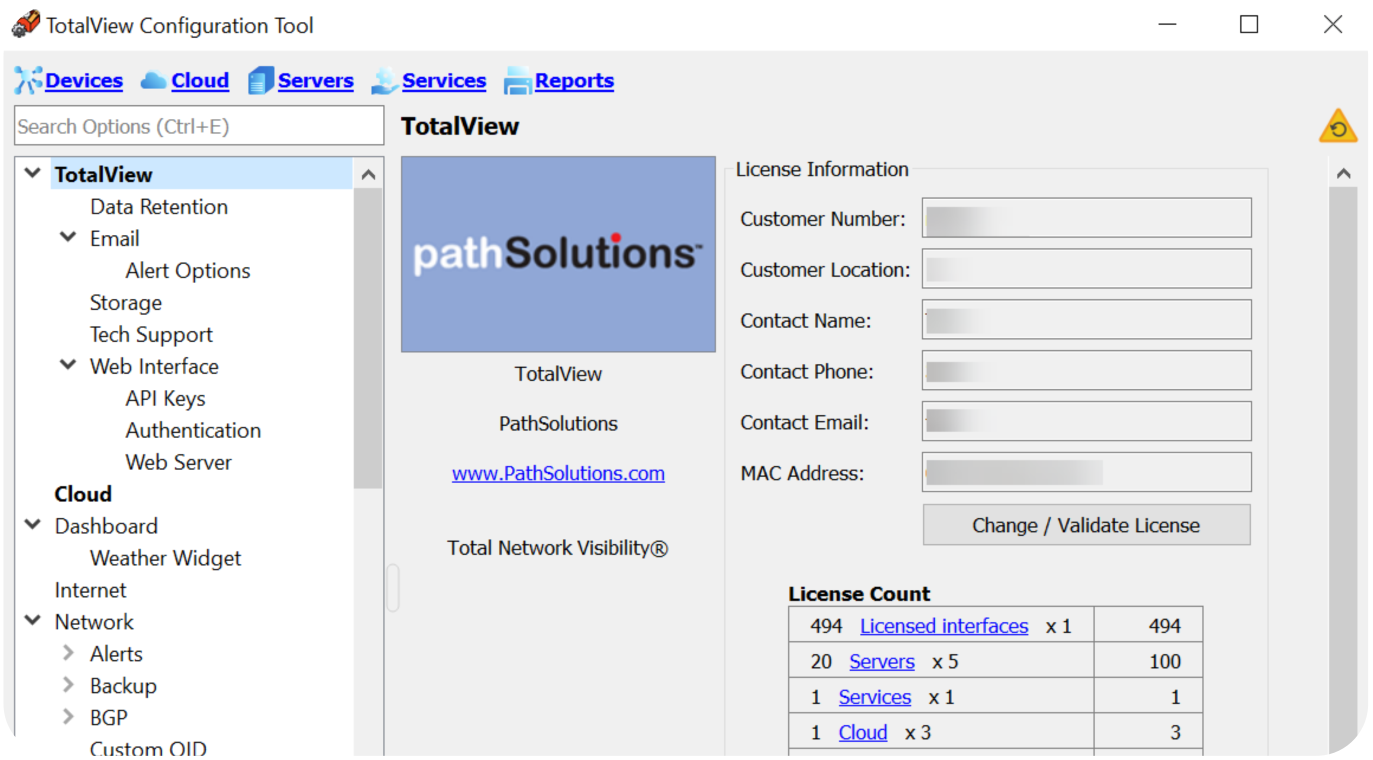
pathSolutions

TotalView 14.1 Administration Guide



TotalView

License Information

Customer Number: [redacted]

Customer Location: [redacted]

Contact Name: [redacted]

Contact Phone: [redacted]

Contact Email: [redacted]

MAC Address: [redacted]

License Count

494 Licensed interfaces x 1	494
20 Servers x 5	100
1 Services x 1	1
1 Cloud x 3	3

NetOps | SecOps | Telecom Ops | RemoteInsight

PathSolutions, Inc.

www.PathSolutions.com | Support@PathSolutions.com | Sales@PathSolutions.com

Document and Software Copyrights

PathSolutions, Inc. reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to, typographical, arithmetic, or listing errors.

Trademarks

PathSolutions, TotalView, QueueVision, RemoteInsight, Total Cloud Visibility, Total Network Visibility, and Total VoIP Visibility are Registered Trademarks of PathSolutions, Inc. in the United States and/or other countries. Network Weather Report and Network Prescription are Trademarks of PathSolutions, Inc. in the United States and/or other countries.

Version Information

TotalView
Version: 14.1
Date: April 17, 2024

Company Information

PathSolutions
3080 Olcott Street #A210
Santa Clara, CA 95054

www.PathSolutions.com
Support@PathSolutions.com
Sales@PathSolutions.com

(877) 748-1777 (toll-free main)
(408) 748-1777 (main)
(408) 748-1666 (fax)
(877) 748-1444 (7x24 Tier 1 telephone support)

Don’t Turtle Your Network

Contents

Conventions

The following conventions are used in this manual:

Italic
Used for emphasis and to signify the first use of a glossary term.

`Courier`
Used for URLs, host names, email addresses, registry entries, and other system definitions.

<TAB>
Used for the tab character on the keyboard.

Bold
Used for calling out buttons, file paths, tabs, fields, checkboxes, links and windows.

Note: Notes are called out to inform you of specific information that is relevant to the configuration or operation of TotalView. Notes may occasionally be used to describe best practices for using the system.

Technical Support

For technical support:

Support@PathSolutions.com

(877) 748-1444 (7x24 tier 1 telephone support)
(408) 748-1777 Select 1 for tier 2 support

Activation and Quick Config Wizard

The simplest way to deploy and start TotalView is by using the Quick Config Wizard. Follow the instructions in the Deployment Guide to activate and use the Quick Config Wizard.

The **QuickConfig Wizard** will auto-configure the PathSolutions TotalView and begin monitoring in minutes.

Using the Configuration Tool

The **Configuration Tool** can change the general configuration options of the product as well as add or remove devices from monitoring.

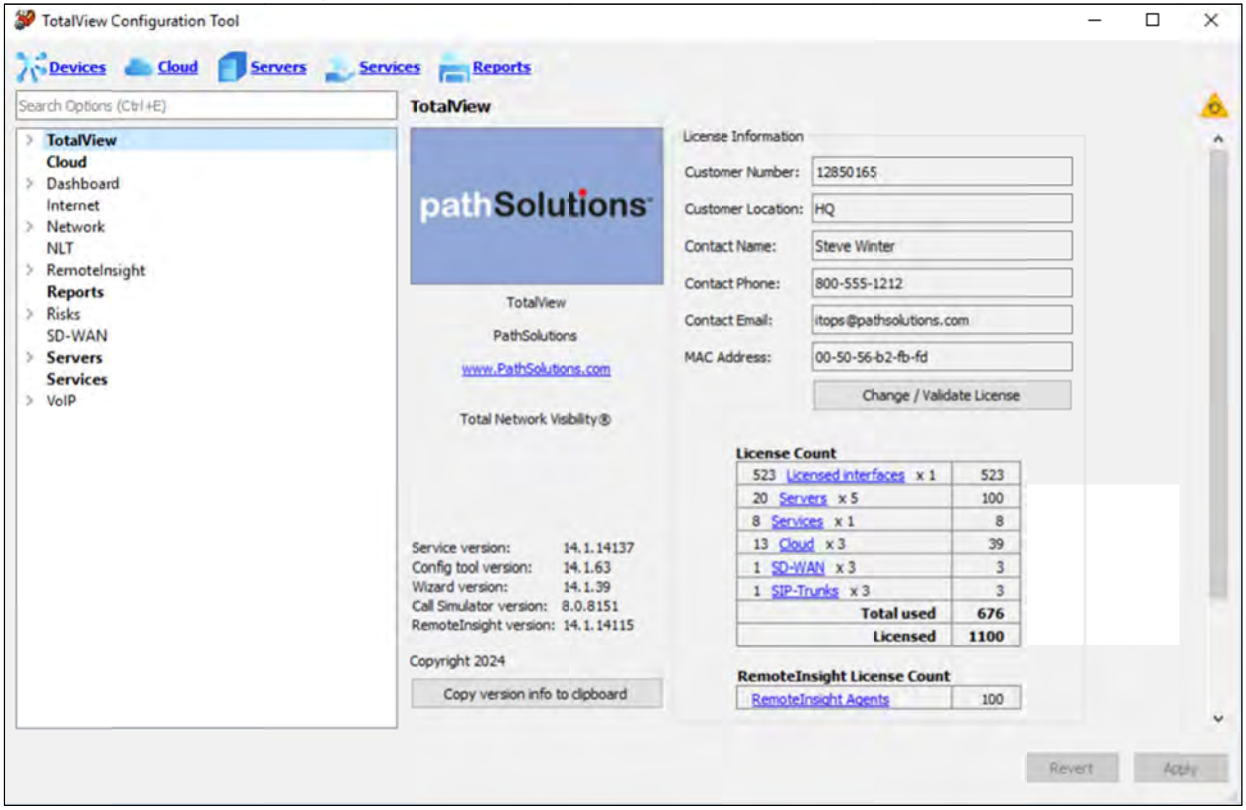
Note: The **Interface Discovery Tool** is an alternate tool used to scan for devices and cut down interfaces that are monitored. See the section Interface Discovery Tool.

Running the Configuration Tool

The **Configuration Tool** can be launched on the server's console by selecting **Start**, choose **Programs > PathSolutions >TotalView > Config Tool.**

Navigation

The menu on the left-hand side displays all the categories for configuration. Expand or contract the sections on the list to see options for each area.



TotalView

TotalView

PathSolutions

www.PathSolutions.com

Total Network Visibility®

Service version: 14.1.14137
Config tool version: 14.1.63
Wizard version: 14.1.39
Call Simulator version: 8.0.8151
RemoteInsight version: 14.1.14115

Copyright 2024

Copy version info to clipboard

License Information

Customer Number: 12850165
Customer Location: HQ
Contact Name: Steve Winter
Contact Phone: 800-555-1212
Contact Email: itops@pathsolutions.com
MAC Address: 00-50-56-b2-fb-fd

Change / Validate License

License Count

523 Licensed interfaces x 1	523
20 Servers x 5	100
8 Services x 1	8
13 Cloud x 3	39
1 SD-WAN x 3	3
1 SIP-Trunks x 3	3
Total used	**676**
Licensed	**1100**

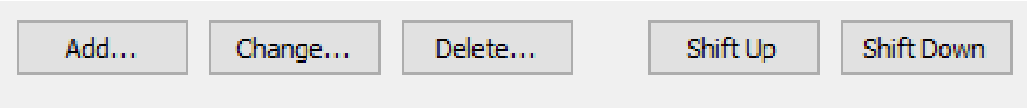
RemoteInsight License Count

RemoteInsight Agents	100

The list can be filtered to search for specific entries. For example, if you enter "alert", it will show all of the pages that have that configuration option.

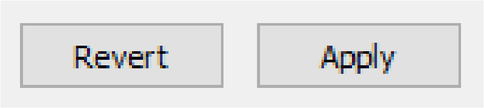
Buttons

Multiple sections include buttons on the bottom of the screen to add, change, or delete settings and to organize the display.



- Use the **Add** button to add new items like device config and alerts to settings.
- Use the **Change** button to change items listed in each section.
- Use the **Delete** button to delete an item listed in each section. For safety reasons, a dialog box will appear requesting confirmation to delete it.
- Use the **Shift U**p and **Shift Down** buttons to shift the order of items in list up and down.

At the very bottom right of all screens, there are also **Revert** and **Apply** buttons that will be available if you have made any edits.



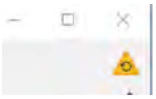
- Use the **Apply** button to apply all the settings you've configured during this session. By selecting **Apply**, it will stop and restart the TotalView service. This could take up to 5 minutes.
- Use the **Revert** button to revert to the last saved configuration.

Toolbars

You can add menu items on the left to the toolbar at the top by right-clicking on a menu item and choose "Add toolbar". You can remove a toolbar from the top by right-clicking on the toolbar and choose "Remove".

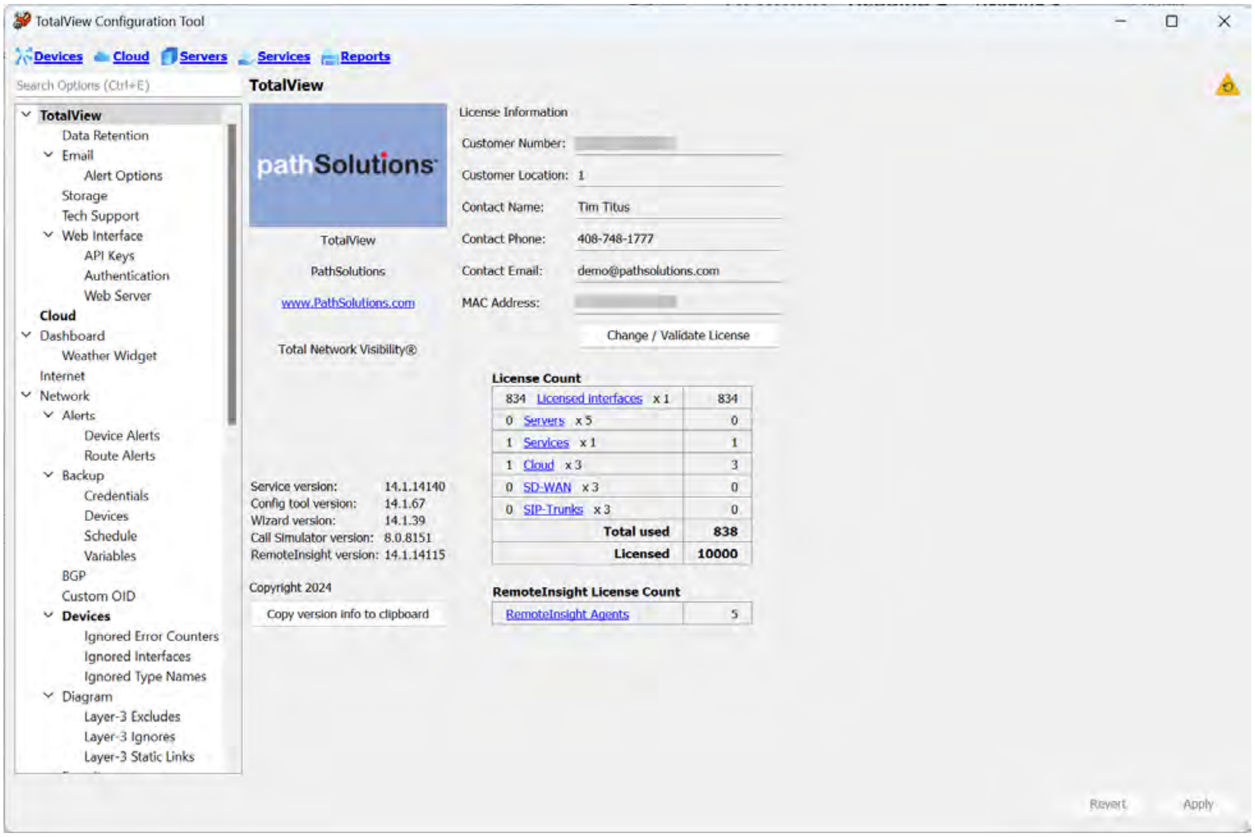
Restart Icon

In the upper right corner of many screens is a yellow restart icon. This icon will prompt a notification for changes that will require a service restart. It is generally best to make multiple changes and then apply all of them at once to have the service only restart once.



TotalView License Page

This page will allow you to review and update the license information for TotalView:



License Information

Customer Number:	[redacted]
Customer Location:	1
Contact Name:	Tim Titus
Contact Phone:	408-748-1777
Contact Email:	demo@pathsolutions.com
MAC Address:	[redacted]

License Count

834 Licensed Interfaces x 1	834
0 Servers x 5	0
1 Services x 1	1
1 Cloud x 3	3
0 SD-WAN x 3	0
0 SIP-Trunks x 3	0
Total used	**838**
Licensed	**10000**

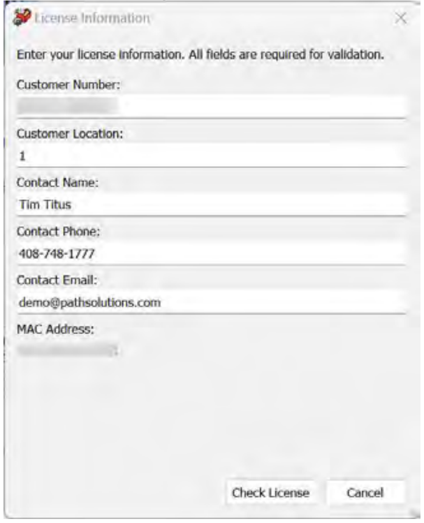
RemoteInsight License Count

RemoteInsight Agents	5

```
Service version:        14.1.14140
Config tool version:    14.1.67
Wizard version:         14.1.39
Call Simulator version: 8.0.8151
RemoteInsight version:  14.1.14115
```

Copyright 2024

Click “Change/Validate License” to make a change to the license information or re-validate the license.



Enter your license information. All fields are required for validation.

Customer Number:
[redacted]

Customer Location:
1

Contact Name:
Tim Titus

Contact Phone:
408-748-1777

Contact Email:
demo@pathsolutions.com

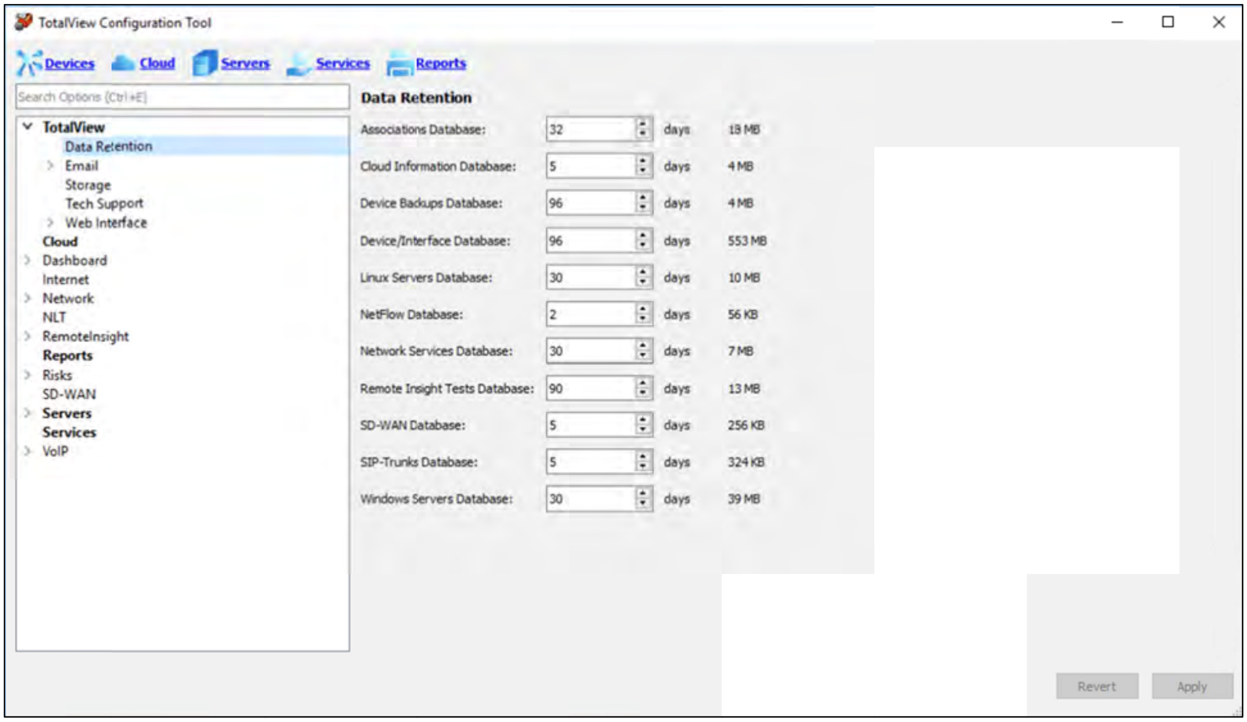
MAC Address:
[redacted]

Enter your subscription information and then select **Check License** to validate the license.

If you purchase additional interfaces for your growing network, just give us a call or email sales@pathsolutions.com. After purchasing additional licenses, use this to re-validate the license.

Data Retention

The **Data Retention** section allows you to determine how much storage is taken up with each data element and control the retention days for each.

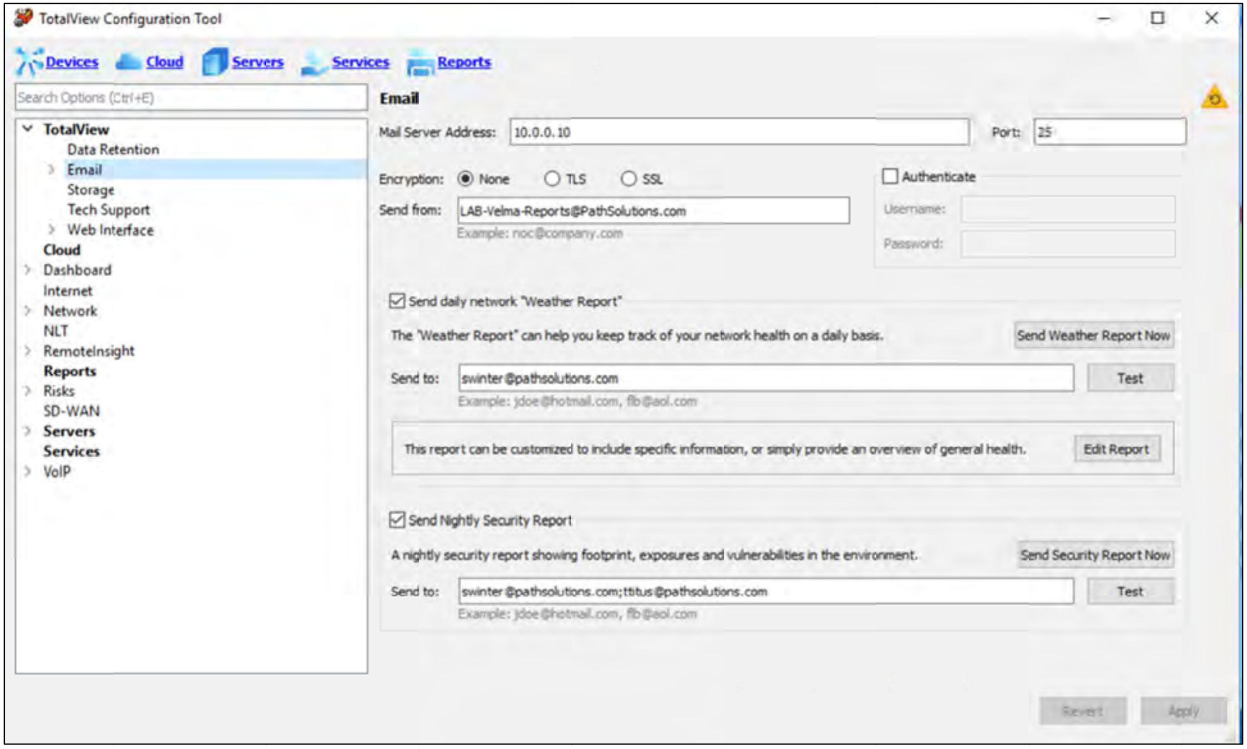


Data Retention

Associations Database:	32	days	18 MB
Cloud Information Database:	5	days	4 MB
Device Backups Database:	96	days	4 MB
Device/Interface Database:	96	days	553 MB
Linux Servers Database:	30	days	10 MB
NetFlow Database:	2	days	56 KB
Network Services Database:	30	days	7 MB
Remote Insight Tests Database:	90	days	13 MB
SD-WAN Database:	5	days	256 KB
SIP-Trunks Database:	5	days	324 KB
Windows Servers Database:	30	days	39 MB

Email Configuration

This section configures the email communications along with the automated Network Weather Report and the Nightly Security Report.



Email

Mail Server Address: 10.0.0.10 Port: 25

Encryption: ● None ○ TLS ○ SSL

□ Authenticate

Username:

Password:

Send from: LAB-Velma-Reports@PathSolutions.com

Example: noc@company.com

☑ Send daily network "Weather Report"

The "Weather Report" can help you keep track of your network health on a daily basis.

Send to: swinter@pathsolutions.com

Example: jdoe@hotmail.com, fb@aol.com

This report can be customized to include specific information, or simply provide an overview of general health.

☑ Send Nightly Security Report

A nightly security report showing footprint, exposures and vulnerabilities in the environment.

Send to: swinter@pathsolutions.com;ttitus@pathsolutions.com

Example: jdoe@hotmail.com, fb@aol.com

Enter your SMTP relay server IP address. This address can be your SMTP mail Internet gateway server's IP address (depending on your mail server configuration). If you are uncertain, check with your email server administrator. See *Appendix B. SMTP Email Forwarding* for additional information on SMTP relay server configuration.

You should select the type of encryption and what type of authentication (if any).

Enter the email address where the emails should be sent from.

Configuring the Weather Report

If you want to receive a daily network Weather Report, select the **Send daily network "Weather Report**" checkbox and enter one or more email addresses. Separate each email address with a space, comma, or semicolon.

Select **Test** to send a test email to all users listed.

If you want to modify the network Weather Report, select **Edit Report**. You will be able to modify the default report template to include your company logo, custom information, or shrink the email to display only the information selected. See **Creating Email Report Templates** for a full list of the objects that can be included in emailed reports.

Note: The report uses MIME encoding to allow email readers to respect the content as HTML formatted content. If you need assistance with modifying this report, and do not understand MIME encoding, refer to the IETF's RFC1521 (www.ietf.org) or contact PathSolutions Technical Support for assistance support@pathsolutions.com.

Note: Do NOT put a period (".") on its own line anywhere in this file.

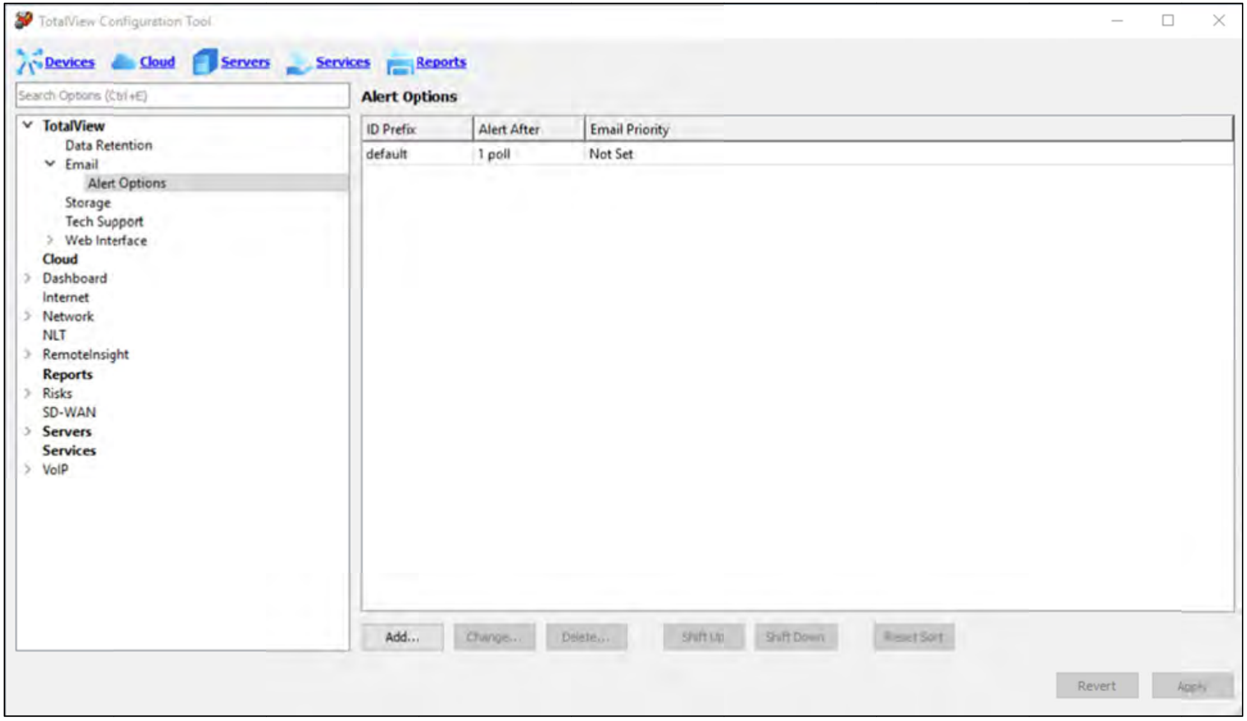
Configuring the Nightly Security Report

If you have the Security Operations Manager module, you can get a nightly security report sent to your mailbox that has a summary of your security posture. If you want to receive the Nightly Security Report, select the **Send Nightly Security Report** checkbox and enter one or more email addresses who should receive the report. Separate each email address with a space, comma, or semicolon

Select **Test** to send a test email to all users listed.

Alert Options

The **Alert Options** section allows you to change how alerts work.

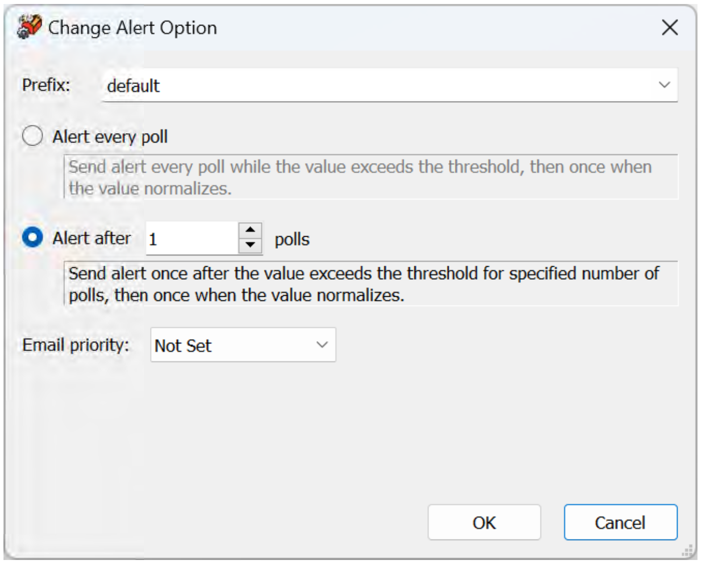


Alert Options

ID Prefix	Alert After	Email Priority
default	1 poll	Not Set

For example: Alerts are triggered the first time an event happens (the default).

If you want alerts to trigger only after the third time it occurs, select the option and click “Change:



Prefix: default

○ Alert every poll

Send alert every poll while the value exceeds the threshold, then once when the value normalizes.

● Alert after 1 polls

Send alert once after the value exceeds the threshold for specified number of polls, then once when the value normalizes.

Email priority: Not Set

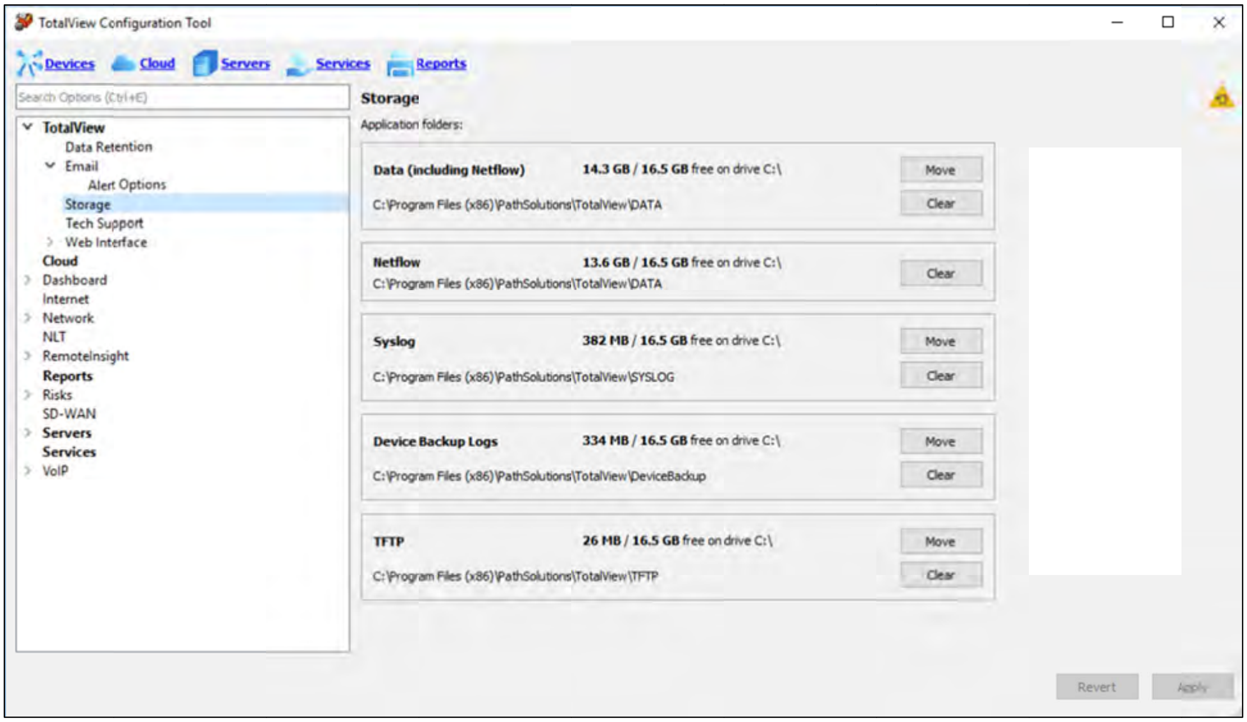
Set the alert to trigger only after X number of successfive failed polls, and the once when the condition recovers.

For example, if every 5 minutes an alert is sent on low disk space on one drive, the frequency of the alerting can fill your mailbox with alerts. In that case, set it to send just the **Low disk space on Fred drive C** alert and then it will be silent until the disk space problem is fixed. Once fixed, it will send out the **Disk space on Fred drive C has recovered** alert.

Note: There are also many other alerts to set up for different conditions and events, available to you when you start to navigate the sections. Create a filter on the word *alerts* to quickly get to the sections for setting Network alerts, Risk alerts, Server alerts, and VoIP alerts. The screenshot below displays an example of the alerts filter.

