



NetObserver™


Operational Manual

Network Health

Monitoring Software

Release V.100

Section 1: About This Manual

Copyright	Copyright ©2020 Vigitron, Inc. All rights reserved. The products and programs described in this User's Manual are licensed products of Vigitron Inc. This User's Manual contains proprietary information protected by copyright. This User's Manual and all accompanying hardware, software, and documentation are copyrighted. No parts of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. This includes photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Vigitron, Inc.
Purpose	This Manual gives specific information on how to operate and use the management functions of NetObserver Vi3000 V1.00.
Audience	The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment. Consequently, it assumes a basic working knowledge of general network communication, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).
Conventions	<p>The following conventions are used throughout this guide to show information:</p> <div style="display: flex; align-items: center;"><div style="margin-right: 10px;"></div><div><hr/>NOTE: Emphasizes important information or calls your attention to related features or instructions.<hr/></div></div>
Warranty	See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to your manufacture products and replacement parts can be obtained from Vigitron, Inc.
Disclaimer	Vigitron, Inc. does not warrant that the software will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Vigitron disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of Vigitron. Vigitron assumes no responsibility for any inaccuracies that may be contained in this User's Manual. Vigitron makes no commitment to update or keep current the information in this User's Manual, and reserves the rights to make improvements to this User's Manual and/or to the products described in this User's manual at any time without notice.

Software Acceptance Terms and Conditions Release of Liability

Acknowledgement:

By installing the software, you acknowledge that you have read and understand the foregoing and that you agree to be bound by its terms and conditions. You also agree that this agreement is the complete and exclusive statement of agreement between the parties and supersedes all proposed or prior agreements, oral or written, and any other communications between the parties relating to the license described herein.

Grant of License:

License for software use is hereby granted to user only provided purchase has been made from an authorized Vigitron dealer or authorized hereby authorized by Vigitron. License is not transferable and is limited to usage only. No permission is hereby given or granted to make any change, modifications and is restricted only for its intended usage. Operation or usage other than described will be considered as a violation of intended use.

Disclaimer of Warranty:

Software is provided As Is with all faults. To the extent permitted by law, Vigitron, its dealers, distributors and other appointed agencies hereby disclaim all warranties, whether expressed or implied, including and without limitations warranties that the product is free of defects, merchantability and fit for a particular purpose and non-infringing. You agree to bear the entire risk as to selection the proper for your purpose and as to the quality and performance of the product.

Limitation of Liability:

Except as required by law, Vigitron and its distributors, directors, licensors, contributors, agents and all associated in with Vigitron in connection with the said software will not be liable for any damages arising out of or in any way relating to this product and/or agreement the inability arising out of or in any way relating to this agreement or the use of the product, and those products associated with said use of products, including limitation damages for loss of physical property, goodwill, work stoppage, lost profits, loss of data and computer failure or malfunction. Even if advised as the potential from such loss or damage regardless of the theory applied of contract, tort or otherwise, which claims are based. Vigitron, its associates and all others collective liability will be limited to the cost of the product itself.

Arbitration:

Any disagreement between the parties relating to any interpretation, construction, performance or breach of this Agreement shall be settled by arbitration to be held in San Diego Country, California, in accordance with the laws of the State of California in accordance with the rules then in effect of the American Arbitration Association. The arbitrator may grant injunctions or other relief in such dispute or controversy. The decision of the arbitrator shall be final, conclusive and binding on the parties to the arbitration. Judgment may be entered on the arbitrator's decision in any court having jurisdiction. The party bring arbitration agrees to incur the total costs and expenses of such arbitration and shall pay their counsel fees and expenses.

Miscellaneous:

This Agreement constitutes the entire agreement between Vigitron and you, concerning the subject matter hereof, and it may only be modified by a written amendment signed by an authorized executive of Vigitron. You further agree that NetObserver is only licensed to be used on one computer/server

Except to the extent applicable law, if any, provides otherwise, this Agreement will be governed by the laws of the state of California, U.S.A., excluding its conflict of law provisions. It is further agreed that if one or more provision of this agreement are held to be illegal or unenforceable under applicable California law, such illegal or unenforceable portion(s) shall be limited or excluded from this Agreement to the minimum extent required that this Agreement shall otherwise remain in full force and effect and enforceable in accordance with its terms.

This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods.

If any part of this Agreement is held invalid or unenforceable, that part will be construed to reflect the parties' original intent, and the remaining portions will remain in full force and effect.

A waiver by either party of any term or condition of this agreement or any breach thereof, in any one instance, will not waive such term or condition or any subsequent breach thereof.

Except as required by law, the controlling language of this Agreement is English.

You may assign your rights under this Agreement to any party that consents to, and agrees to be bound by, its terms; Vigitron may assign its rights under this Agreement without condition.

This Agreement will be binding upon and will inure to the benefit of the parties, their successors and permitted assigns.

SQL CE Requirements for NetObserver

In order to provide full functionality for the device library, NetObserver requires management of a relational database. Due to the need for portability of the library and the program configuration, the Application Programming Interface used to manage the database is Microsoft's SQL Server Compact 4.0. The installation of SQL CE 4.0 is automatically included in the NetObserver installer. The user will be prompted to accept installation of SQL CE 4.0 upon installation of NetObserver, only in the event the host computer does not already have it installed.

Section 2: Introduction

Overview

This user's manual will not only tell you how to install and connect your network system, but how to configure and monitor your computer to receive messages from various network devices

NetObserver is a next generation health monitoring Windows™ based software capable of receiving status messages from up to 240,000 ports using TCP, UDP, Syslog and SNMP communications. NetObserver recognizes network connected devices by means of Onvif, UPnP and also allows for manual entry.

Key Features:

- User Configuration: Enter usernames, passwords, assign operational and viewing rights
- Create a device library of network devices, apply naming conventions
- Create message data bases, customize with user entries
- Built in test generator for confirming communications and network status
- Upload site maps using various formats
- Choose from an icon library or create your own
- Overlay annunciated icon to note warnings and communication failures
- Set ranges for alerts
- Send alerts via private and public email settings

Note: *In order to register your program your computer must be connected to a network.*

Notes on Onvif and UPnP Discover:

1. The use of Onvif or UPnP requires the connected device be able to respond to requests from either.
2. IP Address will be discovered using either Onvif or UPnP.
3. Manufacturer - Onvif requires previous device user name and password access/ UPnP does not.
4. Model Number - Onvif requires previous device user name and password access/ UPnP does not.
5. Mac Address – Onvif requires user name and password access. UPnP does not recover MAC address.

Note: *Map and Topographical Map alerts will change from Green (normal) to Red (Alert). The alert is triggered by a ping or receiving an alert via SNMP/TCPUDP/Syslog.*

- To active alerts- pings must be set to be repetitive.
- If an alert is triggered by SNMP/TCP/UDP/syslog- the alert must be cleared to return to the normal state.

Warning: After you have set up alerts do not disconnect your Network connections without properly exiting NetObserver. This may result in generating multiple alerts

(Table of Contents needs to be updated – when manual is finalized)

Overview of This User’s Manual:

Section 1: About This Manual 2

Section 2: Introduction 2

Section 3: Operation of Software Management and Device Interface..... 2

Section 4: NetObserver Main and Submenus..... 2

Section 5: Installation 2

Section 6: Login..... 2

Section 7: Intro Screens 2

Section 8: User Configuration 2

Section 9: Device Library..... 2

Section 10: NetStat 2

Section 11: Test Generator 2

Section 12: Mapping 2

Section 13: Topology..... 2

Section 14: Alerts..... 2

Section 15: Email Settings 2

Section 16: Logs 2

Section 17: Recovery..... 2

Section 18: Log Out – Run in Background..... 2

Section 3: Operation of Software Management and Device Interface

This chapter instructs you on how to configure and manage NetObserver™ with your network connected devices. Once set up you will be able to receive messages using several different means of communication.

When starting your set up, it is important:

1. Your computer must be on the same network as the connect devices or routed to receive messages from the connected devices.
2. Your devices must be properly programmed to send messages to the client computer running NetObserver.
3. Your client computer must not block transmissions from ports used to communicate from connected devices.
4. If your device has set ups for UDP and TCP Transmission configure these to match the receiving port

Client Computer:

The screenshot shows a configuration window with three main sections:

- Switch Naming:** Includes a 'Switch Name' field with 'TestSwitch' entered. A note states: 'Enter a name for the switch to serve as a prepended identifier in the UDP and TCP alerts. If name field is left empty, alert messages will begin with IP Address of the switch.'
- UDP Alerts:** Features a dropdown menu set to 'Enable', a radio button for 'Broadcast', and a 'UDP Client IP Address' field with '192.168.1.200' entered. A note says: 'Enable Alert UDP alerts for Generic Events. Enter IP Address of client machine, or select the "broadcast option".'
- TCP Alerts:** Features a dropdown menu set to 'Enable' and a 'TCP Server IP Address' field with '192.168.1.200' entered. A note says: 'Enable TCP alerts for Generic Events. Enter IP address of TCP listener, and port number it is listening on.'

An 'Update' button is located at the bottom right of the form.

UDP

UDP Alerts	Enable UDP alerts for generic events
Broadcast	Enable to broadcast the events out
UDP Client IP Address	Enter the IP address of the server which will be listening for the alerts
UDP Port	Enter the UDP port number on which the server is listening

TCP

TCP alerts	Enable TCP alerts for generic events
TCP Server IP	Enter the IP address of the server which will be listening for the alerts
TCP Port	Enter the TCP port number on which the server is listening

Syslog (System Log)

Many devices especially network switches have the ability to transmit status messages on a System Log or Syslog. This means of communications uses port 514.

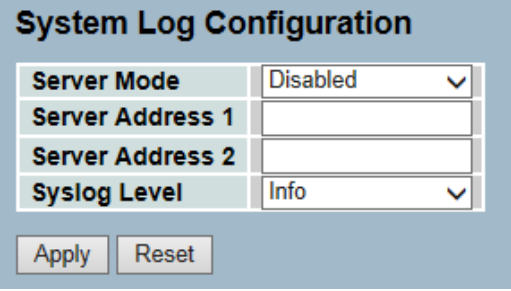
The Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as a generalized informational, analysis, and debugging messages.

This section describes how to configure the system log contained in a typical switch.

Web Interface

To configure Syslog configuration in the web interface:

1. Click SYSTEM, then Syslog.
2. Specify the syslog parameters include IP Address of Syslog server and Port number.
3. Evoke "Syslog" to enable it.
4. Click "Apply".



System Log Configuration	
Server Mode	Disabled
Server Address 1	
Server Address 2	
Syslog Level	Info

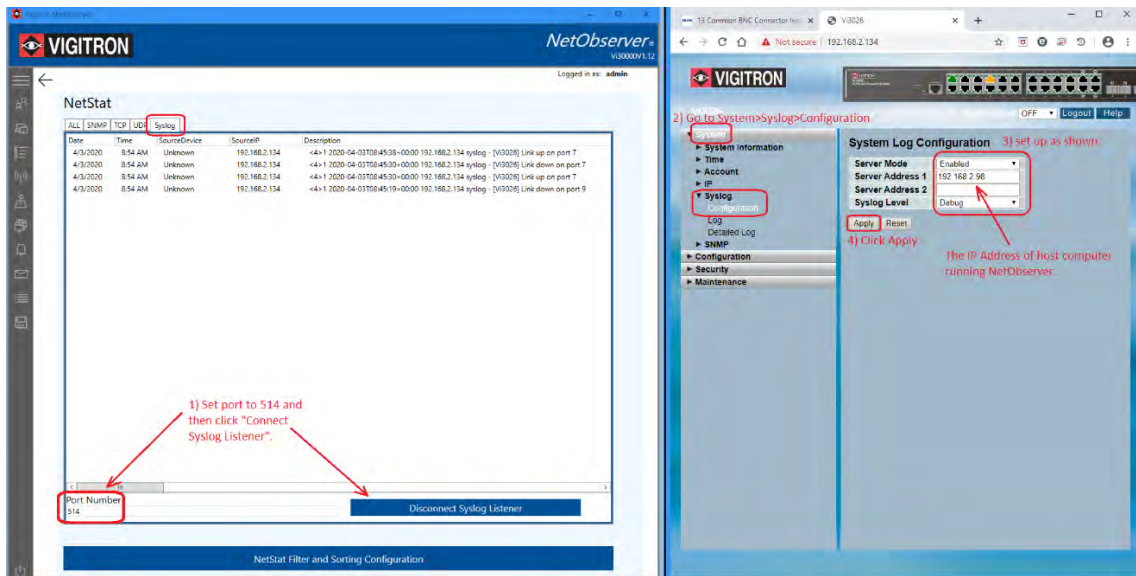
Apply Reset

Example: System Log

Figure 2- 5.1: The System Log Configuration

- **Enabled:** Enables server mode operation.
- **Disabled:** Disables server mode operation
- **Server Address 1 and 2:** Indicates the IPv4 host address of syslog server 1 and server 2 (For redundancy). If the switch provides DNS feature, it also can be a host name.

NetObserver™ contains a Syslog set up for receiving this message. The standard syslog port setting is 514.



Example: Setting Up Syslog Communications

SNMP (Simple Network Management Protocol)

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly in the trap you are using. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

NetObserver™ contains a built in SNMP Trap.

- The following is a typical set up of a switch for SNMP transmission:

Trap Host Configuration	
Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

- There are various set ups for SNMP and will differ for different switches. There are three types of SNMP protocol v1, v2c, and v3. NetObserver operates either on SNMP v1 or v2c.

***Note the port for UDP transmission is 162.**

Important Note: SNMP communications: The ability of a device to communicate using SNMP is based on its MIB (Management Instructional Base). Variations exist with different products. NetObserver only receives communications as sent by the connected device and cannot change their form or format.

Before you get started:

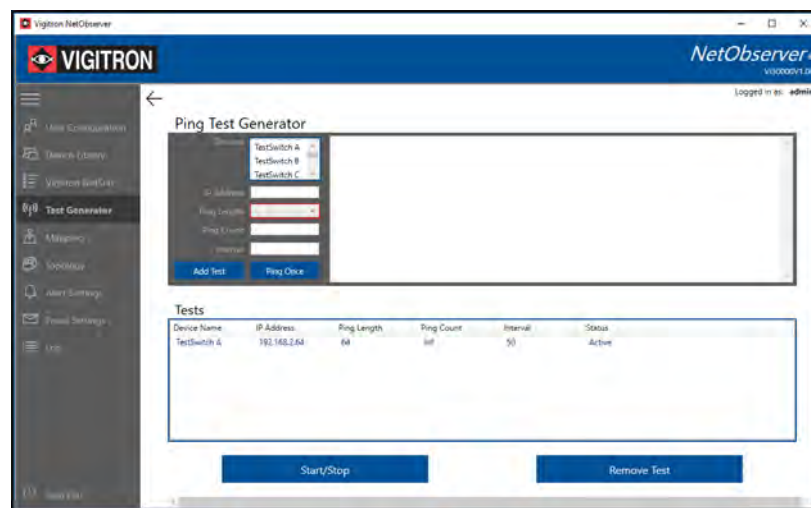
- **Note 1:** Your computer must be connected to the Internet in order to send the registration form. You cannot complete the installation without successfully transmit the registration form. If you cannot connect when installing you will be able to operate NetObserver for 7 calendar days.
- **Note 2:** To communicate with devices contained on your network, they must be properly connected to the same network operating NetObserver™
- **Note 3:** SNMP communications is based on MIB (Management Information Base) which can differ in individual switches and other devices using SNMP. Some SNMP v2c versions may not interface with NetObserver. In this case please use Syslog or if your switch has TCP/UDP that can also be used.
- **Note 4:** Pings will generate alerts and log entries even if SNMP, UDP, TCP and Syslog communications are not active

A word on network ports:

- For computers port numbers are part of addressing information used to identify the senders and receivers of messages. They are found in TCP/IP network connections. In a closed company environment, a Network Administer may need to set up port forwarding to allow the port numbers of you connected devices. You may need to set up port forwarding to allow the port numbers from SNMP, Syslog, TCP, UP application to pass through a firewall. SNMP (Port 162), and Syslog (Port 514) ports are fixed. In some devices TCP and UP ports can be variable and set within the units programming.

NetObserver™ is based on the ability of receiving messages from the connected devices. Prior to operating NetObserver it is important that you verify communications between the client or sever operating NetObserver™ and the connected devices.

- This can be done by using the ping test generator in NetObserver as shown below:



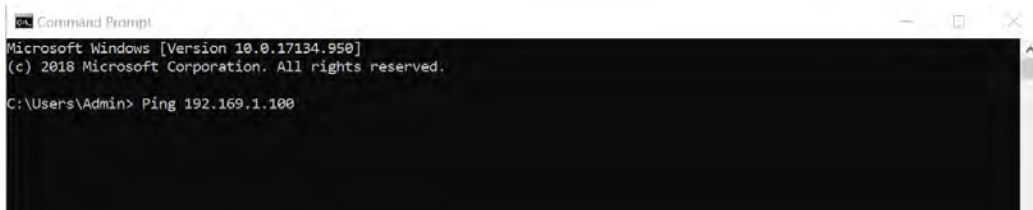
- As an alternative, you can so use the ping command in Windows™ by clicking on the Windows icon and typing in “cmd” in the search space following by the ping and the IP address of the device you want to check. This ping process can be used even without NetObserver™ being installed.
- You can ping an individual site once or set all connected device sites for continuous pings. However, note the more devices operating on continuous pings the slower the response.

Ping defaults are:

Ping Count
Interval

1-20 Events
15- 1800 seconds

The Ping count will determine the sampling rate prior to determining if connect is active or inactive – if one of the samples receives a return ping the connection will be considered active



If your connected device can't communicate SNMP, TCP, UDP and Syslog, the Test Generator Feature can be used to generate Pings communicating to connected device in order to sense alert one of these conditions must be valid.

Each form of communications has a limitation. Some forms of communication will not cross networks meaning that the IP address must be set to the same network range as is the network switch running NetObserver communicating with the example:

- 192.168.1.1 (computer) -----to-----192.168.1.100 network switch will work
- 192.168.1.1 (computer) -----to-----192.168.2.100 network switch will not work

This is no different than the requirements for a computer to access the network switch. With regards to communicating over the same or different networks please note the following:

- SNMP **will cross** networks when set to "broadcast".
- SNMP **will not cross** networks when trap IP address is specified
- UDP **will cross** networks when set to "broadcast".
- UDP **will not cross** networks when sent to a specific IP address.

TCP must be set to the to the same IP address section for both the computer operating NetObserver and the network switch :

- 192.168.1.1 (computer) -----to-----192.168.1.100 network switch will work
- 192.168.1.1 (computer) -----to-----192.168.2.100 network switch will not work

Syslog will not cross networks.

- 192.168.1.1 (computer) -----to-----192.168.1.100 network switch will work
- 192.168.1.1 (computer) -----to-----192.168.2.100 network switch will not work

What if I use a router?

- The use of a router will depend on its proper set up within the network

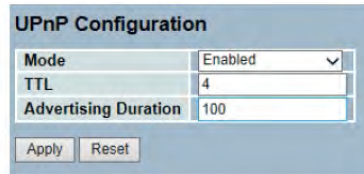
What if a camera connected to a switch is on a different network?

- If camera connected to a switch is on a different network you will not be able to use the ping feature in NetObserver. As the switch is the main communication device within the system it will be able to communicate with network provided it on the same network as the computer operating NetObserver or uses SNMP or UDP in the broadcast settings

UPnP

NetObserver has the ability to discover devices on the network using UPnP. In order to use these features, the connected device must be able to communicate using UPnP protocol.

Check to see if your connected devices offer this feature:




UPnP Configuration

Mode	Enabled
TTL	4
Advertising Duration	100

Apply Reset

Example: UPnP Set Up In Vigitrion Switches

If so, UPnP can be used to automatically discover devices in building your network.



Device Library

Onvif UPnP Manual

Create New Library Add to Existing Library

Devices:

Device Name	IP Address	Host Name	DHCP	Username	Password	Device Type	Manufacturer	Model Name	Serial Number
Vig30128	192.168.1.1		<input type="checkbox"/>			Switch	Vigitrion	Vig30128	A157119AR4800...

- *It is important to note that UPnP is a discovery protocol only.*
- *It does not mean the discovered device is capable to communicating status and messaging.*

Discovery Protocols:

Onvif

Device must have the ability to be discovered.

UPnP

Device must have the ability and be programmed to transmit.

Communication Protocols:

SNMP

Device needs to be set up for v2c Protocol on port.

Both connected device and computer running NetObserver must be set up to transmit and receive on port 162. **NetObserver automatically will set up port 162.**

Syslog

Device needs to be set up to provide messages on Syslog.

Both connected device and computer running NetObserver must be set up to transmit and receive on port 514. **NetObserver automatically will set up port 514.**

TCP

Device needs to be set up to transmit, and computer running NetObserver must be set up and transmit on the same ports.

Including Non-Managed Devices:

Non managed devices generally will not have an IP address. They can be included in library and exhibit all the properties of management devices. These include assigning symbols/devices and the inclusion in mapping functions.

- To add start your IP address as 000.000.000.000-000.177.177.177 following by a configuration similar to an IP address. Example: 000.000.000.001, 000.000.000.002, etc.
- If this address is used as part of a ping test, the system will not monitor nor indicate any connection failures. To test and monitor thru the unmanaged switch ping any device connected to the unmanaged device. If successful it will show the unmanaged device was successful configured.

