you received when you downloaded the product.

Clicking the “Update License” button runs the license update wizard, which steps you through the process of retrieving your license information from the UVexplorer Server licensing server. This is useful when the details of your license have changed, such as when you extend your license or purchase additional devices.

Clicking the “Deactivate License” button runs the license deactivation wizard, which steps you through the process of deactivating your license.

If your UVexplorer Server license is invalid, the product goes into a read-only mode where you can view data that is already in the database, but agents will not be able to add new data to the database (discovery results and monitor data). An invalid license also prevents you from registering new agents with the server. Conditions that cause a license to be invalid include:

1. The license has not been activated
2. The license has expired
3. The license limit has been exceeded (number of discovered network interfaces)

If your license has expired or your license limit has been exceeded, you can contact UVnetworks customer support to extend or upgrade your license. Once your license has been extended or upgraded, you should click the “Update License” button to refresh the license on your server.

Product Information

In the “Manage License” tab you can also view product version information. This information is useful when updating your UVexplorer Server installation or getting customer support.

Software Update

The “Manage License” tab also tells you whether there is a new version of UVexplorer Server available. If there is a new version, it also gives you instructions on how to install the new version.

Start Menu Items

The UVexplorer Server installer creates a Start Menu folder named “UVexplorer Server 2.0” on the server computer that contains several useful items, including the following:

Open Logs

This start menu item opens the UVexplorer Server log files in Notepad. This can be useful when troubleshooting problems with your server.

Open UvxAdmin Window

UvxAdmin is a command-line tool for configuring UVexplorer Server. The installer uses this tool internally to configure the server, but you can also use it to configure the server from the command-line. This start menu item will open a command prompt that can be used to run UvxAdmin commands.

Open Web Console

This start menu item will open the UVexplorer Server web console in a browser.

Stop UVexplorer Server

This start menu item will stop the UVexplorer Server services.

Start UVexplorer Server

This start menu item will start the UVexplorer Server services.

Uninstall UVexplorer Server

This start menu item will uninstall UVexplorer Server.