Storage

The **Storage** section allows you determine how much disk space is taken up for various parts of the product as well as to make it easy to move a section to a different drive on the server.



Storage

Application folders:

Data (including Netflow) 14.3 GB / 16.5 GB free on drive C:\
C:\Program Files (x86)\PathSolutions\TotalView\DATA

Netflow 13.6 GB / 16.5 GB free on drive C:\
C:\Program Files (x86)\PathSolutions\TotalView\DATA

Syslog 382 MB / 16.5 GB free on drive C:\
C:\Program Files (x86)\PathSolutions\TotalView\SYSLOG

Device Backup Logs 334 MB / 16.5 GB free on drive C:\
C:\Program Files (x86)\PathSolutions\TotalView\DeviceBackup

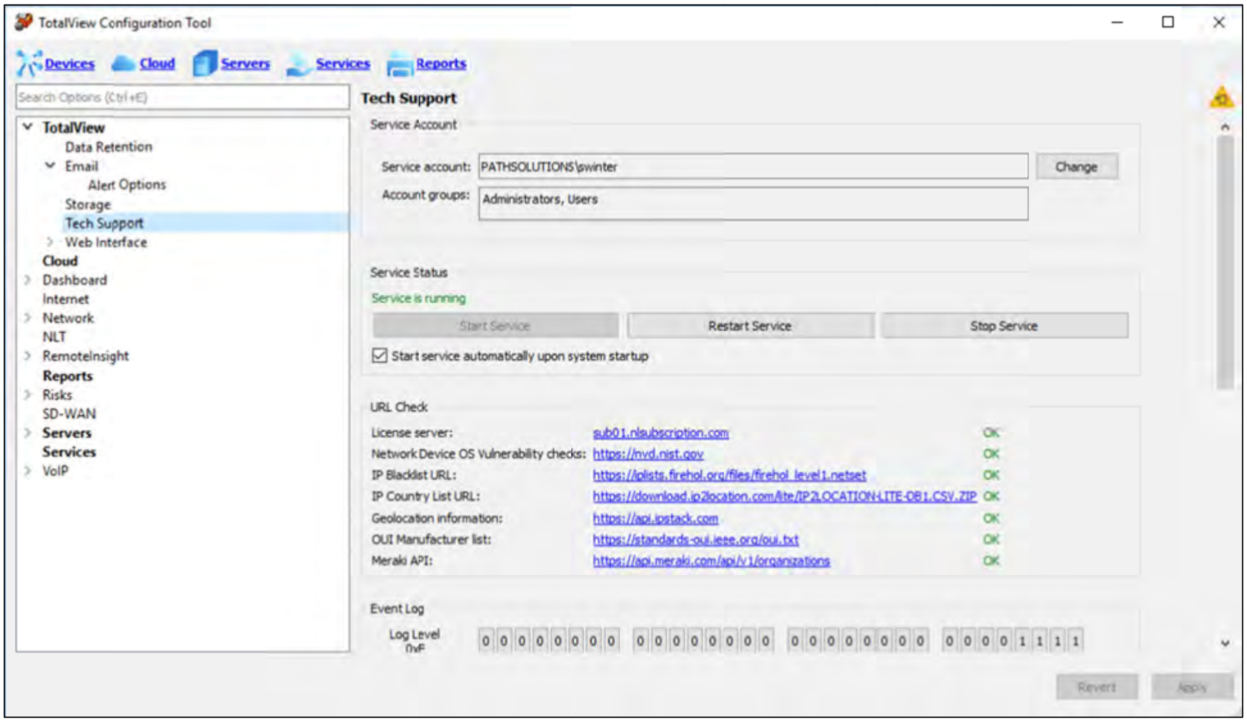
TFTP 26 MB / 16.5 GB free on drive C:\
C:\Program Files (x86)\PathSolutions\TotalView\TFTP

Select **Move** to relocate the folder to a new location or select **Clear** to empty the folder.

Note: If you move a folder, you must specify a local drive on the server, you cannot use a network share.

Tech Support

The **Tech Support** section allows you to change the service account and validate various connections to different external sites that the product uses for external data.



Tech Support

Service Account

Service account: PATHSOLUTIONS\swinter

Account groups: Administrators, Users

Service Status

Service is running

☑ Start service automatically upon system startup

URL Check

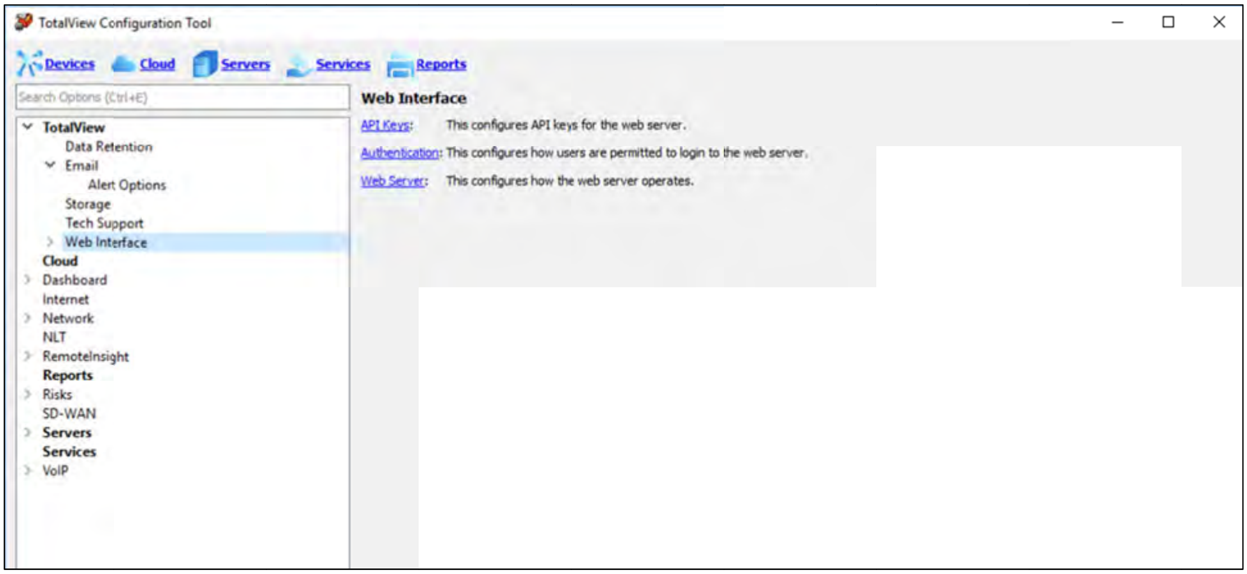
License server:	sub01.nlsubscription.com	OK
Network Device OS Vulnerability checks:	https://nvd.nist.gov	OK
IP Blacklist URL:	https://iplists.firehol.org/files/firehol_level1.netset	OK
IP Country List URL:	https://download.ip2location.com/lite/IP2LOCATION-LITE-DB1.CSV.ZIP	OK
Geolocation information:	https://api.ipstack.com	OK
OUI Manufacturer list:	https://standards-oui.ieee.org/oui.txt	OK
Meraki API:	https://api.meraki.com/api/v1/organizations	OK

Event Log

Log Level 0xF: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1

Web Interface

The **Website Interface** section controls the built-in webserver that is part of TotalView. Select the **Web Interface** section from the left-hand menu and it will show three different areas: API Keys, Authentication, and Web Server.



Web Interface

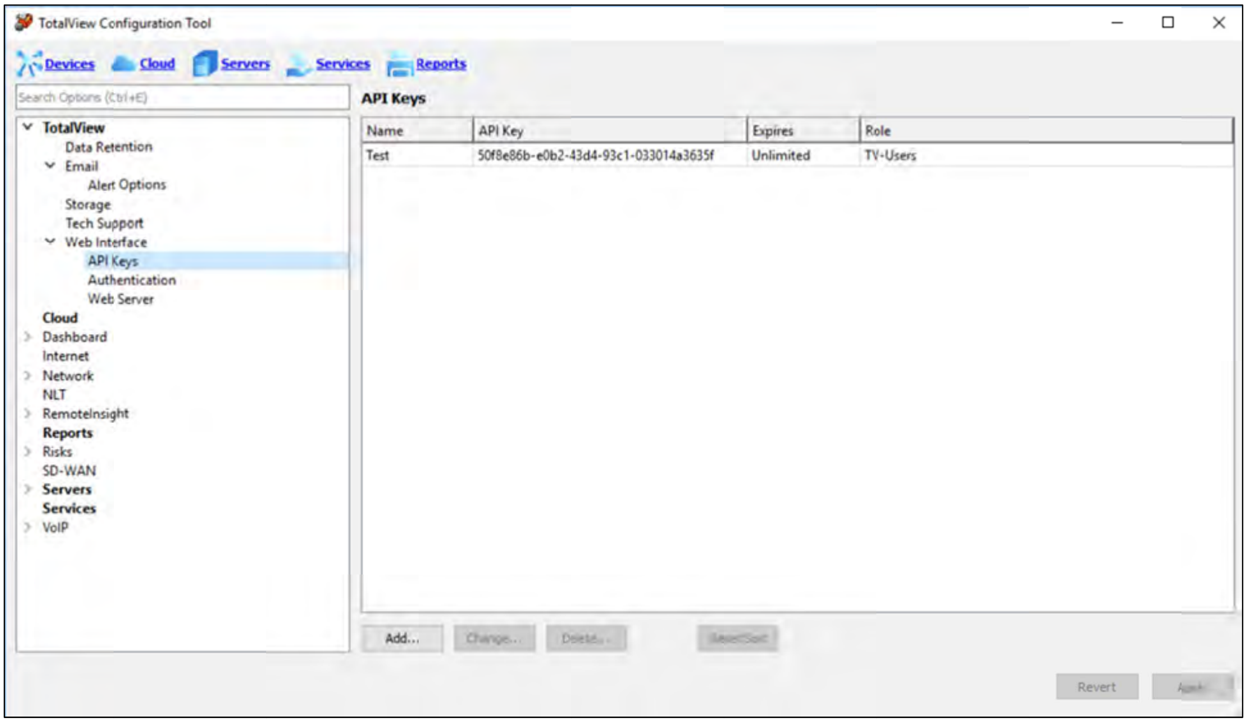
API Keys: This configures API keys for the web server.

Authentication: This configures how users are permitted to login to the web server.

Web Server: This configures how the web server operates.

API Keys

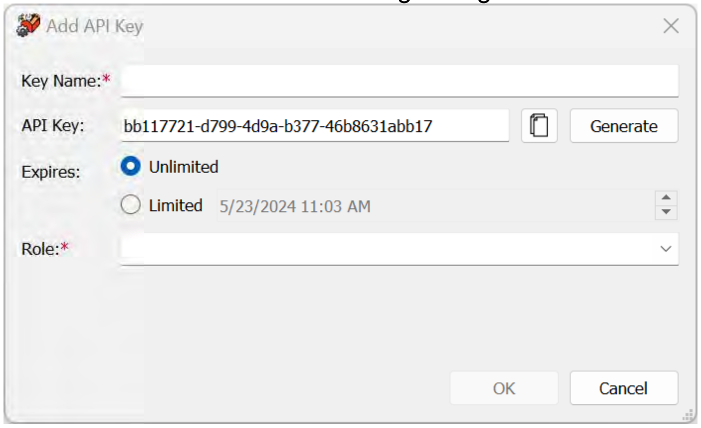
The API Keys section allows you to create accounts that will programmatically collect data from TotalView's RESTful JSON API in a controlled fashion. This can be used for CURL requests, Postman requests, or any other mechanism.



API Keys

Name	API Key	Expires	Role
Test	50f8e86b-e0b2-43d4-93c1-033014a3635f	Unlimited	TV-Users

To create a new key, click **Add**. You will see the following dialog:



Key Name:*

API Key: bb117721-d799-4d9a-b377-46b8631abb17

Expires: ● Unlimited

○ Limited 5/23/2024 11:03 AM

Role:*

You must give the key a name. The API key string is automatically generated. You can re-generate the key string if necessary.

You can also set an expiration date on the key.

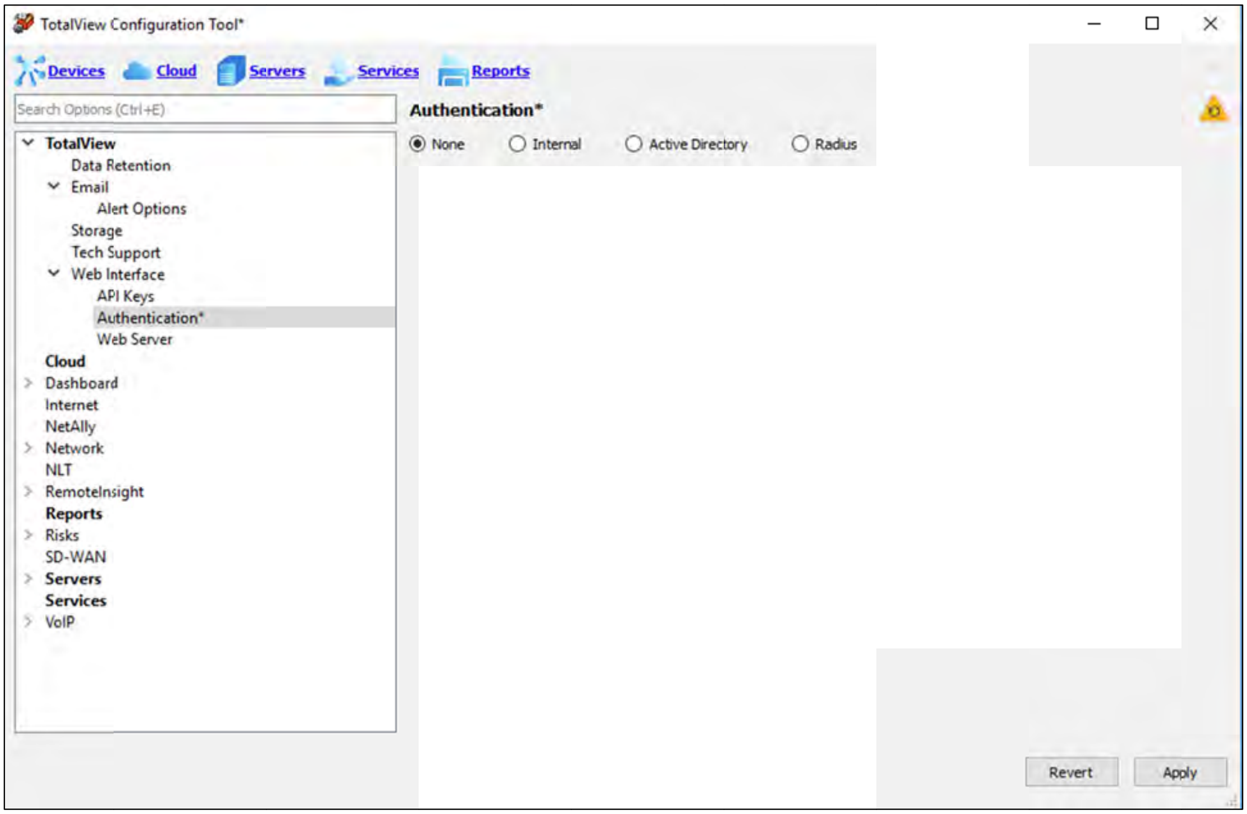
Each key should have a role identified as to what data is available. The role is defined on the Authentication tab.

Authentication

This section allows you to control how the webserver authenticates users, and what type of authentication should be performed. Select from **None, Internal, Active Directory**, or **Other**.

When “None” is selected, there will be no authentication and the web pages are freely available for anyone to view.

Below is a screenshot of the **None** authentication option**.**

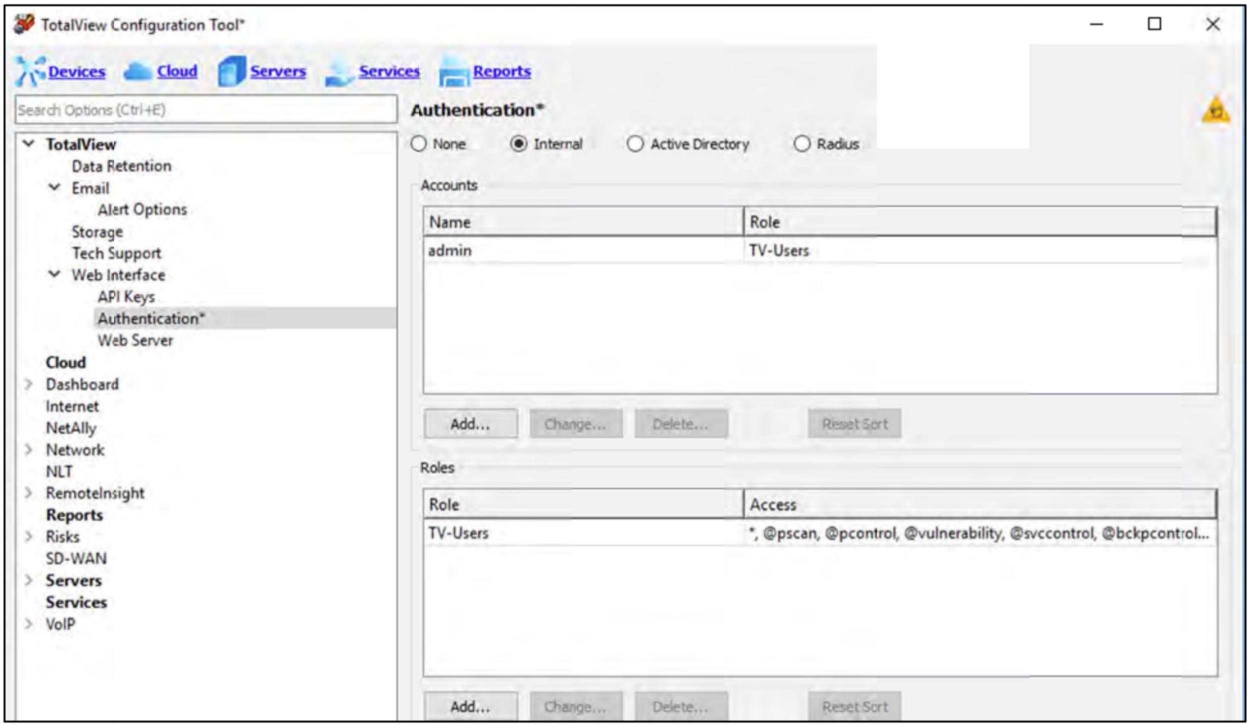


Authentication*

● None ○ Internal ○ Active Directory ○ Radius

When “Internal” is selected, it will use a list of accounts that are local to the TotalView server.

Below is a screenshot of the **Internal** authentication option**.** Accounts and roles can be added, changed, or deleted in this section.



Authentication*

○ None ● Internal ○ Active Directory ○ Radius

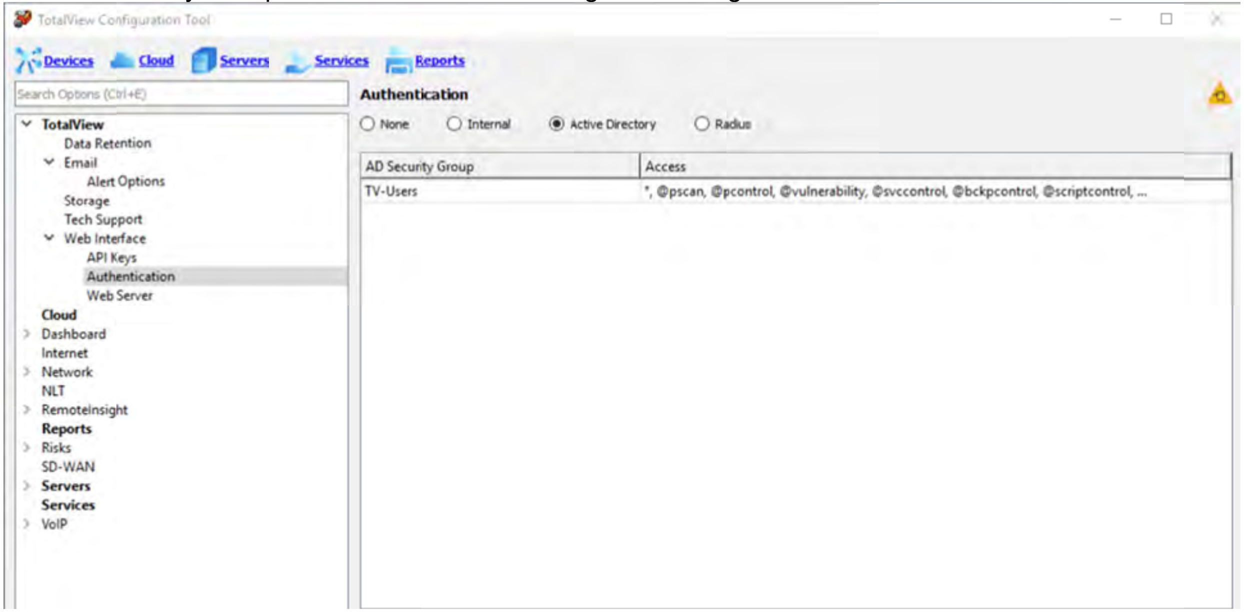
Accounts

Name	Role
admin	TV-Users

Roles

Role	Access
TV-Users	*, @pscan, @pcontrol, @vulnerability, @svccontrol, @bckpcontrol...

When “Active Directory” is selected, it will have AD integration using the domain account. One or more AD groups should be created on the domain that reflect the users who have different rights to TotalView. The AD Security Group name will be used to assign access rights to those users.

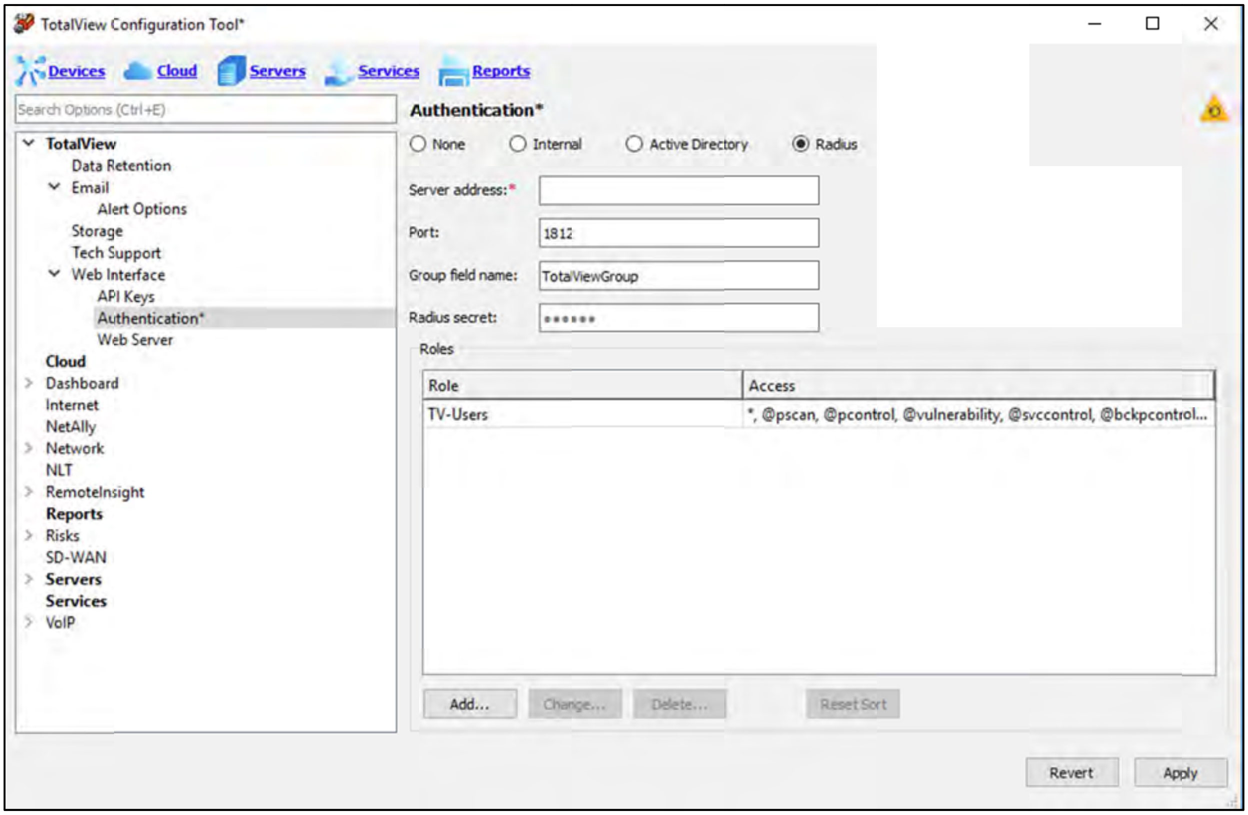


Authentication

○ None ○ Internal ● Active Directory ○ Radius

AD Security Group	Access
TV-Users	*, @pscan, @pcontrol, @vulnerability, @svccontrol, @bckpcontrol, @scriptcontrol, ...

Below is a screenshot of the **Radius** authentication option**.** You will need to enter the Radius server IP address and port and the Radius secret. You will need to have the Radius server send back the group field name to use to identify which security group the logged in user should be assigned to.



Authentication*

○ None ○ Internal ○ Active Directory ● Radius

Server address:*

Port: 1812

Group field name: TotalViewGroup

Radius secret: ••••••

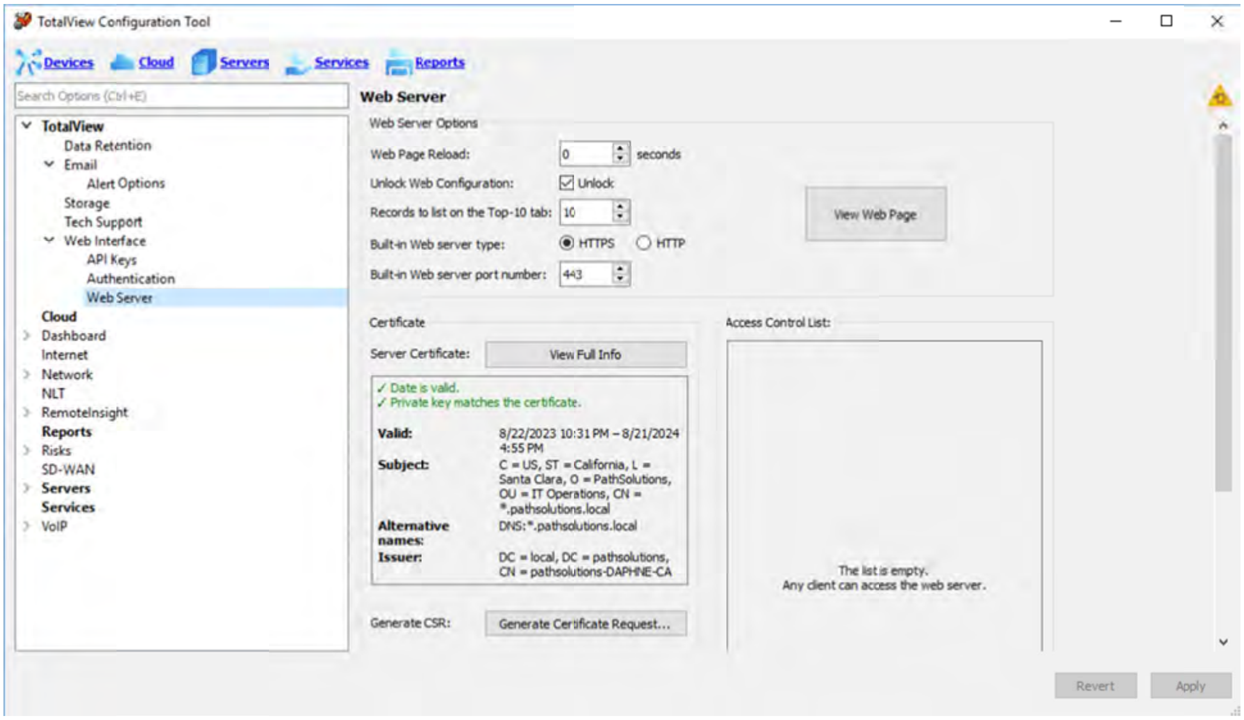
Roles

Role	Access
TV-Users	*, @pscan, @pcontrol, @vulnerability, @svccontrol, @bckpcontrol...

Web Server

This section controls how the webserver will host the pages out and assists with creating a website certificate for the site.

You can also add an access control list to only respond to requests from a specific subnet or IP address.



Web Server

Web Server Options

Web Page Reload: 0 seconds

Unlock Web Configuration: ☑ Unlock

Records to list on the Top-10 tab: 10

Built-in Web server type: ● HTTPS ○ HTTP

Built-in Web server port number: 443

Certificate

Server Certificate:

✓ Date is valid.
✓ Private key matches the certificate.

Valid:	8/22/2023 10:31 PM – 8/21/2024 4:55 PM
Subject:	C = US, ST = California, L = Santa Clara, O = PathSolutions, OU = IT Operations, CN = *.pathsolutions.local
Alternative names:	DNS:*.pathsolutions.local
Issuer:	DC = local, DC = pathsolutions, CN = pathsolutions-DAPHNE-CA

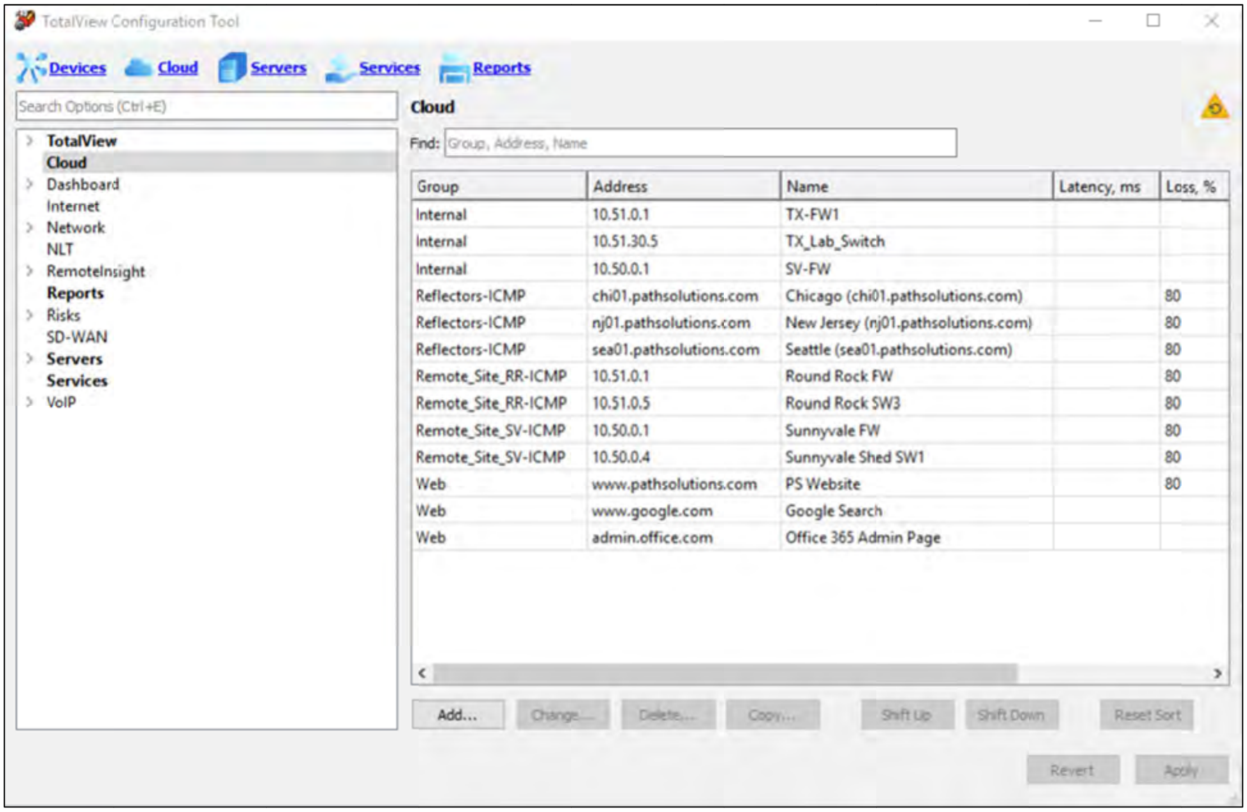
Generate CSR:

Access Control List:

The list is empty.
Any client can access the web server.

Cloud Monitoring

To configure Cloud interfaces, select **Cloud** from the left-hand menu. Here, you can add, change, or delete any websites by name and IP address. Assign a sort order, by using the **Shift Up** or **Shift Down** buttons.

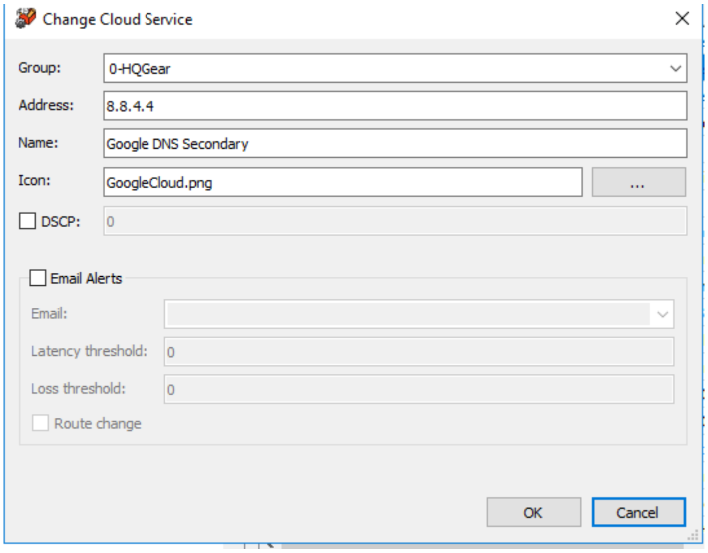


Cloud

Find: Group, Address, Name

Group	Address	Name	Latency, ms	Loss, %
Internal	10.51.0.1	TX-FW1		
Internal	10.51.30.5	TX_Lab_Switch		
Internal	10.50.0.1	SV-FW		
Reflectors-ICMP	chi01.pathsolutions.com	Chicago (chi01.pathsolutions.com)		80
Reflectors-ICMP	nj01.pathsolutions.com	New Jersey (nj01.pathsolutions.com)		80
Reflectors-ICMP	sea01.pathsolutions.com	Seattle (sea01.pathsolutions.com)		80
Remote_Site_RR-ICMP	10.51.0.1	Round Rock FW		80
Remote_Site_RR-ICMP	10.51.0.5	Round Rock SW3		80
Remote_Site_SV-ICMP	10.50.0.1	Sunnyvale FW		80
Remote_Site_SV-ICMP	10.50.0.4	Sunnyvale Shed SW1		80
Web	www.pathsolutions.com	PS Website		80
Web	www.google.com	Google Search		
Web	admin.office.com	Office 365 Admin Page		

Setup email alerts for latency and loss thresholds when you add or change the address on the cloud list: Select an address on the Cloud list, then select **Change**. If you want email alerts, select the **Email Alerts** checkbox and fill out those fields. Select **OK** to save.