How to monitor connected devices without SNMP, TCP, UDP and Syslog Communications:

- As long as a device has an IP address it can be monitored by NetObserver. Enter the devices' IP address in the Ping Generator and set for continuous ping. Assigned naming conventions as normal with any alert information. In the event a ping is not responded an alert with the associated messages and responses will be generated.
-

Alert Requirements:

NetObserver provides two methods of receiving alerts or Alert. They are program specific methods such as SNMP, UDP, TCP, Syslog or using ping (Test Generator). When programming alerts you can specify specific text and conditions requiring the Alert.

The ping generator will allow programming individual pings to connected devices. When pings cannot be sensed an Alert will be generated.

One of these methods must be programmed in order to generate an Alert.

Logging and NetStat functions

Important Note: NetObserver is designed to receive alerts via SNMP, TCP, UDP and Syslog transmissions. These messages are different than alerts. They will be logged but will not change the icon Alert status.

NetStat is only a logging function but must be programmed in order to receive alerts

Notes on Device Communications

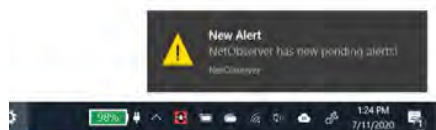
SNMP transmission can differ from different devices. Even if a device is capable of SNMP it may not be able to be read by NetObserver. In these cases Syslog, TCP, UDP or ping can be used.

Minimized Mode:



NetObserver has the ability to operate in a minimized mode.

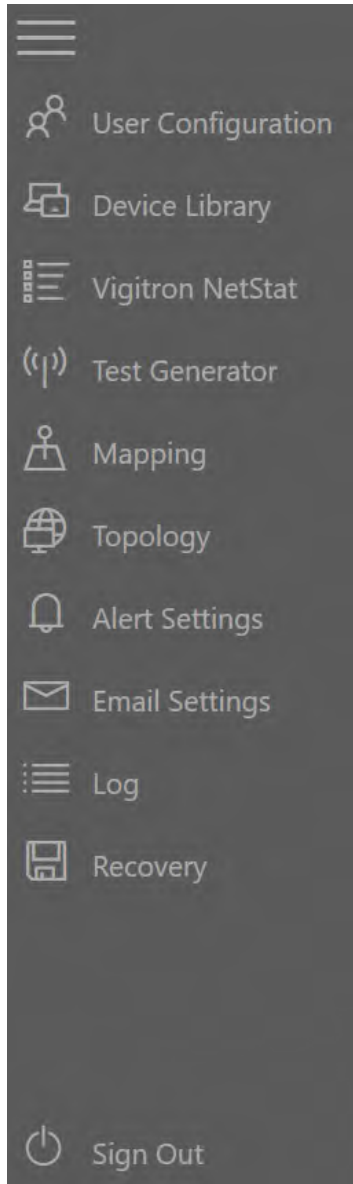
If an Alert is received the icon will flash. Click on the icon to expand NetObserver to full screen



NetObserver can also operate in the background of other Windows™ based programs. When Windows alerts are permitted it will issue them as NetObserver

Section 4: NetObserver Main and Submenus

NetObserver provides several main and submenus. Selecting the main menu will show the related submenus.



User Configuration

- Sets up user names, passwords, adds, changes user names and passwords, assigns admin or viewer functions.

Device Library

- Assigns devices such as switches, and devices connected to individual switches and transmission points, allows for port and device naming.

Vigitron NetStat

- Receives and logs errors messages, allows for filtering of messages

Test Generator

- Connected device test based on IP address, can vary packet size, tests can be done for single or multiple address; one or multiple times.

Mapping

- Insert maps in various formats, drop & drag library devices to specific map locations. Device information & operating status is shown on map.

Topology

- Display individual status mapping of devices connected to switch or headend points or show what an individual device is connected to. All devices are shown with their operating status.

Alert Settings

- Allows you to select which Alerts are registered; customize messaging and responses.

Email Settings

- Programs messages via private or public emails services.

Log

- Records messaging from connected devices. Allows for custom sorting and filtering. Logs can be exported.

Recovery

- Allows downloading of all custom settings and recovery

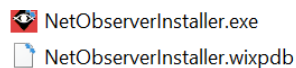
Sign Out

- Click this button to sign out of NetObserver.

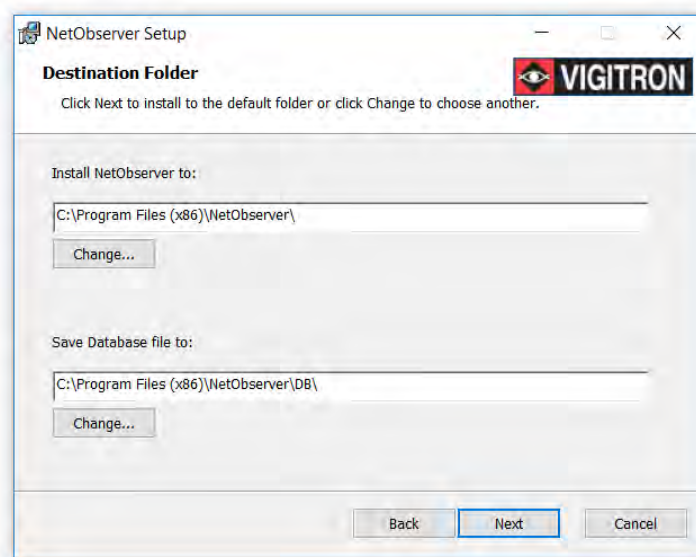
Section 5: Installation

Steps

1. Download the file.
2. Copy file on to your desktop.
3. Open file.
4. The following files will be shown: (shown are NetObserver software only)



Installation



1. You can change the location where you want to store the main program.
 - If required enter a new location.
 - If a new location is programmed click "Change."
2. You can change the location as to where data files are stored.
 - If required enter a new location.
 - If a new location is programmed click "Change."
3. Once you either elect to accept the pre-programmed locations or enter new ones, click "Next."
4. Select the "NetObserverInstaller.exe"
5. Depending on your Windows™ security set up loading the program maybe blocked. If you see the following screen select the [more info](#).



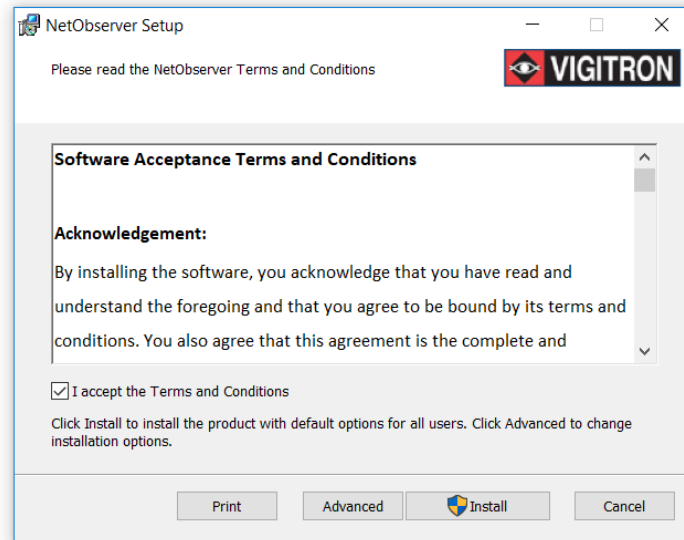
6. Select the “Run anyway” function.



Important Note: Depending on your anti-virus software it may also block NetObserver from loading. If this is the case follow instructions for your software and grant permission to load.

If Your Computer Has Virus Protection Software

Many computers use virus protection software in addition Windows™ Defender. All of these operate differently and may or may not allow NetObserver to be installed. If this is the case refer to your virus protection software and give it permission. In other cases, you may have to temporarily disable your virus protection software, load NetObserver and re-enable it. If these problems exist please refer to the operation of your virus protection software.



7. Accept Software Terms and Conditions

- Review software terms and conditions.
- You can elect to print out a copy if you wish.
- Click advance if you want to change to the locations of the installation and database directory.
- You must click “I accept the Terms and Conditions” in order to continue
- Click the “Install” button.



8. Select the country using the drop down menu- once the country is selected the City drop down box will show the cities in that country.



9. If the United States is selected the city drop down will reflect cities in the United States

10. Incorrect messaging and registration confirmation

If the form isn't completed and or the wrong information is filled in the following pop up will appear (below):



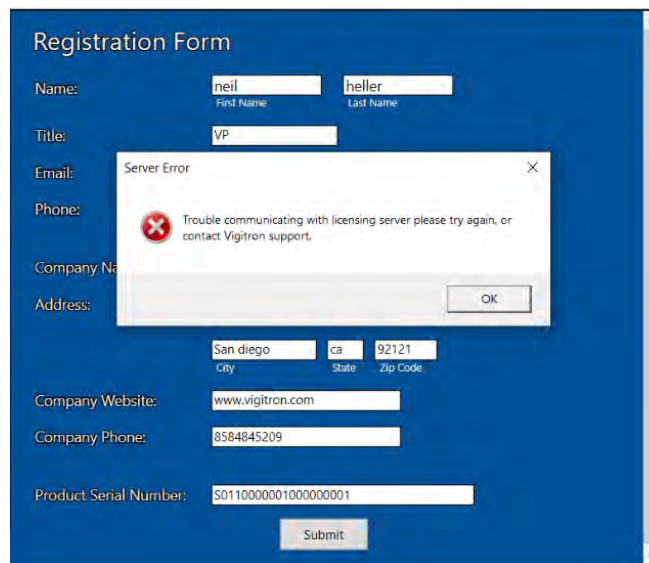
The Registration form must be filled out completely.

- *Make certain to include the product serial number as provided in your file.*

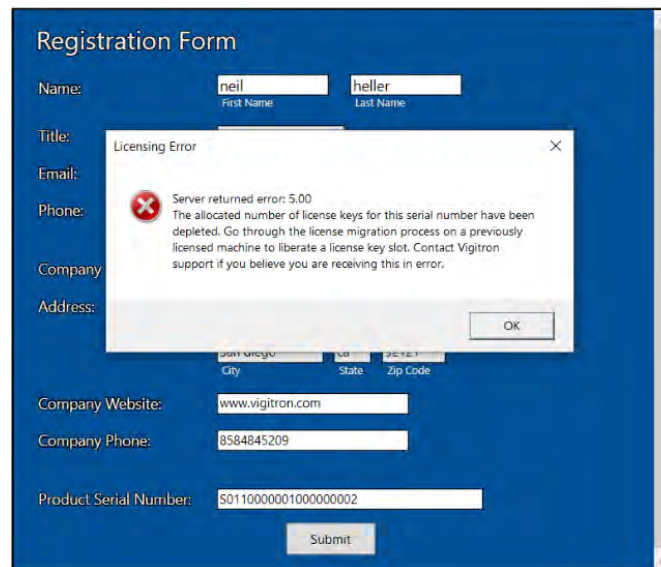


The serial number is provided in your download file

- *Make certain it matches the number you are entering in the Product Serial Number section.*



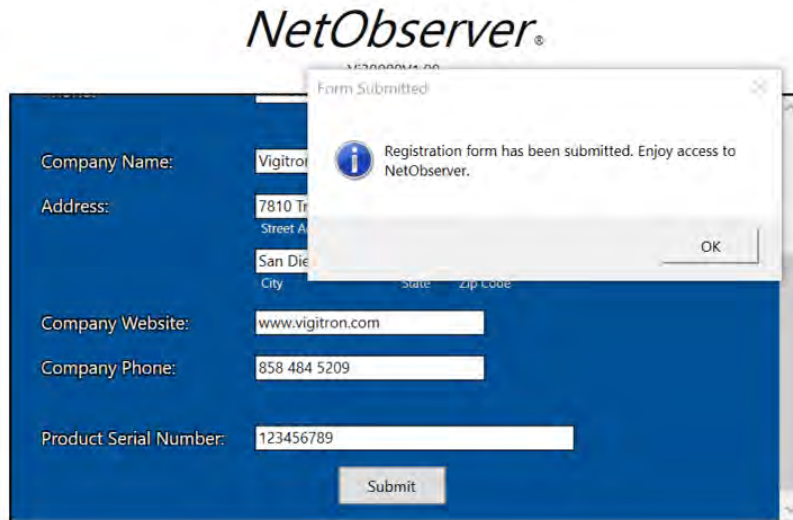
The following message will display if the NetObserver cannot communicate with server:



If you attempt to register using a previous license the above message will appear:



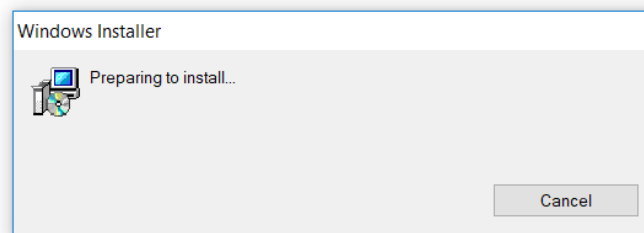
Registration requires connection to outside network access. You can operate NetObserver for up to 7 days without confirmed registration.



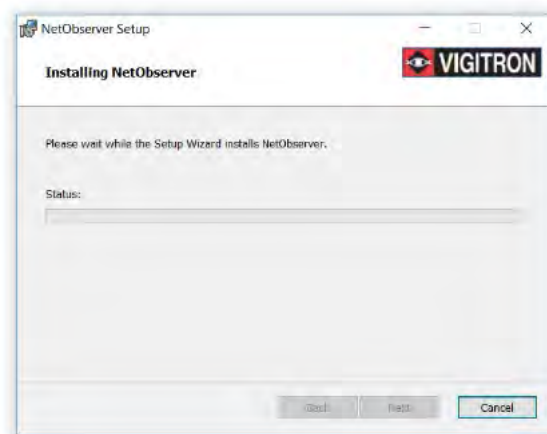
If you have successfully filled in and submitted the registration form the system will provide an acknowledgement

If you have successfully filled out the form and submitted it the following pop up will appear.

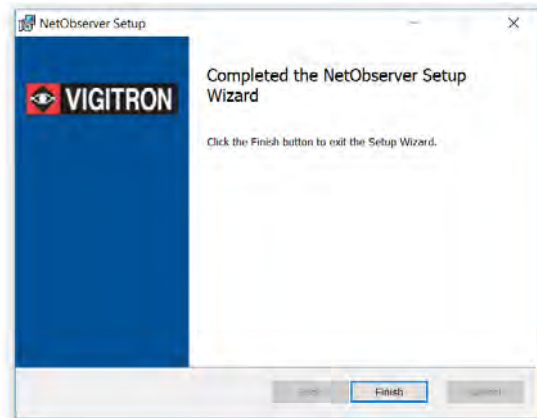
Note: *You must be connected to a network with ability to access the Internet*



If you have acknowledged the terms and conditions correctly the installation will start.



The progress bar will appear:



8. Click the Finish button to exit the Setup Wizard and start the installation process.
 - Click the Back button will go back to the previous screen
 - Cancel exits the installation process

The NetObserver shortcut will be placed on your desktop.



Section 6: Login

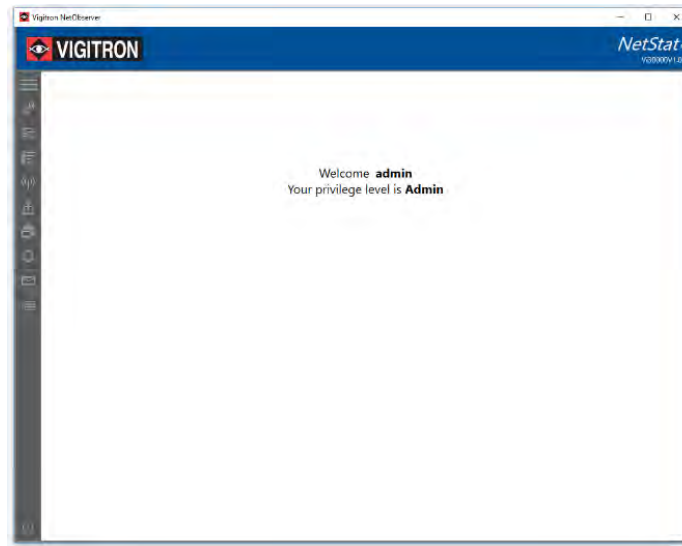


1. Enter a valid Username and Password.
 - Default Username: admin
 - Default Password: system
2. Click the "Login" button.



3. If a wrong Username or Password is entered the following pop up will appear (above):
 - If you have forgotten your User name or Password you will need to contact Vigitron. It is strongly recommended you save your configuration file. As an alternative you can delete NetObserver and re-install it.

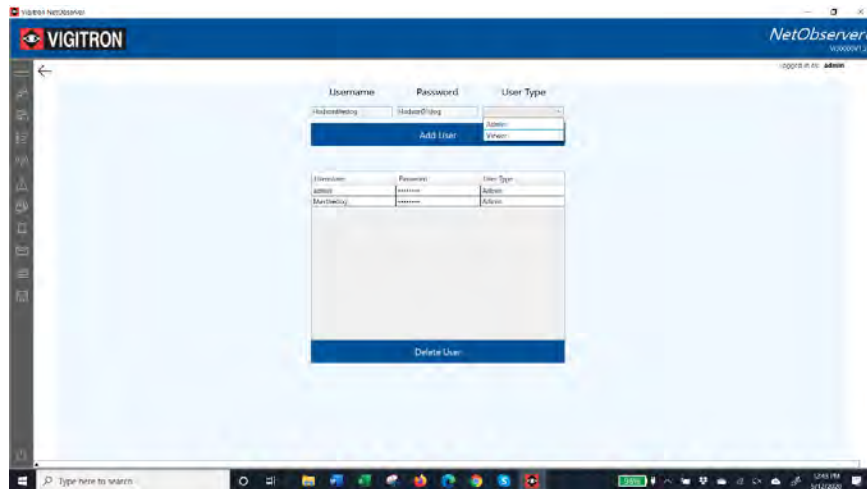
Section 7: Intro Screens



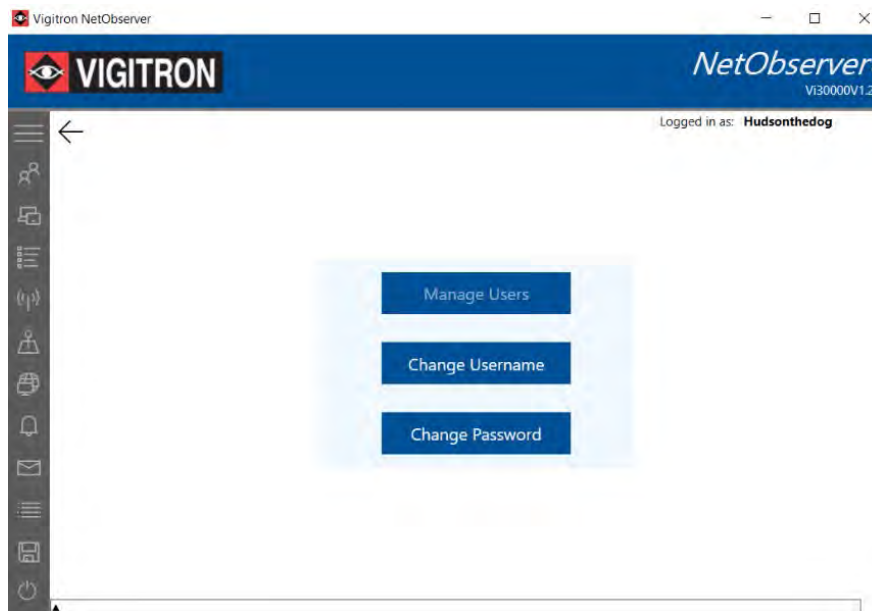
1. Once your password and user name have been entered correctly the Intro screen will appear (above):
2. Each menu icon is shown on the left-hand side.



3. To expand sidebar menu, click to view icon descriptions.
4. To contract sidebar menu, click to contract.
 - If the user is defined as viewer

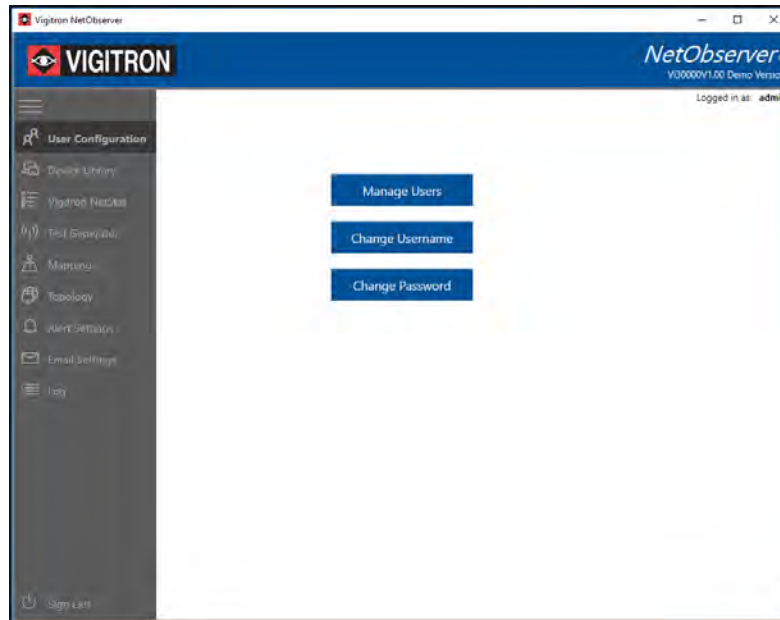


If the operator is signed in as Viewer—access to programming functions will not be allowed



Section 8: User Configuration

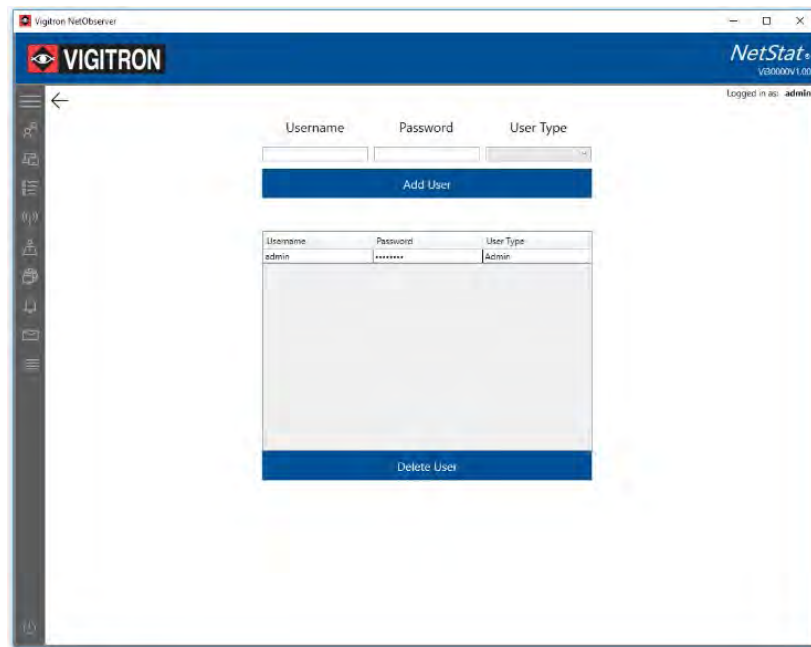
This Section will cover how to create passwords, user names, assign privilege levels, and delete users.



1. Click the User Configuration tab. The following selections will appear:
 - a. **Manage Users**
 - i. This allows the admin to create new usernames, passwords and assign access levels
 - b. **Change User Name**
 - i. This allows the admin to change an existing user name
 - c. **Change Password**
 - i. This allows the admin to change an existing password
2. Click on the appropriate tab to add or change setting.

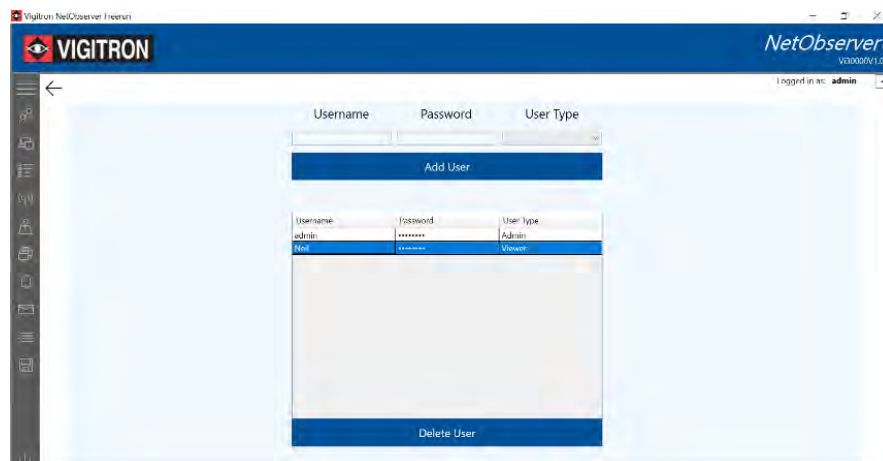
Assigning Username, Password, and Type

1. Adding a user name and password is only available to admin level.
2. Enter a User Name and Password.
3. From the drop-down menu select the access level as admin or viewer.
4. Click Add User and confirm the information appears the access box below.

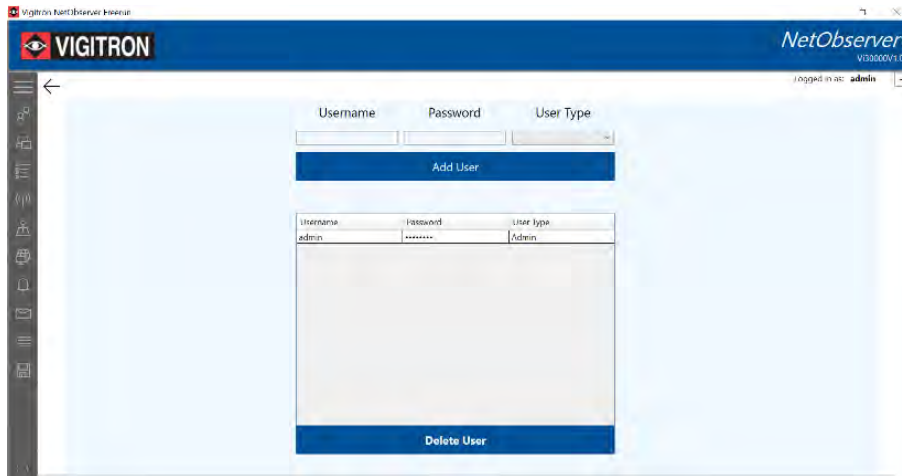


Deleting a Username

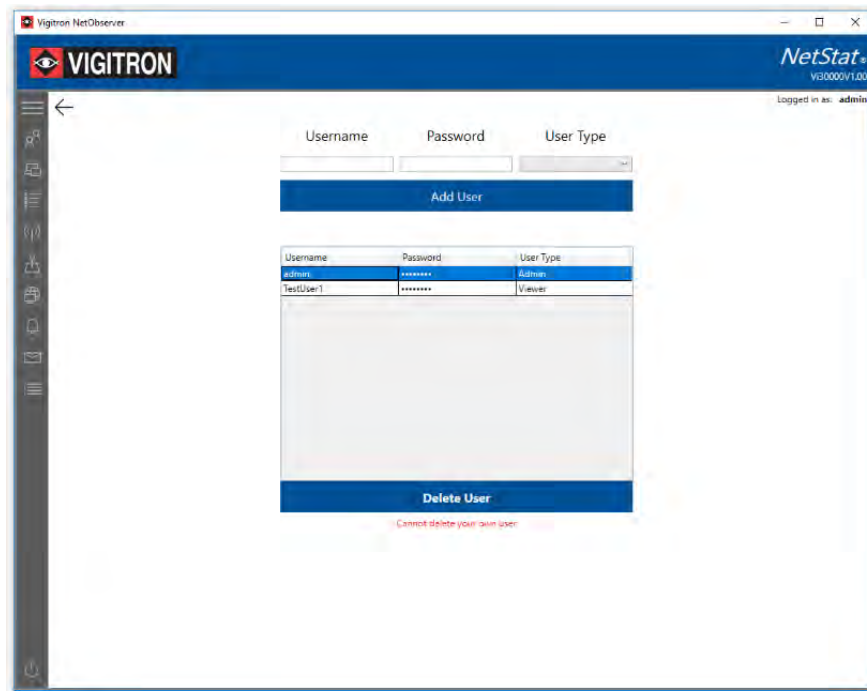
1. Highlight the username to be deleted.



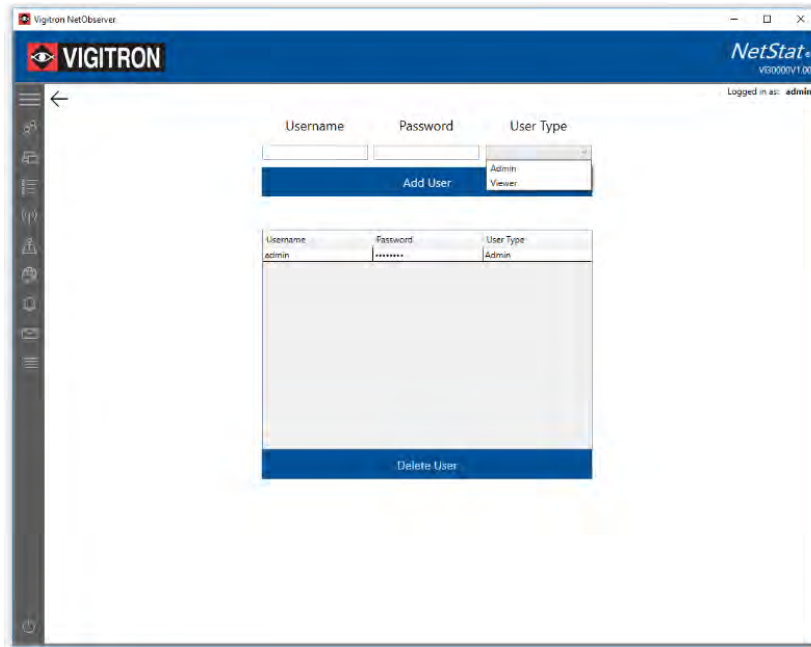
2. Select "Delete User."



Note: If you are the admin you cannot delete the name you are signed in with.

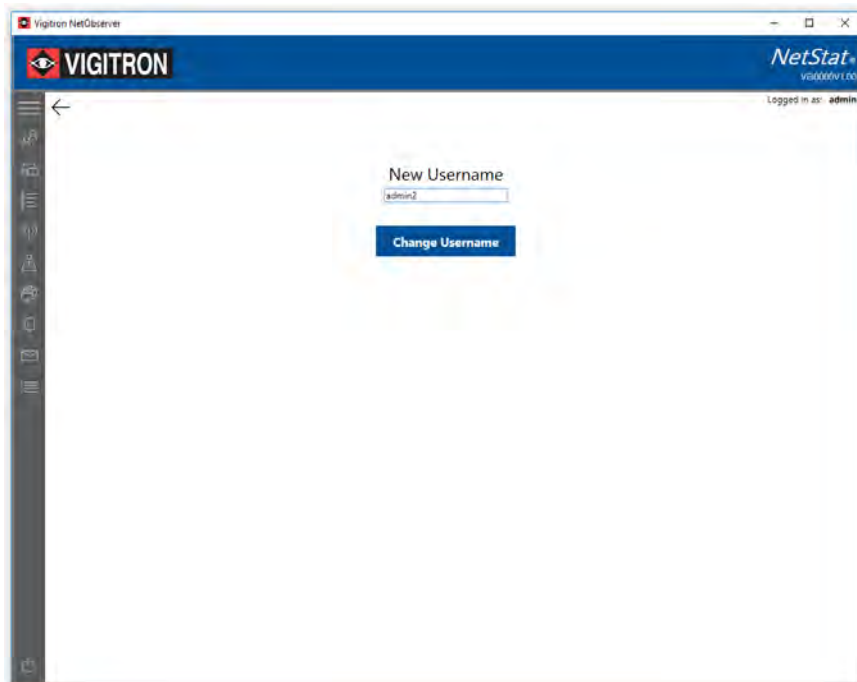


3. Confirm the entry no longer appears.

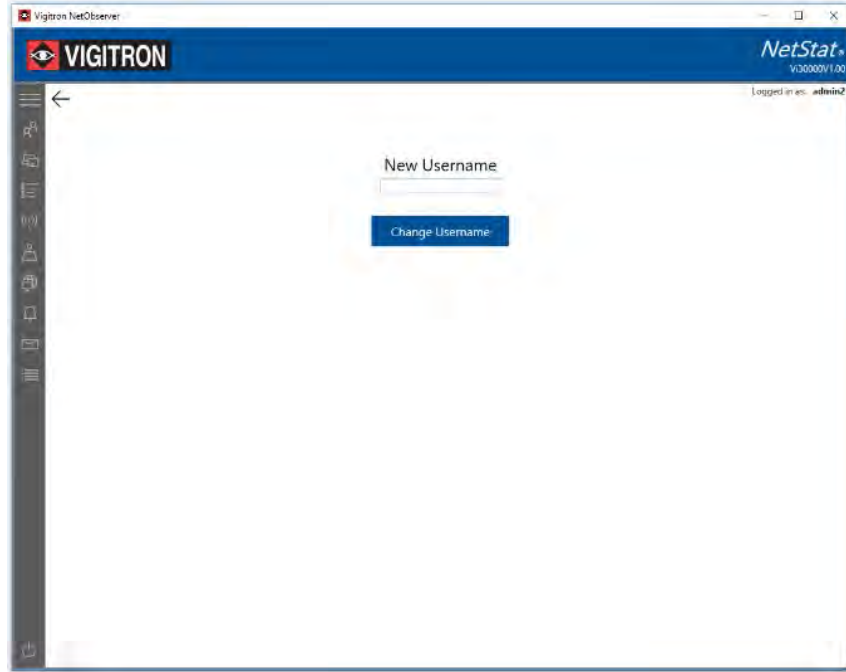


Changing a Username

1. Select the username and click on "Change Username."



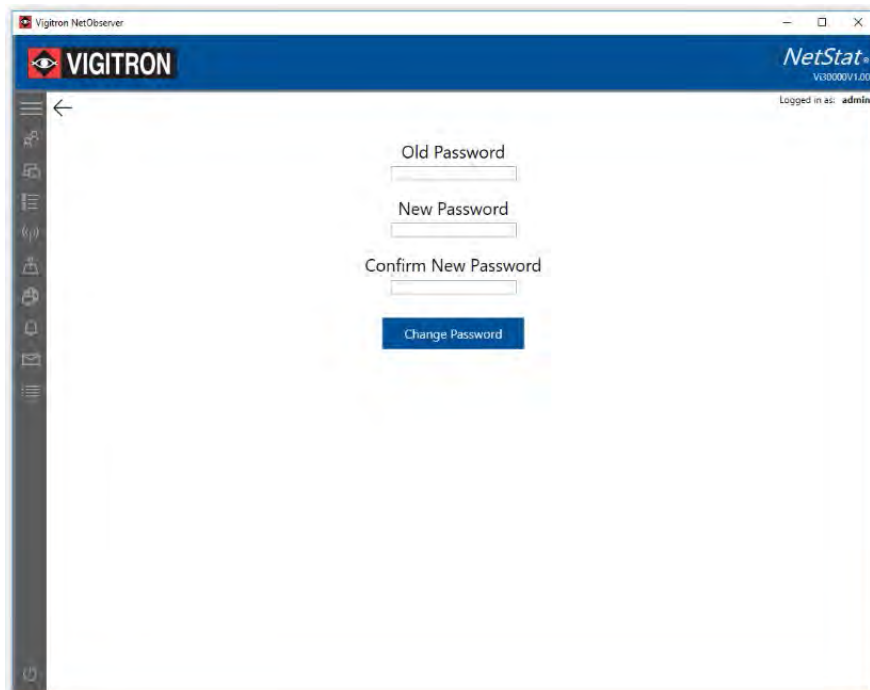
2. Enter the new user name and click "Change Username."



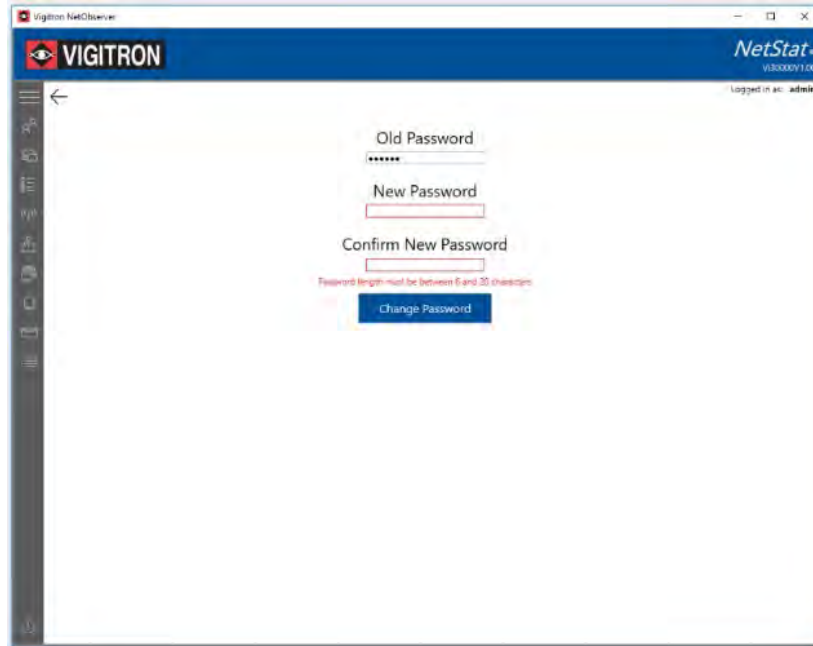
Changing a User Password

1. Select change password

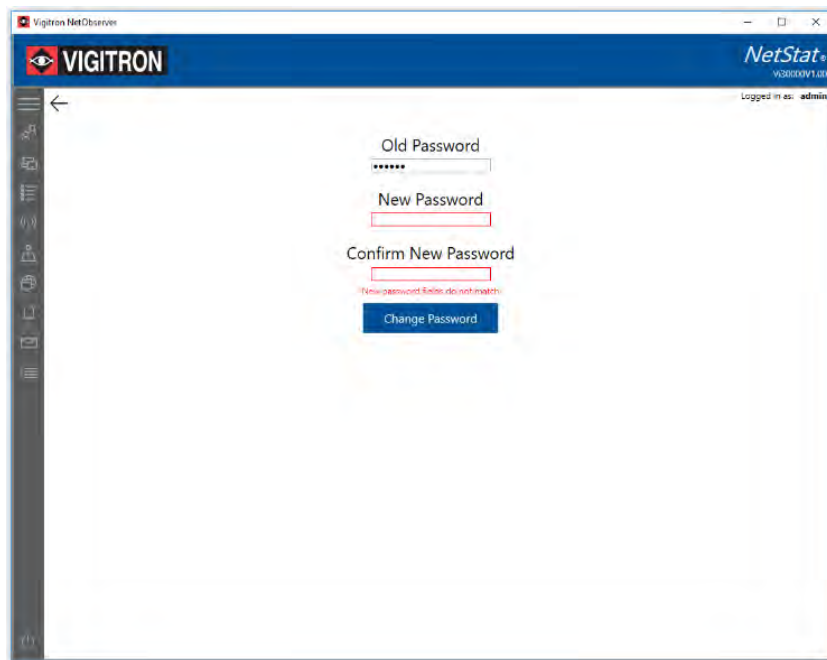
**In order to change a password, you must know the previous password*



2. New or replacement passwords must be 6 and 20 characters.



3. Passwords must match or you will be notified with a warning.



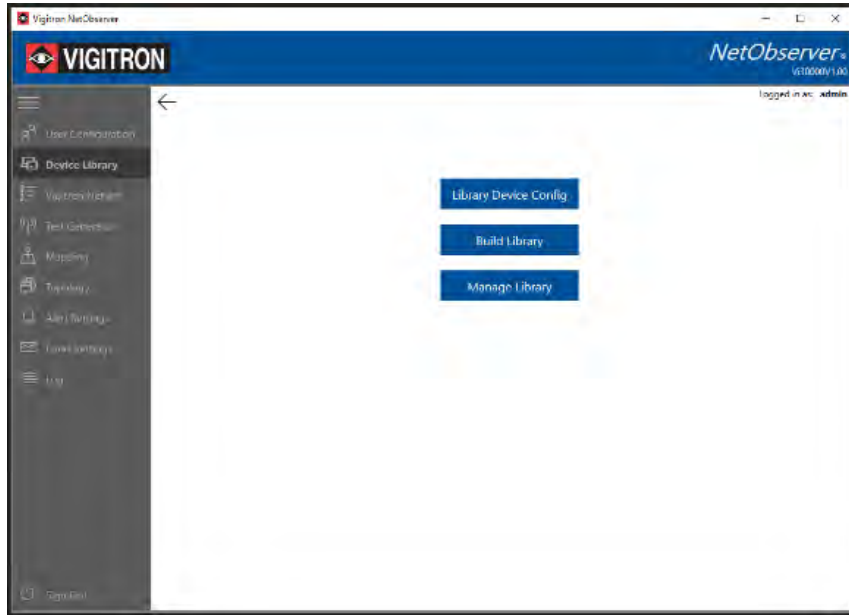
Important Notes on Adding and Deleting User Names and Passwords:

- a. Admin level can delete any username and password
- b. Only the person that has programmed their user name and password can make changes to their own user name and password
- c. The selection of what user name and password you are changing is based on your sign in user name and password

Section 9: Device Library

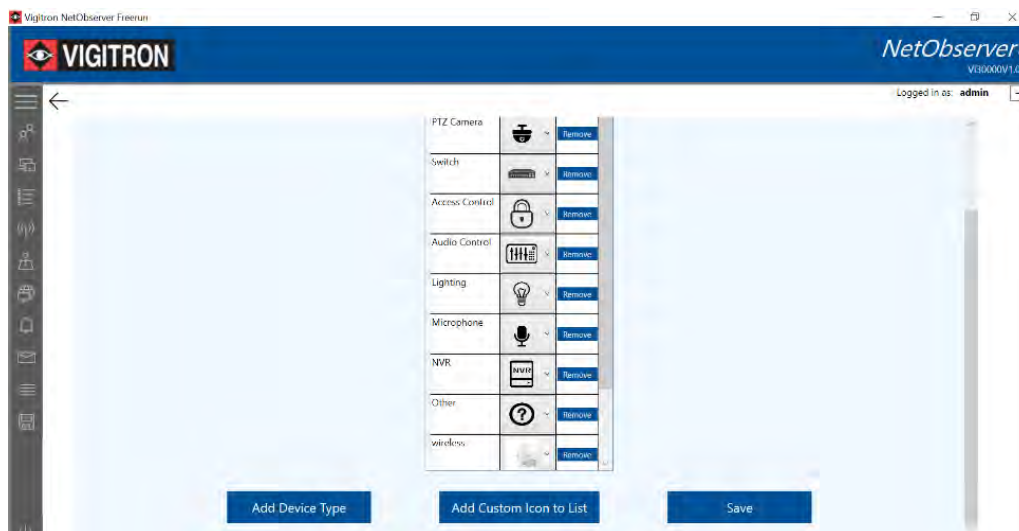
The Device Library allows you to Configure Devices, build a Library and manage the Library Configuration.