Group: 0-HQGear

Address: 8.8.4.4

Name: Google DNS Secondary

Icon: GoogleCloud.png

☐ DSCP: 0

☐ Email Alerts

Email:

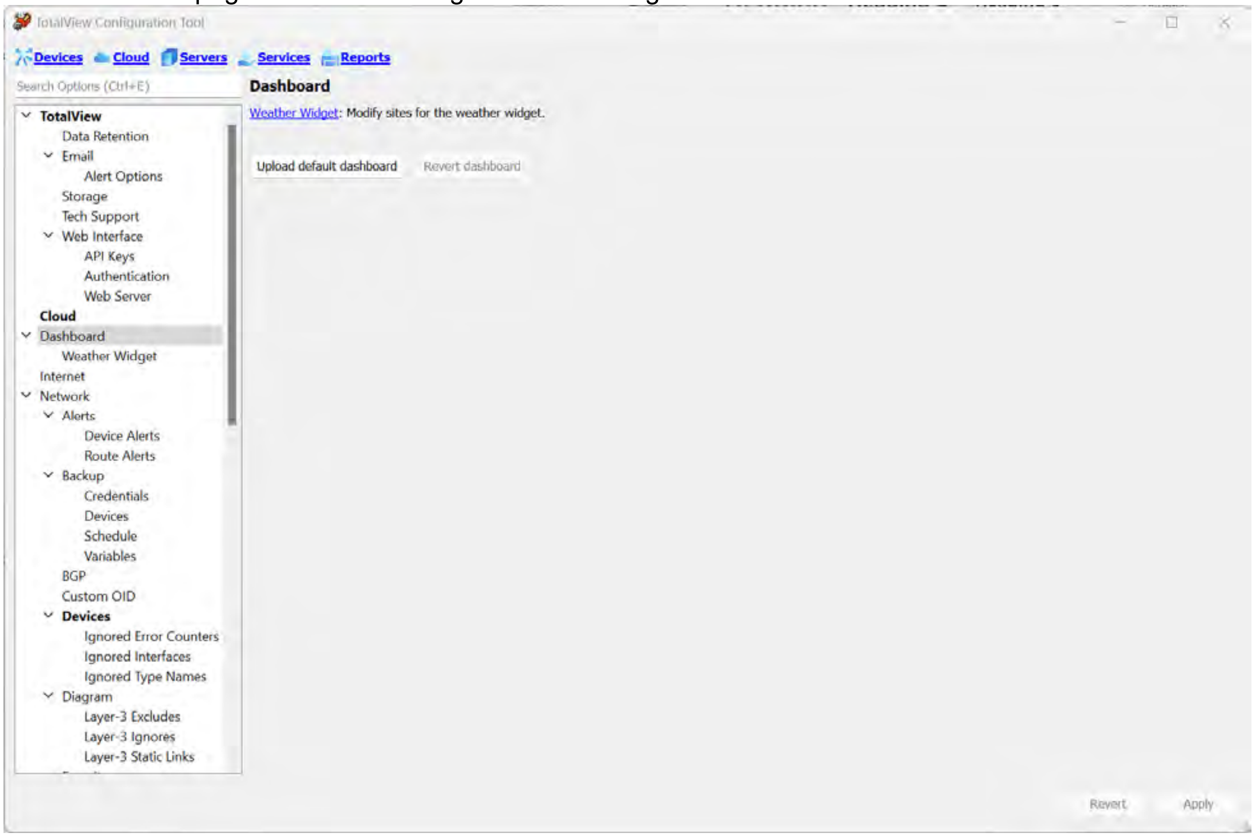
Latency threshold: 0

Loss threshold: 0

☐ Route change

Dashboard Settings

The Dashboard page allows controlling dashboard widgets.



Weather Widget: Modify sites for the weather widget.

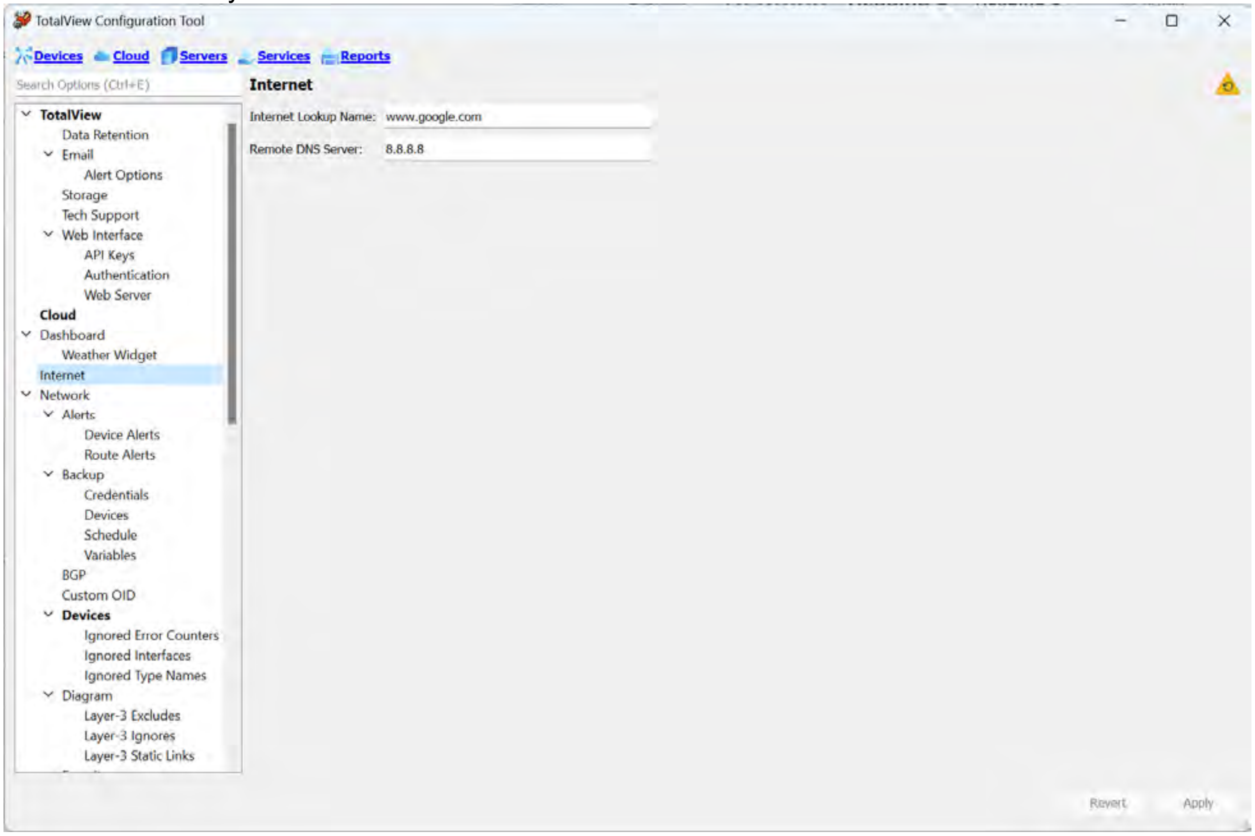
If you want to change the default dashboard that all new users see, create the dashboard on your local browser and then choose “Save” and the dashboard will be downloaded to your local machine. Copy this file to the TotalView server and then click “Upload default dashboard” to import it as the new default.

Weather Widget Page

The Weather Widget page allows you to add locations to the weather dashboard widget. These locations are typically office locations and datacenters so you can correlate when weather events will affect these sites.

Internet Settings

The Internet page configures the external DNS and remote connection that should be tested to validate Internet connectivity on the Internet tab.



Internet

Internet Lookup Name: www.google.com

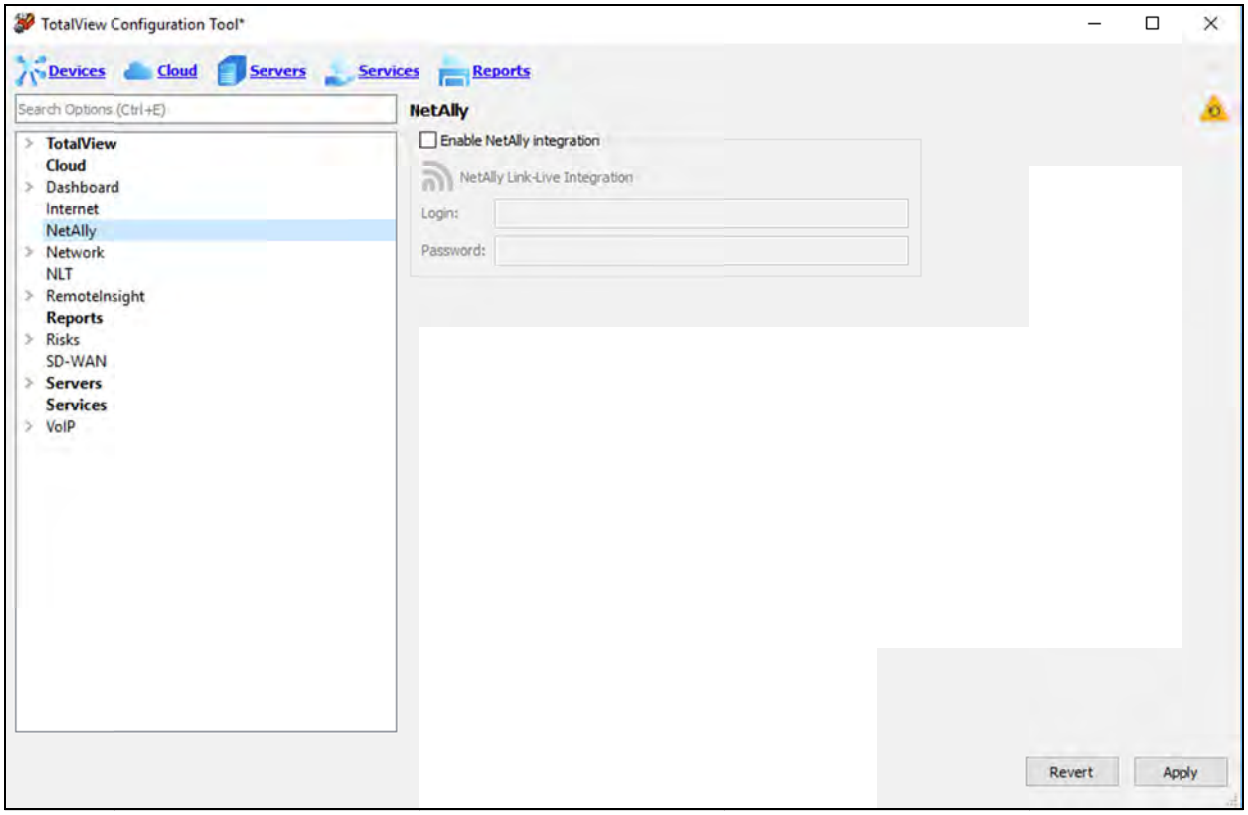
Remote DNS Server: 8.8.8.8

The name will be used to do a local DNS check as well as a remote DNS check to validate that Internet connectivity is working smoothly.

NetAlly Settings

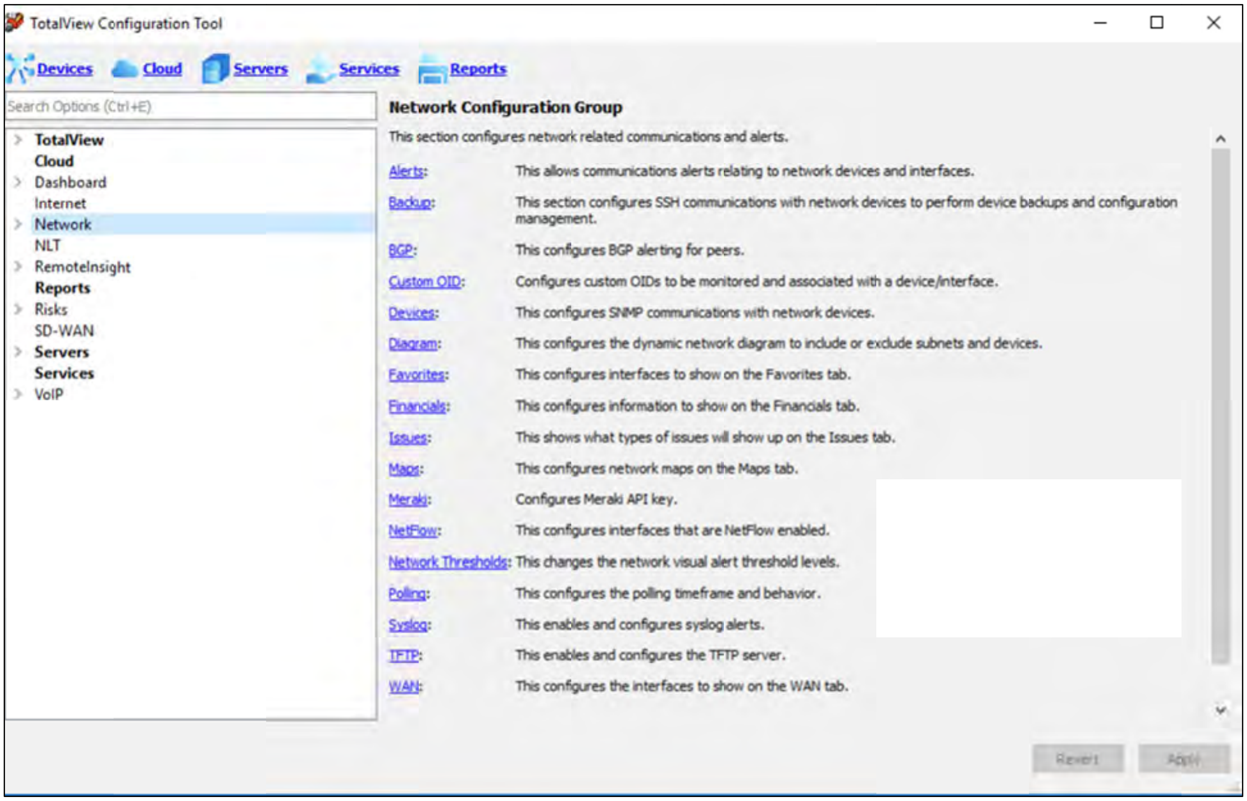
Select **NetAlly** from the left-hand menu, then select the **Enable NetAlly Integration** checkbox and the section on NetAlly link-Live Integration will become available.

Then enter your NetAlly login and password in the **Login** and **Password** fields.



Network Monitoring

Select **Network** from the left-hand menu. This section configures network related communications and alerts. The top menu provides a short description of each subsection.



Network Configuration Group

This section configures network related communications and alerts.

Alerts: This allows communications alerts relating to network devices and interfaces.

Backup: This section configures SSH communications with network devices to perform device backups and configuration management.

BGP: This configures BGP alerting for peers.

Custom OID: Configures custom OIDs to be monitored and associated with a device/interface.

Devices: This configures SNMP communications with network devices.

Diagram: This configures the dynamic network diagram to include or exclude subnets and devices.

Favorites: This configures interfaces to show on the Favorites tab.

Financials: This configures information to show on the Financials tab.

Issues: This shows what types of issues will show up on the Issues tab.

Maps: This configures network maps on the Maps tab.

Meraki: Configures Meraki API key.

NetFlow: This configures interfaces that are NetFlow enabled.

Network Thresholds: This changes the network visual alert threshold levels.

Polling: This configures the polling timeframe and behavior.

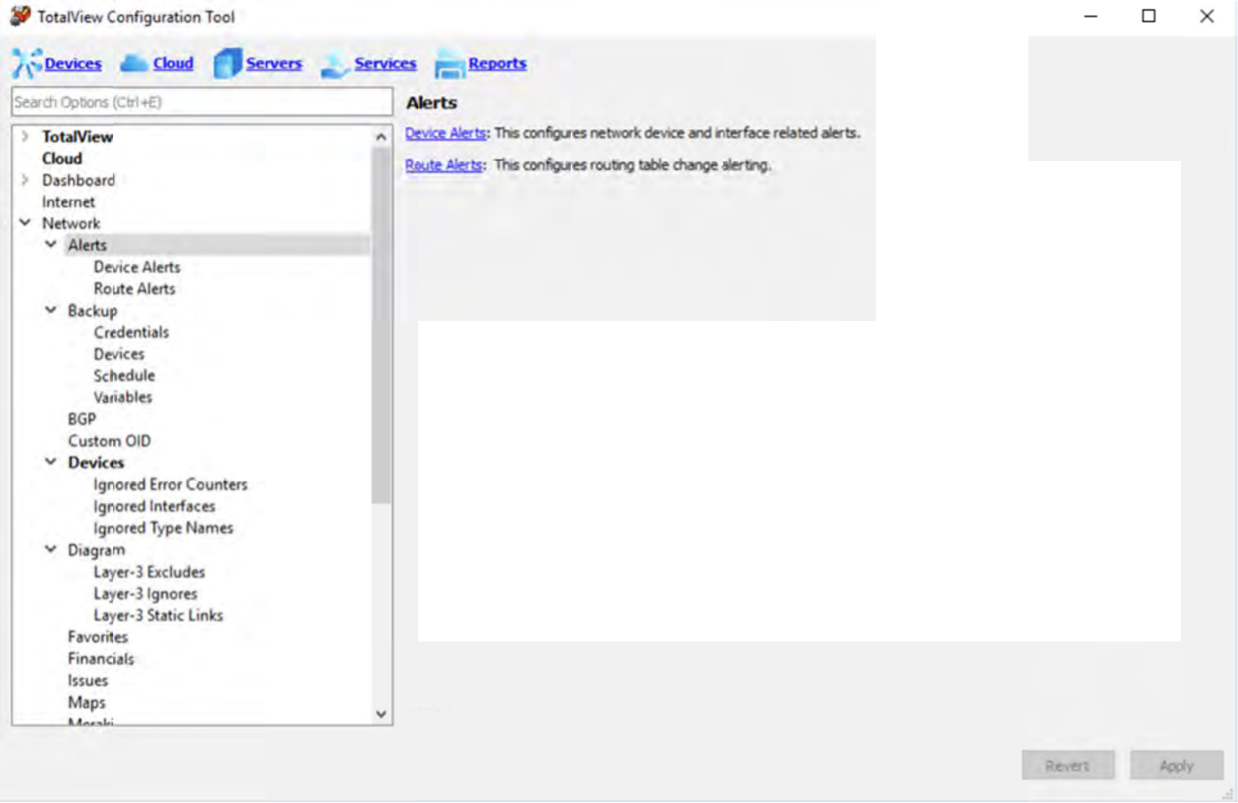
Syslog: This enables and configures syslog alerts.

TFTP: This enables and configures the TFTP server.

WAN: This configures the interfaces to show on the WAN tab.

Alerts

Select **Network > Alerts** from the left-hand menu. This section allows for you to set **Device Alerts** and **Route Alerts**.



Alerts

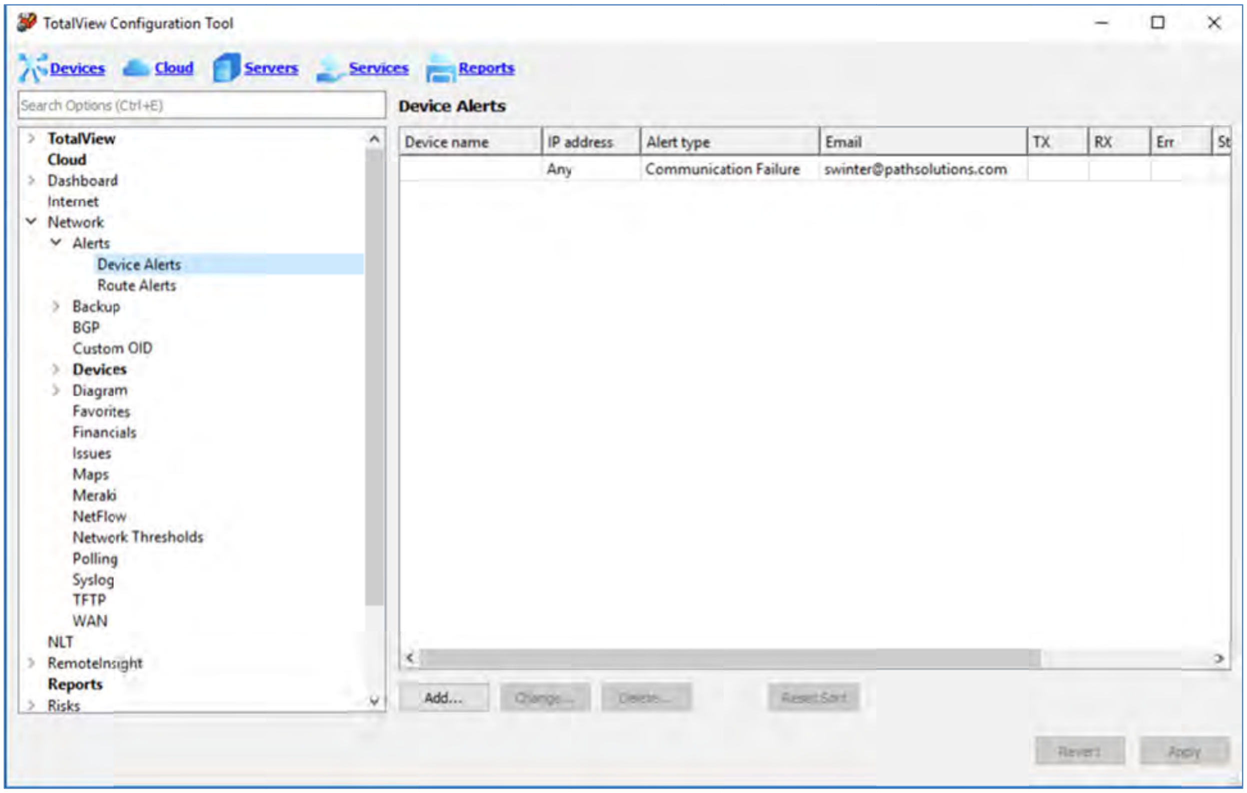
Device Alerts: This configures network device and interface related alerts.

Route Alerts: This configures routing table change alerting.

Note: There are other network alerts to set up for different conditions and events, available when you start to navigate the sections.

Device Alerts

Go to **Networks > Alerts > Device Alerts**. The system can generate alerts if interfaces change status or exceed set levels of utilization or errors.

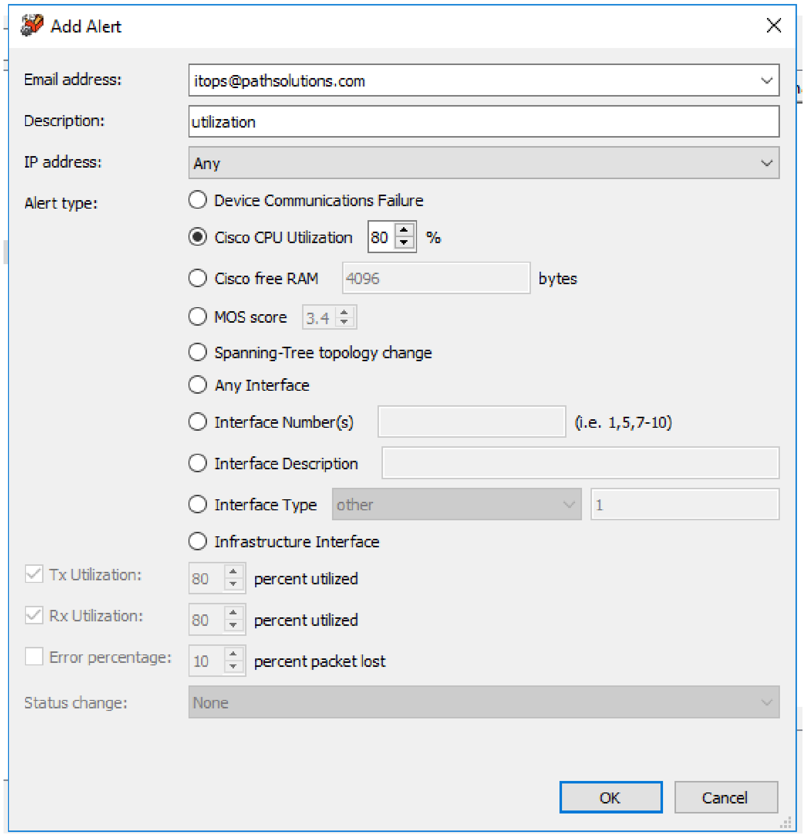


Device Alerts

Device name	IP address	Alert type	Email	TX	RX	Err	St
	Any	Communication Failure	swinter@pathsolutions.com				

Add or change alerting for interfaces or devices on the **Alerts** section.

For Device Alerts, if you select the **Add** button, you should see the following alert configuration dialog.



Add Alert

Email address: itops@pathsolutions.com

Description: utilization

IP address: Any

Alert type:

- ○ Device Communications Failure
- ● Cisco CPU Utilization 80 %
- ○ Cisco free RAM 4096 bytes
- ○ MOS score 3.4
- ○ Spanning-Tree topology change
- ○ Any Interface
- ○ Interface Number(s) (i.e. 1,5,7-10)
- ○ Interface Description
- ○ Interface Type other 1
- ○ Infrastructure Interface

☑ Tx Utilization: 80 percent utilized

☑ Rx Utilization: 80 percent utilized

□ Error percentage: 10 percent packet lost

Status change: None

Enter the email address that should receive the alert and a short description of the alert.

Enter the IP address of the device or select **Any** from the **IP address field** to match any device or device group.

Choose a device-related alert like the following:

- **Device Communications Failure**: This will trigger if the device does not respond to the initial SNMP query at the start of a poll. If it does not respond, it will attempt to ping the device to see if it is completely unreachable and then send the appropriate alert.
- **Cisco CPU utilization**: This will trigger if the Cisco device shows its 5 minute average CPU utilization above the threshold level.
- **Cisco free RAM**: This will trigger if the amount of free RAM on the device drops below this level.
- MOS score: This will trigger if the MOS score to/from the device drops below this level.
- **Spanning-tree topology change**: This will trigger if the spanning-tree topology changes for the layer-2 domain.

Choose an interface-related alert. The interface related alerts allow selecting interfaces based on the following criteria.

- **Any interface**: Any interface on the selected device(s)
- **Interface number:** This allows selecting a specific interface number
- **Interface description**: This allows entering an interface description that will match with text that exists on the interface description or interface alias.
- **Interface type**: This allows selecting a specific interface type that would match interfaces.
- **Infrastructure Interface**: This type of interface matches any interface that is a switch interface that connects to another switch (more than 4 MAC addresses on an interface), or connects to

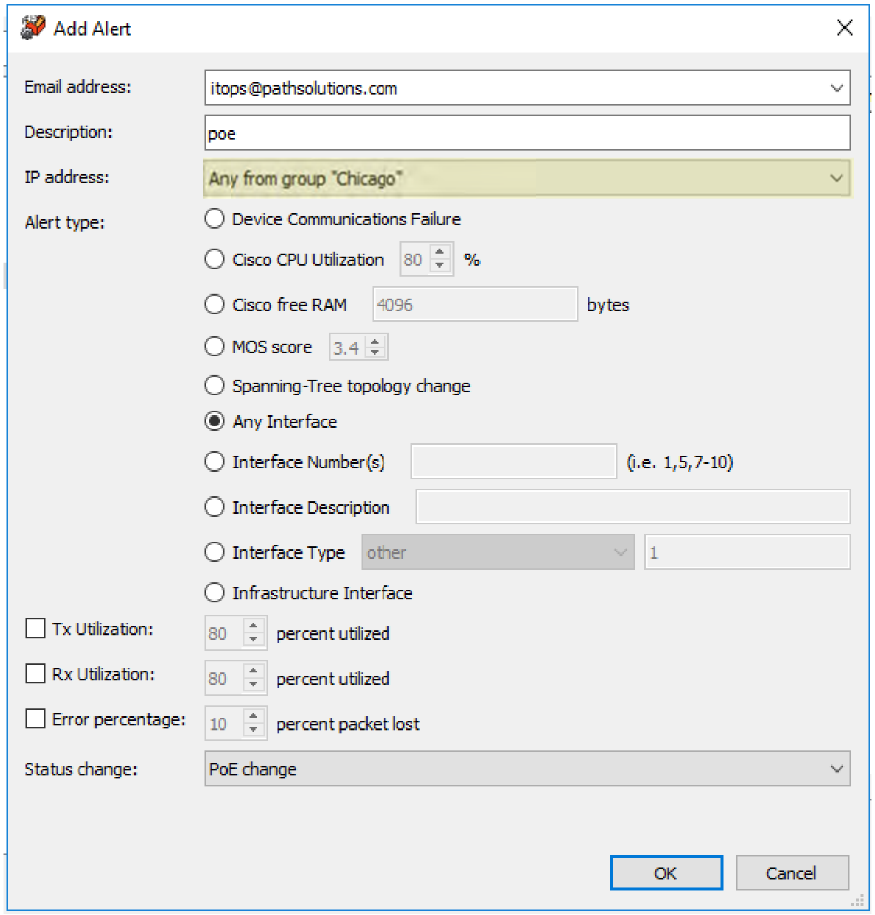
another monitored device (switch, server, or router), or is an interface on a server or router. This allows selecting “all non-user switch interfaces” with one selection.

For interface alerts, trigger thresholds can be set for one or multiple conditions.

- Transmit Utilization Rate
- Receive Utilization Rate
- Error Rate
- Status Change: PoE change or up/down change

Group Alerting

To setup an alert for devices in a group, select the dropdown menu for **IP address** and select **Any from group NAME**. For example, if you want to know when any device in the *Chicago* group has an interface with high utilization, select the **IP address** drop-down menu, and select “Any from group “Chicago.” Write a concise description, such as *Chicago Group Alert* and fill out the parameters that will trigger the alerts.



Add Alert

Email address: itops@pathsolutions.com

Description: poe

IP address: Any from group "Chicago"

Alert type:

○ Device Communications Failure
○ Cisco CPU Utilization 80 %
○ Cisco free RAM 4096 bytes
○ MOS score 3.4
○ Spanning-Tree topology change
● Any Interface
○ Interface Number(s) (i.e. 1,5,7-10)
○ Interface Description
○ Interface Type other 1
○ Infrastructure Interface

□ Tx Utilization: 80 percent utilized

□ Rx Utilization: 80 percent utilized

□ Error percentage: 10 percent packet lost

Status change: PoE change

PoE Alerts

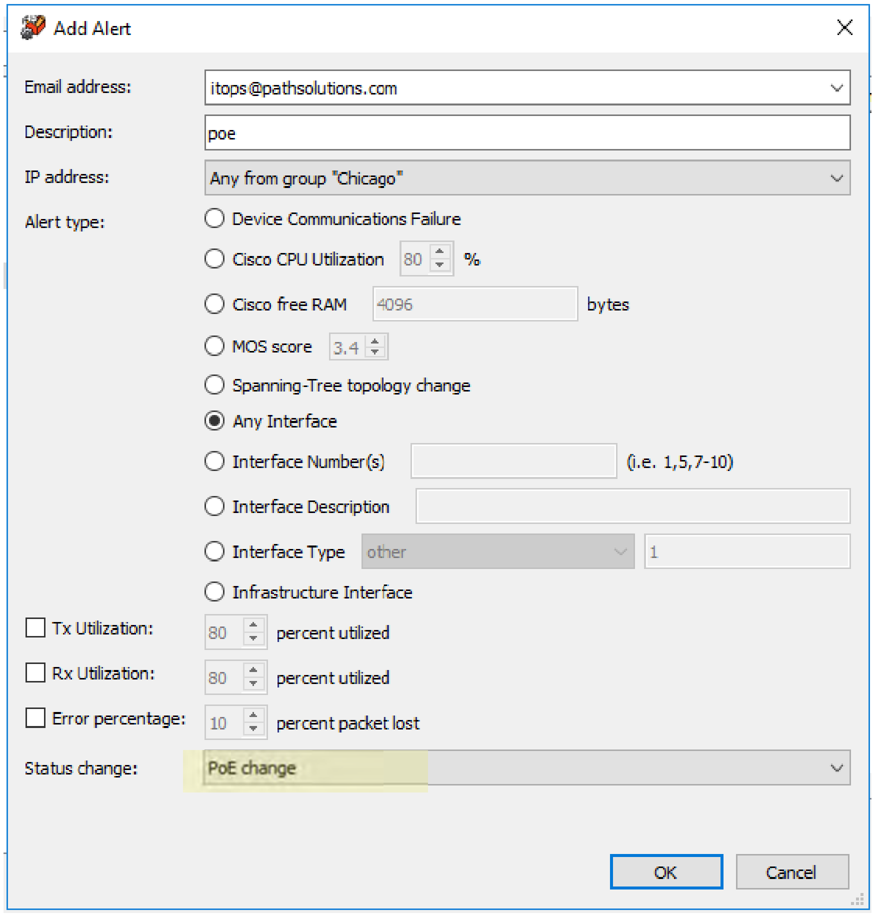
If you want to set an alert when a PoE-enabled device is connected or disconnected from your network, go to the **Network Alerts** section and select **Add**.

Setup an email address from the drop-down menu for the alert.

Add a concise description, such as *PoE alert*, and complete the **Alert type** field and the settings that will trigger the alerts.

Select **PoE change** from the **Status Change** drop-down menu and then select **OK**.

Note: You must first select an option in the **Alert type** field for the **Status Change** field to become active.



Add Alert

Email address: itops@pathsolutions.com

Description: poe

IP address: Any from group "Chicago"

Alert type:
○ Device Communications Failure
○ Cisco CPU Utilization 80 %
○ Cisco free RAM 4096 bytes
○ MOS score 3.4
○ Spanning-Tree topology change
● Any Interface
○ Interface Number(s) (i.e. 1,5,7-10)
○ Interface Description
○ Interface Type other 1
○ Infrastructure Interface

□ Tx Utilization: 80 percent utilized

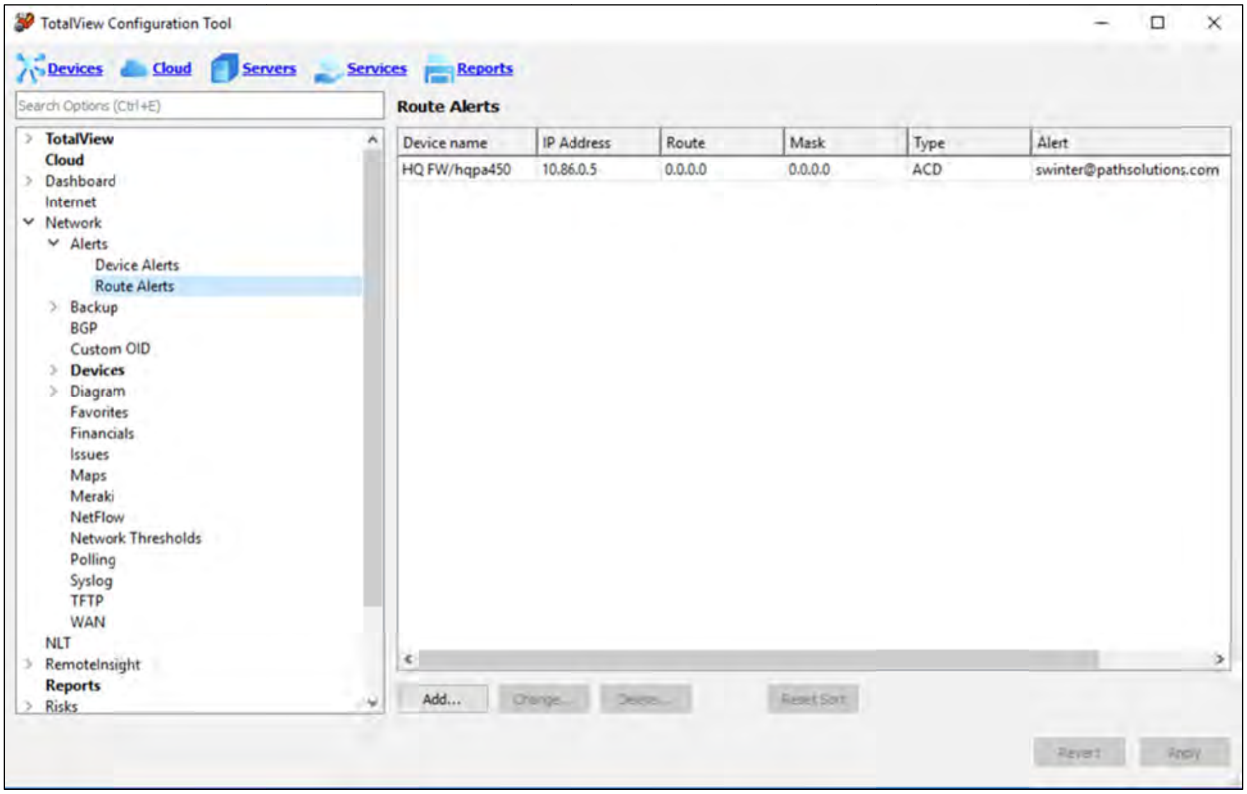
□ Rx Utilization: 80 percent utilized

□ Error percentage: 10 percent packet lost

Status change: PoE change

Route Alerts

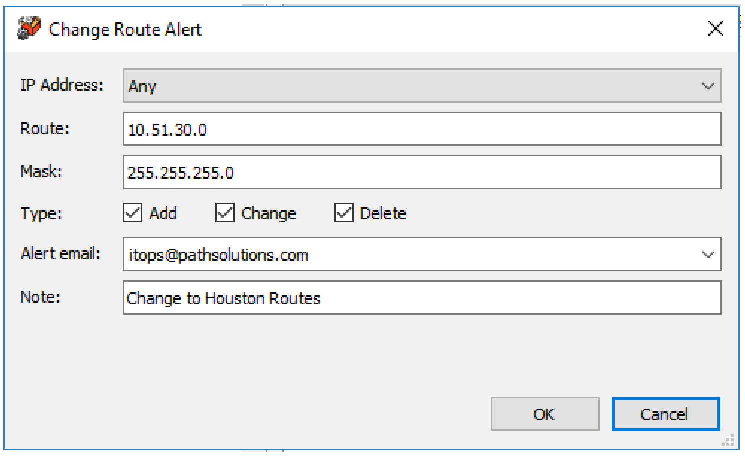
Go to **Network > Alerts > Route Alerts** to configure route alerts. This displays the list of configured Route Alerts.



Route Alerts

Device name	IP Address	Route	Mask	Type	Alert
HQ FW/hqpa450	10.86.0.5	0.0.0.0	0.0.0.0	ACD	swinter@pathsolutions.com

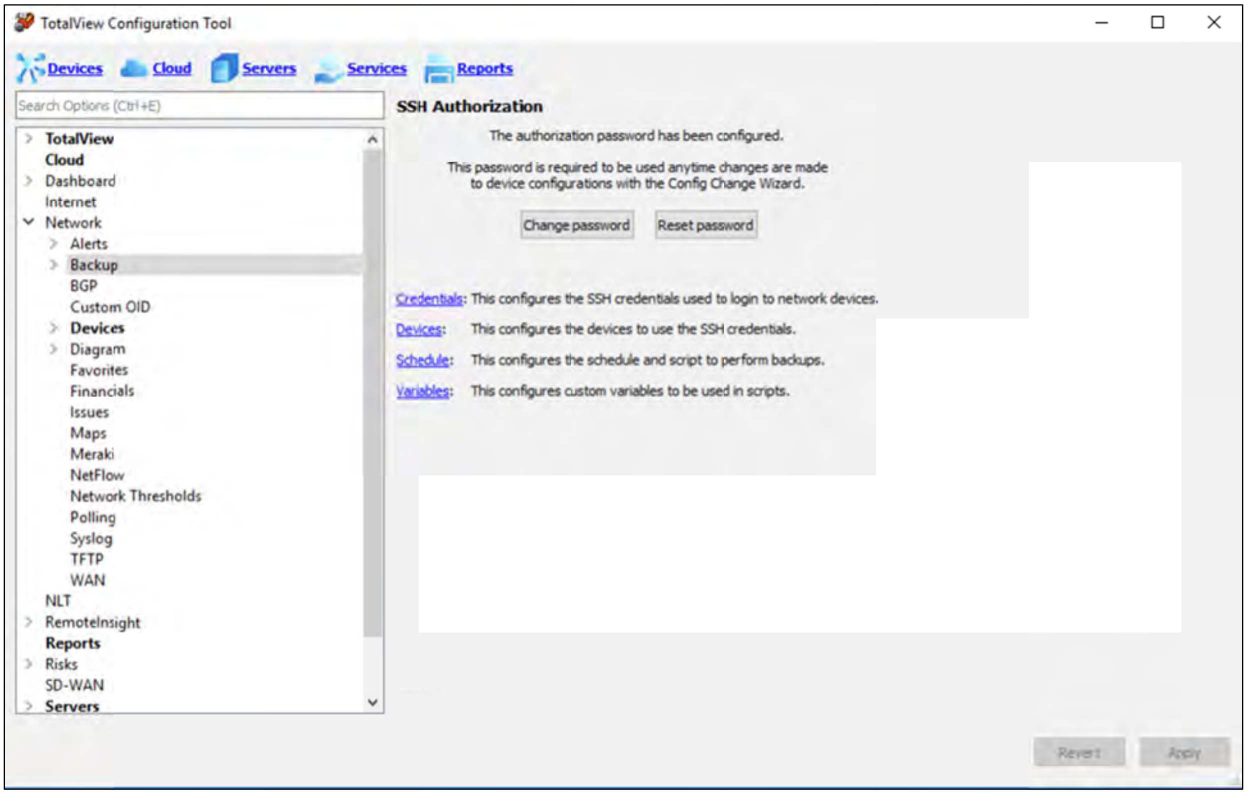
Use the **Add** and **Change** buttons to add and change the route alerts (IP address and mask), the type of alerts to send, and the email recipient.



IP Address:	Any
Route:	10.51.30.0
Mask:	255.255.255.0
Type:	☑ Add ☑ Change ☑ Delete
Alert email:	itops@pathsolutions.com
Note:	Change to Houston Routes

Backup Configuration

Go to **Network > Backups**. This section permits network equipment configurations to have scheduled backups. TotalView shows backup configurations can also do a diff against previous versions to see what has changed. Also, view the logfile of backups and initiate a manual backup from the web interface.



SSH Authorization

The authorization password has been configured.

This password is required to be used anytime changes are made to device configurations with the Config Change Wizard.

Credentials: This configures the SSH credentials used to login to network devices.

Devices: This configures the devices to use the SSH credentials.

Schedule: This configures the schedule and script to perform backups.

Variables: This configures custom variables to be used in scripts.

To use the device configuration backup capability, a master password must be set. This master password is used to protect the device login credentials from being used illicitly.

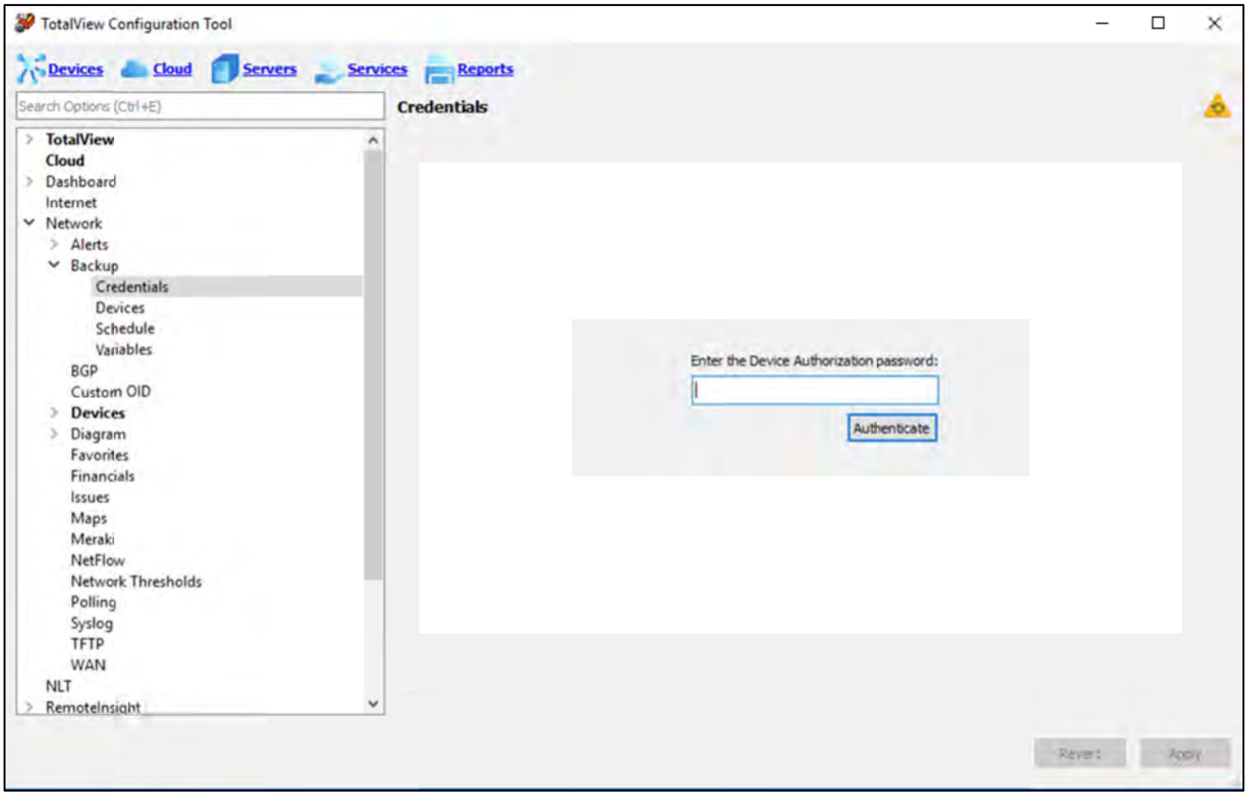
Once the master password has been set, it must be used for any changes made to the configuration, or anytime that the Device Configuration Wizard is used.

Note: If you must reset the password because it was lost, all credentials will be deleted in the system and will need to be re-entered.

Once the master authorization password is set, select the **Credentials** section.

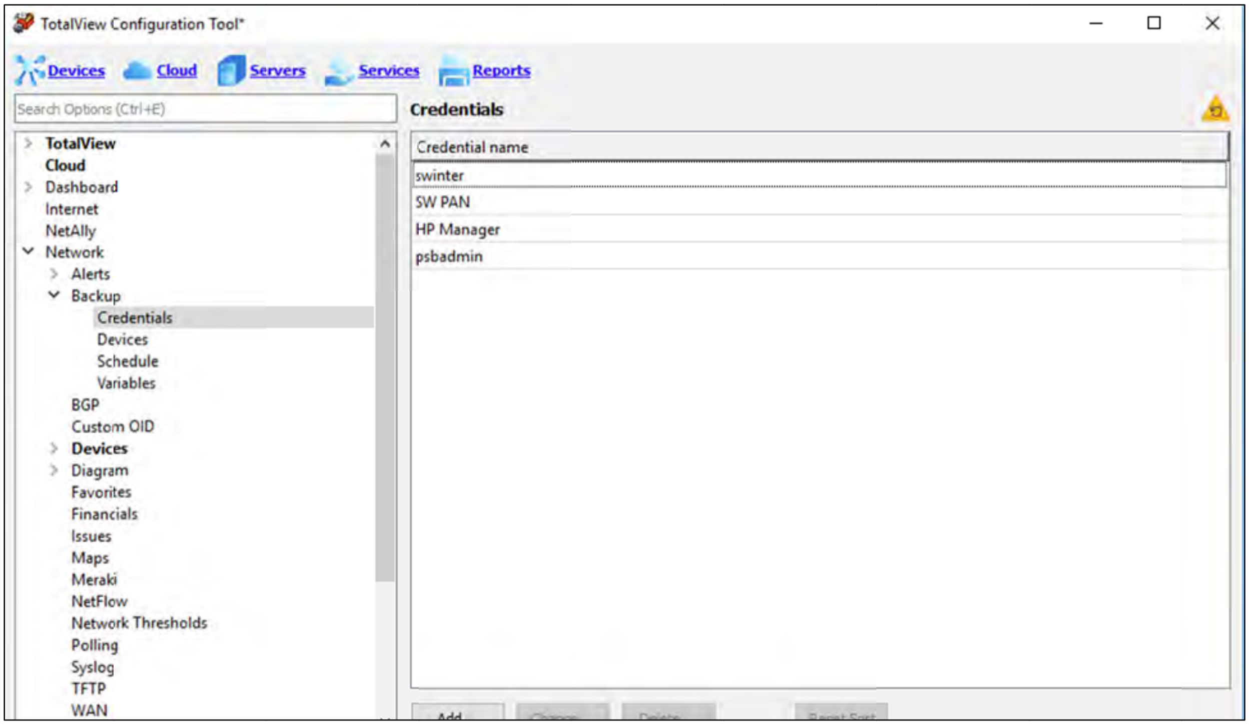
Credentials

The first time you select **Backup > Credentials** in the menu (or any other Backup subsection), you will get a message that states **Enter the Device Authorization password** field.



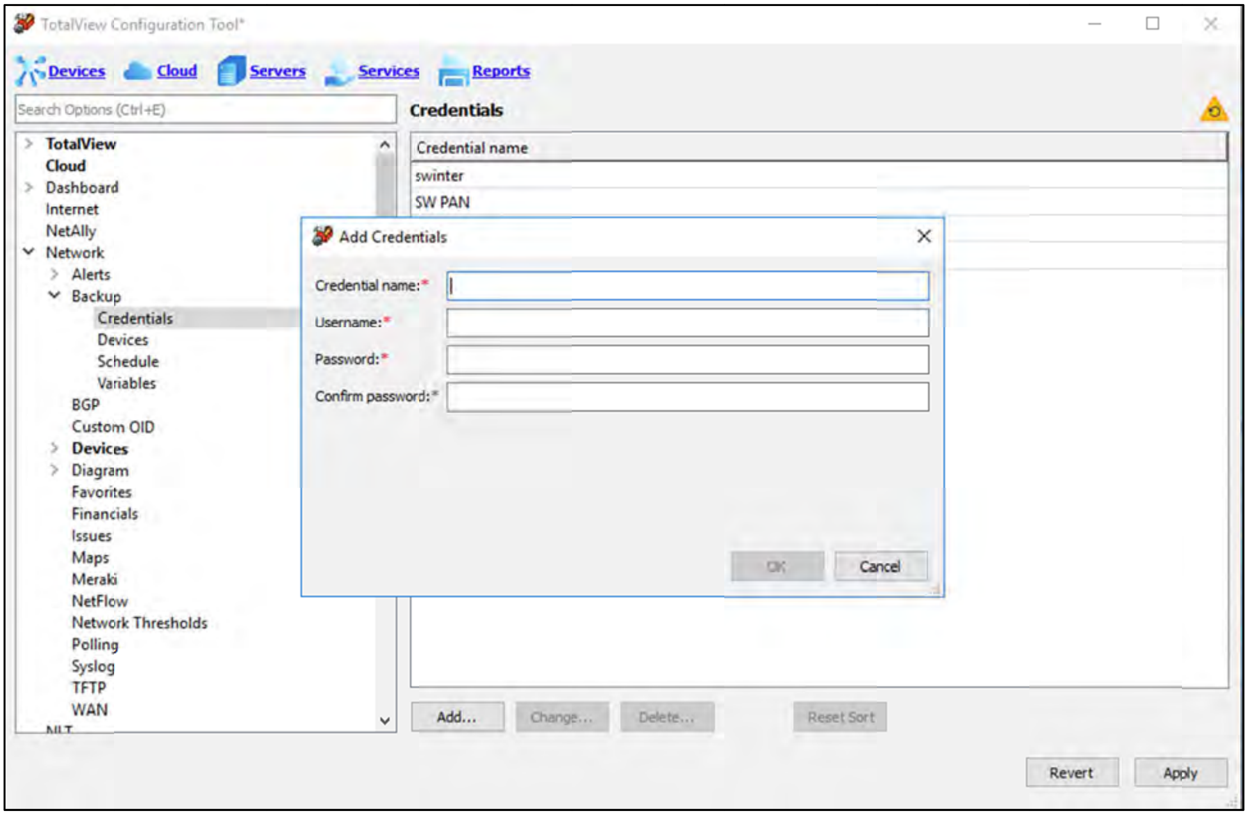
Enter the Device Authorization password:

Enter the password and select **Authenticate**. This displays the list of configured credentials.



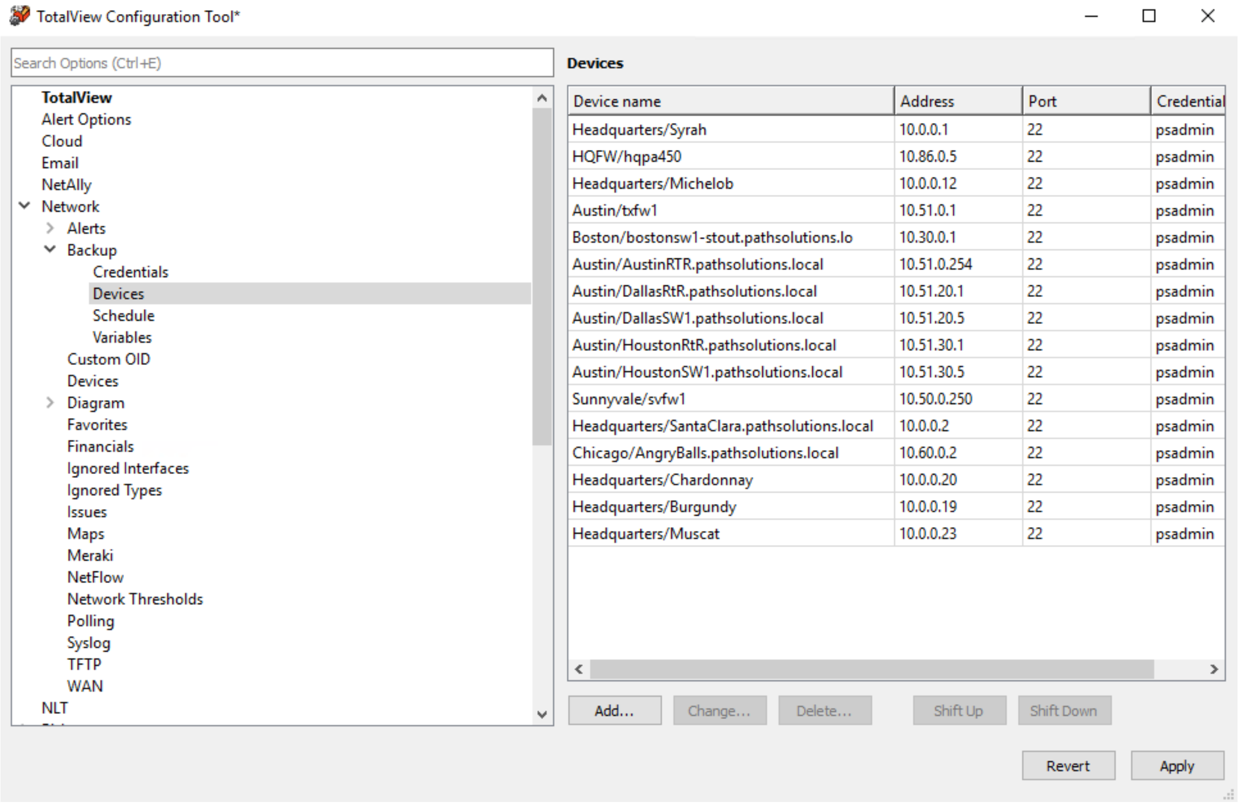
Credential name
swinter
SW PAN
HP Manager
psbadmin

Select **Add** to add credentials to the system. The dialog box asks you to enter the username and password that you would use for SSH connect to a switch or router. Typically, this would be your Radius server credentials or a set of credentials created on the system for TotalView to use.



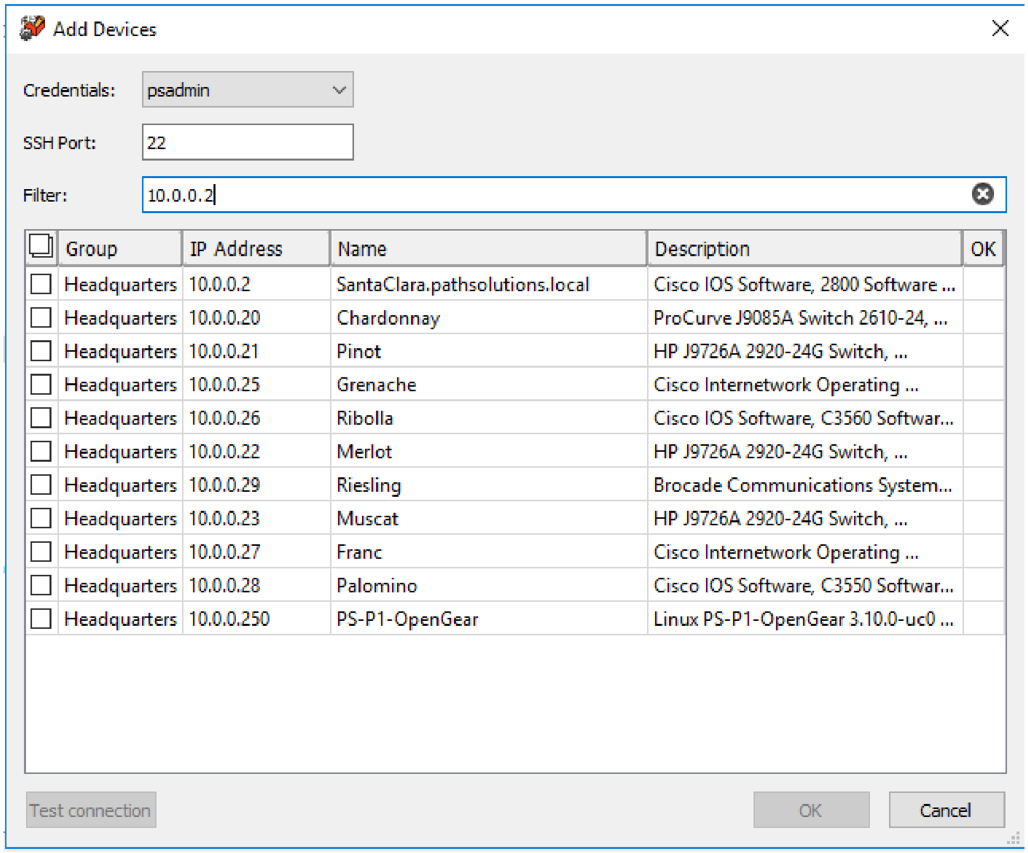
Devices

Go to **Backup > Devices** section to assign device backups. This displays the list of devices with backup configurations.



Device name	Address	Port	Credential
Headquarters/Syrah	10.0.0.1	22	psadmin
HQFW/hqpa450	10.86.0.5	22	psadmin
Headquarters/Michelob	10.0.0.12	22	psadmin
Austin/txfw1	10.51.0.1	22	psadmin
Boston/bostonsw1-stout.pathsolutions.lo	10.30.0.1	22	psadmin
Austin/AustinRTR.pathsolutions.local	10.51.0.254	22	psadmin
Austin/DallasRtR.pathsolutions.local	10.51.20.1	22	psadmin
Austin/DallasSW1.pathsolutions.local	10.51.20.5	22	psadmin
Austin/HoustonRtR.pathsolutions.local	10.51.30.1	22	psadmin
Austin/HoustonSW1.pathsolutions.local	10.51.30.5	22	psadmin
Sunnyvale/svfw1	10.50.0.250	22	psadmin
Headquarters/SantaClara.pathsolutions.local	10.0.0.2	22	psadmin
Chicago/AngryBalls.pathsolutions.local	10.60.0.2	22	psadmin
Headquarters/Chardonnay	10.0.0.20	22	psadmin
Headquarters/Burgundy	10.0.0.19	22	psadmin
Headquarters/Muscat	10.0.0.23	22	psadmin

Select **Add** if you need to add a device to the configuration.



Credentials: psadmin

SSH Port: 22

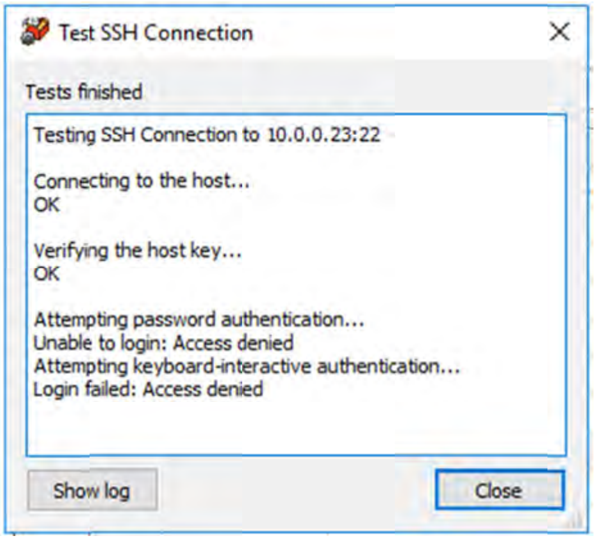
Filter: 10.0.0.2

□	Group	IP Address	Name	Description	OK
□	Headquarters	10.0.0.2	SantaClara.pathsolutions.local	Cisco IOS Software, 2800 Software ...	
□	Headquarters	10.0.0.20	Chardonnay	ProCurve J9085A Switch 2610-24, ...	
□	Headquarters	10.0.0.21	Pinot	HP J9726A 2920-24G Switch, ...	
□	Headquarters	10.0.0.25	Grenache	Cisco Internetwork Operating ...	
□	Headquarters	10.0.0.26	Ribolla	Cisco IOS Software, C3560 Softwar...	
□	Headquarters	10.0.0.22	Merlot	HP J9726A 2920-24G Switch, ...	
□	Headquarters	10.0.0.29	Riesling	Brocade Communications System...	
□	Headquarters	10.0.0.23	Muscat	HP J9726A 2920-24G Switch, ...	
□	Headquarters	10.0.0.27	Franc	Cisco Internetwork Operating ...	
□	Headquarters	10.0.0.28	Palomino	Cisco IOS Software, C3550 Softwar...	
□	Headquarters	10.0.0.250	PS-P1-OpenGear	Linux PS-P1-OpenGear 3.10.0-uc0 ...	

Select the credentials from the **Credentials** drop-down menu to show you a list of devices, so you can use the appropriate credentials for the device and use the **Filter** field to filter the list.

It is recommended to select the device then select **Test connection** to verify those credentials and ensure the security token is read and stored. If this is the first time communicating with the device, it will ask you to verify the hardware security token.

The screenshot below displays an example of testing a connection.

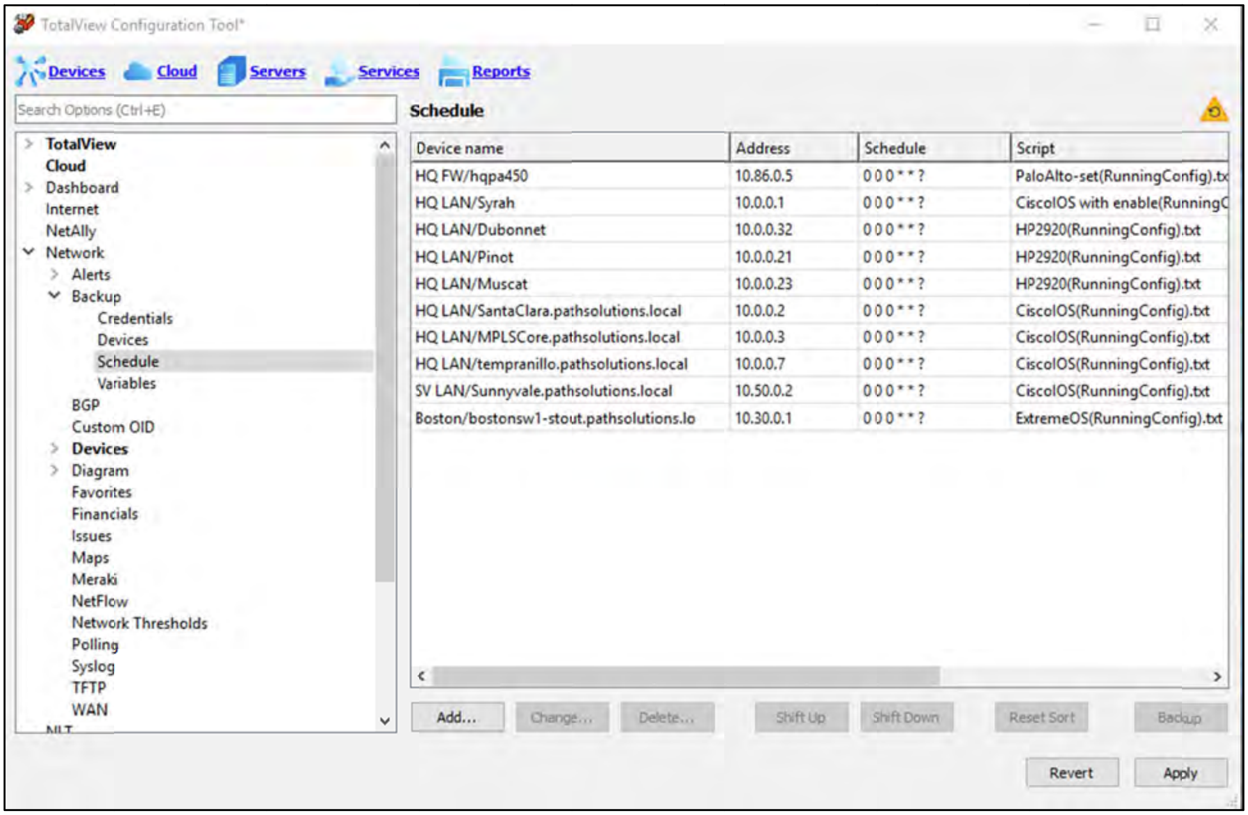


Tests finished

```
Testing SSH Connection to 10.0.0.23:22

Connecting to the host...
OK

Verifying the host key...
OK

Attempting password authentication...
Unable to login: Access denied
Attempting keyboard-interactive authentication...
Login failed: Access denied
```

Schedule Backup

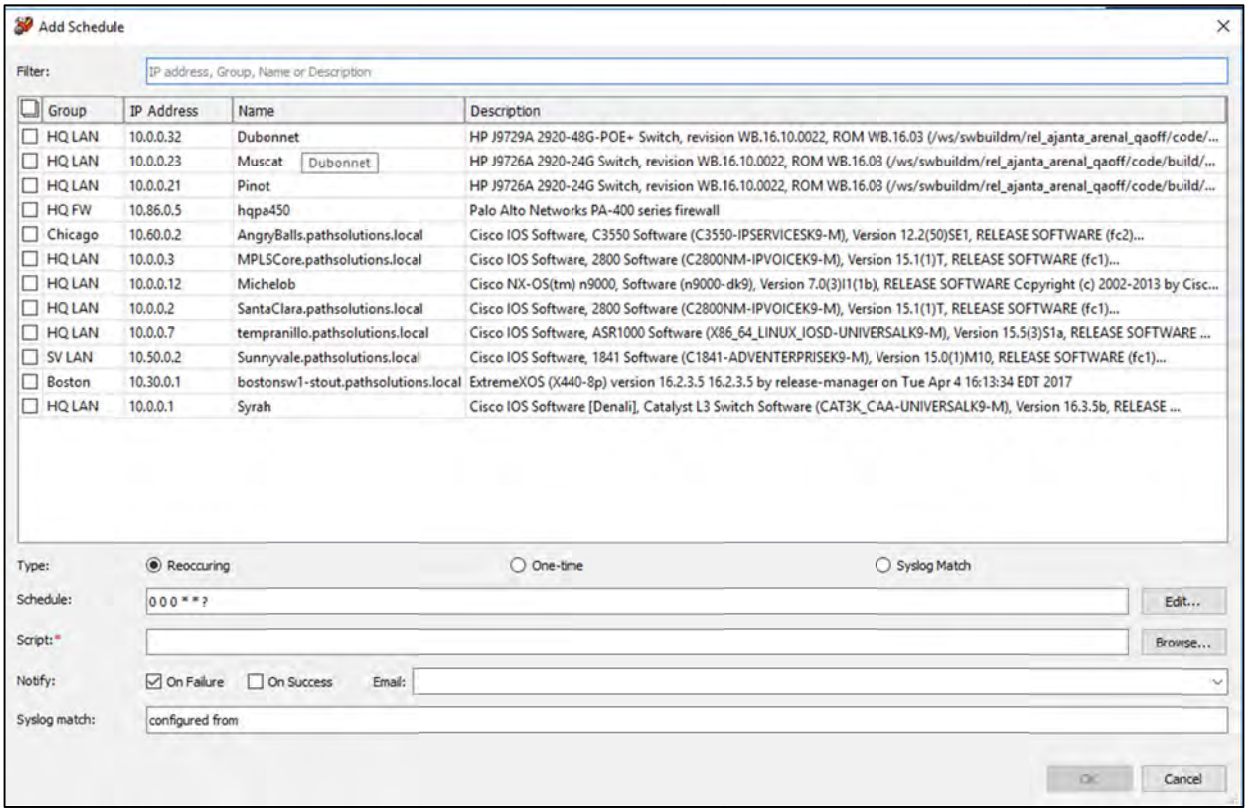
Go to **Backup > Schedule** section to create a backup schedule of network devices. This displays the list of devices with schedules.