1. Select the “Device Library” from the side bar.



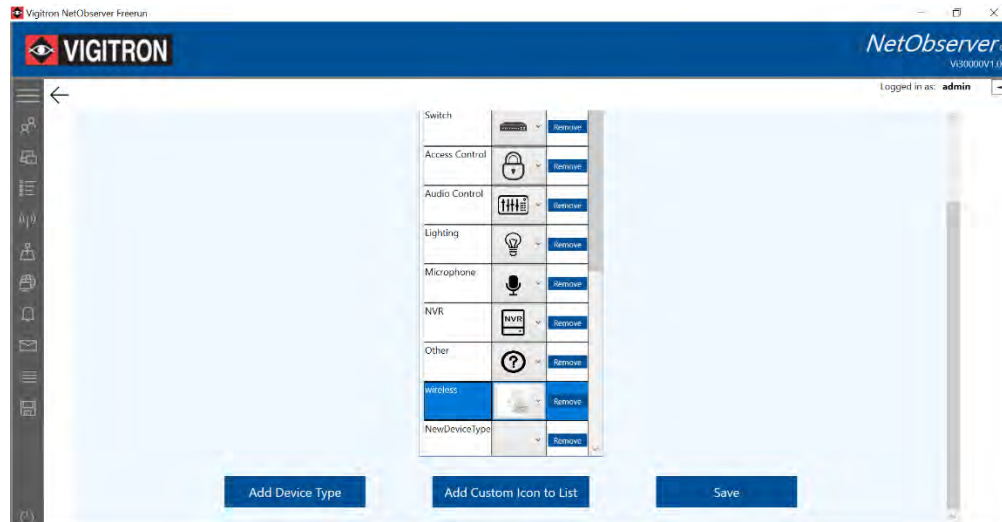
Library Device Configuration

1. Select the “Library Device Config” to show the following screen.

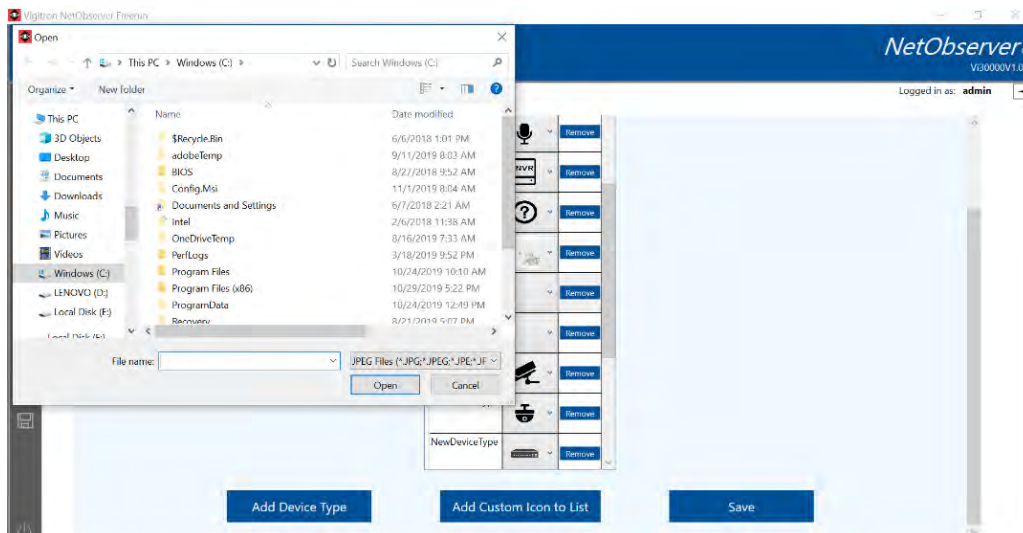


2. To add a device, select the “Add Device Type.”

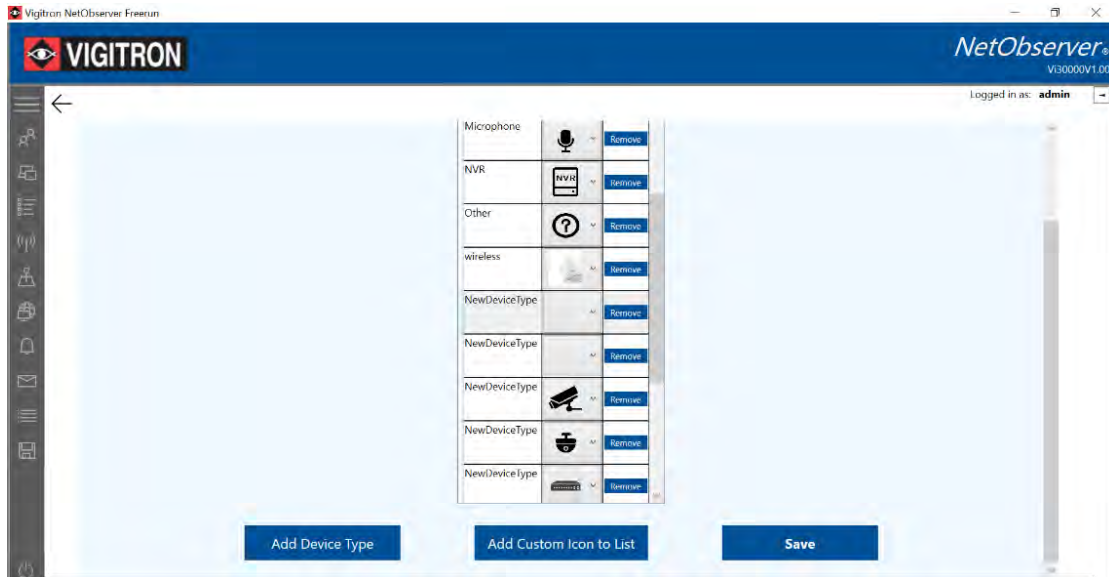
3. Highlight the box labeled "New Device Type" and insert your device description.



4. You can select any of the existing icons by using the drop-down menu and clicking on the selected icon.
5. To select a custom icon.
 - a. Select "Add Custom Icon to List."
 - b. A dialog box will open.
 - c. Select an icon. *It must be in .jpg, .png or similar image format.*

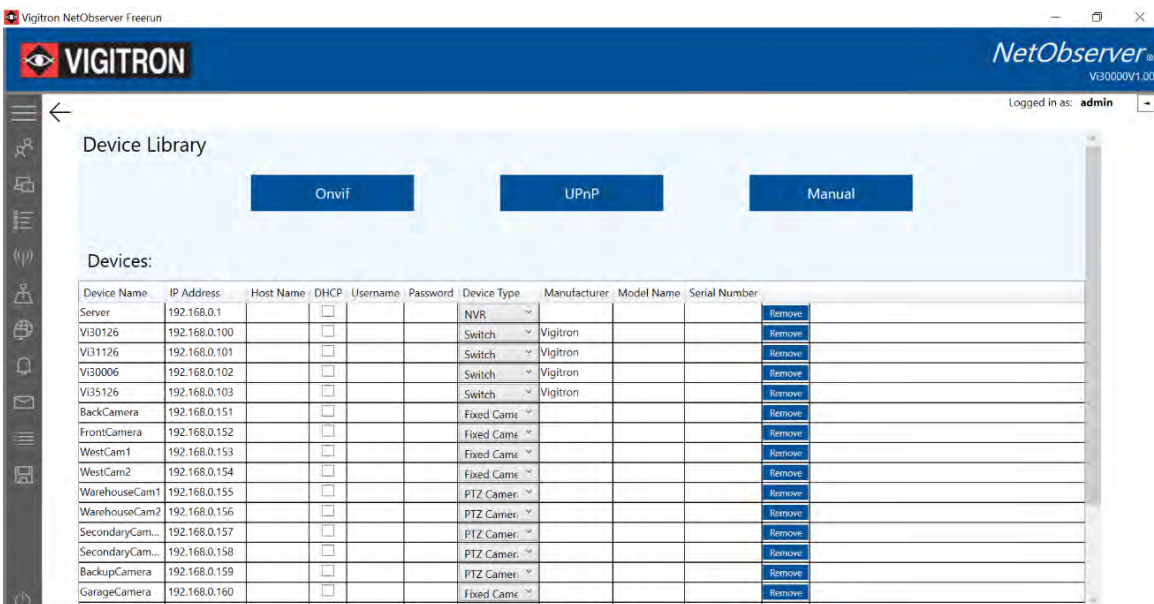


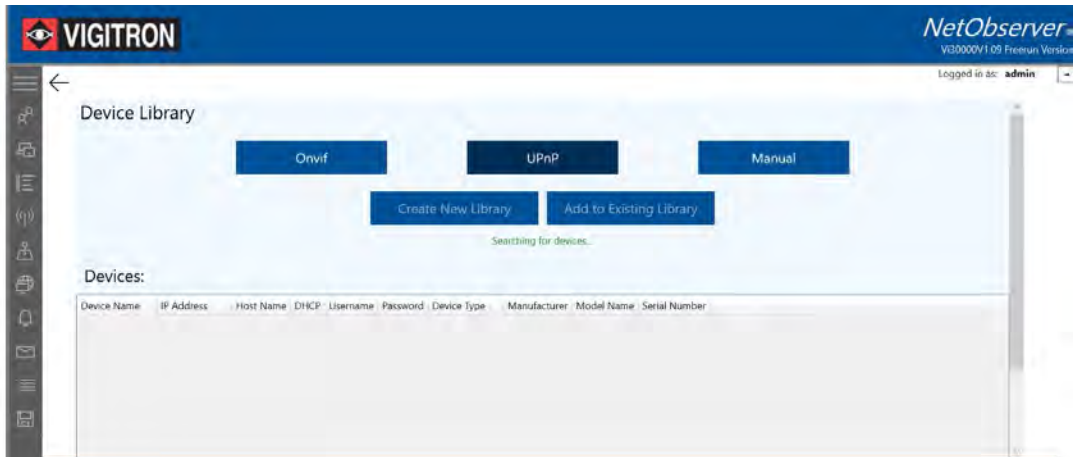
6. If the icon is in an acceptable format it will inserted in the box.
 - a. Select "Save" to save the configuration.



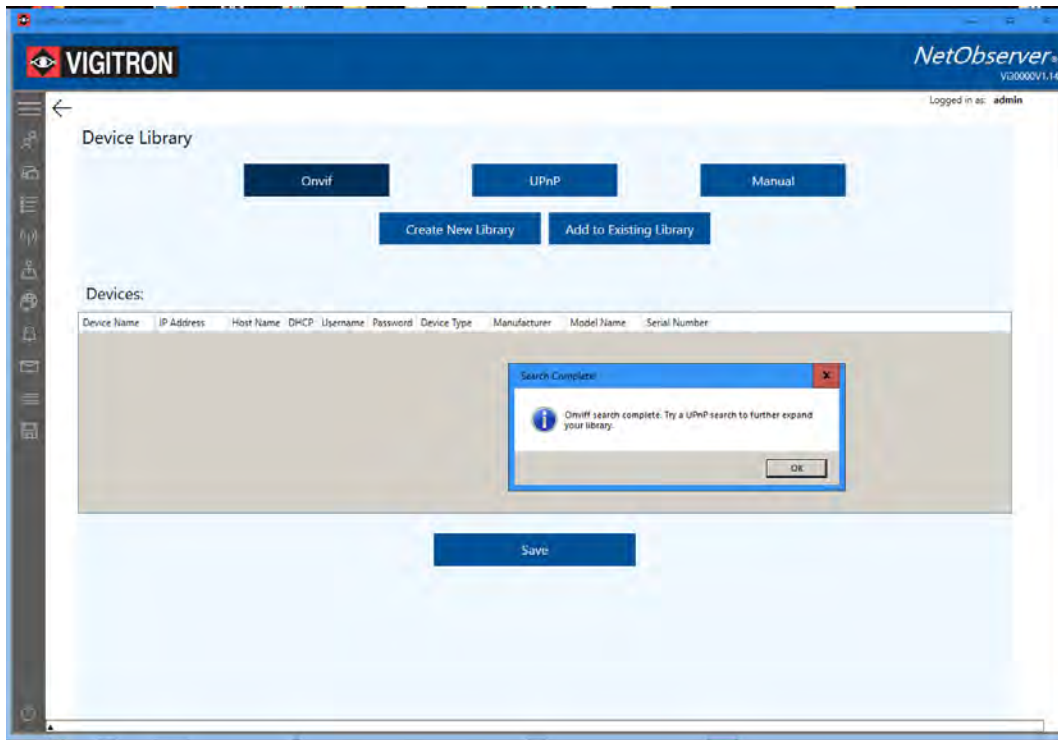
Building a Library (Manage Devices)

1. Select the "Build Library" button and the following screen will appear (below):
2. You can select to scan connected devices that are Onvif and UPnP.
3. Once discovered the device will be automatically added to the list.

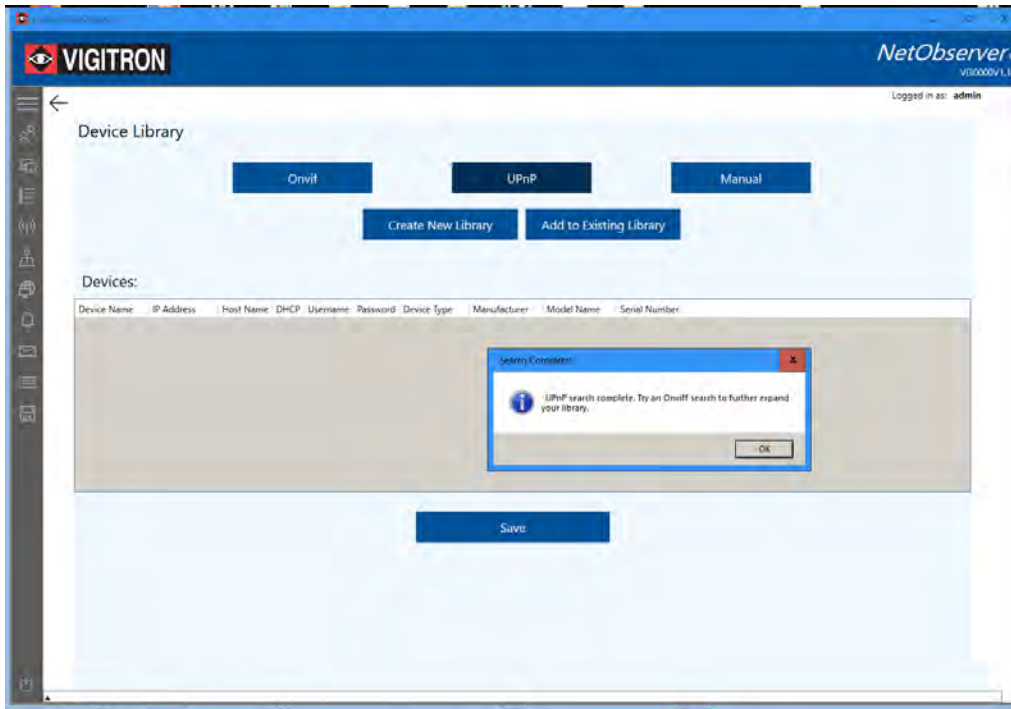




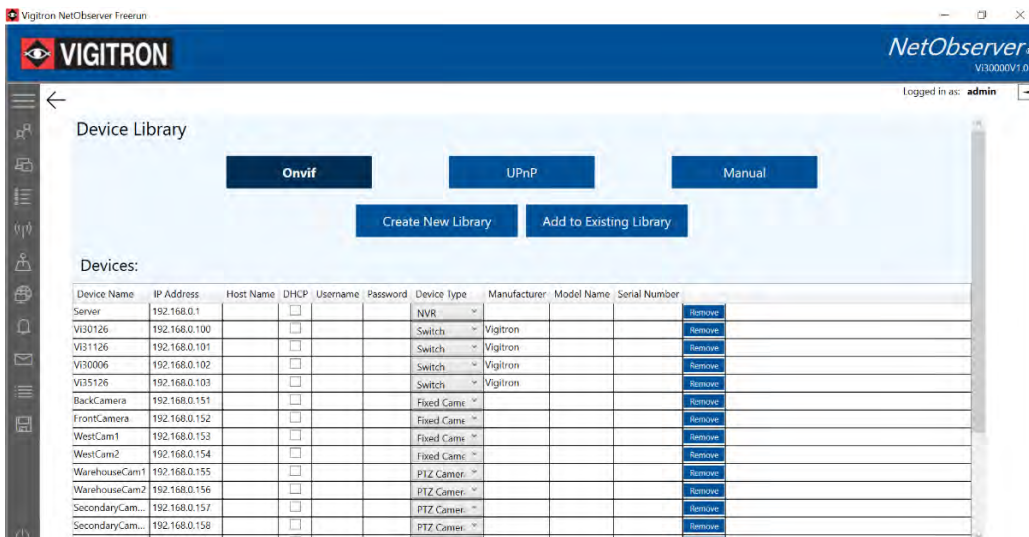
4. You can add devices to an existing library or create a new library.
5. If the search method you select cannot identify any devices the pop up will suggest another method.



6. If an Onvif search yields no results the above pop up will appear



7. if the UPnP yields no results the above pop up will appear:



8. If a connected device is neither Onvif or UPnP detectable you can select the manual button and add the device manually by entering its IP address, the name given to its Host.

- If the device assigns its IP address via DHCP, select the DHCP settings.
- Regardless of how a connected device is detected, when complete select the "Add Device" button.

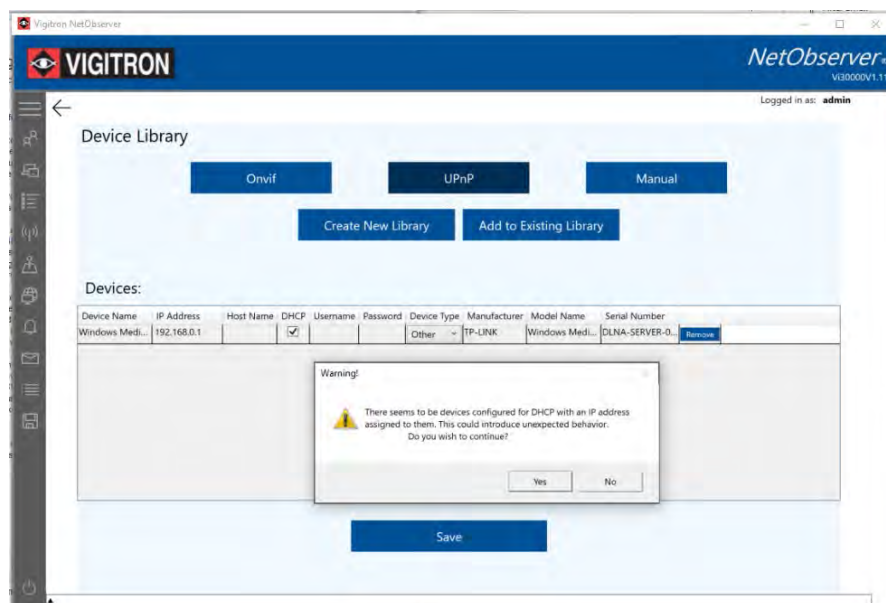
Note: While Onvif and UPnP can discover connected devices, they may not provide complete information

- You can manually add the Host name, device user name and password, manufacturer, model number and serial number.

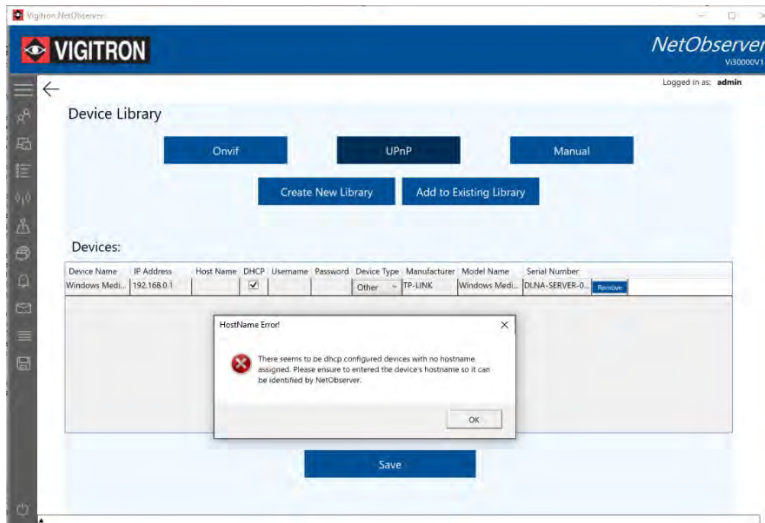


Note: The same device cannot be assigned to different libraries.

9. DHCP - is usually used in larger systems when a central server assigns IP address



- a. When scanning using Onvif or UPnP NetObserver will be able to detect if a connected device has been assigned an IP address using DHCP. It is important to note that using DHCP can result in an IP Address changes and its ability for the device to communicate with NetObserver.