Schedule

Device name	Address	Schedule	Script
HQ FW/hqpa450	10.86.0.5	0 0 0 * * ?	PaloAlto-set(RunningConfig).tx
HQ LAN/Syrah	10.0.0.1	0 0 0 * * ?	CiscoIOS with enable(RunningC
HQ LAN/Dubonnet	10.0.0.32	0 0 0 * * ?	HP2920(RunningConfig).txt
HQ LAN/Pinot	10.0.0.21	0 0 0 * * ?	HP2920(RunningConfig).txt
HQ LAN/Muscat	10.0.0.23	0 0 0 * * ?	HP2920(RunningConfig).txt
HQ LAN/SantaClara.pathsolutions.local	10.0.0.2	0 0 0 * * ?	CiscoIOS(RunningConfig).txt
HQ LAN/MPLSCore.pathsolutions.local	10.0.0.3	0 0 0 * * ?	CiscoIOS(RunningConfig).txt
HQ LAN/tempranillo.pathsolutions.local	10.0.0.7	0 0 0 * * ?	CiscoIOS(RunningConfig).txt
SV LAN/Sunnyvale.pathsolutions.local	10.50.0.2	0 0 0 * * ?	CiscoIOS(RunningConfig).txt
Boston/bostonsw1-stout.pathsolutions.lo	10.30.0.1	0 0 0 * * ?	ExtremeOS(RunningConfig).txt

Select **Add** to add backup schedules for devices. Then select the backup type, set a schedule, pick a script (browse from the scripts provided with TotalView), and an email to notify once finished.



Filter: IP address, Group, Name or Description

□	Group	IP Address	Name	Description
□	HQ LAN	10.0.0.32	Dubonnet	HP J9729A 2920-48G-POE+ Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/...
□	HQ LAN	10.0.0.23	Muscat Dubonnet	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/build/...
□	HQ LAN	10.0.0.21	Pinot	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm/rel_ajanta_arenal_qaoff/code/build/...
□	HQ FW	10.86.0.5	hqpa450	Palo Alto Networks PA-400 series firewall
□	Chicago	10.60.0.2	AngryBalls.pathsolutions.local	Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(50)SE1, RELEASE SOFTWARE (fc2)...
□	HQ LAN	10.0.0.3	MPLSCore.pathsolutions.local	Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-M), Version 15.1(1)T, RELEASE SOFTWARE (fc1)...
□	HQ LAN	10.0.0.12	Michelob	Cisco NX-OS(tm) n9000, Software (n9000-dk9), Version 7.0(3)I1(1b), RELEASE SOFTWARE Copyright (c) 2002-2013 by Cisc...
□	HQ LAN	10.0.0.2	SantaClara.pathsolutions.local	Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-M), Version 15.1(1)T, RELEASE SOFTWARE (fc1)...
□	HQ LAN	10.0.0.7	tempranillo.pathsolutions.local	Cisco IOS Software, ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(3)S1a, RELEASE SOFTWARE ...
□	SV LAN	10.50.0.2	Sunnyvale.pathsolutions.local	Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 15.0(1)M10, RELEASE SOFTWARE (fc1)...
□	Boston	10.30.0.1	bostonsw1-stout.pathsolutions.local	ExtremeXOS (X440-8p) version 16.2.3.5 16.2.3.5 by release-manager on Tue Apr 4 16:13:34 EDT 2017
□	HQ LAN	10.0.0.1	Syrah	Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.5b, RELEASE ...

Type: ● Reoccuring ○ One-time ○ Syslog Match

Schedule: 0 0 0 * * ?

Script:*

Notify: ☑ On Failure □ On Success Email:

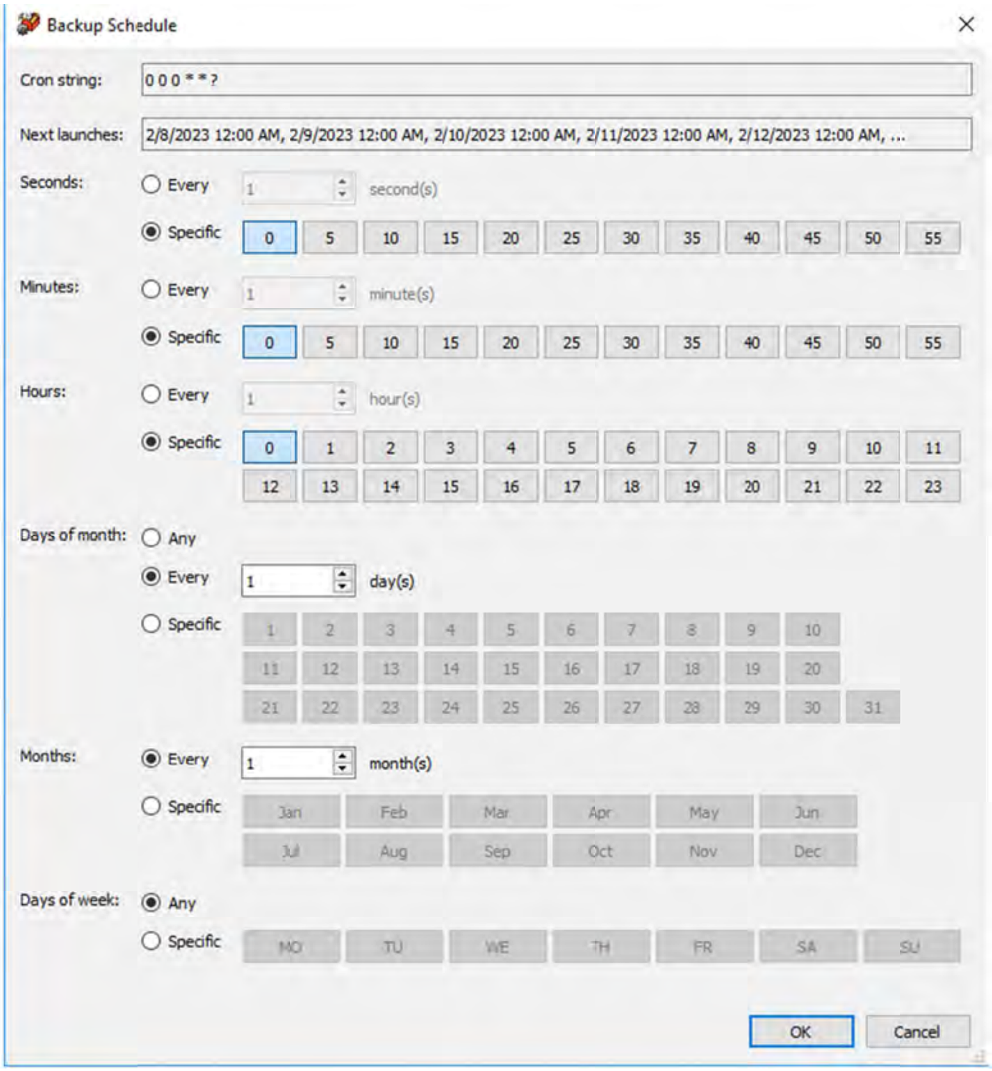
Syslog match: configured from

For the selected device, it will show the internal system description to help you determine what schedule and script to use to perform the backup.

The Script should be chosen based on the device manufacturer and OS.

Enter an email address that should be notified of backup success or failure.

The schedule information is entered in **CRON** tab format but can easily be modified by selecting **Edit** to see the full set of timing options.



Backup Schedule

Cron string: 0 0 0 * * ?

Next launches: 2/8/2023 12:00 AM, 2/9/2023 12:00 AM, 2/10/2023 12:00 AM, 2/11/2023 12:00 AM, 2/12/2023 12:00 AM, ...

Seconds: ○ Every 1 second(s)
● Specific 0

Minutes: ○ Every 1 minute(s)
● Specific 0

Hours: ○ Every 1 hour(s)
● Specific 0

Days of month: ○ Any
● Every 1 day(s)
○ Specific

Months: ● Every 1 month(s)
○ Specific

Days of week: ● Any
○ Specific

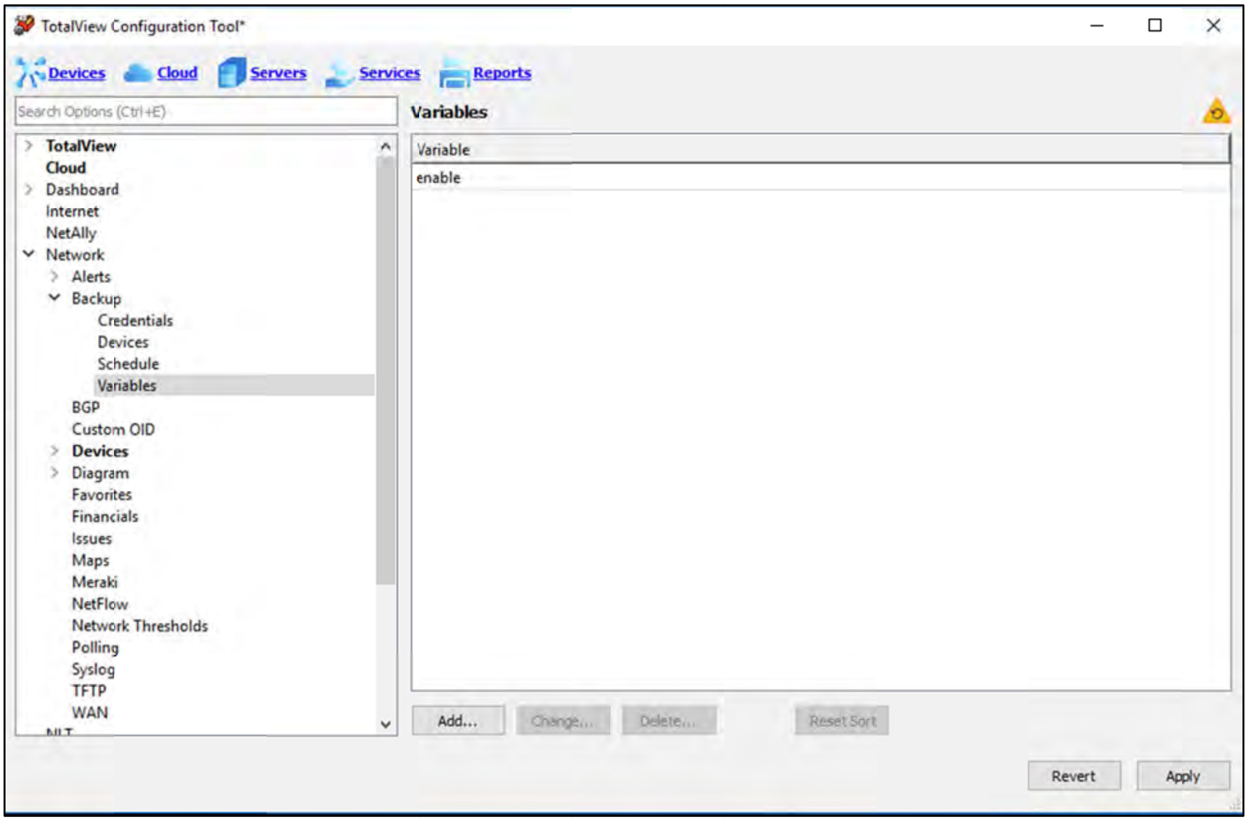
Note the “Next Launches” field as it will show when the backups would be scheduled with the selected entries.

Select **OK** to completed the schedule changes.

Variables

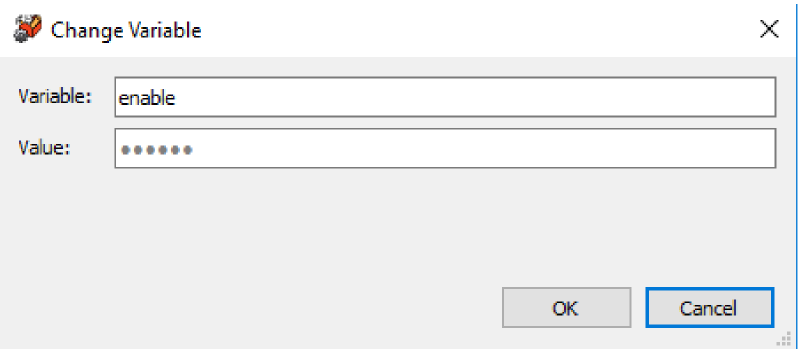
Go to **Network Backup > Variables** section for setting up backup variables for the backup scripts. This calls up the list of variables.

In some cases, you may want to use a variable in a script, and have TotalView fill in the variable when the script runs. This variable may be a password (for security reasons it will not save the variables to the files made during backup). Or the variable may be a variable that you may want to use in multiple scripts, such as a domain name.



Variable
enable

Add or change variables by selecting the **Add** and **Change** buttons and filling out the **Variable** and **Value** fields.

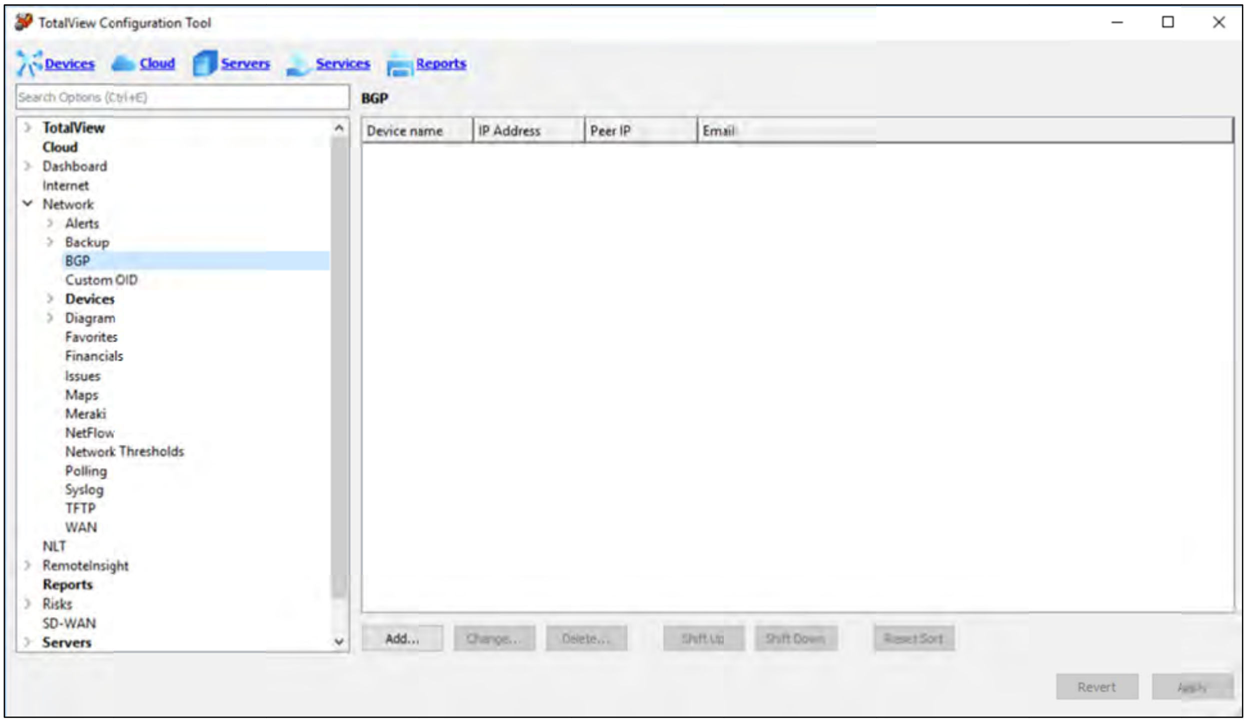


Variable: enable

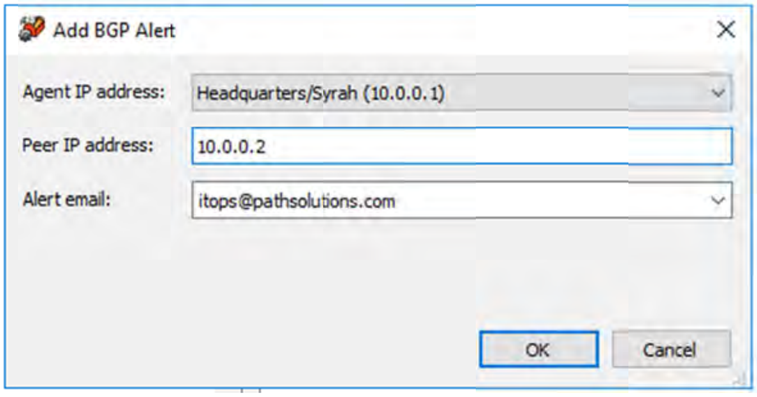
Value: ●●●●●●

BGP

Go to **Network > Alerts > BGP Alerts**. If a BGP peer gets disconnected or changes status, you can receive alerts.



Use the **Add** or **Change** buttons to add or modify agents and peers on the list, and email for the alert.



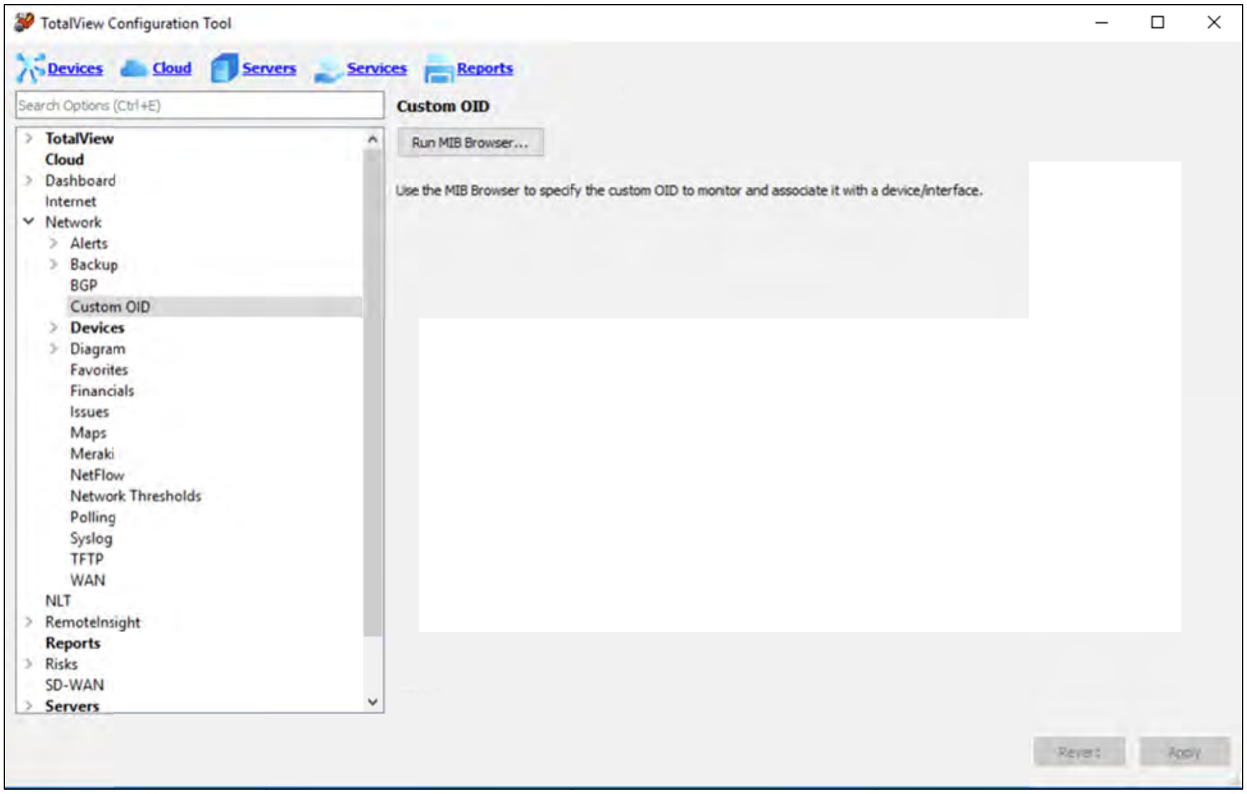
Agent IP address: Headquarters/Syrah (10.0.0.1)

Peer IP address: 10.0.0.2

Alert email: itops@pathsolutions.com

Custom OID

PathSolutions TotalView can monitor custom OIDs such as CPU utilization, memory usage, and temperature if the device provides this information via SNMP. The Config Tool has a button **Run MIB Browser** to specify the custom OID to monitor and associate it with a device/interface.



Use the MIB Browser to specify the custom OID to monitor and associate it with a device/interface.

The **MIB Browser** will open in a separate window. See the section MIB Browser for OID lookups, OID monitoring and OID graphing.

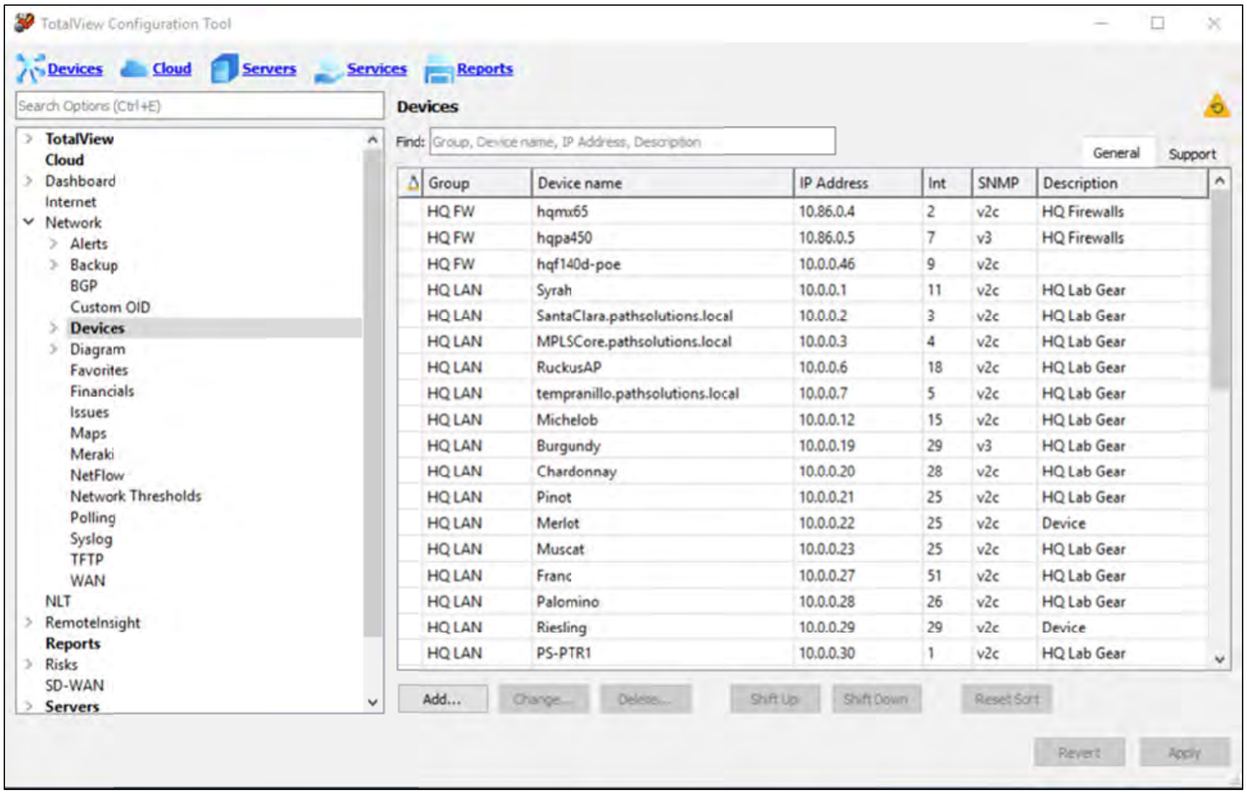
Note: Customize OID monitoring reports by editing the cfg file. See Appendix F. Custom OID Monitoring.

Devices Configuration

Go to **Network > Devices** section, to see the list of currently monitored devices.

Note: All interfaces for each switch are monitored by default, ignore individual interfaces from being monitored on the web interface.

Note: If SNMPv3 is not enabled and is desired, contact support@pathsolutions.com.

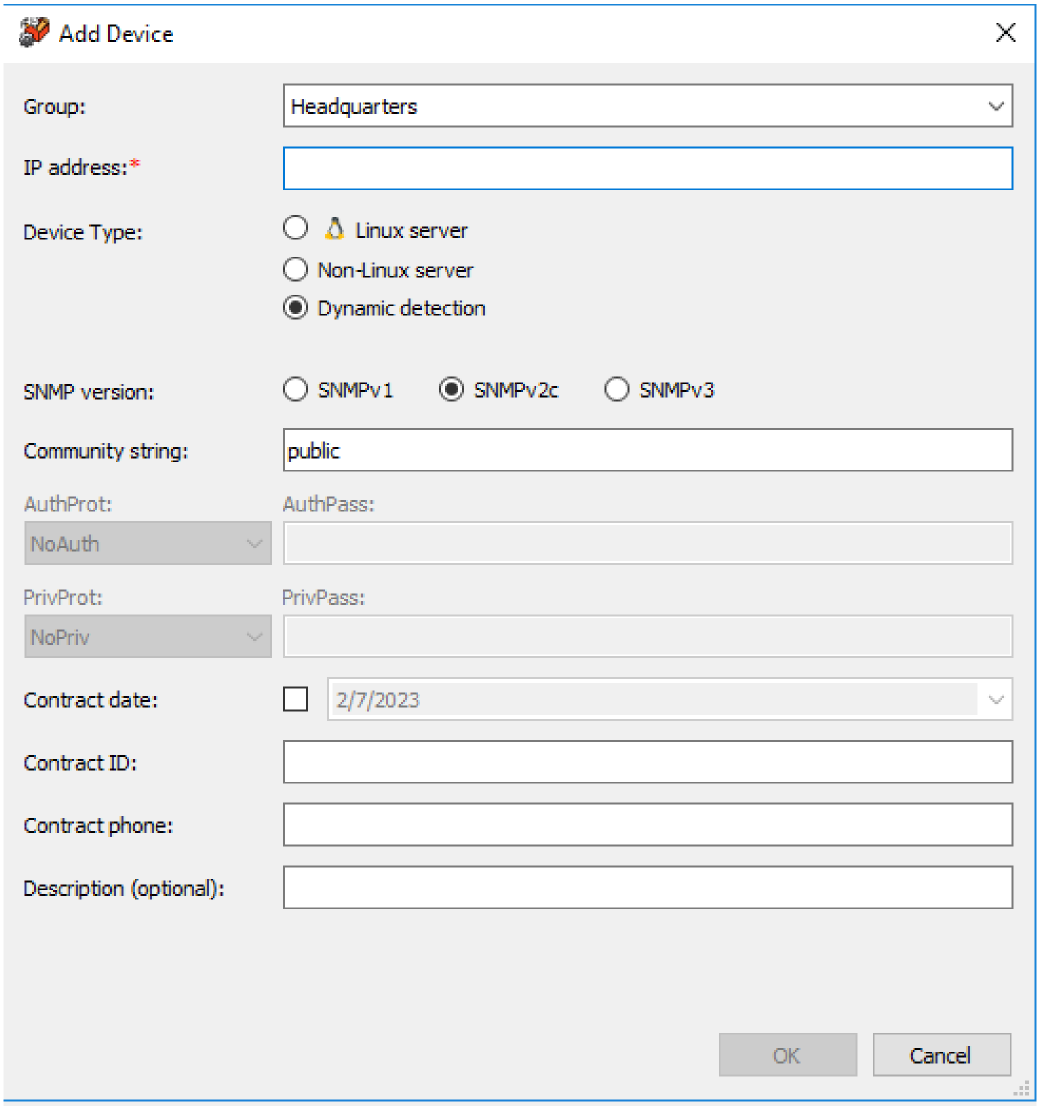


Group	Device name	IP Address	Int	SNMP	Description
HQ FW	hqmx65	10.86.0.4	2	v2c	HQ Firewalls
HQ FW	hqpa450	10.86.0.5	7	v3	HQ Firewalls
HQ FW	hqf140d-poe	10.0.0.46	9	v2c	
HQ LAN	Syrah	10.0.0.1	11	v2c	HQ Lab Gear
HQ LAN	SantaClara.pathsolutions.local	10.0.0.2	3	v2c	HQ Lab Gear
HQ LAN	MPLSCore.pathsolutions.local	10.0.0.3	4	v2c	HQ Lab Gear
HQ LAN	RuckusAP	10.0.0.6	18	v2c	HQ Lab Gear
HQ LAN	tempranillo.pathsolutions.local	10.0.0.7	5	v2c	HQ Lab Gear
HQ LAN	Michelob	10.0.0.12	15	v2c	HQ Lab Gear
HQ LAN	Burgundy	10.0.0.19	29	v3	HQ Lab Gear
HQ LAN	Chardonnay	10.0.0.20	28	v2c	HQ Lab Gear
HQ LAN	Pinot	10.0.0.21	25	v2c	HQ Lab Gear
HQ LAN	Merlot	10.0.0.22	25	v2c	Device
HQ LAN	Muscat	10.0.0.23	25	v2c	HQ Lab Gear
HQ LAN	Franc	10.0.0.27	51	v2c	HQ Lab Gear
HQ LAN	Palomino	10.0.0.28	26	v2c	HQ Lab Gear
HQ LAN	Riesling	10.0.0.29	29	v2c	Device
HQ LAN	PS-PTR1	10.0.0.30	1	v2c	HQ Lab Gear

Change the sort order for TotalView web display if desired. To move items on the list up or down, select on the item, and then select **Shift Up** or **Shift Down**.

Adding Devices

To add a device, select **Add**. the **Add device** dialog will display.



Add Device

Group: Headquarters

IP address:*

Device Type: ○ Linux server ○ Non-Linux server ● Dynamic detection

SNMP version: ○ SNMPv1 ● SNMPv2c ○ SNMPv3

Community string: public

AuthProt: NoAuth AuthPass:

PrivProt: NoPriv PrivPass:

Contract date: □ 2/7/2023

Contract ID:

Contract phone:

Description (optional):

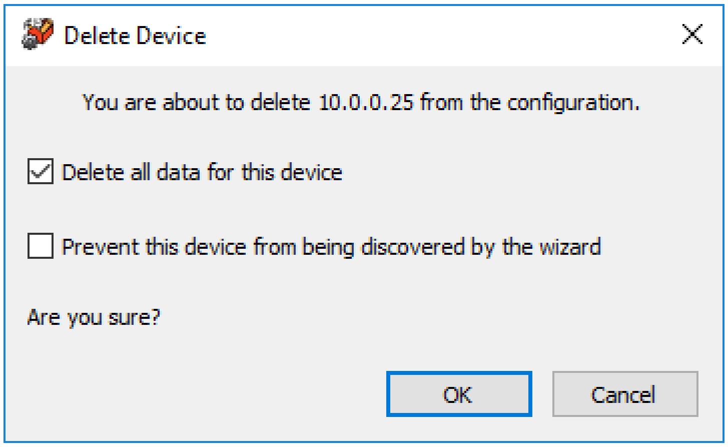
Enter the IP address and SNMP read-only community string for the device.

Optionally, add the support contract date, ID, contract phone and contract description for the device. This contract information will appear on TotalView's **Support** tab.

Select **OK** to add the device or select **Cancel**.

Deleting Devices

To delete a device, select the device and select **Delete**. The **Delete Device** dialog will display.



Delete Device

You are about to delete 10.0.0.25 from the configuration.

☑ Delete all data for this device

☐ Prevent this device from being discovered by the wizard

Are you sure?

If you select on the **Prevent this device from being discovered by the wizard** checkbox, the device will no longer be discovered when running the wizard.

Note: Deleting a device from monitoring will not delete the previously collected graph data. Add the device back to monitoring and it will continue to use the same data file for graph data storage.