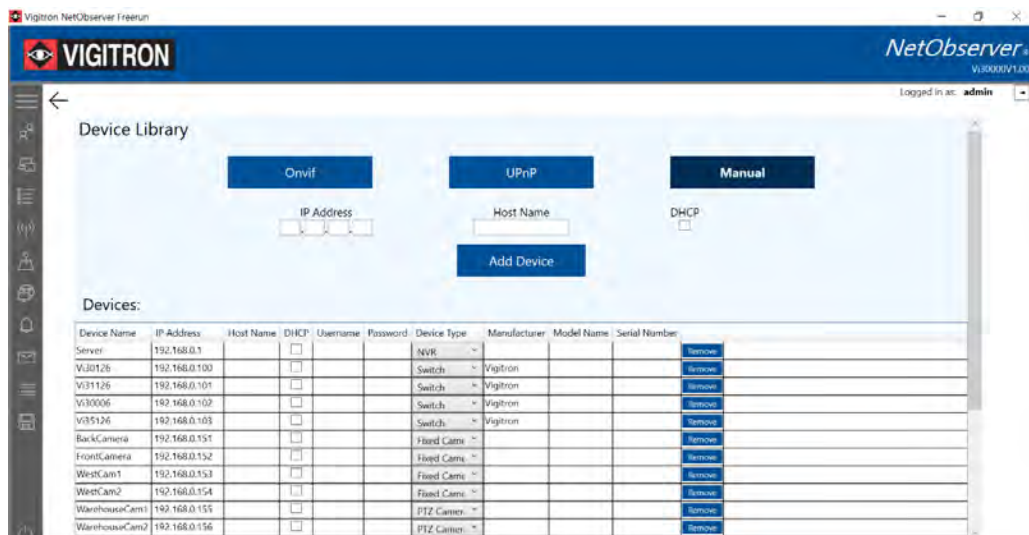


- b. Should a device have its IP address assigned using DHCP will be necessary to assign the hostname that provides the IP Address

Building a Library (Unmanaged Devices)

1. In many cases unmanaged devices do not have an IP address such as an Unmanage network switch
2. The devices connected to the switch, such as network cameras, will have an IP address but may not have the necessary SNMP, UDP, TCP and Syslog to communicate with NetObserver.
3. In this case it is still possible to detect status from the cameras.

Step One:

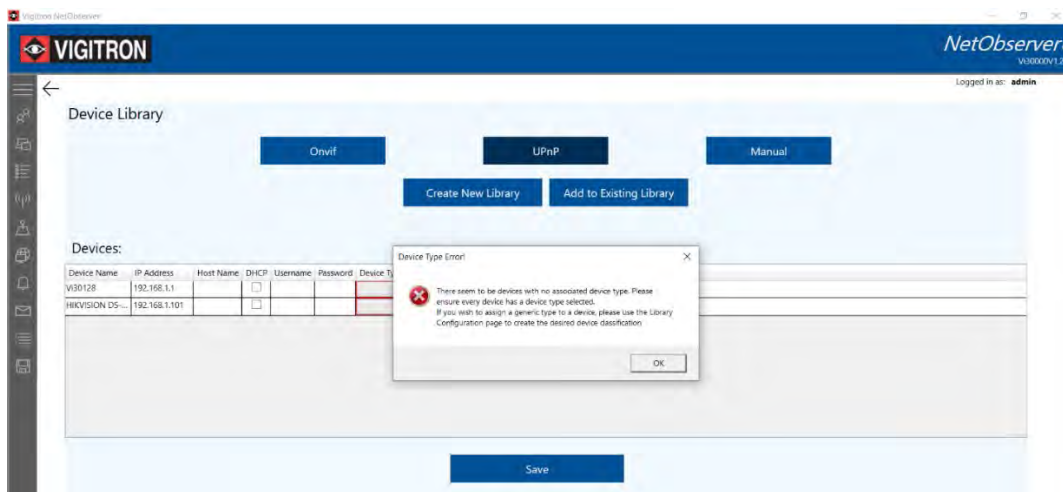


1. In the device library setup use the manual entry to assign any unused IP address. Example is 000.000.000.001
 - a. This IP address will only be to Identity the unmanaged switch so it can be included in mapping and topographical programming
3. Enter the IP address of the of the connected devices such as cameras connected to the switch

4. In the Managed Library programming associate the IP devices connected to the unmanaged switch (see Section 9 Managing the Library)
5. Set up the Ping (see Section 11 Test Generator) To continuously ping IP addressed devices connected to the unmanaged switch. (The Ping must be active to detect status change)
6. You can add unmanaged devices without an IP address by entering an IP address starting with 000.xxx.x.xxx ranging to 000.177.177.177. Once entered you can use the address as with another device in the Map and Topographical Map functions. However, you will not be able to ping the device nor will it indicate connection problems. However, you will be able to access devices with IP connected to an unmanaged device.

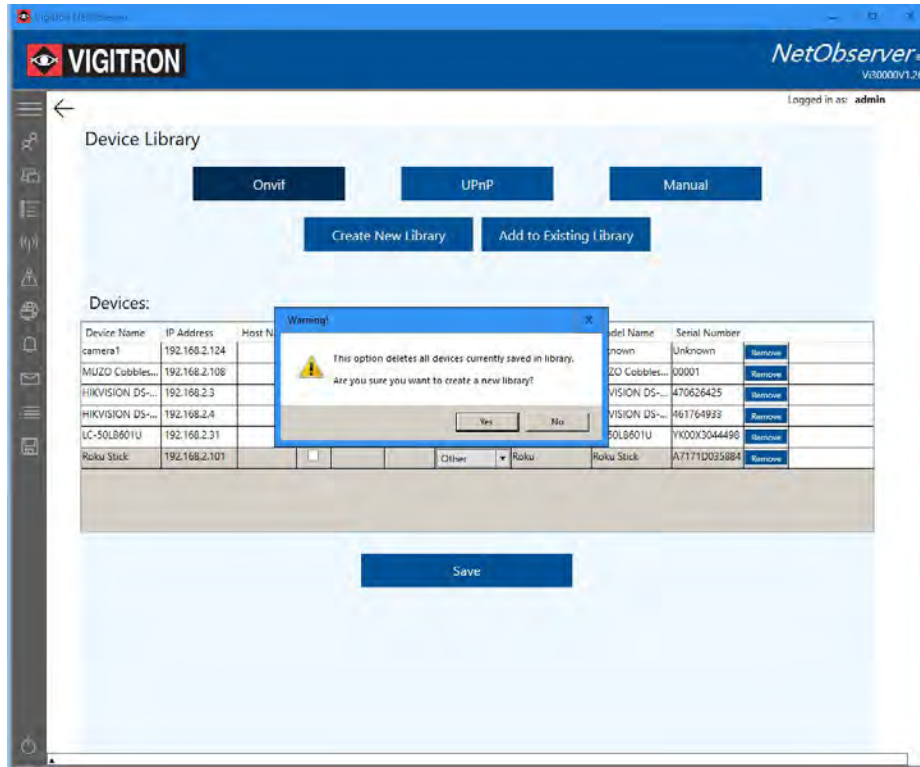
If the device you entered does not have an associated device type:

- Every device must have an associated device type. If an individual device does not please use the Library Configuration and create one.



Creating a New Library

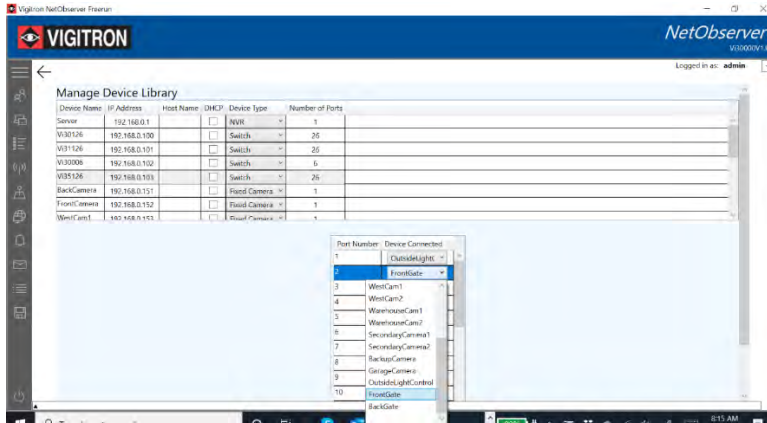
Important Note: If you elect to create a new library it will delete all the devices that were saved in the previous library you are deleting!



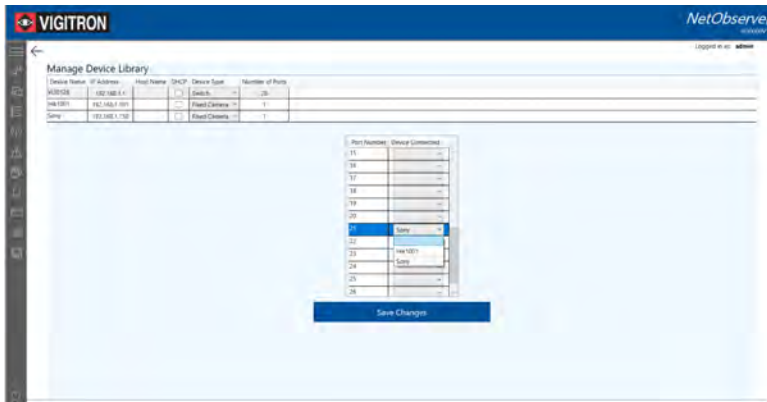
Managing the Library

1. Opening the manage Library button will display all the connected devices.
2. Select a device and using the drop down menu to select a device
3. For devices with more than one port, such as a network switch, you can assign the device connected to the port of that switch by selecting it from the menu for that individual port.
4. When complete select "Save Changes."



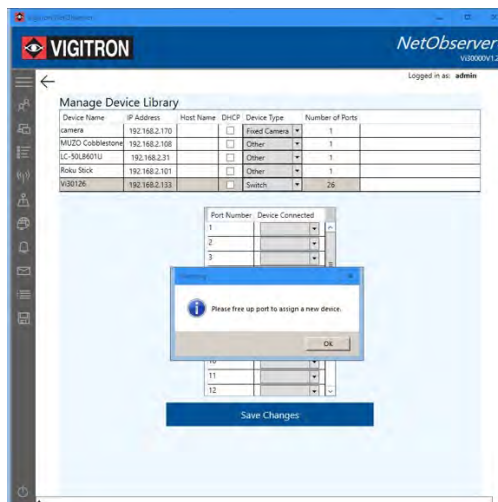


Changing a program device to a port. This is required for connected devices to properly be shown in Map and Topographical Map displays

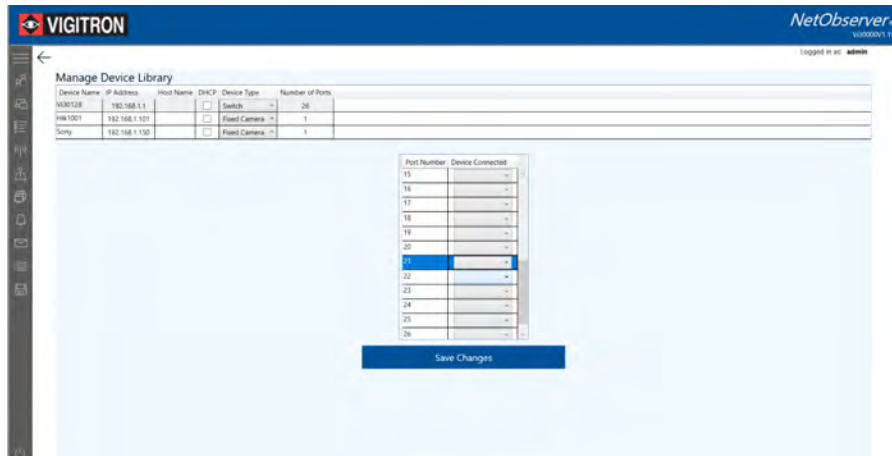


To Free up a port and assign a new device:

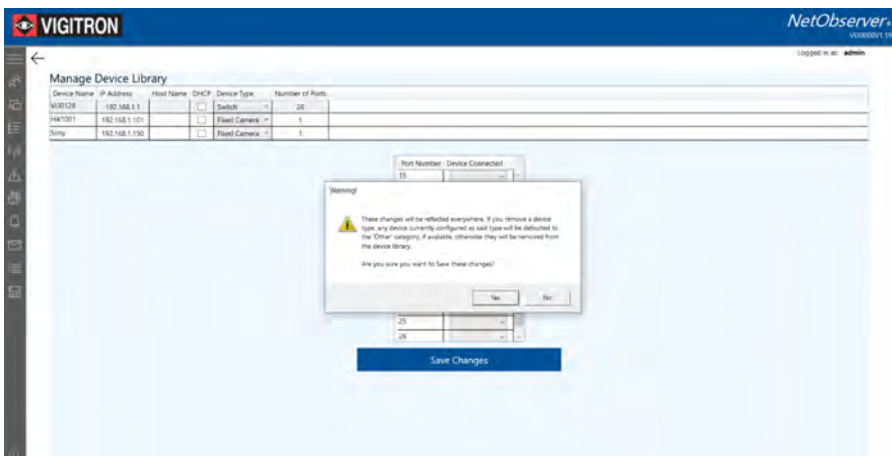
- a. Select and assign a blank device to the port
- b. Save the port to the blank device
- c. Repeat the procedure to assign a new device to the port



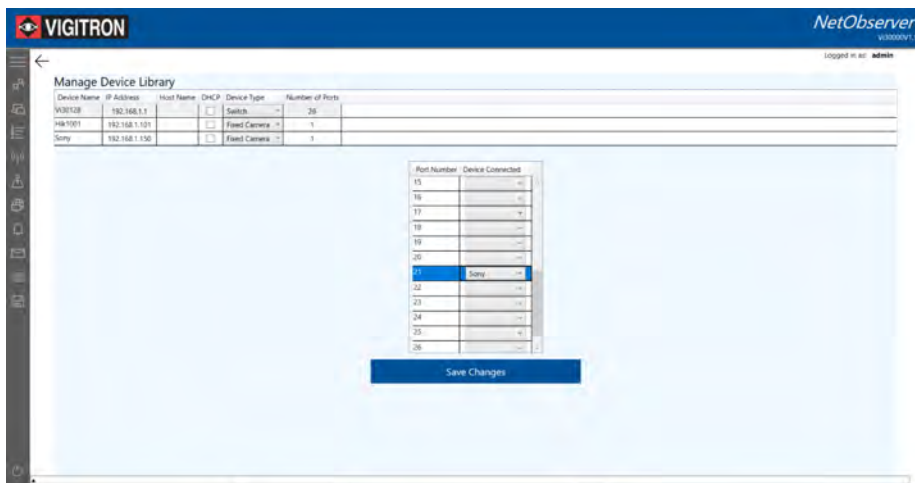
Click on the port where you want to change the connected device.



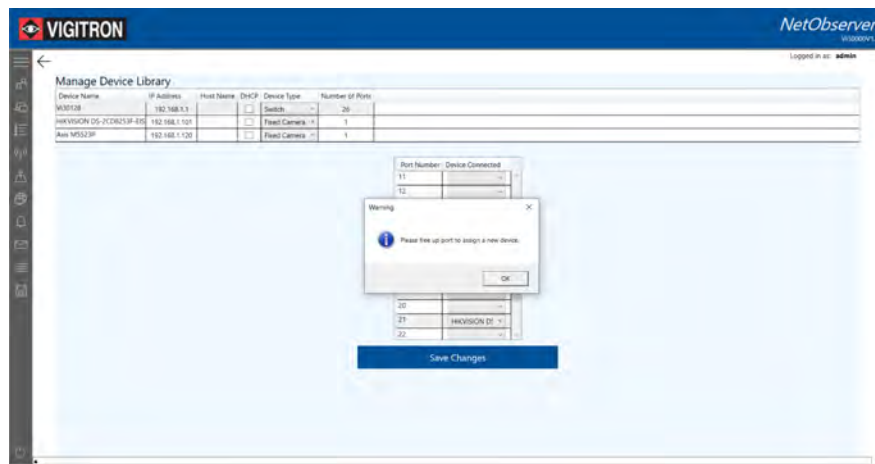
Use the drop-down menu and select a blank input followed by “Save Changes.”



The confirmation will appear – click Yes



Select the new device assigned to the ports and select Save Changes



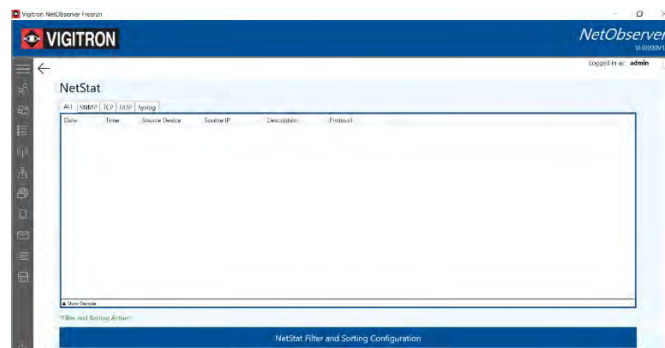
If the previous connected device has not been properly cleared the following pop up will appear—Repeat the procedure.

Section 10: NetStat

Selecting SNMP, TCP, UDP or Syslog will display the received messages from the selected connected devices.

NetStat is only a logging function for Messages and will NOT generate Alerts, but must be programmed in order to receive alerts. Programming requires Enabling each type of communications.

Messages received by NetStat are dependent and generated by the connected device and not NetStat Alerts will NOT function unless NetStat is programmed

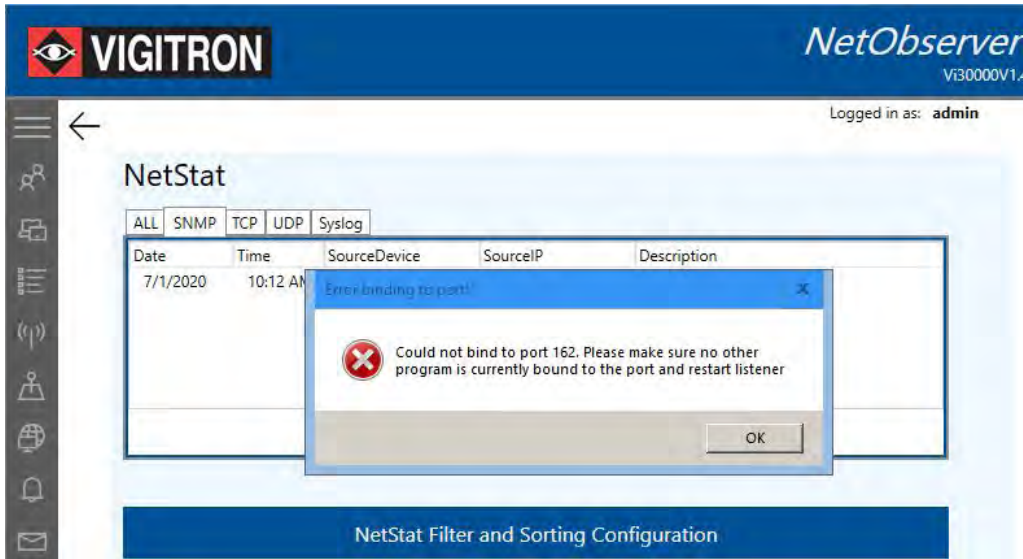


1. For **SNMP** you have to enable or if active disable the listener:

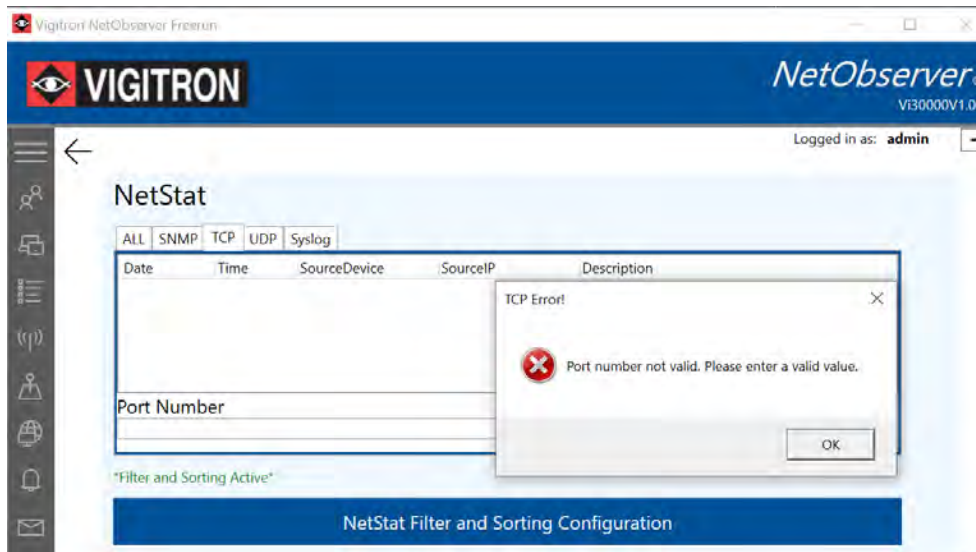


2. If selecting the SNMP function the port is unable to bind the following message will appear (below):

Note: Messages received by NetStat will not result in Alerts or Map color Icon changes unless Alerts are programmed



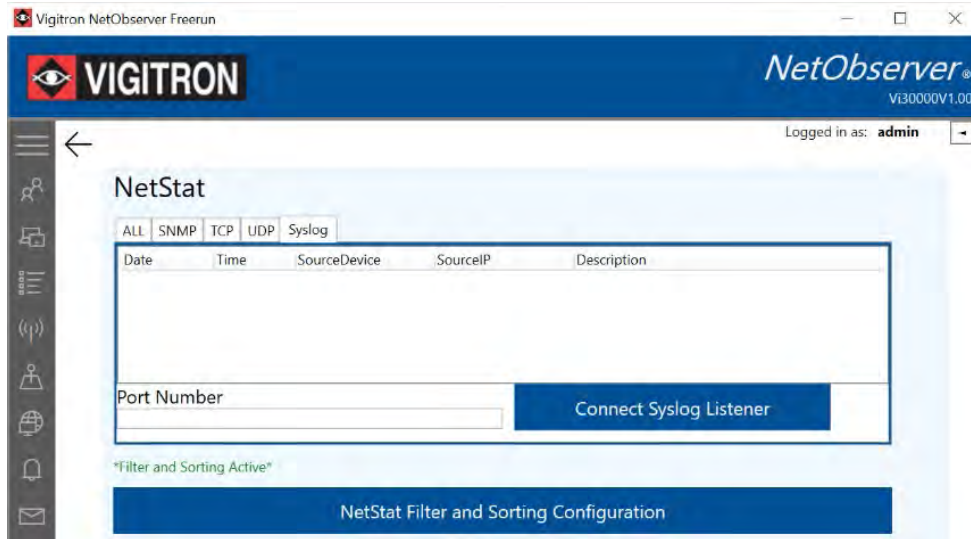
3. When selecting TCP or UDP if the port number is not valid, the following message will appear.
4. You must have a communication link between your network devices and the method selected for communications.
5. The ability to ping a connected device does not mean it will be able to communicate its messages. Specific communication methods require the ports required for communicates are opened and accessible: Syslog Port 514; SNMP Port 162.