Note: Any device prevented from being re-discovered when the QuickConfig Wizard runs can be added back again by removing the device from being ignored in the **SwMonIgnore.cfg** file or by adding the device to be monitored again in the **SwitchMonitor.cfg** file. These files can be found in one of the following directories:

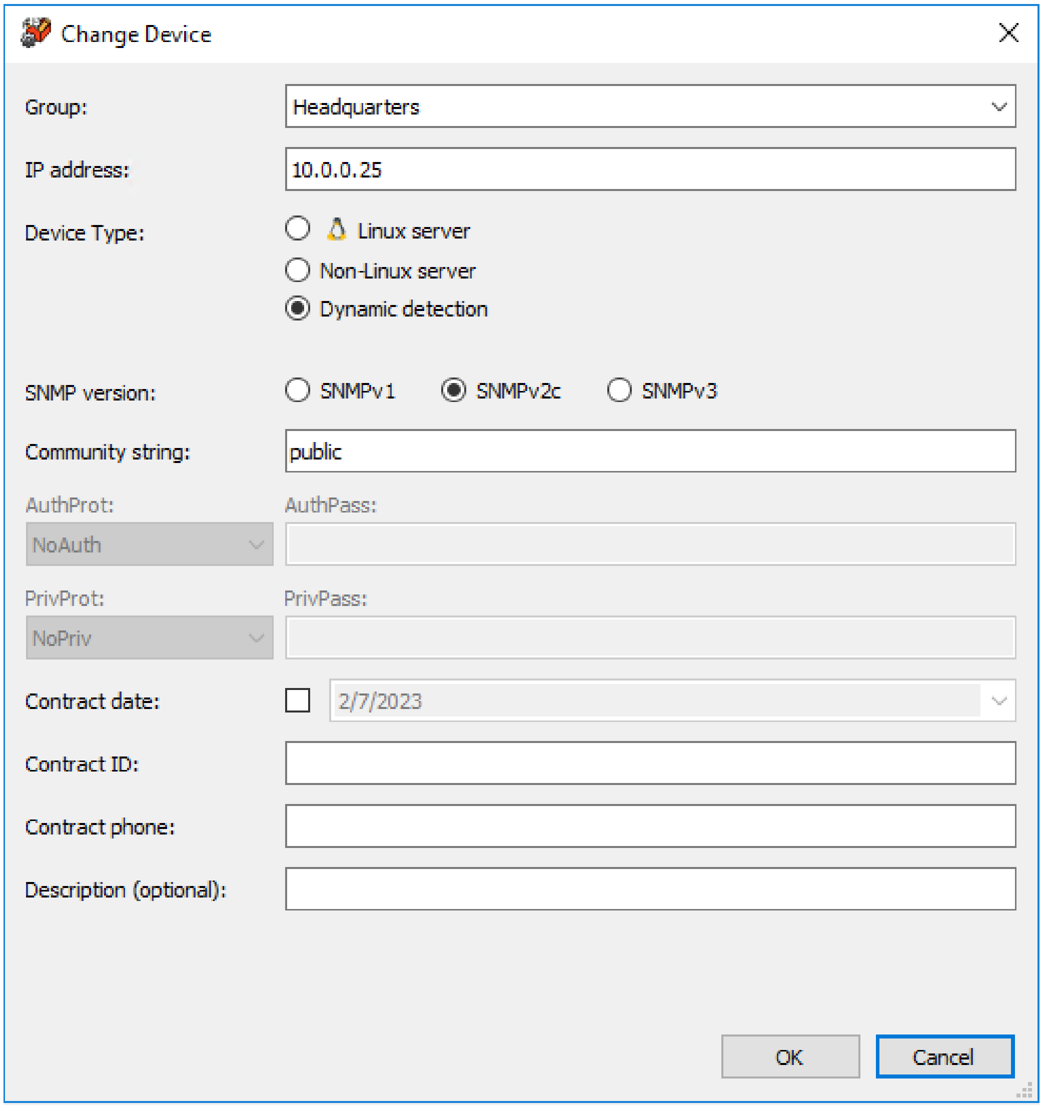
C:\Program Files\PathSolutions\TotalView\
C:\Program Files (x86)\PathSolutions\TotalView\

Save the file after any modification.

Changing Device Information

To modify a device, double-select on an existing device IP address or select the device's IP address and select **Change**.

The **Change Device** dialog will display.



Change Device

Group: Headquarters

IP address: 10.0.0.25

Device Type: ○ Linux server ○ Non-Linux server ● Dynamic detection

SNMP version: ○ SNMPv1 ● SNMPv2c ○ SNMPv3

Community string: public

AuthProt: NoAuth AuthPass:

PrivProt: NoPriv PrivPass:

Contract date: □ 2/7/2023

Contract ID:

Contract phone:

Description (optional):

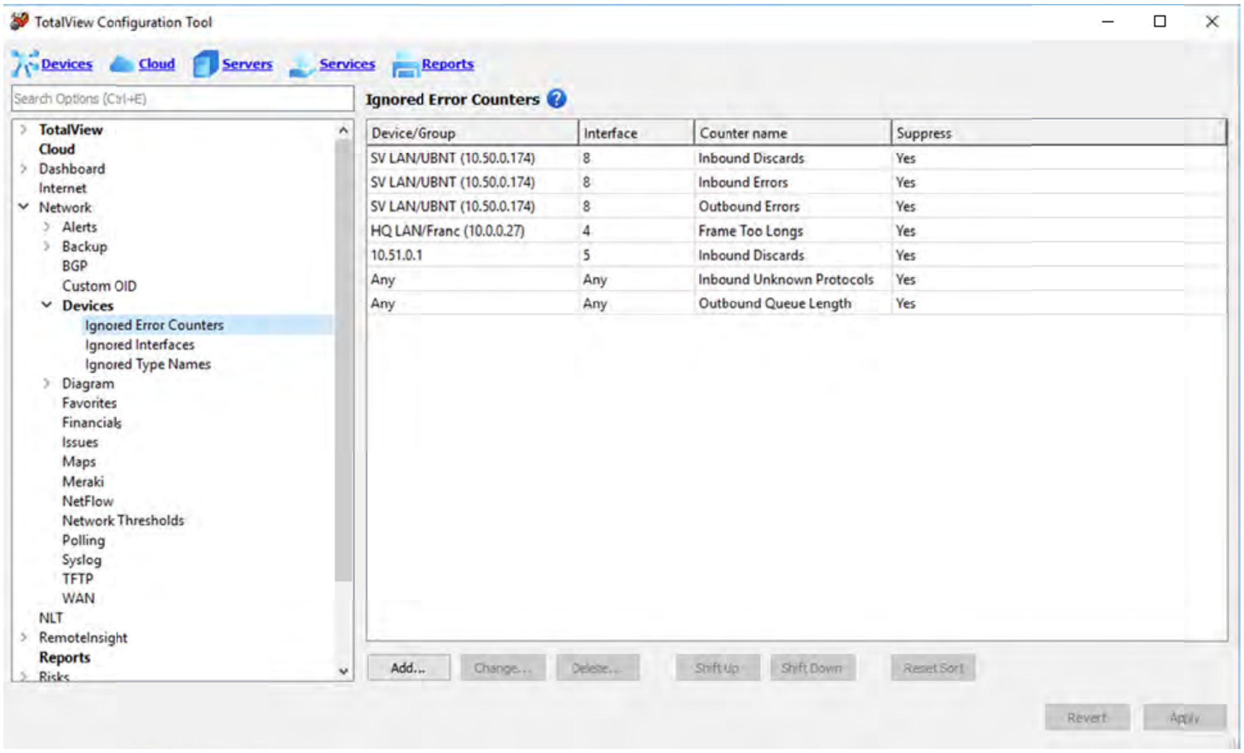
The only required fields for a device are the Group, IP address, and SNMP community string fields.

Configuring the Support Tab

If you add the support contract date, ID, contract phone and contract description for devices, this information will appear on TotalView's **Support** tab.

Ignored Error Counters

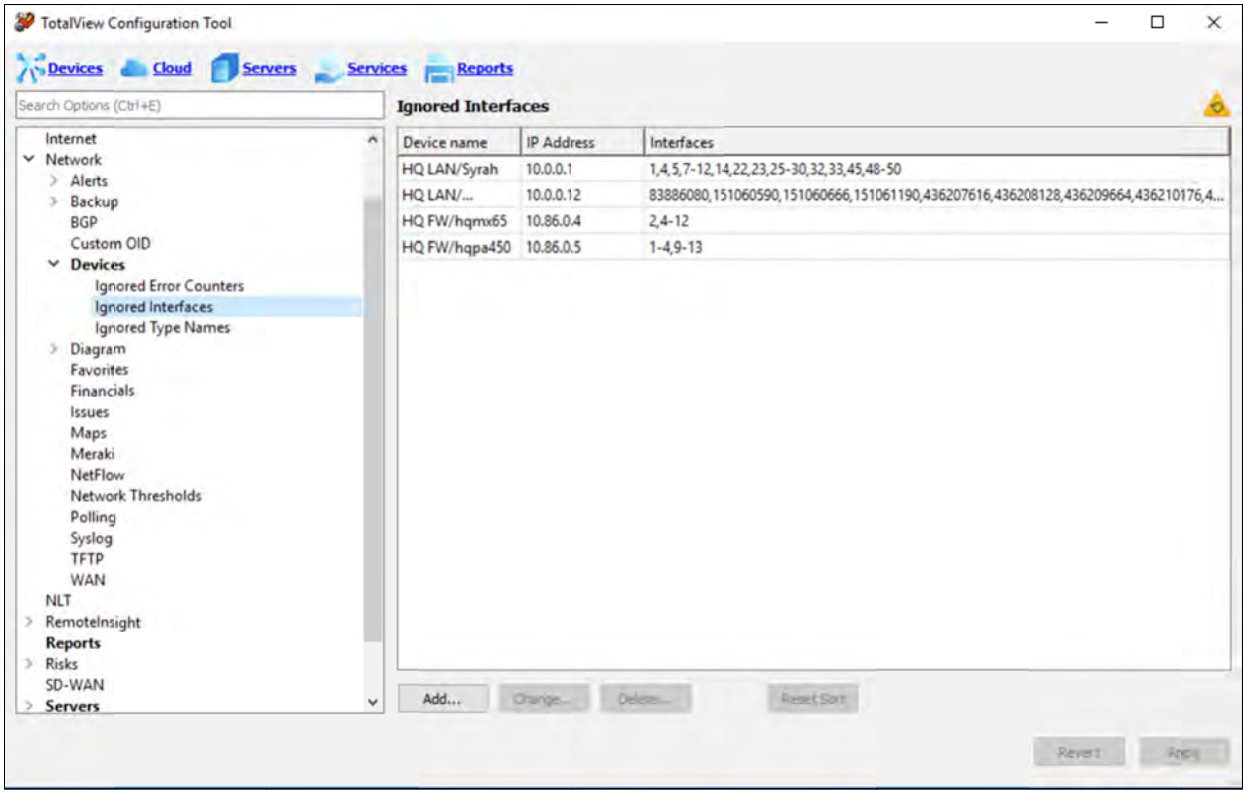
Select **Network > Devices > Ignored Error Counters** then add, change or delete the error counters that you want to no longer respect as errors. This can be done for a single interface on a device, an entire device, or all devices and interfaces in the deployment.



Device/Group	Interface	Counter name	Suppress
SV LAN/UBNT (10.50.0.174)	8	Inbound Discards	Yes
SV LAN/UBNT (10.50.0.174)	8	Inbound Errors	Yes
SV LAN/UBNT (10.50.0.174)	8	Outbound Errors	Yes
HQ LAN/Franc (10.0.0.27)	4	Frame Too Longs	Yes
10.51.0.1	5	Inbound Discards	Yes
Any	Any	Inbound Unknown Protocols	Yes
Any	Any	Outbound Queue Length	Yes

Ignored Interfaces

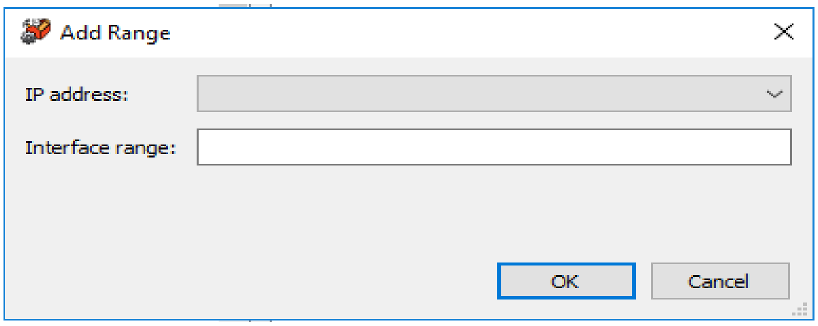
Go to **Network > Devices > Ignored Interfaces**, and add, delete and change the list of interfaces to ignore here. These interfaces will not be monitored and will not count towards licensing.



Ignored Interfaces

Device name	IP Address	Interfaces
HQ LAN/Syrah	10.0.0.1	1,4,5,7-12,14,22,23,25-30,32,33,45,48-50
HQ LAN/...	10.0.0.12	83886080,151060590,151060666,151061190,436207616,436208128,436209664,436210176,4...
HQ FW/hqmx65	10.86.0.4	2,4-12
HQ FW/hqpa450	10.86.0.5	1-4,9-13

Select **Add** or **Change** buttons to add devices by IP address and interface ranges to the ignored list.



IP address:

Interface range:

Alternate Methods to Ignore Interfaces

There are two other ways of ignoring interfaces, outside of using the Config Tool.

1) The **IgnoreList.cfg** allows you to ignore ranges of interfaces on devices.

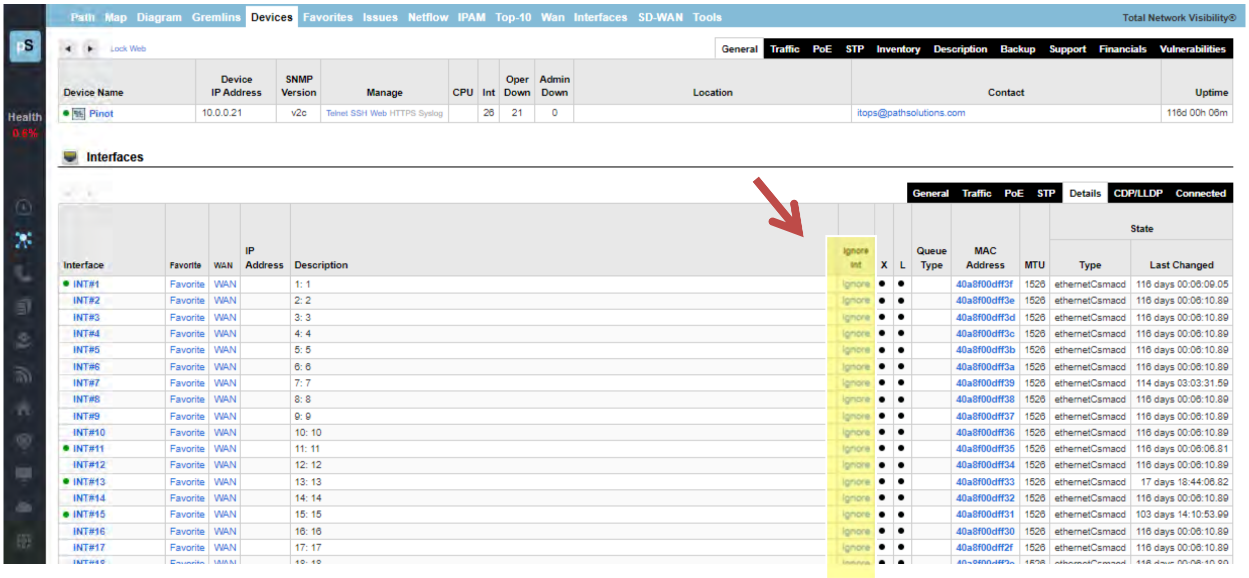
The above file should be opened in Notepad for editing. After you save the file, stop and restart the service to have this change take effect.

This file is located in one of the following directories:

C:/Program Files (x86)/PathSolutions/TotalView/IgnoreList.cfg
C:/Program Files/PathSolutions/TotalView/IgnoreList.cfg

2) If you only have a couple of ports you would like to ignore, go to the TotalView Web Interface, **Device List** tab and select on a device and then select on the **Ignore** link towards the right-hand side of the table for each interface number you would like to ignore.

Note: The web server must unlocked in order for the Ignore column to show up in TotalView. See the section ***Error! Reference source not found.*** for how to lock and unlock the web server.

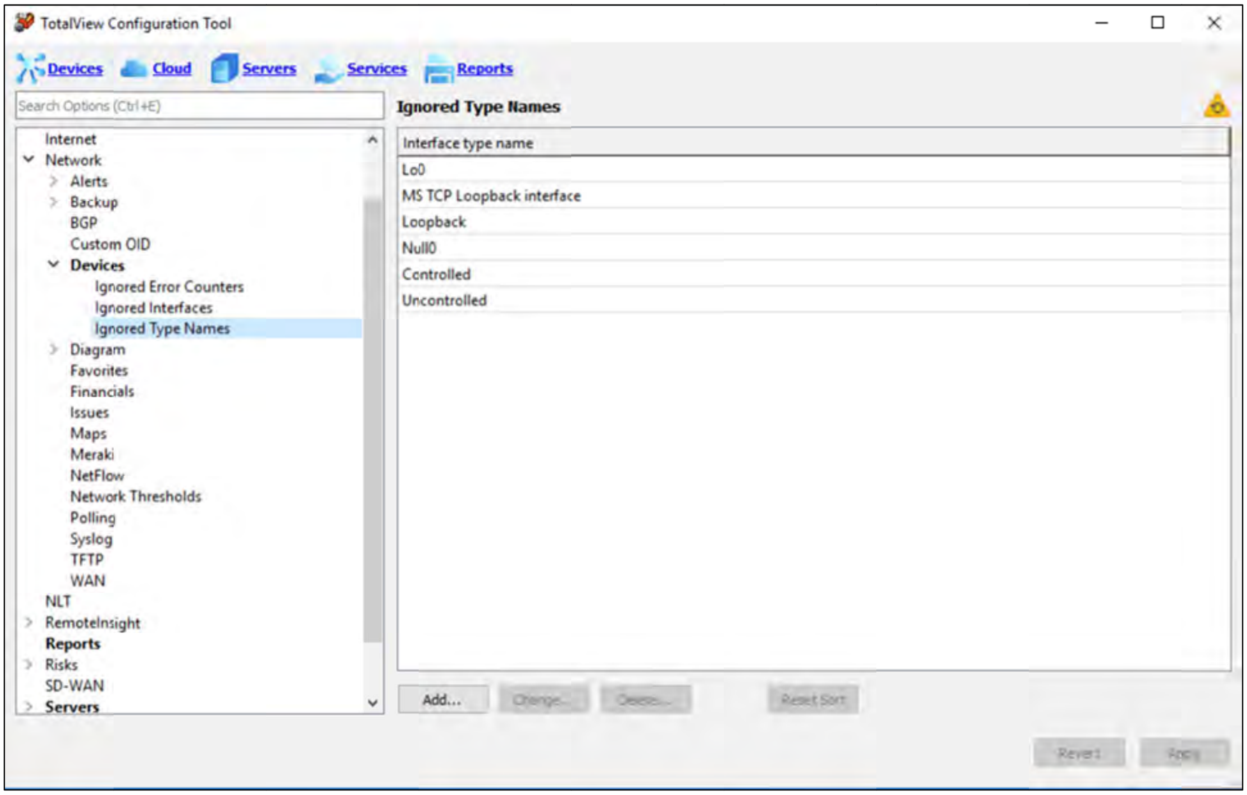


Device Name	Device IP Address	SNMP Version	Manage	CPU	Int	Oper Down	Admin Down	Location	Contact	Uptime
● Pinot	10.0.0.21	v2c	Telnet SSH Web HTTPS Syslog		26	21	0		itops@pathsolutions.com	116d 00h 06m

Interface	Favorite	WAN	IP Address	Description	Ignore Int	X	L	Queue Type	MAC Address	MTU	State	
											Type	Last Changed
● INT#1	Favorite	WAN		1: 1	Ignore	●	●		40a8f00dff3f	1526	ethernetCsmacd	116 days 00:06:09.05
INT#2	Favorite	WAN		2: 2	Ignore	●	●		40a8f00dff3e	1526	ethernetCsmacd	116 days 00:06:10.89
INT#3	Favorite	WAN		3: 3	Ignore	●	●		40a8f00dff3d	1526	ethernetCsmacd	116 days 00:06:10.89
INT#4	Favorite	WAN		4: 4	Ignore	●	●		40a8f00dff3c	1526	ethernetCsmacd	116 days 00:06:10.89
INT#5	Favorite	WAN		5: 5	Ignore	●	●		40a8f00dff3b	1526	ethernetCsmacd	116 days 00:06:10.89
INT#6	Favorite	WAN		6: 6	Ignore	●	●		40a8f00dff3a	1526	ethernetCsmacd	116 days 00:06:10.89
INT#7	Favorite	WAN		7: 7	Ignore	●	●		40a8f00dff39	1526	ethernetCsmacd	114 days 03:03:31.59
INT#8	Favorite	WAN		8: 8	Ignore	●	●		40a8f00dff38	1526	ethernetCsmacd	116 days 00:06:10.89
INT#9	Favorite	WAN		9: 9	Ignore	●	●		40a8f00dff37	1526	ethernetCsmacd	116 days 00:06:10.89
INT#10	Favorite	WAN		10: 10	Ignore	●	●		40a8f00dff36	1526	ethernetCsmacd	116 days 00:06:10.89
● INT#11	Favorite	WAN		11: 11	Ignore	●	●		40a8f00dff35	1526	ethernetCsmacd	116 days 00:06:06.81
INT#12	Favorite	WAN		12: 12	Ignore	●	●		40a8f00dff34	1526	ethernetCsmacd	116 days 00:06:10.89
● INT#13	Favorite	WAN		13: 13	Ignore	●	●		40a8f00dff33	1526	ethernetCsmacd	17 days 18:44:06.82
INT#14	Favorite	WAN		14: 14	Ignore	●	●		40a8f00dff32	1526	ethernetCsmacd	116 days 00:06:10.89
● INT#15	Favorite	WAN		15: 15	Ignore	●	●		40a8f00dff31	1526	ethernetCsmacd	103 days 14:10:53.99
INT#16	Favorite	WAN		16: 16	Ignore	●	●		40a8f00dff30	1526	ethernetCsmacd	116 days 00:06:10.89
INT#17	Favorite	WAN		17: 17	Ignore	●	●		40a8f00dff2f	1526	ethernetCsmacd	116 days 00:06:10.89

Ignored Type Names

Select **Network > Devices > Ignored Type Names** then add, change or delete the interface types you want to ignore.



Interface type name
Lo0
MS TCP Loopback interface
Loopback
Null0
Controlled
Uncontrolled

Select **Add** or **Change** buttons to modify the types on the ignored list.

Alternate Method to Ignore Types

The **IgnoreType.cfg** allows you to ignore types via descriptions system-wide – like if you wanted to always ignore any interface with the description of **Loopback**.

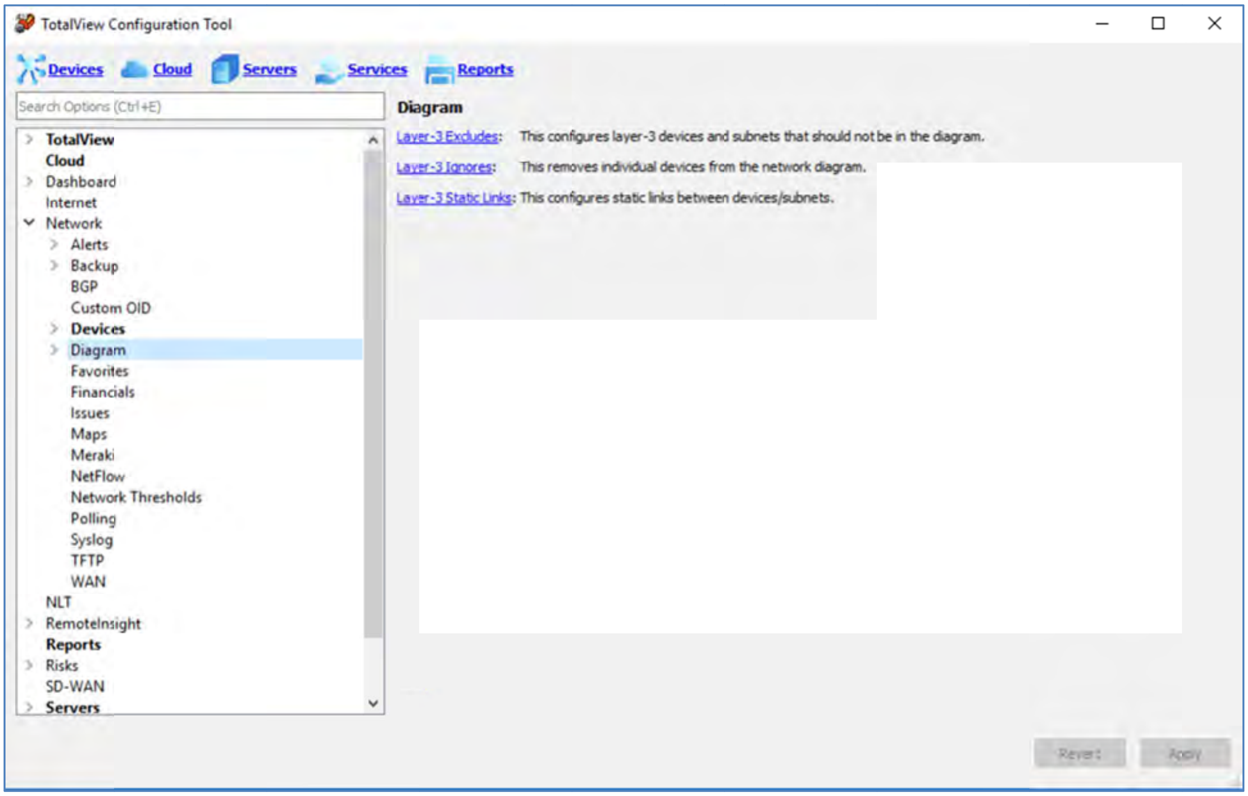
The above file should be opened in Notepad for editing. After you save the file, stop and restart the service to have this change take effect.

This file is located in one of the following directories:

C:/Program Files (x86)/PathSolutions/TotalView/IgnoreType.cfg
C:/Program Files/PathSolutions/TotalView/IgnoreType.cfg

Diagram (Interactive Diagrams)

To configure how to display the interfaces and devices on the Automatic Interactive Network Diagram, go to the **Network > Diagram** section from the left-hand menu. There are three sub-sections: Layer-3 Excludes, Layer-3 Ignores and Layer-3 Static Links.



Diagram

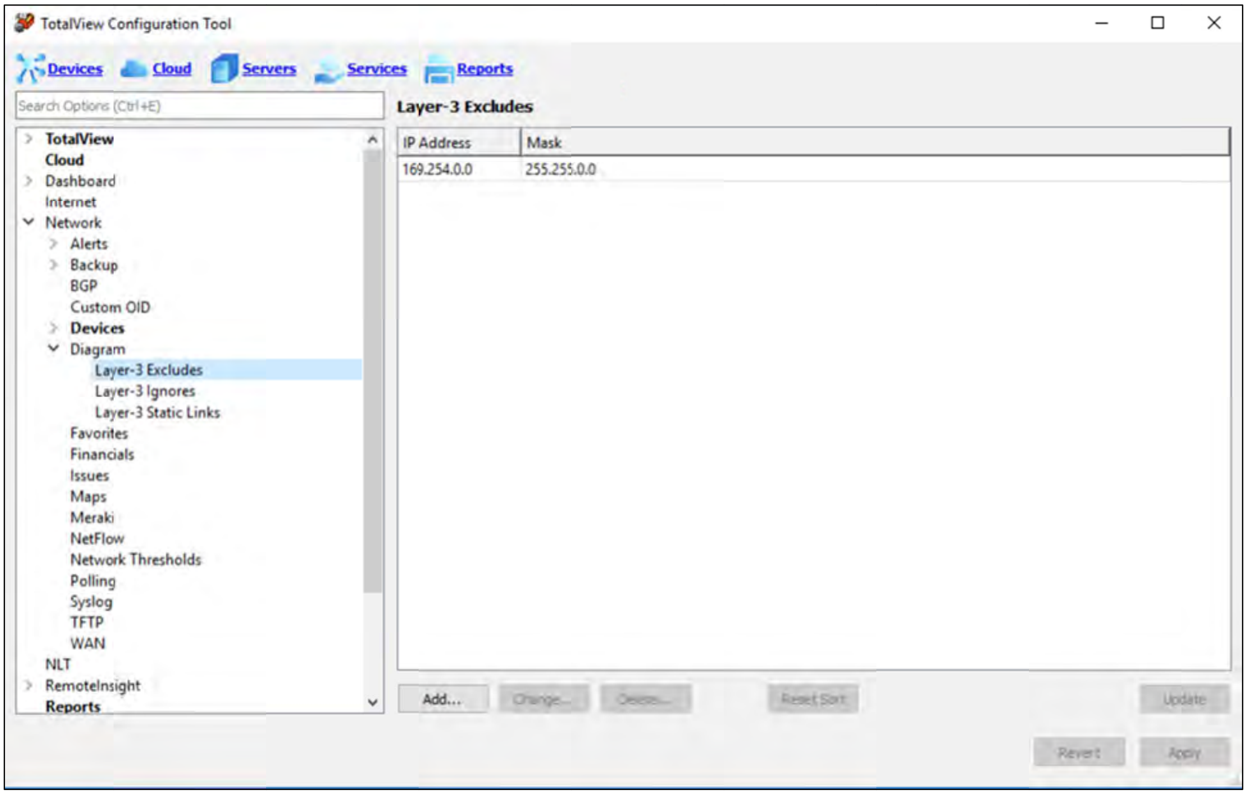
Layer-3 Excludes: This configures layer-3 devices and subnets that should not be in the diagram.

Layer-3 Ignores: This removes individual devices from the network diagram.

Layer-3 Static Links: This configures static links between devices/subnets.

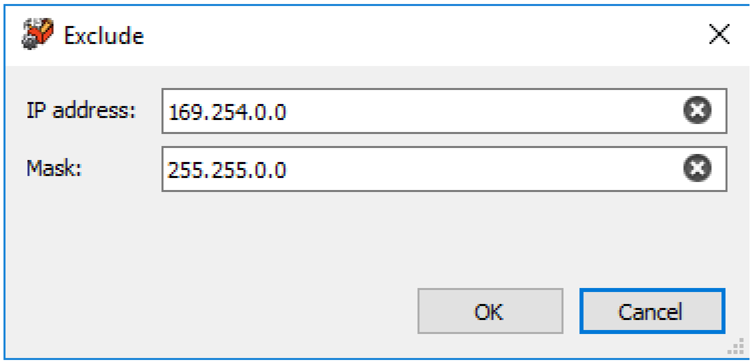
Layer-3 Excludes

The **Layer-3 Excludes** section allows you to exclude large sections of your network from the diagram (devices and subnets). This is useful if you have a lab network that you do not want to be part of the diagram, but still want to be monitored.



IP Address	Mask
169.254.0.0	255.255.0.0

Use the **Add** and **Change** buttons to specify an IP address and subnet mask of a device/subnet that you wanted to exclude from display on the diagram. Then select **OK** to close this dialog and the subnets and devices will be removed from the diagram.



IP address: 169.254.0.0

Mask: 255.255.0.0

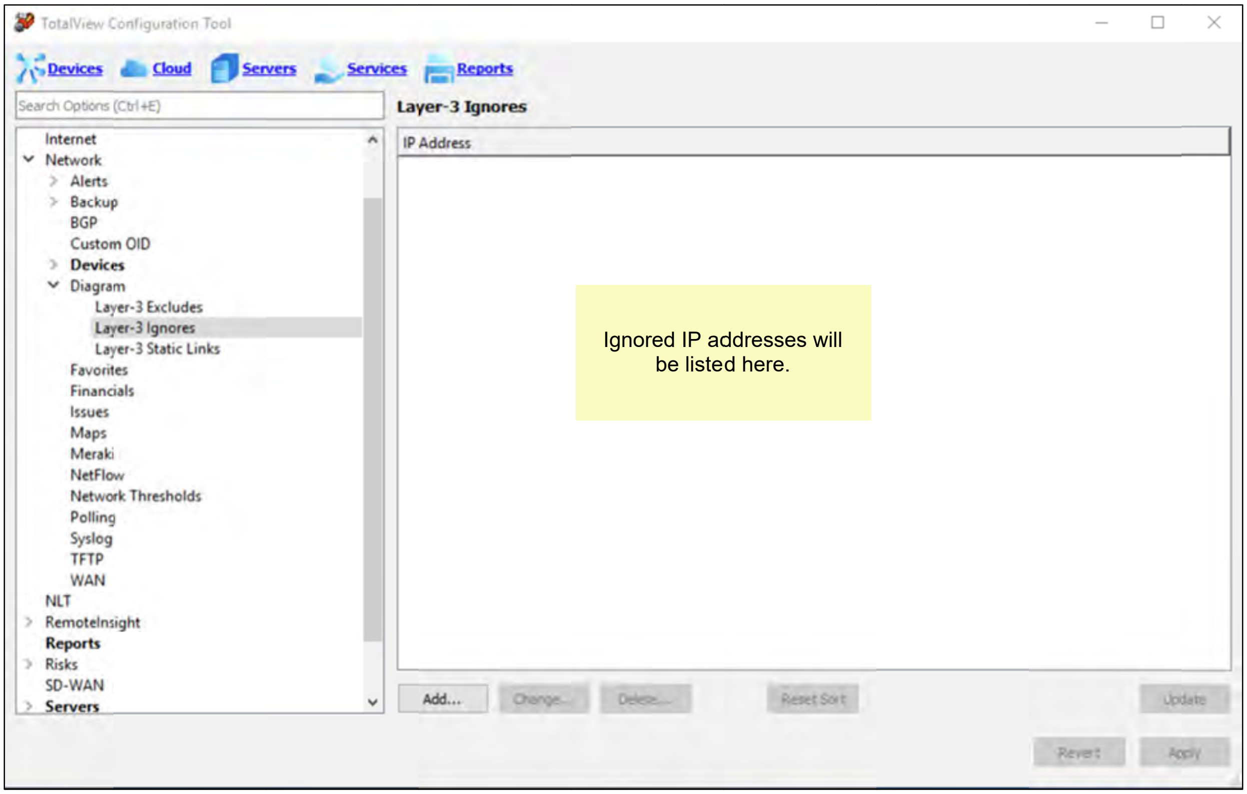
After finishing a batch of additions and changes, to preview the changes to the diagram, select **Update** and then refresh your browser window.