1. For **TCP and UDP** once selected the port to the listener:



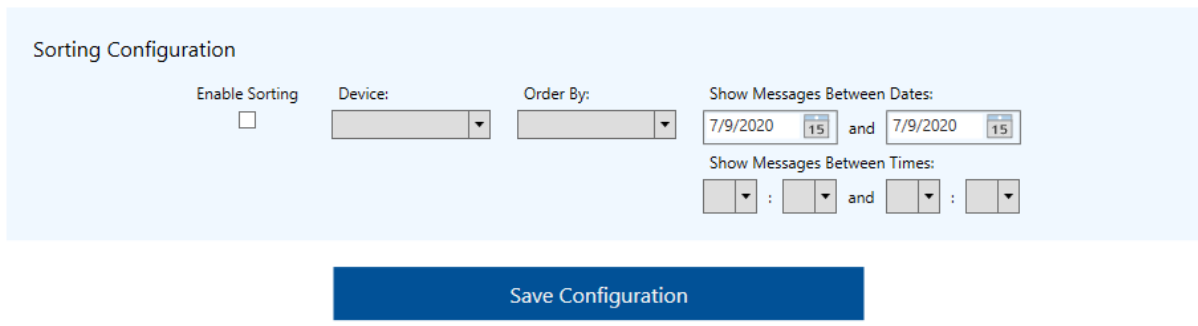
2. The system will automatically default to Port 514 the most used Port for syslog transmission.



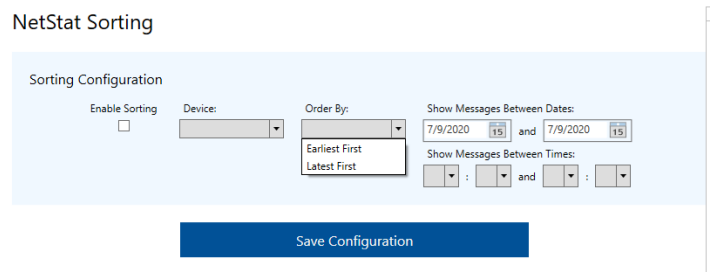
NetStat Sorting Configuration

1. Enable NetStat Sorting by checking the Enable Sorting box .
2. Select the communications: SNMP/TCP/UDP/Syslog or All

NetStat Sorting



3. Select the device to sort using the drop-down menu
4. Select the sorting order
 - a. Earliest First
 - b. Latest First



5. Select the dates to sort.

NetStat Sorting

Sorting Configuration

Enable Sorting

Device:

Order By:

Show Messages Between Dates: 7/9/2020 and 7/9/2020

Show Messages Between Times: : and :

6. Sort works in the following manners: **Both Date and Time must be programmed**
 - a. From is determined by the programmed date + time.
 - b. To is determined by the programmed date + time.
 - c. The result will be: Programmed Device + From (Date + Time) -To (Date + Time)

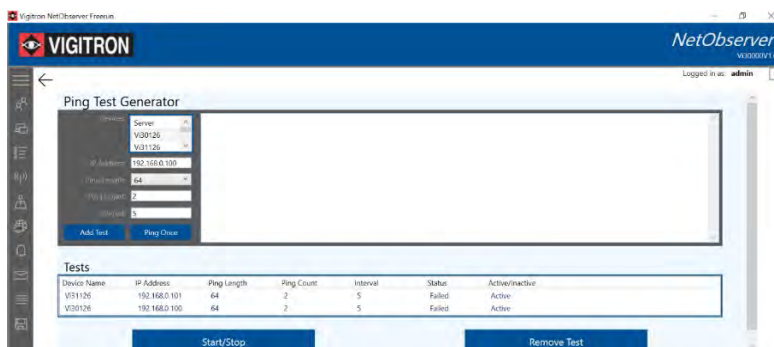
NETSTAT

- 1) Messages received through NetStat are also recorded in the Log.
- 2) **To create alerts from the messages received by NetStat, the device sending the message must have Alerts configured.**
- 3) To set this up, go to "Alerts" and then click on "Alert Configuration."

Section 11: Ping Test Generator

The ping generator is can be used for generating alerts even if SNMP, UDP, TCP and Syslog are not active

1. Select the device from the drop-down menu. The IP address will automatically be filled in.
 - a. You can also enter any IP to determine if it is connected.
2. Enter the ping word size from 64 to 9600 bytes - *it is suggested you use the packet size for that connected device.*
 - a. Enter the number of pings.
 - b. Enter the duration in seconds in between pings.
3. Select Add Test and confirm your setting appear under Test
 - a. You can select only one device at a time and the system will conduct the test in the order set by your programming.
 - b. Select the Ping Once to conduct the test the selected device and the system will conduct one test and stop.
 - c. If you select “Ping Once,” the test will occur once and stop.
 - d. Set the Ping Count to a number between 1 to 20
 - e. Set the Interval between 15-1800 Seconds
 - f. If you select “Add Test” the test will result in a continuous ping of all programmed devices
 - g. You can select any active device and pressing the Start/Stop will “Stop” the ping for that device
 - h. To start pinging after “Stop” is active click the Start/Stop button
4. To delete any test, select the test and click “Remove Test.”

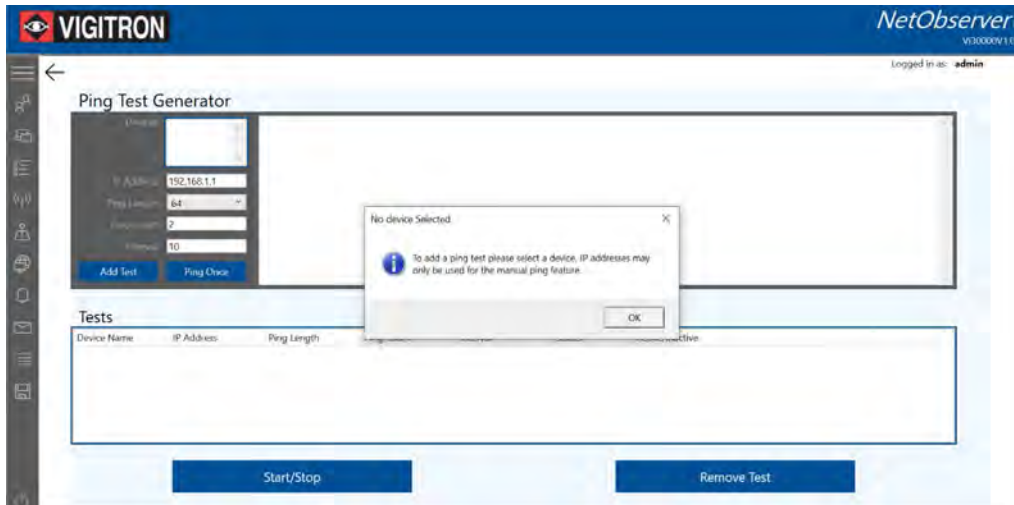


Note: *If you want to continuously monitor a connected device or monitor a connection that is not using SNMP, TCP, UDP and Syslog to communicate with the NetObserver host, add it to the test list.*

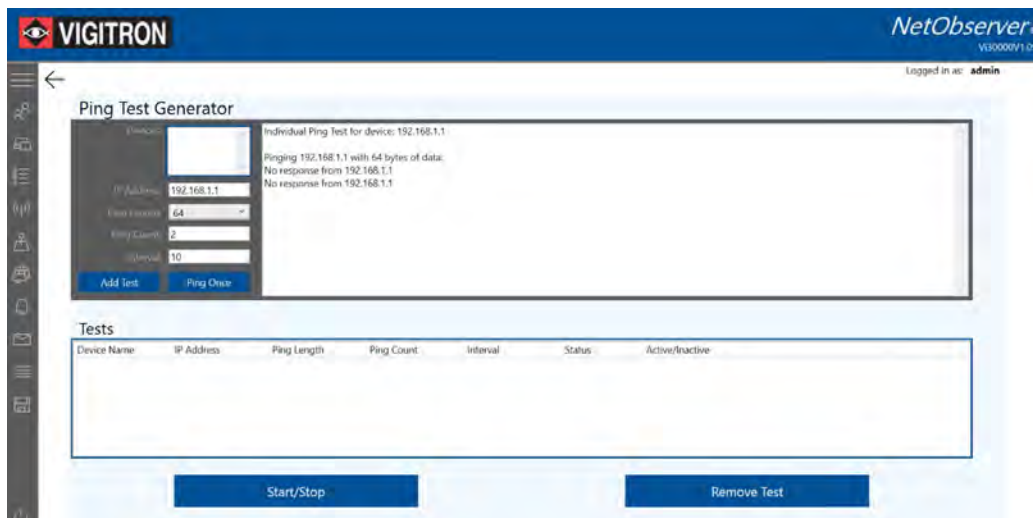
Note: *Pings operate independently from the programming of NetStat and Alerts. When programmed if a Ping is not responded to:*

- a. An Alert will be issued
- b. If NetObserver is minimized the icon located at the bottom of the screen will flash
- c. Alert will be logged
- d. If programmed an email will be sent

The Ping count will determine the sampling rate prior to determining if connect is active or inactive – if one of the samples receives a return ping the connection will be considered active



Devices that are already programmed in NetObserver will appear in the device area and can be directly selected. Only devices programmed in NetObserver can be selected for automatic testing.



You can manually enter any IP address; however, it can only be used as a manual test.

If you enter an address for a non-managed, non-IP addressable device, starting with 000, it will appear on the list but cannot be accessed. If selected the ping will ignore the selection. Example: 000.000.000.001

Note: Occasionally a "Ping" may not be received due to Network traffic. If the Ping Count is set to "1 or even 2, you may experience false "Failed Ping Test" Alerts. To remedy this situation, you should increase your Ping Count. NetObserver will considered a Ping Test successful if any of the pings in the Test are received.

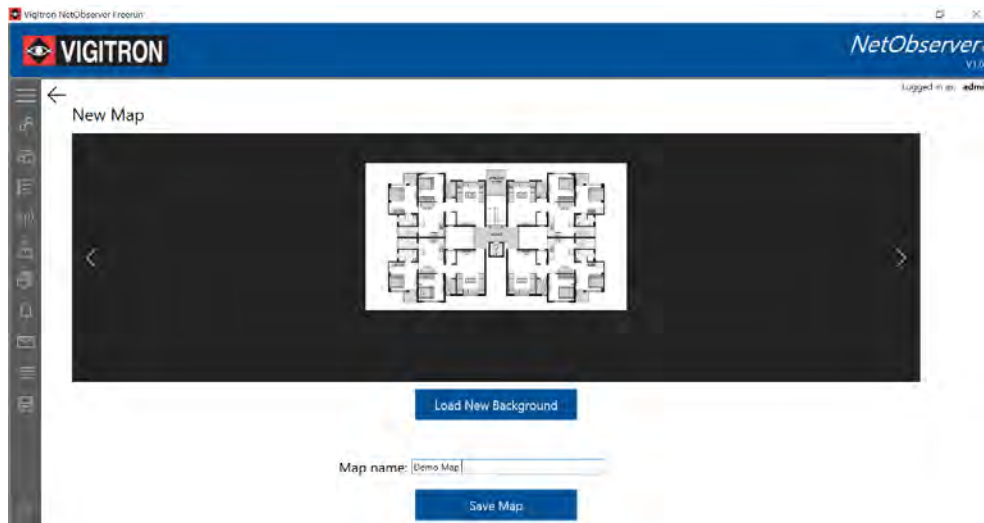
Note: Occasionally a "Ping" may not be received due to Network traffic. If the Ping Count is set to "1 or even 2, you may experience false "Failed Ping Test" Alerts. To remedy this situation, you should increase your Ping Count. NetObserver will considered a Ping Test successful if any of the pings in the Test are received.

Section 12: Mapping

1. Open the mapping feature. Programmed devices will appear on the left.



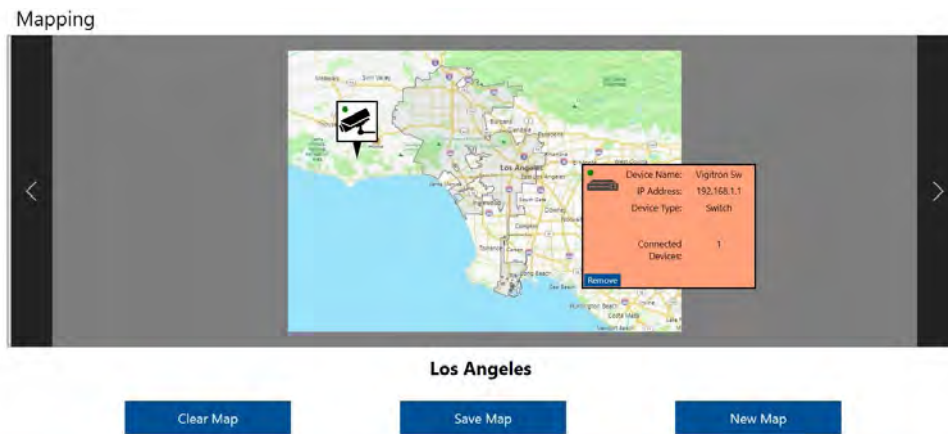
2. Select "load new map" to select a map from your database.
 - a. Give the maps a name and select save – the map will automatically appear on the main map screen.
 - b. Use the right and left arrows to scroll through the saved maps.
 - c. The map will only show the status of individual devices.
 - d. In order to see connections between individual devices to their parent devices, please use the topographical maps.



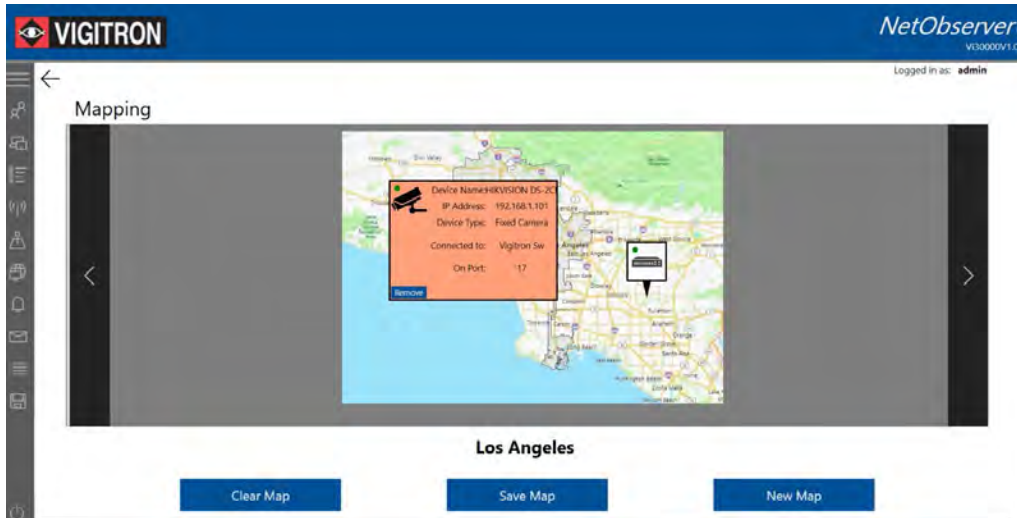
3. Point and click on the connected devices on the left-hand side.
 - a. Drag the device to the desired position on the map.
 - b. The color dot in the device will indicate its status.
 - i. Green: online
 - ii. Red: offline



4. Click on the individual connected device to show its connection information.
 - a. If the connected device has been assigned to a switch the switch and connected port will be shown.

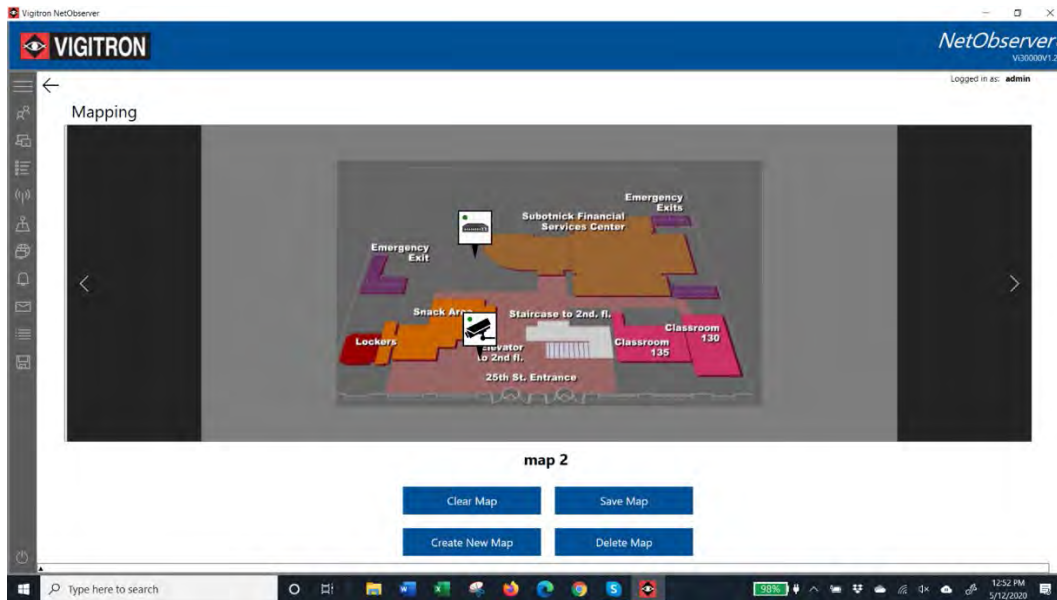


Switches and other “parent” devices will display the number of connected devices.



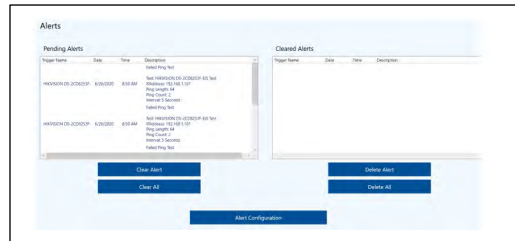
Connected devices will indicate the device and port it is connected to.

Note: When an alert is received the device icon will change from Green to Red. It will remain in the alert state even if the alert is no longer active. To extinguish the alert either delete it from the Alert menu or Refresh the map.



Once a device is positioned within a map it cannot be positioned in any other map.

Mapping and Alerts:



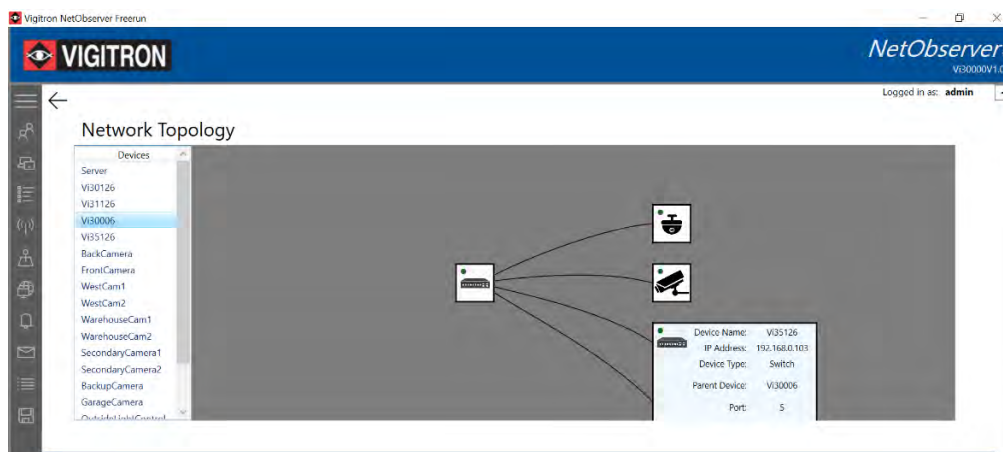
When an Alert occurs the Alerted device's icon status will change from green to red. It will remain as red until the operator acknowledges the Alert and deleting the Alert. After being deleted and if the connection is valid the icon will turn green,

Section 13: Topology

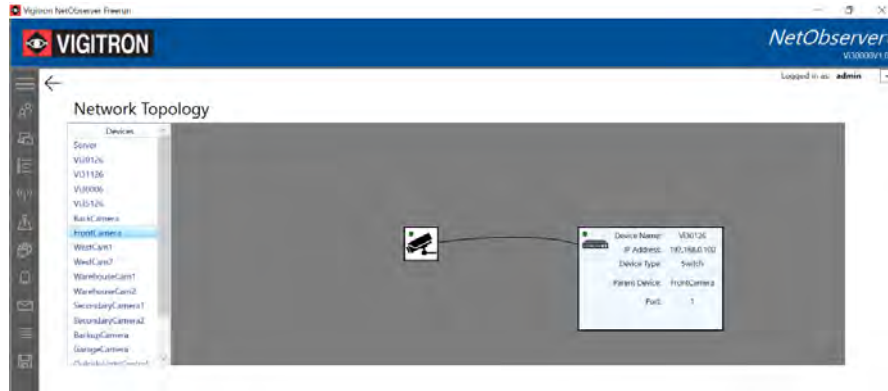
1. Select the Network Topology icon to enter the function.
 - a. Connected devices will appear on the left-hand side of the screen.



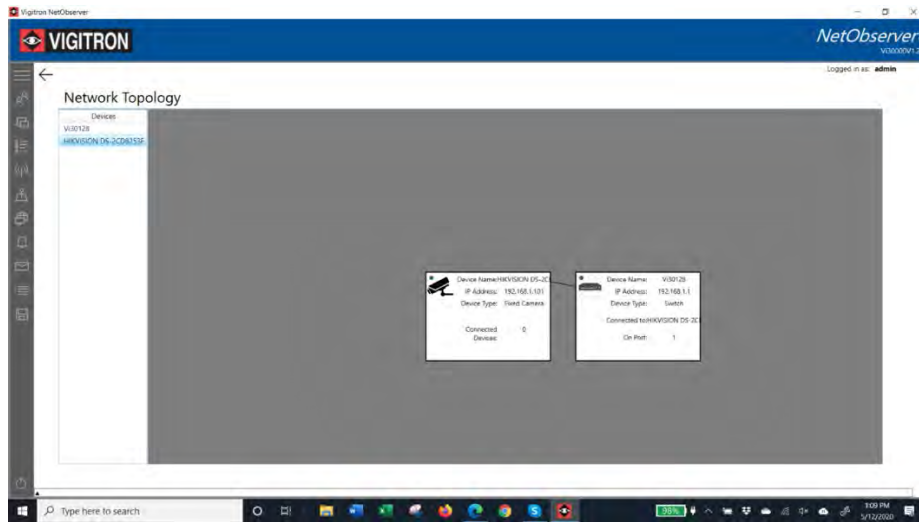
2. Click on a device in the left column to view connected devices.
 - a. If the device has multiple ports point and click on the device icon to view its information and connected devices.
 - b. The color dot in the device will indicate its status.
 - i. Green: online
 - ii. Red: offline



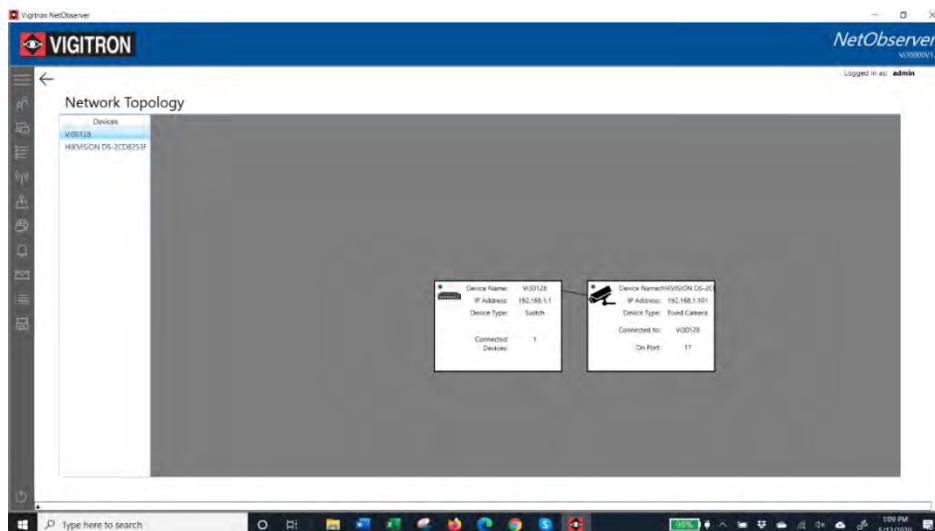
3. To see the status of an individually connected device (i.e. camera), select the device. main screen.
 - a. Point and click on the device to show its information and what it is connected to.



4. If a device connected to a switch is selected it will show as a single port connection. The port to the main device such as switch will show as Port 1.



5. If a switch is selected it will show the port of the connected device to the switch



Alerts

Pending Alerts

Trigger Name	Date	Time	Description
			Failed Ping Test
HIKVISION DS-2CD8253F	6/26/2020	8:50 AM	Test: HIKVISION DS-2CD8253F-EIS Test IPAddress: 192.168.1.101 Ping Length: 64 Ping Count: 2 Interval: 5 Seconds Failed Ping Test
HIKVISION DS-2CD8253F	6/26/2020	8:50 AM	Test: HIKVISION DS-2CD8253F-EIS Test IPAddress: 192.168.1.101 Ping Length: 64 Ping Count: 2 Interval: 5 Seconds Failed Ping Test

Cleared Alerts

Trigger Name	Date	Time	Description
--------------	------	------	-------------

Clear Alert

Clear All

Alert Configuration

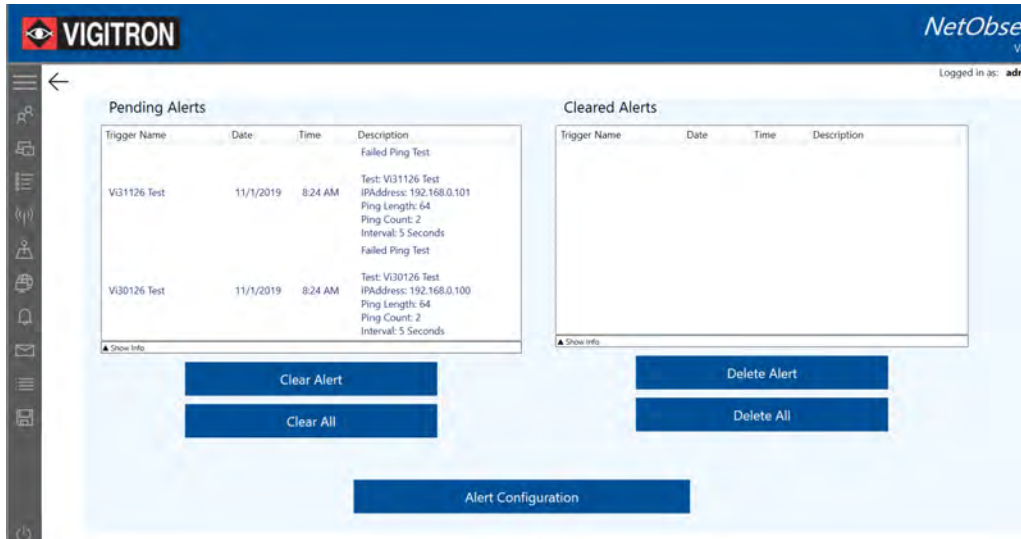
Delete Alert

Delete All

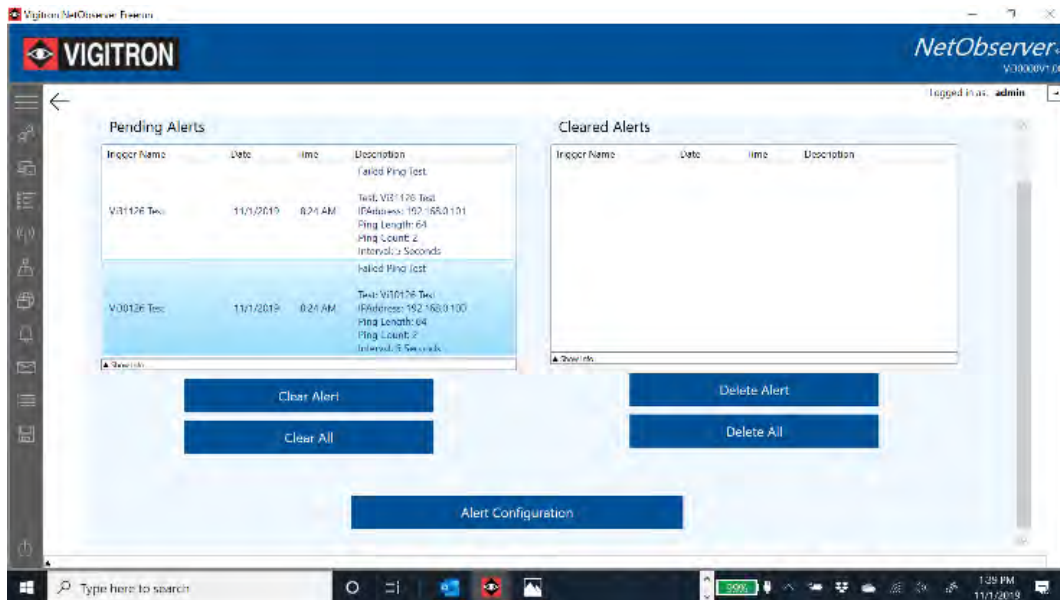
If a status icon is shown in Red. It will remain in Red until the operator deletes the alerts

Section 14: Alerts

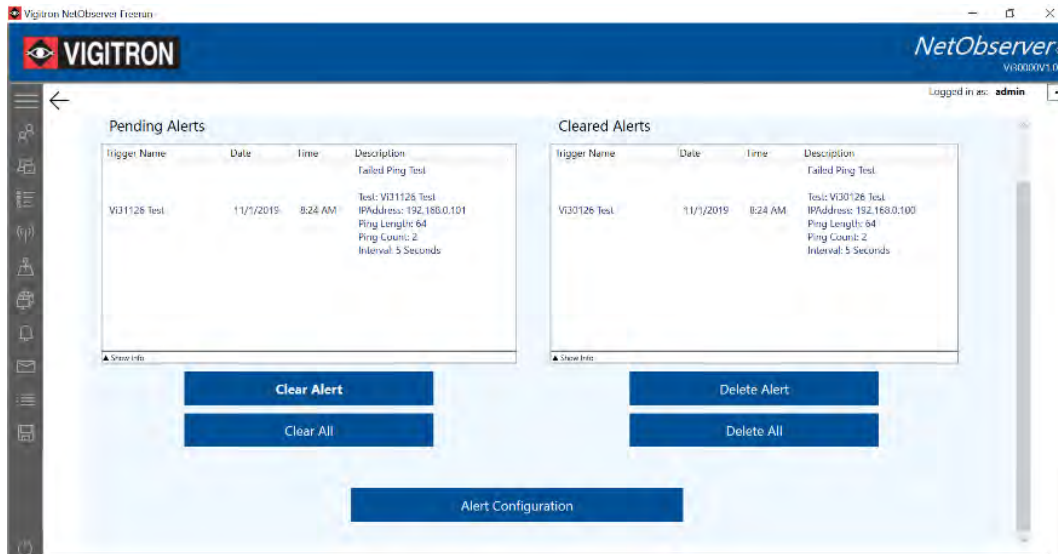
1. The Pending Alerts will show all alerts as per the previous programming.



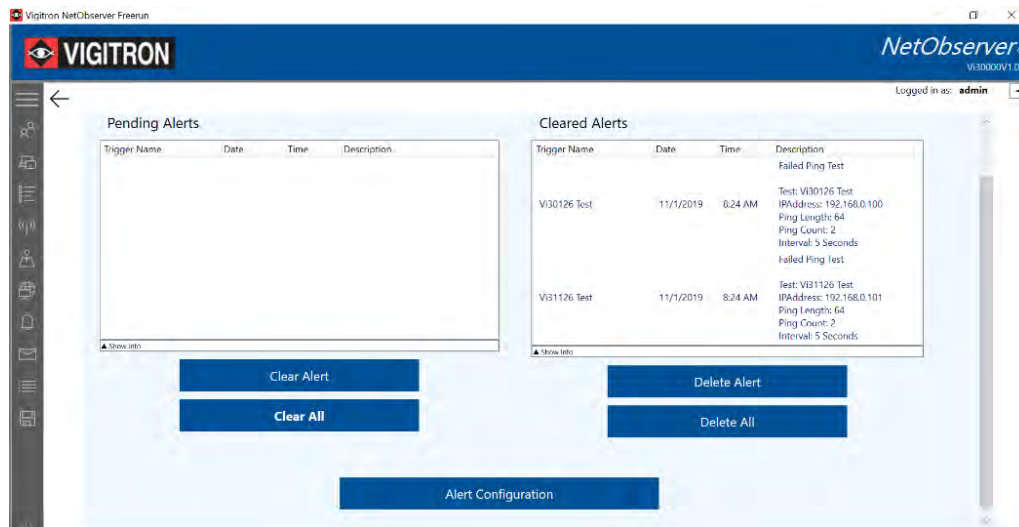
2. To Delete an individual alert, highlight the alert and select "Clear Alert."



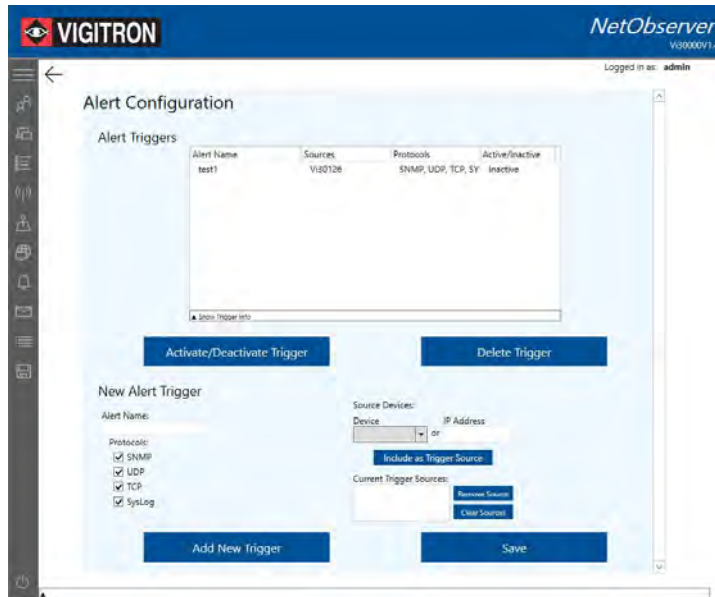
3. The selected alert will move over to the “Cleared Alerts” box.



4. To clear all the alerts, select the “Clear All” button.
 - a. All the alerts in the “Pending Alerts” box will move over to the “Cleared Alerts” box.



5. To set up alerts, select the “Alert Configuration.”
 - a. You can enter a custom name for your trigger.
 - b. Select the Protocol - this must match the protocol the message will be transmitted on.
 - c. Select all the trigger events that will apply.
 - d. Select a device from the drop down menu or enter an IP address.
 - i. Enter as “Include as Trigger Source.”
6. To remove a source, highlight and select “Remove Source.”
 - a. To remove all sources, select “Clear Sources.”



ALERTS

1) Steps to set up Alerts:

- a) Name the Alert.
- b) Select one or more communication protocols the particular device will be using to communicate with NetObserver.
- c) Select the device from the drop down menu or input the device's IP Address, and then click "Include as Trigger Source".
- d) Click "Add New Trigger", and a summary of the Alert will appear above in the "Alert Triggers" box.
- e) Click "Save" to store and activate the alert.
- f) **For Alerts to be captured by NetObserver the protocol/s must be enabled in NetStat.**

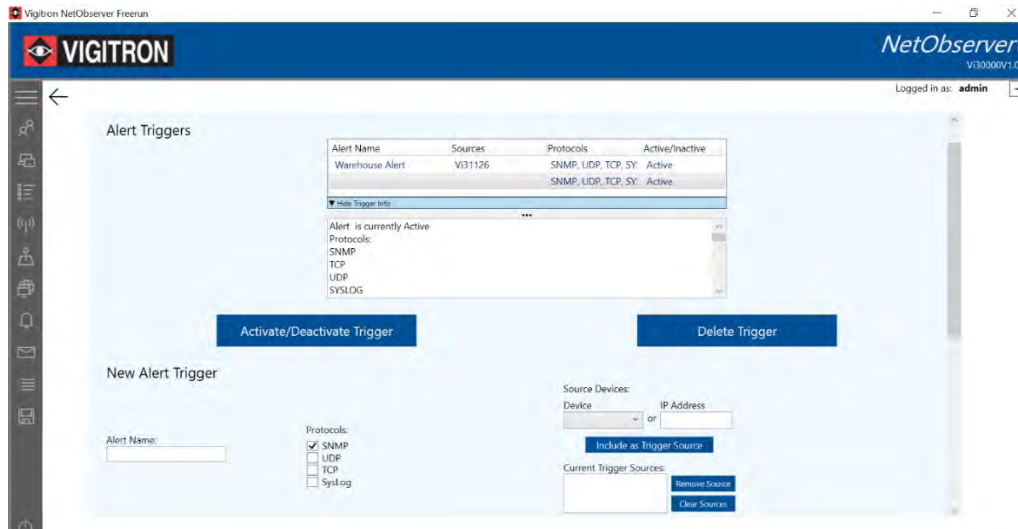
2) After activating or deactivating an alert, be sure to click "Save" or the changes will not be applied.

3) After deleting an alert, click "Save".

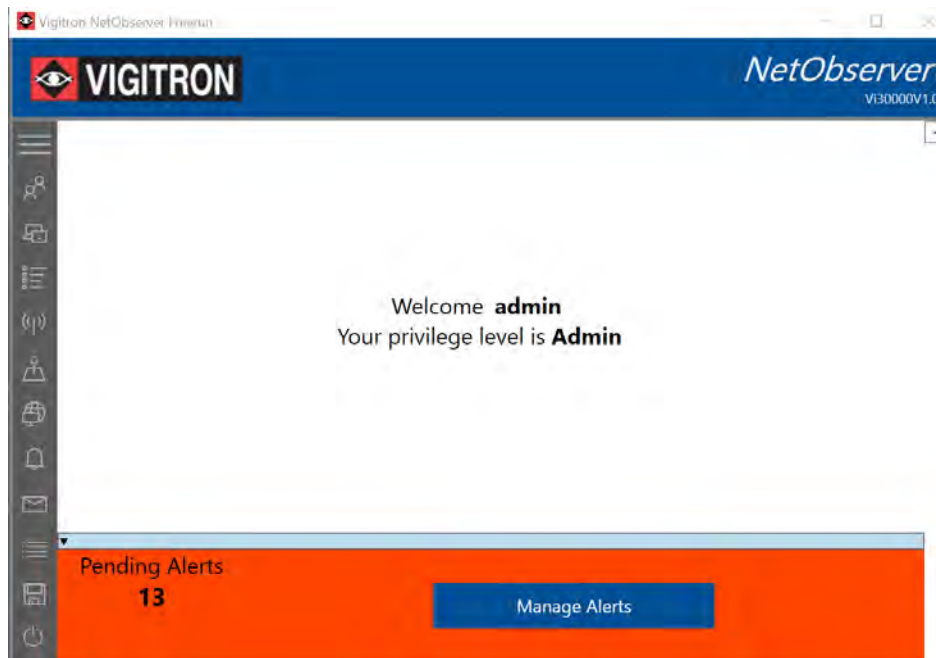
4) **Alert must be programmed for the following to occur:**

- a. Map and Topographical map icon changes
- b. Alerts to appear on the bottom of the screen if NetObserver is operating in the minimized mode.
- c. Alerts to appear at bottom of the screen if NetObserver is operating in the full screen mode
- c. Sending emails if programmed

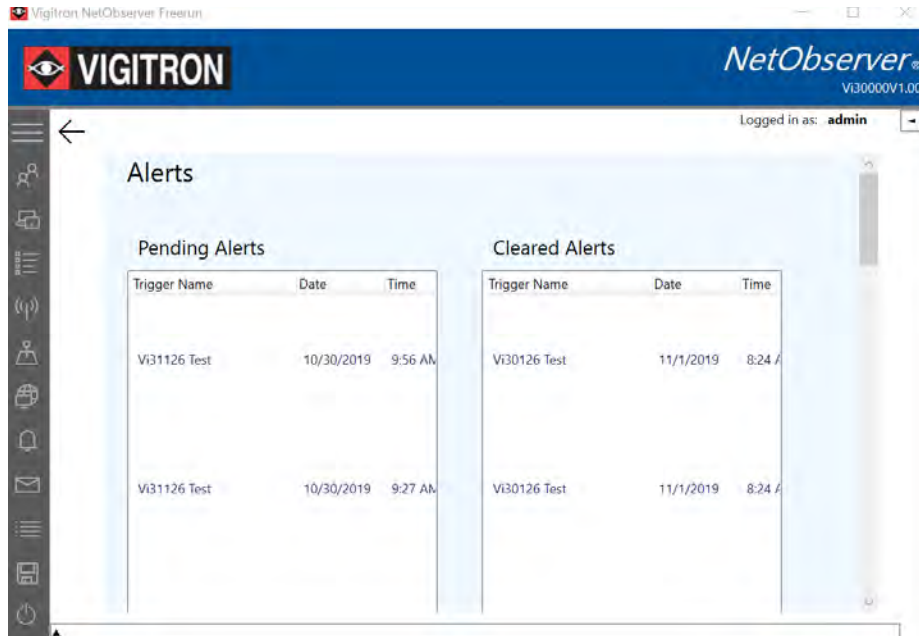
7. To view your triggers, select “Activate/Deactivate Triggers.”
 - a. It will show the source, protocols, and the state as Active/Inactive.
 - b. Select the Trigger to verify its status and the selected protocol.