Note: The **Update** button will do an instant update (approximately 2 seconds) of any diagram changes that you have made.
It is good practice to use the **Update** button rather than the **Apply** button for checking the

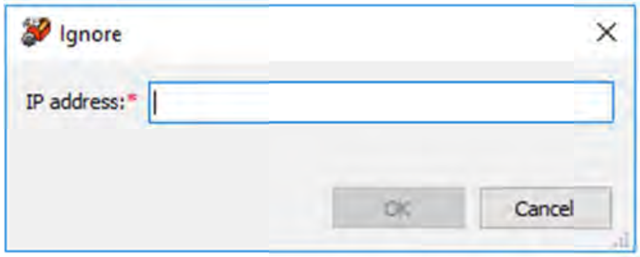
diagrams. The **Apply** button would stop and start TotalView with the latest configured settings, which may take a lot longer.

Layer-3 Ignores

This configures layer-3 devices and subnets that should not be in the diagram. If you want to remove a specific link from the diagram, enter it on this section.



Use the **Add** and **Change** buttons to specify an IP address that should be ignored and not displayed on the diagram. Then select **OK** to close this dialog.



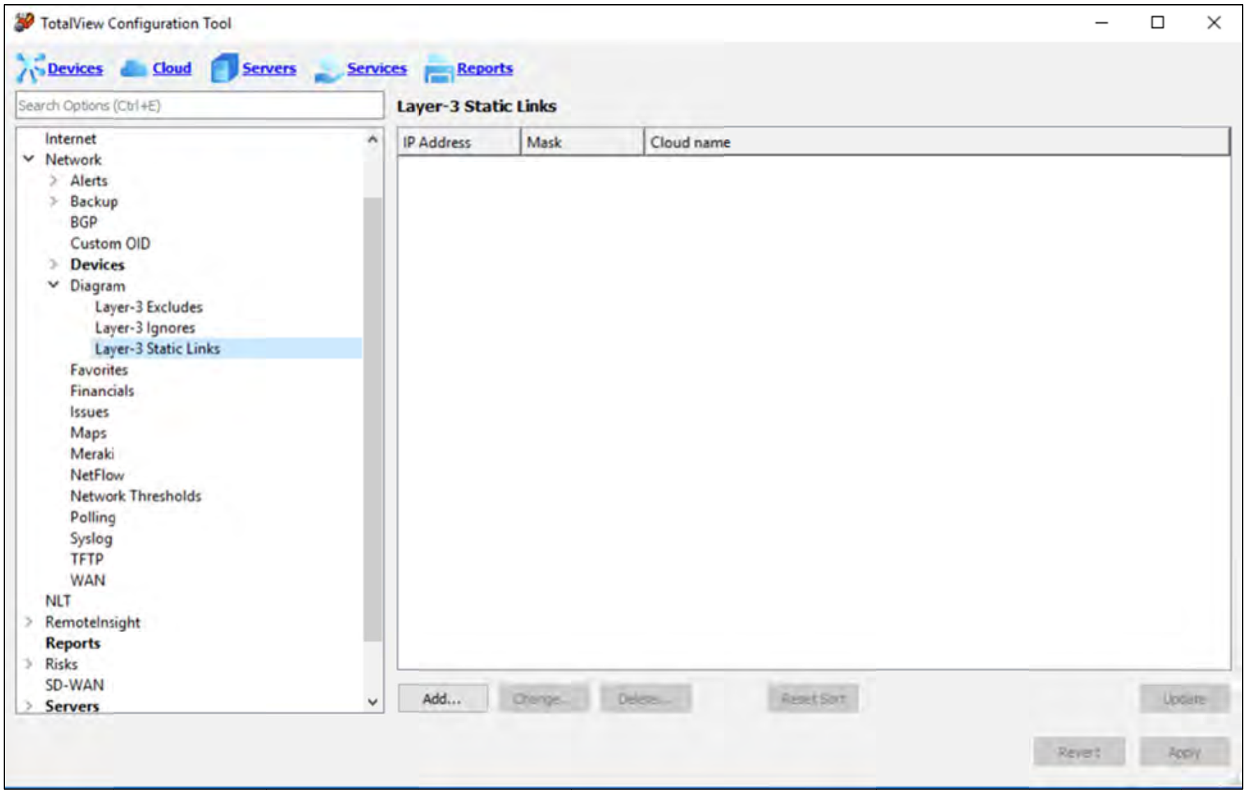
To review your work on the diagram, select **Update** and then refresh your browser window to verify that item was removed.

Note: The **Update** button will do an instant update (approximately 2 seconds) of any diagram changes that you have made. It is good practice to use the **Update** button rather than the **Apply** button for checking the diagram.

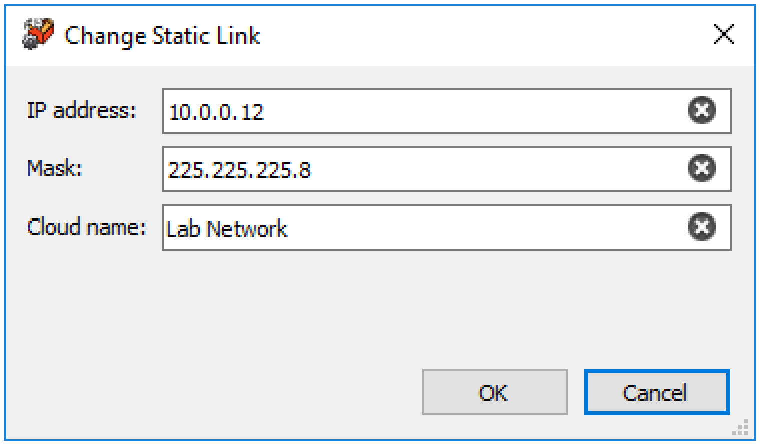
Layer-3 Static Links

This configures static links between devices/subnets.

The Layer-3 Static Links section is used to tie separate networks together when they have no direct connection like when an MPLS or VPN cloud is between subnets.



Enter the **IP address**, **Mask** of an existing subnet and the **Cloud name** that you want to connect.



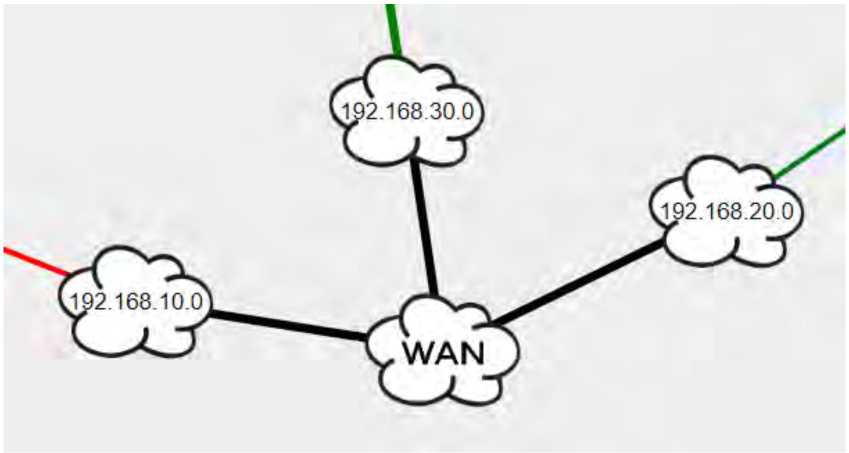
IP address: 10.0.0.12

Mask: 225.225.225.8

Cloud name: Lab Network

In general, you will want multiple subnets to connect to the same Cloud Name. The **Cloud name** field must be identical to have them connect to each other.

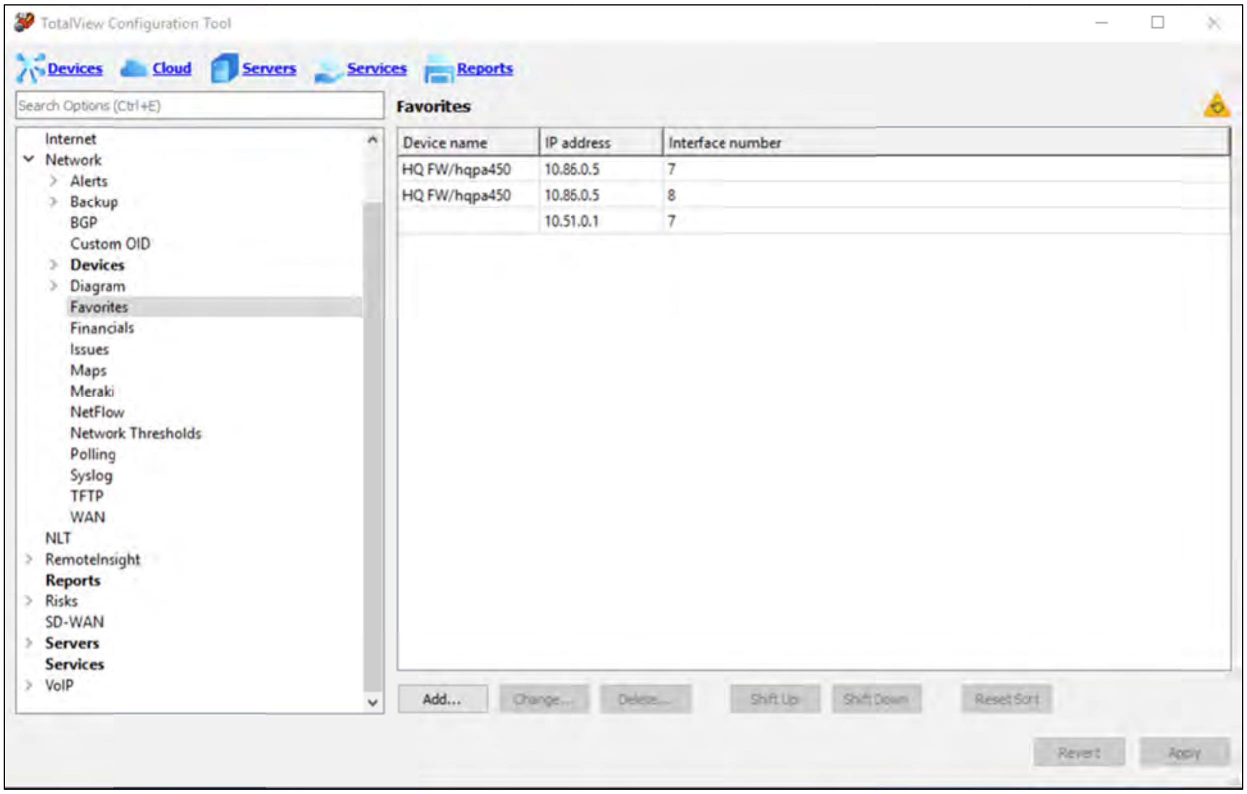
The screenshot below is an example of a WAN cloud that connects three subnets together.



When you are finished adding your links, select **Update** and then refresh the web page to see how it takes effect. This allows you to quickly make changes and see the results.

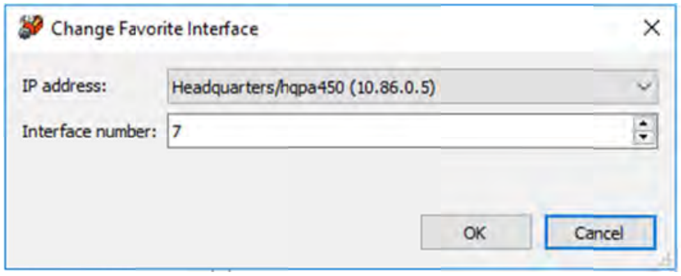
Favorites

Specific interfaces can be selected to appear on the **Favorites** tab in TotalView.



Device name	IP address	Interface number
HQ FW/hqpa450	10.86.0.5	7
HQ FW/hqpa450	10.86.0.5	8
	10.51.0.1	7

Select the **Add** and **Change** buttons to add or change the items on the list of Favorites.



IP address: Headquarters/hqpa450 (10.86.0.5)

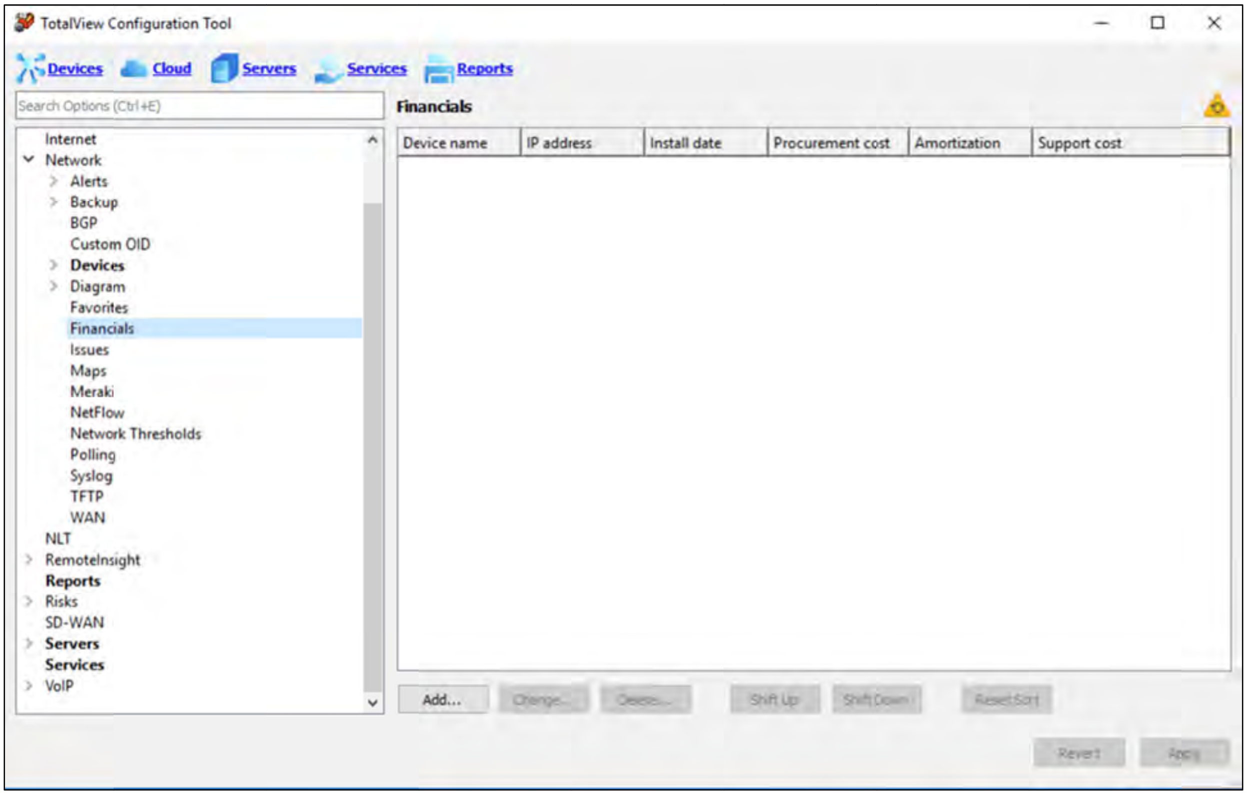
Interface number: 7

Configure it so that users can chose Favorites while in the TotalView web interface.

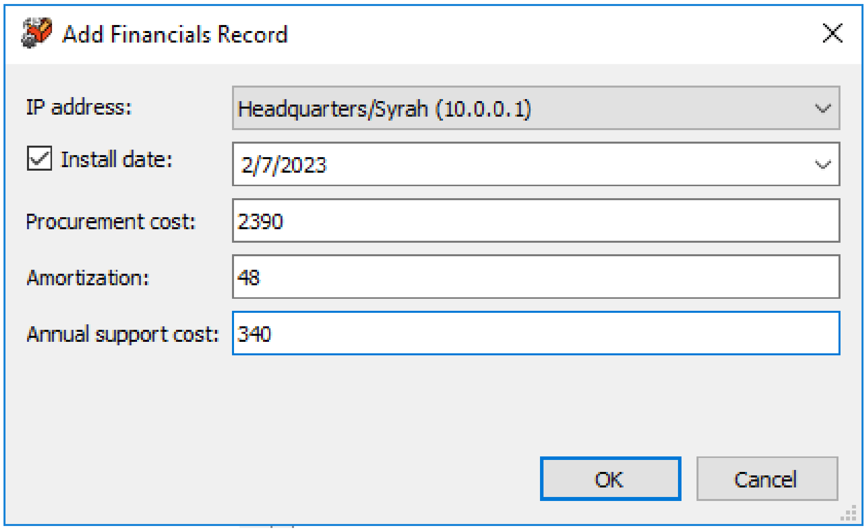
Note: The web server must be unlocked for the **Favorites** column to show up in TotalView.

Financials

You may add your procurement cost and other financial information if you would like TotalView to track it for you. Select **Network > Financials** from the left-hand menu to get this section.



Add and change financial records, by selecting the **Add** and **Change** buttons and entering new information.


Add Financials Record

IP address: Headquarters/Syrah (10.0.0.1)

☑ Install date: 2/7/2023

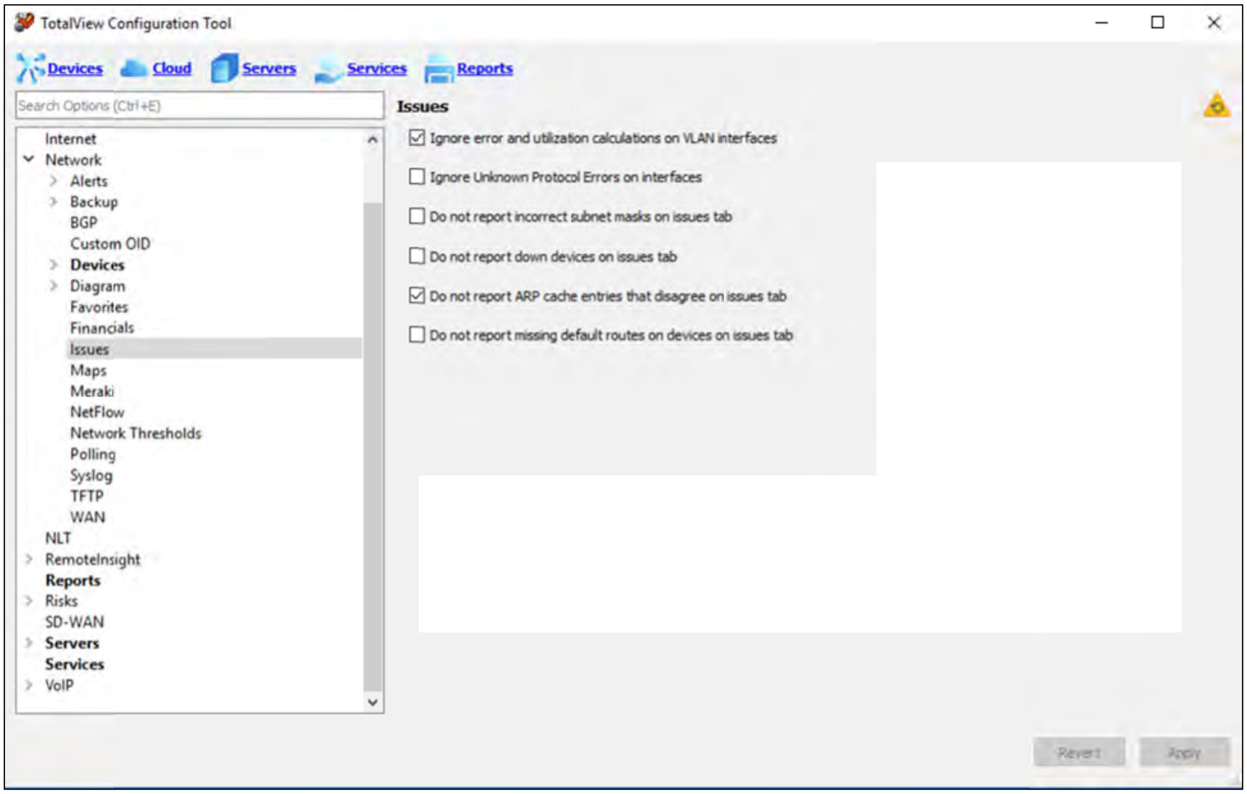
Procurement cost: 2390

Amortization: 48

Annual support cost: 340

Issues

Specify what issues you want to view or ignore on the **Issues** list.



Issues

☑ Ignore error and utilization calculations on VLAN interfaces

□ Ignore Unknown Protocol Errors on interfaces

□ Do not report incorrect subnet masks on issues tab

□ Do not report down devices on issues tab

☑ Do not report ARP cache entries that disagree on issues tab

□ Do not report missing default routes on devices on issues tab

How to Ignore Unknown Protocol Errors

Select the **Ignore Unknown Protocol Errors** checkbox, if you do not want to regard Inbound Unknown Protocols as errors.

By default, devices will increment the Inbound Unknown Protocols error counters on interfaces if strange protocols are received. This is typically when network adapters receive IPX, AppleTalk, or Cisco Discovery Protocol (CDP) broadcasts from devices. These packets can be perceived as errors since they may be unwanted protocols on the network, or the network administrator may view these as valid packets that were successfully delivered although are of no use to the recipient device.

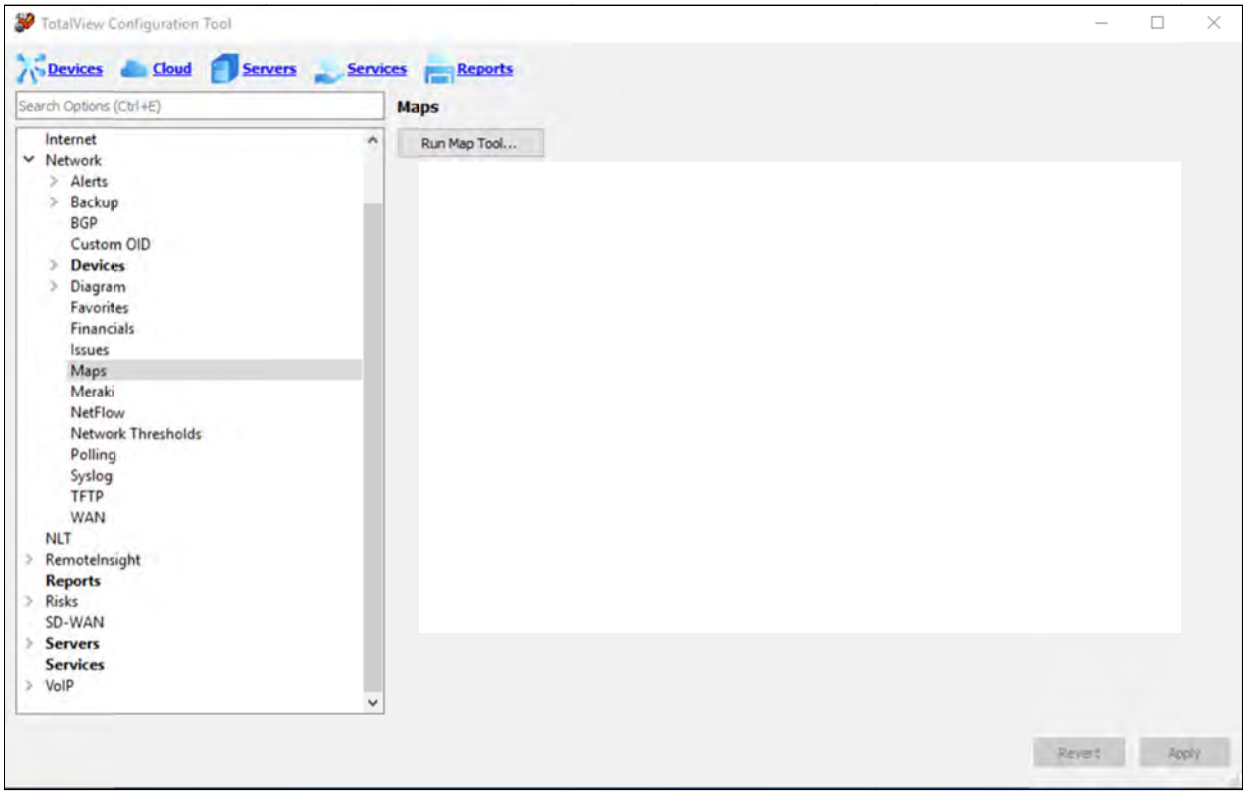
How to Ignore VLAN Interface Errors

Select the **Ignore errors and utilization calculations on VLAN** interfaces checkbox in the **Network > Issues** section.

For some switch manufacturers, VLAN interfaces report anomalous errors. If you do not want the error rate of VLAN interfaces calculated, select the **Ignore error calculations on VLAN interfaces** checkbox. The VLAN interface will still be listed, but it will not be listed on the TotalView **Issues** tab.

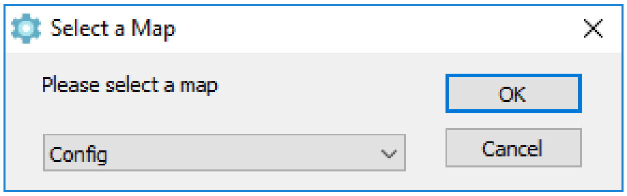
Maps

Select **Network > Maps** from the left-hand side. It will bring you to this screen to open the Map Config Tool.



Note: Ignore select the **Apply** and **Revert** buttons on screen in this section. They do not save the map or revert the map.

Select **Run Map Tool**. The Map Config Tool will open in a new window and will ask you to select a map. Select a map from the drop-down menu.



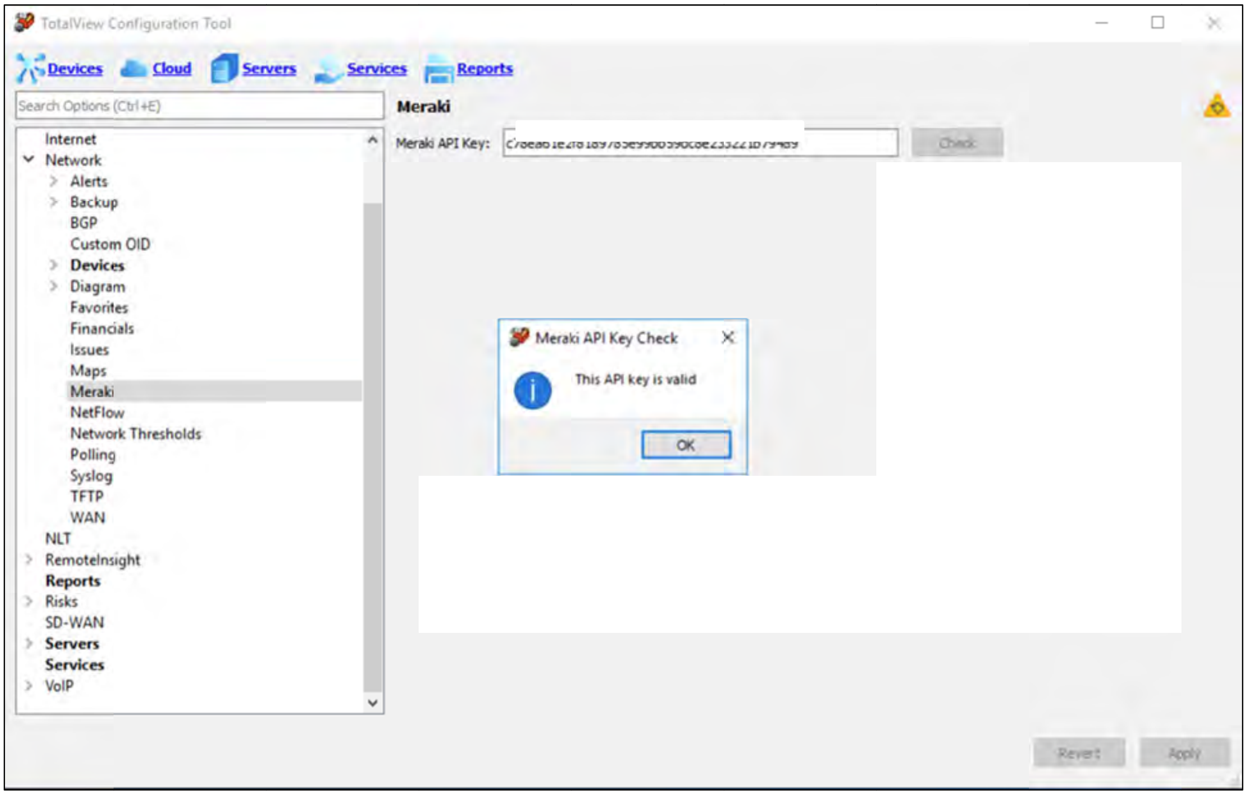
Please select a map

Config

See the section on the *Map Config Tool* for instructions how to use this tool.

Meraki

Select **Network > Meraki** from the left-hand list. Enter the Meraki API key. Select **Check** to check the key is valid. A notice will verify if the API key is valid.



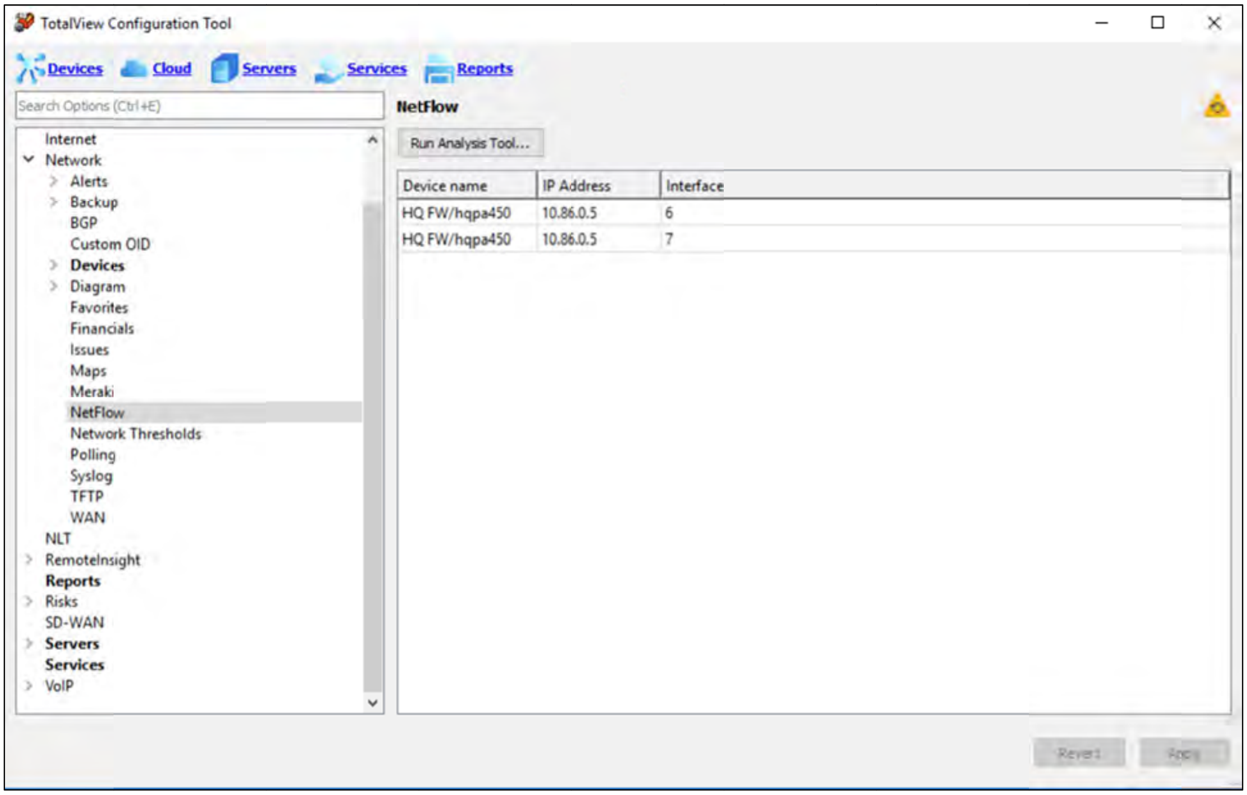
Meraki API Key:

Meraki API Key Check

This API key is valid

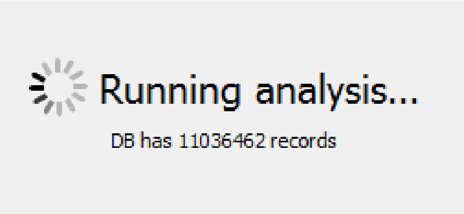
NetFlow

To configure NetFlow, select **Network > NetFlow** from the left-hand menu. Select **Run Analysis Tool** at the top to run a NetFlow Analysis and adjust the interfaces displayed on the **NetFlow** section.



Device name	IP Address	Interface
HQ FW/hqpa450	10.86.0.5	6
HQ FW/hqpa450	10.86.0.5	7

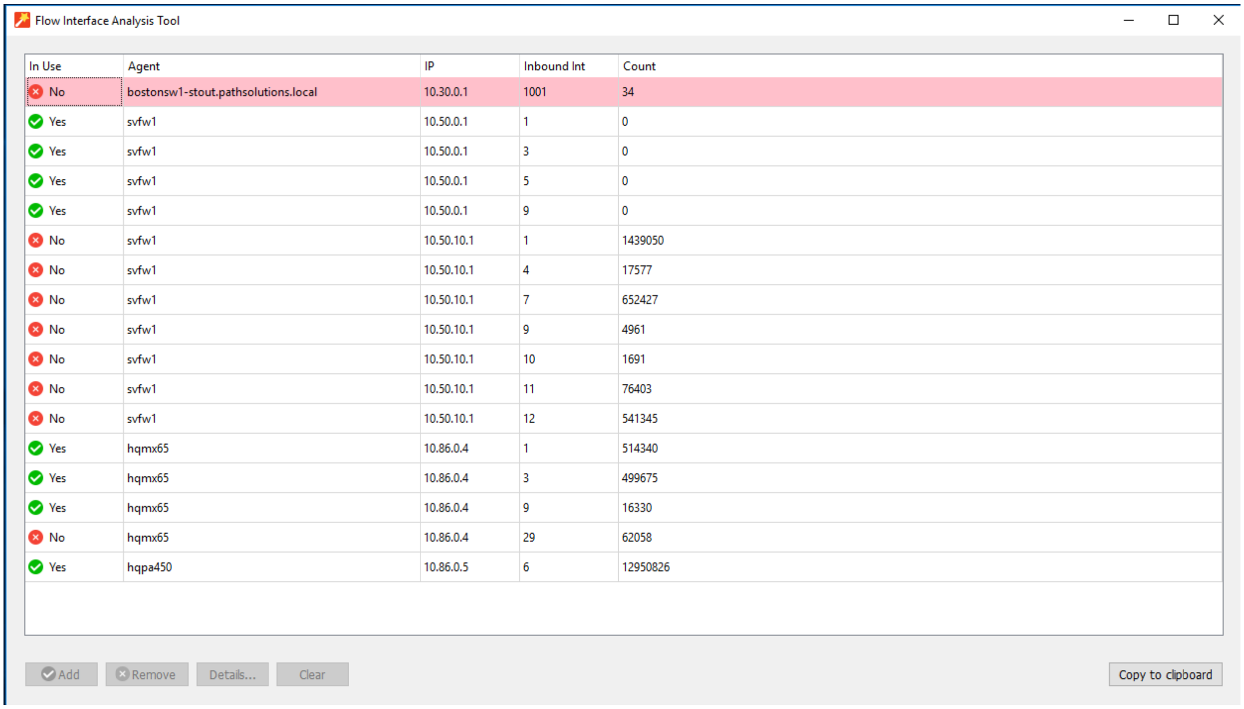
The **Run Analysis Tool** button performs a NetFlow analysis **(**this may take up to 30 minutes depending on the size of your NetFlow database).