8. To deactivate an alert, select the alert and click “Delete Trigger.”



9. When alerts are active and receive the above notification will appear:



10. Click the “Managed Alerts” button to see and manage alerts.

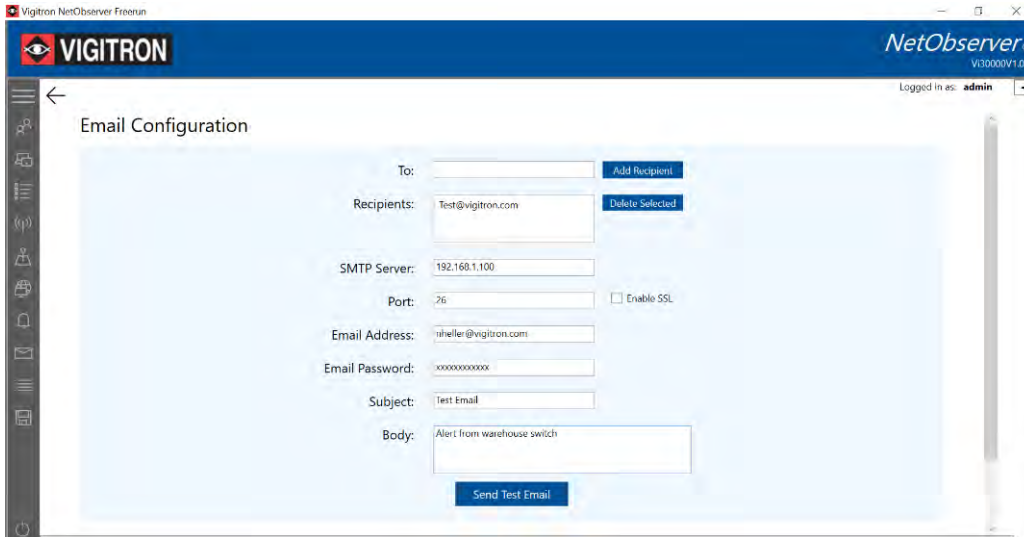
Section 15: Email Settings

The screenshot shows the 'Email Configuration' interface in the VigitrON NetObserver. The 'To:' field is populated with 'Test@vigitrON.com'. The 'Add Recipient' button is highlighted in blue. The 'Recipients' box is currently empty. Below this, there are input fields for 'SMTP Server', 'Port' (set to 25), 'Email Address', 'Email Password', 'Subject', and 'Body'. An 'Enable SSL' checkbox is also present. At the bottom of the form is a 'Send Test Email' button.

1. Selecting the “Add Recipient” will move the programmed email address to the “Recipients” box, allowing a new email address to be entered.

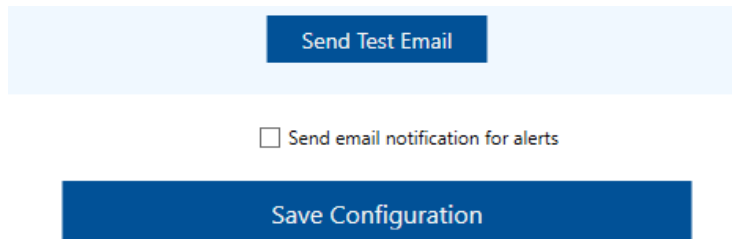
This screenshot shows the same 'Email Configuration' page after the 'Add Recipient' action. The 'To:' field is now empty, and the 'Recipients' box contains 'test@vigitrON.com'. The 'Add Recipient' button remains highlighted. The other configuration fields (SMTP Server, Port, Email Address, Email Password, Subject, Body, and Send Test Email button) are unchanged from the previous screenshot.

2. Fill in the rest of the information making certain it complies - Subject and Body can be customized.
 - a. It is suggested you send a test email to verify the settings are correct.



3. Public Email

- a. Configuring messages to public email address is possible.
- b. However, if NetObserver is operating within a private network, outgoing email messages to public emails maybe blocked by firewalls.
 - i. If this is the case please check with your IT Director.



4. To activate email for alerts check the “Send email notification for alerts”

Email Alert Configuration – Gmail

To	Insert the email address that the notifications should be sent to, and then click “Add Recipient.” Multiple addresses can be added to this list. To remove a recipient’s address, highlight and then click “Delete Selected.”
SMTP Server	Type “smtp.gmail.com” into this text box.
Port	Type “587” in the text box and check the “Enable SSL” box.
Email Address	Insert your Gmail Address. (You can also include this address as a recipient)
Email Password	Insert your Gmail password.
Subject	Type the text that will be displayed in the recipients’ email. For example: “NetObserver Alert Notification”.
Body	NetObserver will insert detailed alert information in the body of the email. You may include extra text to the messages by inserting it here.

- The “Send Test Email” button is used to verify that the email messages are configured properly.
- Check the “Send email notification for alerts” to enable this feature.
- Click the “Save Configuration” button to prevent loss of your setup information.
- By default, Gmail will block 3rd party applications from using the email server. To enable this feature, you will need to log into your Gmail account and turn on “Less secure app access.”

Email Alert Configuration - Yahoo

POP Settings for Yahoo Mail:

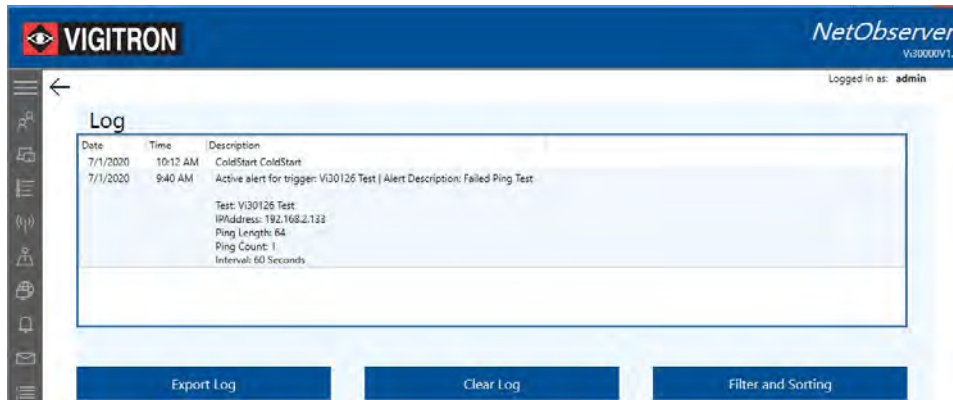
- Server - smtp.mail.yahoo.com
- Port - 465 or 587
- Requires SSL - Yes
- Requires TLS - Yes (if available)
- Requires authentication – Yes

IMAP server settings for Yahoo Mail:

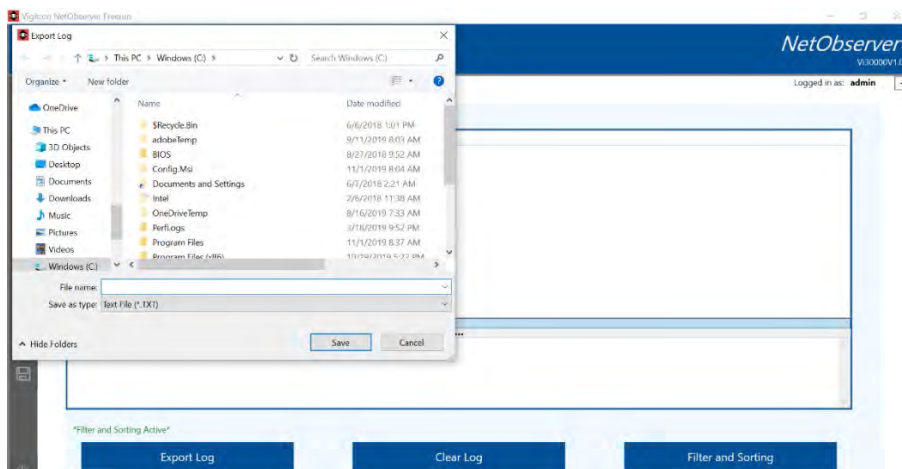
- Server - smtp.mail.yahoo.com
- Port - 465 or 587
- Requires SSL - Yes
- Requires authentication - Yes

Section 16: Logs

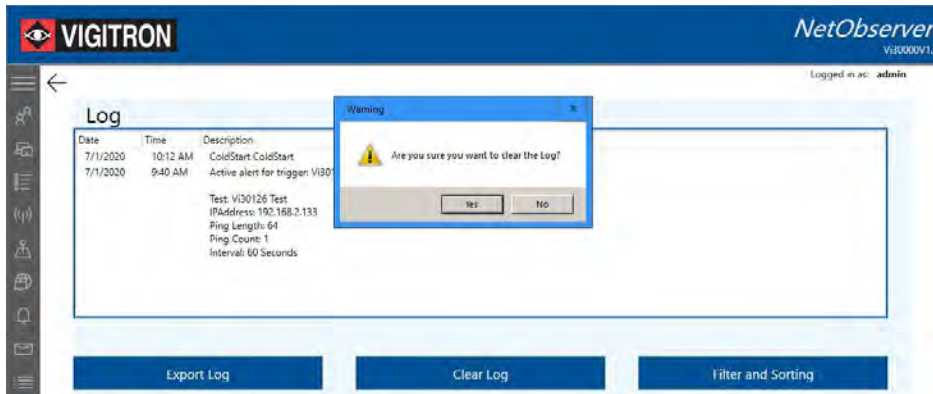
1. Select the “Log” icon to enter the Log mode.
 - a. All messages received as per previous programming will be shown.



2. To Save the log, select “Export Log.”
 - a. The Windows™ file screen will appear.
 - b. Name the file and save it in the same manner as any Window™ file.
 - c. Files can be saved as .txt or .csv formats.



3. To clear the log, Select “Clear Log.” A pop up will ask you to verify your decision:



4. Sorting the Log

Log Sorting

Sorting Configuration

Enable Sorting

Device:

Order By:

Show Messages Between Dates: 7/9/2020 15 and 7/9/2020 15

Show Messages Between Times: : and :

Save Configuration

5. Check the box enable sorting
6. Use the drop-down menu to select the device to be sorted from the list.
 - a. Selecting the Blank field to include all entries within the programmed range
7. Sort works in the following manners: Both Date and Time must be programmed
 - a. From is determined by the programmed date + time.
 - b. To is determined by the programmed date + time.
 - c. The result will be: Programmed Device + From (Date + Time) -To (Date + Time)

Reading Logs. Logs will show the source of the received information: Message (Netstat/Alert/Ping)

Date	Time	Description
7/8/2020	9:44 AM	PoE_Off Port 01
7/8/2020	9:44 AM	Link Down physical port 01
7/8/2020	9:43 AM	Active alert for trigger: V330126 Alert Description: Message Received: Trigger Name: V330126 Device Source: V330126 IPAddress Source: 192.168.2.133 Message Content:PoE_Off Port 07
7/8/2020	9:43 AM	Active alert for trigger: V330126 Alert Description: Message Received: Trigger Name: V330126 Device Source: V330126 IPAddress Source: 192.168.2.133 Message Content:Link Up physical port 01
7/8/2020	9:43 AM	Active alert for trigger: V330126 Alert Description: Message Received: Trigger Name: V330126 Device Source: V330126 IPAddress Source: 192.168.2.133 Message Content:PoE_Off Port 01
7/8/2020	9:43 AM	Active alert for trigger: V330126 Alert Description: Message Received: Trigger Name: V330126 Device Source: V330126 IPAddress Source: 192.168.2.133 Message Content:Link Down physical port 07
7/8/2020	9:37 AM	Active alert for trigger: V330126 Test Alert Description: Failed Ping Test Test: V330126 Test IPAddress: 192.168.2.133 Ping Length: 64 Ping Count: 1 Interval: 60 Seconds
7/8/2020	9:36 AM	Active alert for trigger: V330126 Test Alert Description: Failed Ping Test Test: V330126 Test IPAddress: 192.168.2.133 Ping Length: 64 Ping Count: 1 Interval: 60 Seconds

Message format

Format of Messages when elevated to Alert conditions

Alert format from failed Ping Tests

NetState and Log Viewing

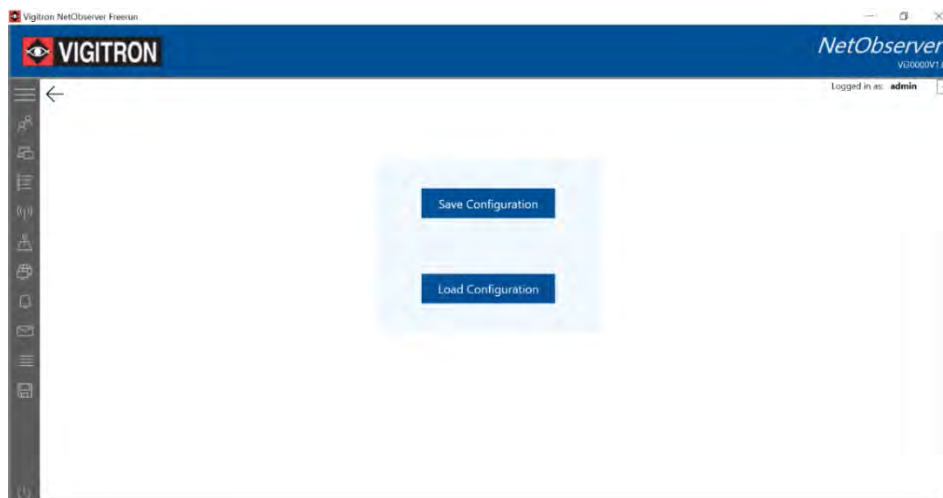
NetStat						
All	SNMP	TCP	UDP	System		
Date	Time	Source Device	Source IP	Description	Protocol	
7/14/2020	8:27 AM	V30126	192.168.2.133	PoE_Off Port 15	SNMP	
7/14/2020	8:27 AM	V30126	192.168.2.133	PoE_On Port 13	SNMP	
7/14/2020	8:27 AM	V30126	192.168.2.133	Link Up physical port 13	SNMP	
7/14/2020	8:27 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	7:41 AM	Unknown		Error decoding message.	SNMP	
7/14/2020	7:56 AM	V30126	192.168.2.133	Link Up physical port 21	SNMP	
7/14/2020	7:56 AM	V30126	192.168.2.133	PoE_On Port 21	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	Link Down physical port 21	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	PoE_Off Port 21	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	Link Up physical port 19	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	PoE_On Port 19	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	Link Up physical port 19	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	PoE_On Port 19	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	PoE_Off Port 19	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	Link Up physical port 15	SNMP	
7/14/2020	8:13 AM	V30126	192.168.2.133	PoE_On Port 15	SNMP	
7/14/2020	8:13 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_Off Port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	Link Up physical port 07	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_On Port 07	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_Off Port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	Link Up physical port 07	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_On Port 07	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	Link Down physical port 07	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	Link Up physical port 07	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	PoE_On Port 15	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	PoE_Off Port 15	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	Link Up physical port 17	SNMP	
7/14/2020	8:18 AM	V30126	192.168.2.133	PoE_On Port 15	SNMP	
7/14/2020	8:18 AM	V30126	192.168.2.133	PoE_On Port 17	SNMP	
7/14/2020	8:22 AM	V30126	192.168.2.133	Link Down physical port 13	SNMP	

As alerts are received, they will be positioned at the top of the log

NetStat						
All	SNMP	TCP	UDP	System		
Date	Time	Source Device	Source IP	Description	Protocol	
7/14/2020	7:41 AM	Unknown		Error decoding message.	SNMP	
7/14/2020	7:56 AM	V30126	192.168.2.133	Link Up physical port 21	SNMP	
7/14/2020	7:56 AM	V30126	192.168.2.133	PoE_On Port 21	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	Link Down physical port 21	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	PoE_Off Port 21	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	Link Up physical port 19	SNMP	
7/14/2020	8:11 AM	V30126	192.168.2.133	PoE_On Port 19	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	PoE_Off Port 19	SNMP	
7/14/2020	8:12 AM	V30126	192.168.2.133	Link Up physical port 15	SNMP	
7/14/2020	8:13 AM	V30126	192.168.2.133	PoE_On Port 15	SNMP	
7/14/2020	8:13 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_Off Port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	Link Up physical port 07	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_On Port 07	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:15 AM	V30126	192.168.2.133	PoE_Off Port 07	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	Link Down physical port 07	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	Link Up physical port 15	SNMP	
7/14/2020	8:17 AM	V30126	192.168.2.133	PoE_On Port 15	SNMP	
7/14/2020	8:18 AM	V30126	192.168.2.133	Link Down physical port 15	SNMP	
7/14/2020	8:18 AM	V30126	192.168.2.133	Link Up physical port 17	SNMP	
7/14/2020	8:18 AM	V30126	192.168.2.133	PoE_On Port 15	SNMP	
7/14/2020	8:18 AM	V30126	192.168.2.133	PoE_On Port 17	SNMP	
7/14/2020	8:22 AM	V30126	192.168.2.133	Link Down physical port 13	SNMP	

When the log is re-entered alerts will appear in the time order

Section 17: Recovery



It is recommended once your software is configured you save your configuration. In the event you have to re-load select the "Load Configuration" followed by selecting the file containing your configuration.

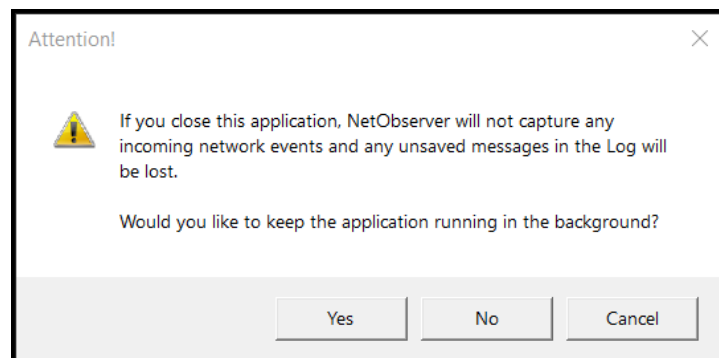
After your programming is complete you can save your program by clicking the Save/load configuration button.

Selecting the “Save” configuration will expose the Windows™ file menu, select a location and name for your file.

To load your configuration, select the “Load Configuration” button followed by your file.

Note: *If you want to load your file on another computer than the one it was created on, it must be authorized to run the NetObserver software*

Section 18: Log Out – Run in Minimize /Background/Shut Down



Important Note: Prior to downloading your configuration use the Log feature and save your Alert logs. They will Not be saved when downloading and restoring the configuration

Minimize Operation

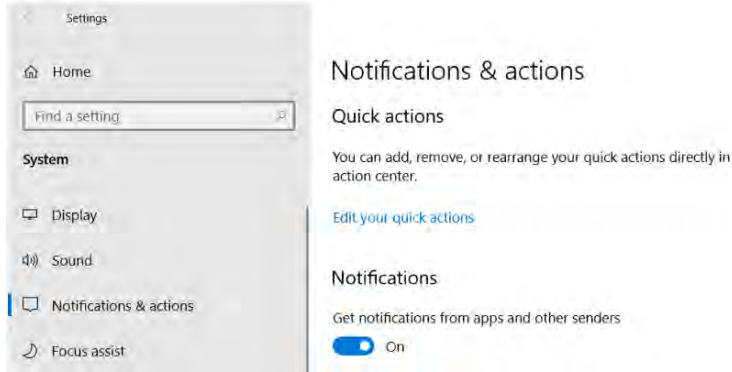
You can minimize NetObserver. When NetObserver is minimized it remain operational in the background. When alerts are received the icon will flash indicating the alert. Click on the icon to expand NetObserver to full screen to investigate the Alert



Running in Background Operation

2. You can also choose to run NetObserver in the background

First confirm your Windows™ program is set up to receive notifications



In Windows settings make certain Notifications are set to on



When running the background NetObserver will display Alerts. In order to receive these Alerts Windows 10 Must be configured to receive alerts



To configure Windows alert right click the alert icon located at the screen right side, select Focus assist and select Off

Shutting Down or Putting Computer in Sleep Mode

Restarting a computer while NetObserver is running will close NetObserver. When the computer is again running NetObserver remains closed. However once NetObserver is opened to the login screen, It will immediately begin listening and reacting to Alerts even without being logged into. The user will need to log back in to view or configure Alerts. Any previously logged data in the prior to shut down or restart in Log or NetStat will be lost.

Hibernating or putting a computer to sleep does not affect NetObserver. However, NetObserver will not be able to function during this time.



1. If you select that you want to exit the program, to avoid losing the existing log, select "No " and then "Would you like to save the log" will appear, if you select yes.
 - a. Save the file to a location you select as .CSV or .Txt
 - b. .CSV can then be opened in Excel and convert to an Excel file

It is recommended to save logs each day or whenever it contains important information