Running analysis...

DB has 11036462 records

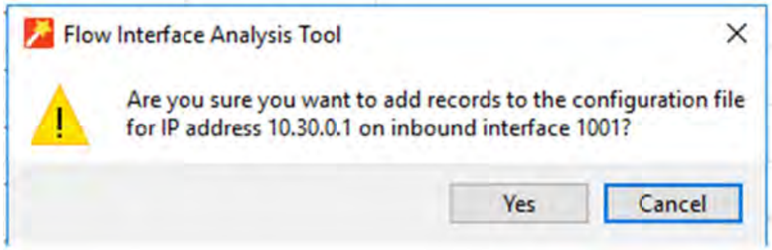
The NetFlow analysis report then gets called up in a new window and displays similar to the screenshot below.



In Use	Agent	IP	Inbound Int	Count
✗ No	bostonsw1-stout.pathsolutions.local	10.30.0.1	1001	34
✓ Yes	svfw1	10.50.0.1	1	0
✓ Yes	svfw1	10.50.0.1	3	0
✓ Yes	svfw1	10.50.0.1	5	0
✓ Yes	svfw1	10.50.0.1	9	0
✗ No	svfw1	10.50.10.1	1	1439050
✗ No	svfw1	10.50.10.1	4	17577
✗ No	svfw1	10.50.10.1	7	652427
✗ No	svfw1	10.50.10.1	9	4961
✗ No	svfw1	10.50.10.1	10	1691
✗ No	svfw1	10.50.10.1	11	76403
✗ No	svfw1	10.50.10.1	12	541345
✓ Yes	hqmx65	10.86.0.4	1	514340
✓ Yes	hqmx65	10.86.0.4	3	499675
✓ Yes	hqmx65	10.86.0.4	9	16330
✗ No	hqmx65	10.86.0.4	29	62058
✓ Yes	hqpa450	10.86.0.5	6	12950826

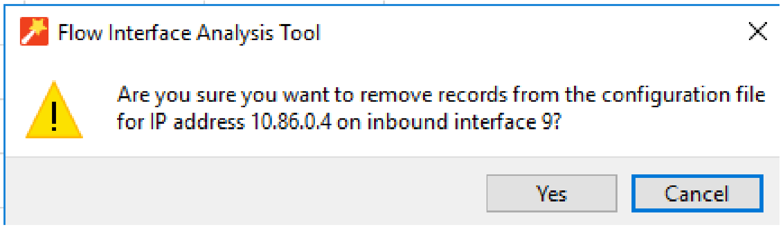
Change the sort order, by selecting items on the list, selecting the **Shift Up** or **Shift Down** buttons. You can also assign the sort order by entering an Interface number.

To add an interface, select something marked **No** from the list. Then select the **Add** button at the bottom. It will ask if you are sure you want to add records to the configuration file? Select **Yes** or **Cancel**.



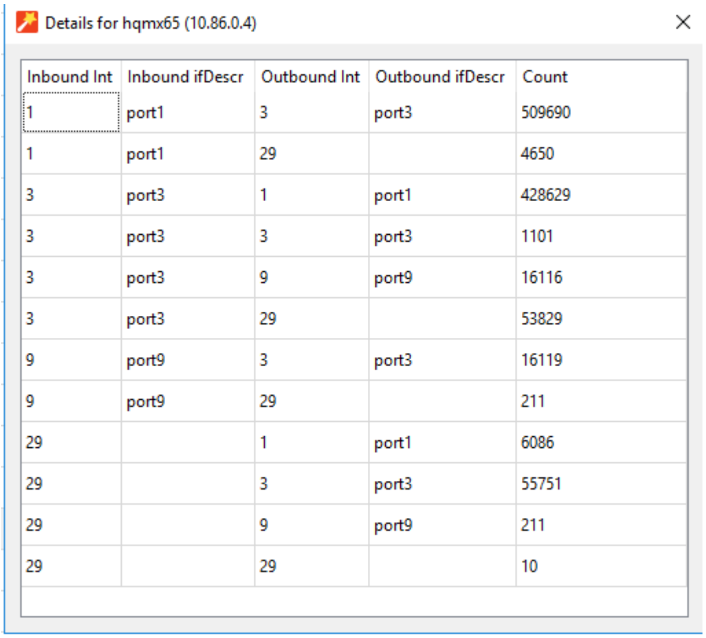
Are you sure you want to add records to the configuration file for IP address 10.30.0.1 on inbound interface 1001?

To remove an interface, select something from the list marked **Yes**. Then select **Remove** at the bottom. A dialog box will ask if you are sure you want to remove records from the configuration file? Select **Yes** or **Cancel**.



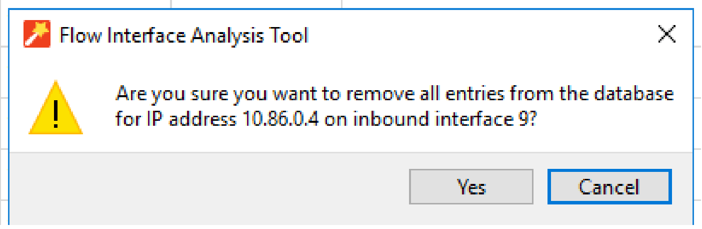
Are you sure you want to remove records from the configuration file for IP address 10.86.0.4 on inbound interface 9?

To view the NetFlow details of any agent, select something from the list, then select the **Details** button.



Inbound Int	Inbound ifDescr	Outbound Int	Outbound ifDescr	Count
1	port1	3	port3	509690
1	port1	29		4650
3	port3	1	port1	428629
3	port3	3	port3	1101
3	port3	9	port9	16116
3	port3	29		53829
9	port9	3	port3	16119
9	port9	29		211
29		1	port1	6086
29		3	port3	55751
29		9	port9	211
29		29		10

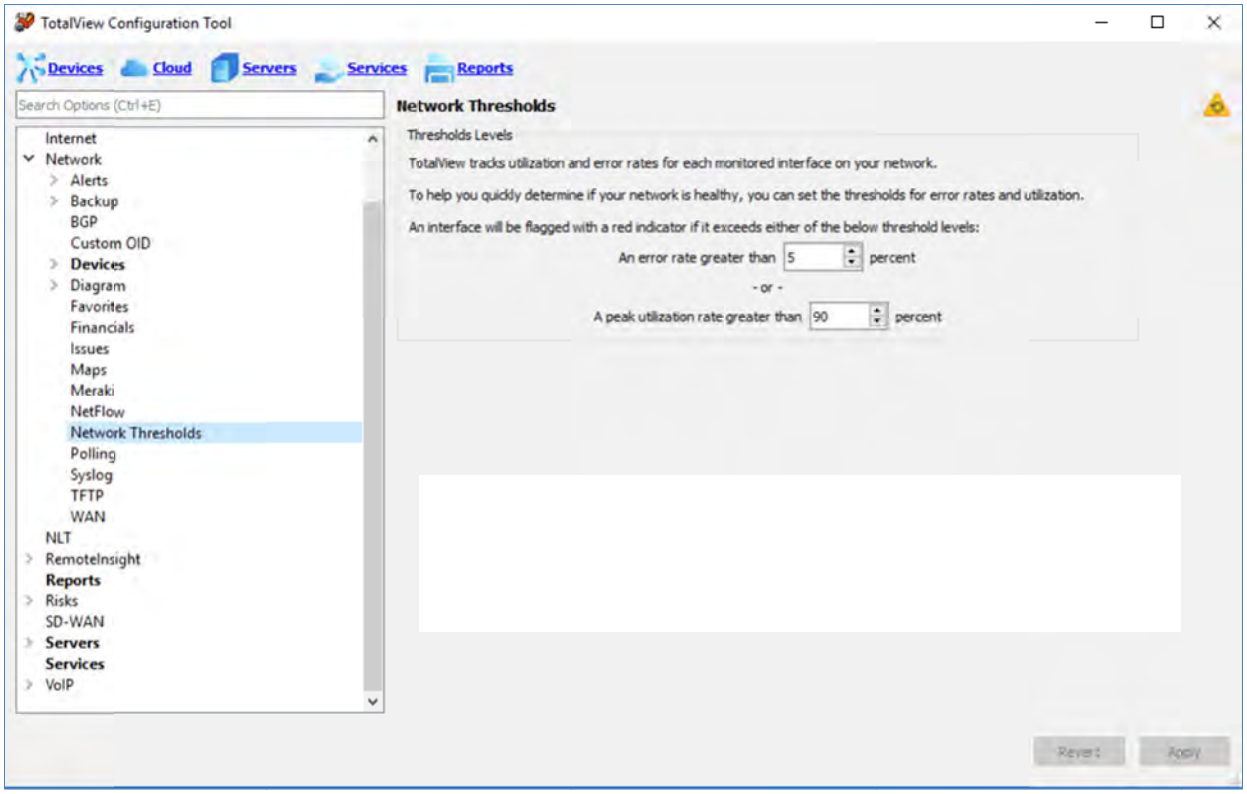
The **Clear** button asks if you want to remove all entries from the database for an address at the IP address selected? Select **Yes** or **Cancel**.



Are you sure you want to remove all entries from the database for IP address 10.86.0.4 on inbound interface 9?

Network Thresholds

To edit thresholds for on-screen alerts in the Web Interface, select **Network > Thresholds** from the left-hand menu. Set what percentages of errors will be flagged with a red indicator on the TotalView Interface or a peak utilization rate is greater than a specified percent.



Network Thresholds

Thresholds Levels

TotalView tracks utilization and error rates for each monitored interface on your network.

To help you quickly determine if your network is healthy, you can set the thresholds for error rates and utilization.

An interface will be flagged with a red indicator if it exceeds either of the below threshold levels:

An error rate greater than 5 percent

- or -

A peak utilization rate greater than 90 percent

For example, if an interface has an error rate higher than 5%, the network status will be changed to 'Degraded'.

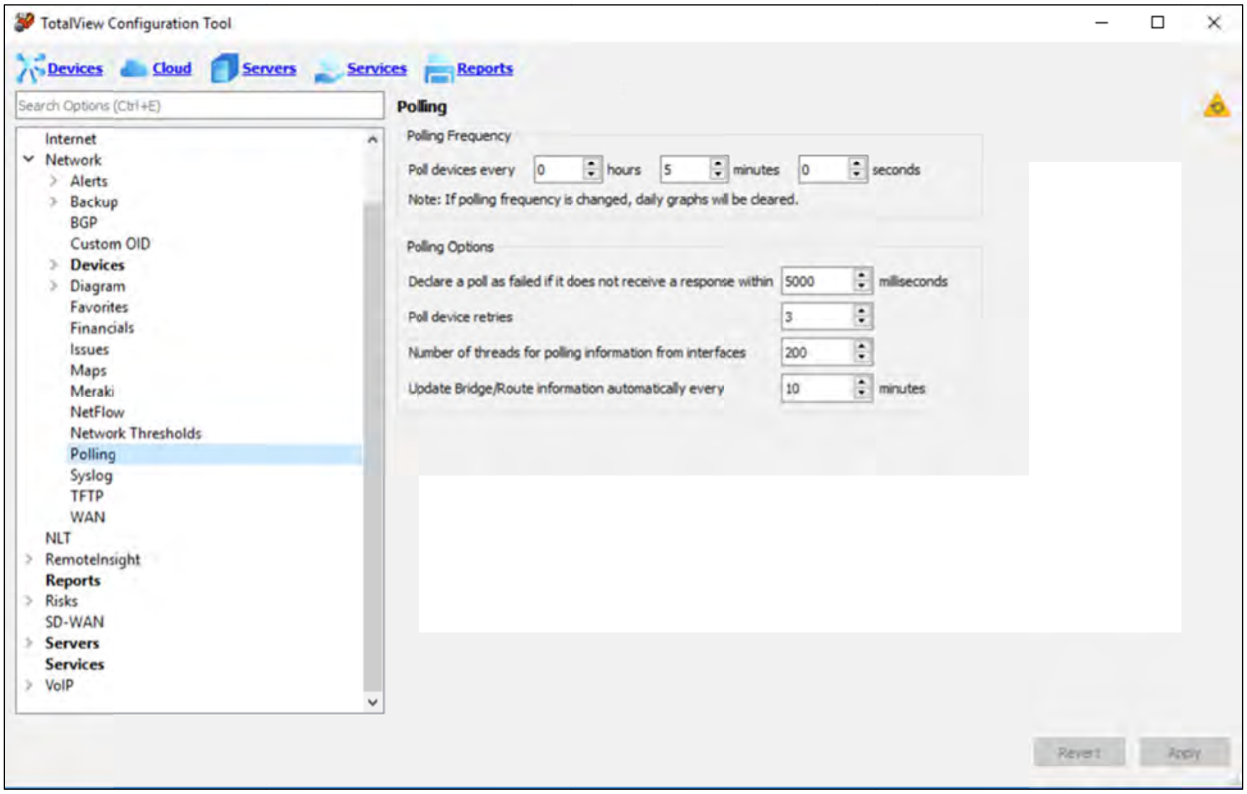
If an interface has a peak utilization rate (transmitted or received) over 90%, the network status will be changed to **Degraded**.

These numbers can be adjusted to suit your specific network environment, and your tolerance for errors.

When you are finished making changes, select **Apply** to commit the changes to memory.

Polling Behavior

Go to the **Network > Polling** section to configure polling behaviors: frequency and options.



Polling

Polling Frequency

Poll devices every 0 hours 5 minutes 0 seconds

Note: If polling frequency is changed, daily graphs will be cleared.

Polling Options

Declare a poll as failed if it does not receive a response within 5000 milliseconds

Poll device retries 3

Number of threads for polling information from interfaces 200

Update Bridge/Route information automatically every 10 minutes

TotalView is network friendly and makes every attempt to prevent the network from flooding with requests. One minimum sized SNMP packet is sent per interface.

Polling Options

TotalView will need to know how long to wait for a response before declaring an individual poll as failed. The default is 3000ms (3 seconds). If you have a network that has extremely high latencies, you may choose to increase this number. If you want the PathSolutions TotalView to declare a device as failed if it does not respond within a smaller response window, adjust this number down.

Polling Threads

PathSolutions' TotalView uses 20 threads for polling devices for SNMP information. If you have a faster computer, you may choose to increase this number. If you have a slower computer and PathSolutions TotalView is utilizing 100% of the system's CPU during a polling cycle, you may get better performance by reducing the CPU. This will cause less thread overhead in the system.

Configuring the Polling Frequency

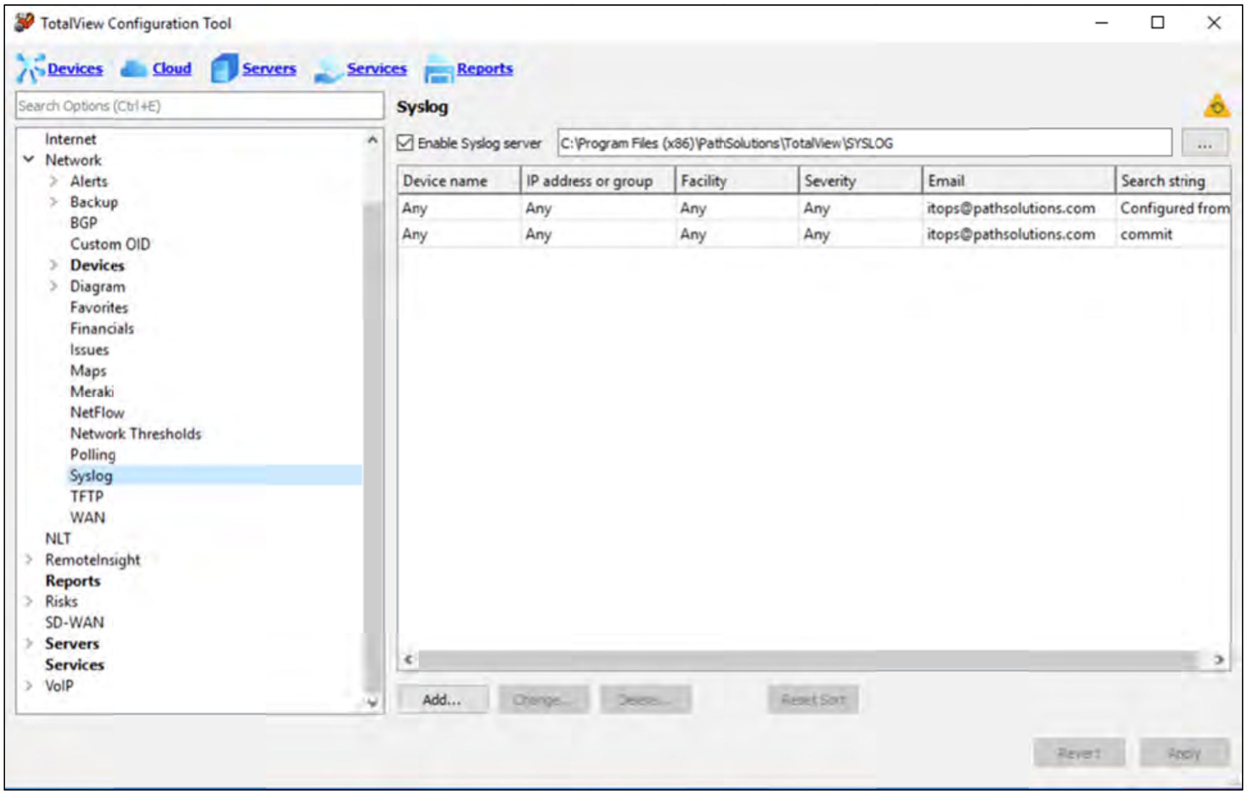
You will want to select how often the program should poll each interface. The default is 5 minutes. Less frequent polls will decrease the traffic on your network. However, it will not provide you with as granular information on utilization and error rates.

Note: If you change the polling frequency, all historical utilization information (daily, weekly, monthly, and yearly graphs) will be erased when you select **OK** or **Apply**.

Note: It is important not to poll your devices too often, as this can add to network overhead. In general, you should poll your interfaces every 5 minutes.

Syslog

The system has a built-in syslog server to receive and organize syslog messages received from network devices.



☑ Enable Syslog server C:\Program Files (x86)\PathSolutions\TotalView\SYSLOG

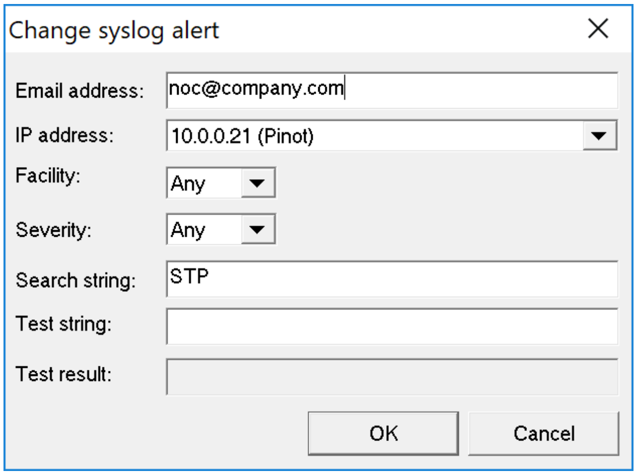
Device name	IP address or group	Facility	Severity	Email	Search string
Any	Any	Any	Any	itops@pathsolutions.com	Configured from
Any	Any	Any	Any	itops@pathsolutions.com	commit

To enable the syslog server, select the **Enable Syslog Server** checkbox.

Syslog messages will be captured and be visible from the web pages. Select the **Syslog** link to the right of **Telnet** and **Web** to view the received syslog messages from each device.

Note: You will have to configure each of your network devices to send their syslog messages to the PathSolutions TotalView server.

Add or change alerting for syslog messages by selecting the **Add** and **Change** buttons. The dialog shown below will display.



Change syslog alert

Email address: noc@company.com

IP address: 10.0.0.21 (Pinot)

Facility: Any

Severity: Any

Search string: STP

Test string:

Test result:

Enter the search string with a regular expression to enter a test string and see if it matches.

Enter the email address that should receive the alert, the IP address where the syslog message should come from, the facility number (or **Any** if it could be any facility number) the Severity number (or **Any**), The Search String, The Test String, to view the Test Result.

The Syslog matching capability is ECMAScript compatible.

Facility Levels

A facility level is used to specify what type of program is logging the message. This lets the configuration file specify that messages from different facilities will be handled accordingly .[4] The list of facilities available are defined by RFC 3164.

Facility Number	Keyword	Facility Description
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslog
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)
20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

The mapping between Facility Number and Keyword is not uniform over different operating systems and different syslog implementations. For cron either 9,15, or both may be used. The confusion is even greater regarding auth/authpriv. 4 and 10 are most common, but 13 and 14 can be used.

Severity Levels

RFC 5424 defines eight severity levels.

Code	Severity	Keyword	Description	General Description
0	Emergency	emerg (panic)	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	Alert	alert	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	Critical	crit	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	Error	err (error)	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	Warning	warning (warn)	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	Notice	notice	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	Informational	info	Informational messages.	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	Debug	debug	Debug-level messages.	Information useful to developers for debugging the application, not useful during operations.

ECMAScript Regular Expressions Pattern Syntax (regex)

The following syntax is used to construct regex objects (or assign) that have selected ECMAScript as its grammar.

A regular expression pattern is formed by a sequence of characters. Regular expression operations look sequentially for matches between the characters of the pattern and the characters in the target sequence. In principle, each character in the pattern is matched against the corresponding character in the target sequence, one by one. The regex syntax allows special characters and expressions in the pattern.

Special Pattern Characters

Special pattern characters or sequences of characters have a special meaning when they appear in a regular expression pattern, either to represent a character that is difficult to express in a string, or to represent a category of characters. Each of these special pattern characters is matched in the target sequence against a single character (unless a quantifier specifies otherwise).

characters	description	matches
`.`	not newline	any character except *line terminators* (LF, CR, LS, PS).
`\t`	tab (HT)	a horizontal tab character (same as **`\u0009`**).
`\n`	newline (LF)	a newline (line feed) character (same as **`\u000A`**).
`\v`	vertical tab (VT)	a vertical tab character (same as **`\u000B`**).
`\f`	form feed (FF)	a form feed character (same as **`\u000C`**).
`\r`	carriage return (CR)	a carriage return character (same as **`\u000D`**).
`\c`*letter*	control code	a control code character whose *code unit value* is the same as the remainder of dividing the *code unit value* of *letter* by 32. For example: `\ca` is the same as `\u0001`, `\cb` the same as `\u0002`, and so on...
`\x`*hh*	ASCII character	a character whose *code unit value* has a hex value equivalent to the two hex digits *hh*. For example: `\x4c` is the same as `L`, or `\x23` the same as `#`.
`\u`*hhhh*	Unicode character	a character whose *code unit value* has a hex value equivalent to the four hex digits *hhhh*.
`\0`	null	a null character (same as **`\u0000`**).
`\`*int*	backreference	the result of the submatch whose opening parenthesis is the *int*-th (*int* shall begin by a digit other than `0`). See groups below for more info.
`\d`	digit	a decimal digit character (same as **`[[:digit:]]`**).
`\D`	not digit	any character that is not a decimal digit character (same as **`[^[:digit:]]`**).
`\s`	whitespace	a whitespace character (same as **`[[:space:]]`**).
`\S`	not whitespace	any character that is not a whitespace character (same as **`[^[:space:]]`**).
`\w`	word	an alphanumeric or underscore character (same as **`[_[:alnum:]]`**).
`\W`	not word	any character that is not an alphanumeric or underscore character (same as **`[^_[:alnum:]]`**).

\*character*	character	the *character* as it is, without interpreting its special meaning within a regex expression. Any *character* can be escaped except those which form any of the special character sequences above. Needed for: ^ $ \ . * + ? ( ) [ ] { } |
[*class***]**	character class	the target character is part of the class (see character classes below)
[^*class***]**	negated character class	the target character is not part of the class (see character classes below)

Notice that, in C++, character and string literals also escape characters using the backslash character (\), and this affects the syntax for constructing regular expressions from such types. For example:

```
std::regex e1 ("\\d");  // regular expression: \d -> matches a digit character
std::regex e2 ("\\\\"); // regular expression: \\ -> matches a single backslash (\) character
```

Quantifiers

Quantifiers follow a character or a special pattern character. They can modify the number of times that character is repeated in the match.

characters	times	effects
*****	0 or more	The preceding atom is matched 0 or more times.
+	1 or more	The preceding atom is matched 1 or more times.
?	0 or 1	The preceding atom is optional (matched either 0 times or once).
{*int***}**	*int*	The preceding atom is matched exactly *int* times.
{*int***,}**	*int* or more	The preceding atom is matched *int* or more times.
{*min***,***max***}**	between *min* and *max*	The preceding atom is matched at least *min* times, but not more than *max*.

By default, all these quantifiers are greedy (i.e., they take as many characters that meet the condition as possible). This behavior can be overridden to ungreedy (i.e., take as few characters that meet the condition as possible) by adding a question mark (?) after the quantifier.

For example:
Matching "(a+).*" against "aardvark" succeeds and yields aa as the first sub match.
While matching "(a+?).*" against "aardvark" also succeeds, but yields a as the first sub match.

Groups

Groups allow applying quantifiers to a sequence of characters (instead of a single character). There are two kinds of groups.

characters	description	effects
(*subpattern***)**	Group	Creates a backreference.
(?:*subpattern***)**	Passive group	Does not create a backreference.

When a group creates a backreference, the characters that represent the subpattern in the target sequence are stored as a submatch. Each submatch is numbered after the order of appearance of their opening parenthesis (the first submatch is number 1; the second is number 2, and so on...).

These submatches can be used in the regular expression itself to specify that the entire subpattern should appear again somewhere else (see \int in the special characters list). They can also be used in the replacement string or retrieved in the match results object filled by some regex operations.

Assertions

Assertions are conditions that do not consume characters in the target sequence: they do not describe a character, but a condition that must be fulfilled before or after a character.

characters	description	condition for match
^	Beginning of line	Either it is the beginning of the target sequence or follows a *line terminator*.
$	End of line	Either it is the end of the target sequence or precedes a *line terminator*.
\b	Word boundary	The previous character is a *word character* and the next is a *non-word character* (or vice-versa). Note: The beginning and the end of the target sequence are considered here as *non-word characters*.
\B	Not a word boundary	The previous and next characters are both *word characters* or both are *non-word characters*. Note: The beginning and the end of the target sequence are considered here as *non-word characters*.
(?=*subpattern***)**	Positive lookahead	The characters following the assertion must match *subpattern*, but no characters are consumed.
(?!*subpattern***)**	Negative lookahead	The characters following the assertion must not match *subpattern*, but no characters are consumed.

Alternatives

A pattern can include different alternatives:

character	description	effects
|	Separator	Separates two alternative patterns or subpatterns.

A regular expression can contain multiple alternative patterns simply by separating them with the *separator operator* (|): The regular expression will match if any of the alternatives match, and as soon as one does.

Subpatterns (in groups or assertions) can also use the *separator operator* to separate different alternatives.

Character Classes

A character class defines a category of characters. It is introduced by enclosing its descriptors in square brackets ([and]).
The regex object attempts to match the entire character class against a single character in the target sequence (unless a quantifier specifies otherwise).
The character class can contain any combination of:

- **Individual characters:** Any character specified is considered part of the class (except \, [,] and -, which have a special meaning under some circumstances and may need to be escaped to be part of the class).
  For example:
  [abc] matches a, b or c.
  [^xyz] matches any character except x, y and z.
- **Ranges:** They can be specified by using the hyphen character (-) between two valid characters.
  For example:
  [a-z] matches any lowercase letter (a, b, c ... until z).
  [abc1-5] matches either a, b or c, or a digit between 1 and 5.
- **POSIX-like classes:** A whole set of predefined classes can be added to a custom character class. There are three kinds:

class	description	notes
[:*classname***:]**	character class	Uses the *regex traits*' isctype member with the appropriate type gotten from applying lookup classname member on *classname* for the match.
[.*classname***.]**	collating sequence	Uses the *regex traits*' lookup collatename to interpret *classname*.
[=*classname***=]**	character equivalents	Uses the *regex traits*' transform primary of the result of regex_traits::lookup collatename for *classname* to check for matches.

- The choice of available classes depends on the regex traits type and on its selected locale, but at least the following character classes shall be recognized by any regex traits type and locale:

class	description	equivalent (with **regex_traits**, default locale)
[:alnum:]	alpha-numerical character	isalnum
[:alpha:]	alphabetic character	isalpha
[:blank:]	blank character	isblank
[:cntrl:]	control character	iscntrl
[:digit:]	decimal digit character	isdigit
[:graph:]	character with graphical representation	isgraph
[:lower:]	lowercase letter	islower
[:print:]	printable character	isprint
[:punct:]	punctuation mark character	ispunct
[:space:]	whitespace character	isspace
[:upper:]	uppercase letter	isupper
[:xdigit:]	hexadecimal digit character	isxdigit

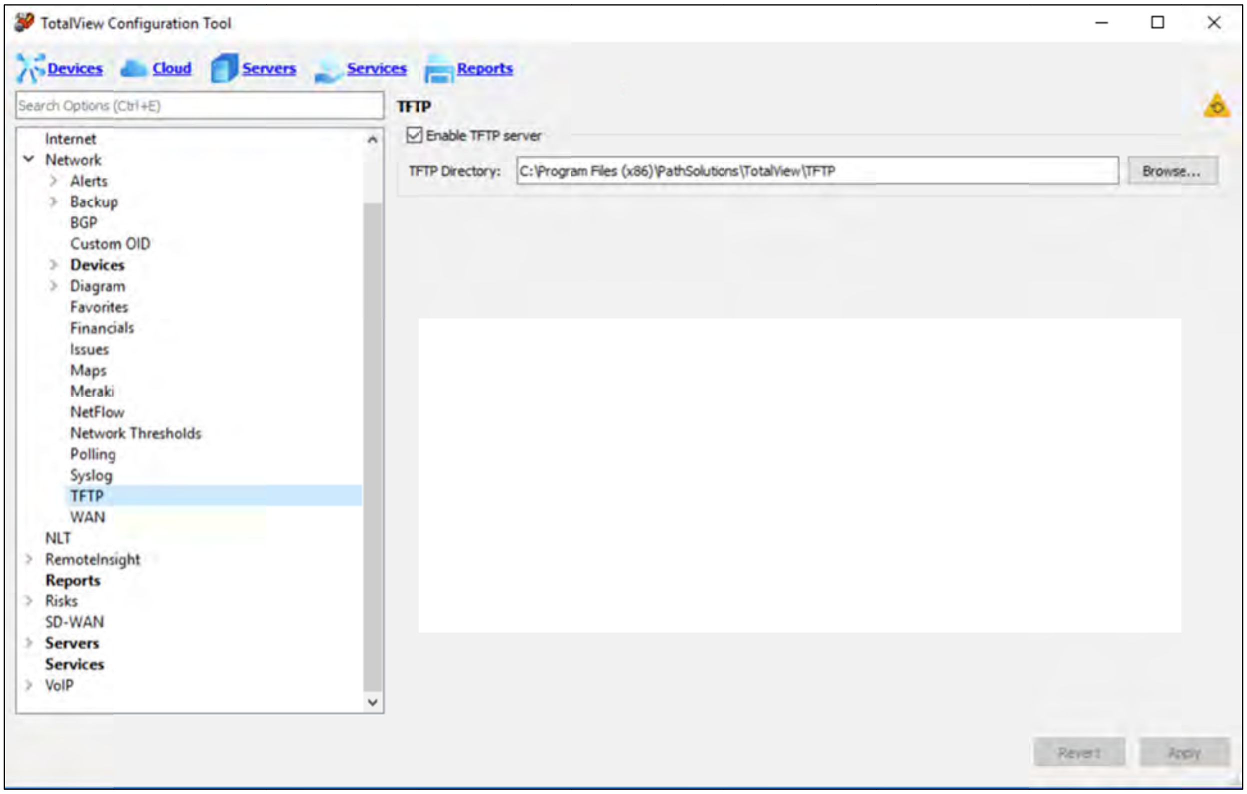
[:d:]	decimal digit character	isdigit
[:w:]	word character	isalnum
[:s:]	whitespace character	isspace

- Please note that the brackets in the class names are additional to those opening and closing the class definition.
  For example:
  [[:alpha:]] is a character class that matches any alphanumeric character.
  [abc[:digit:]] is a character class that matches a, b, c, or a digit.
  [^[:space:]] is a character class that matches any character except a whitespace.
- **Escape characters:** All escape characters described above can also be used within a character class specification. The only change is with \b, that here is interpreted as a backspace character (\u0008) instead of a word boundary.
  Notice that within a class definition, those characters that have a special meaning in the regular expression (such as *, ., $) don't have such a meaning and are interpreted as normal characters (so they do not need to be escaped). Instead, within a class definition, the hyphen (-) and the brackets ([and]) do have a special meaning under some circumstances, in which case they should be escaped with a backslash (\) to be interpreted as normal characters.

Character class support depends on the regex traits used by the regex object: the regex object calls its traits' isctype member function with the appropriate arguments. For the standard regex_traits object using the default locale, see cctype for a classification of characters.

TFTP Server

The system can receive TFTP files from network devices via the built-in TFTP server.



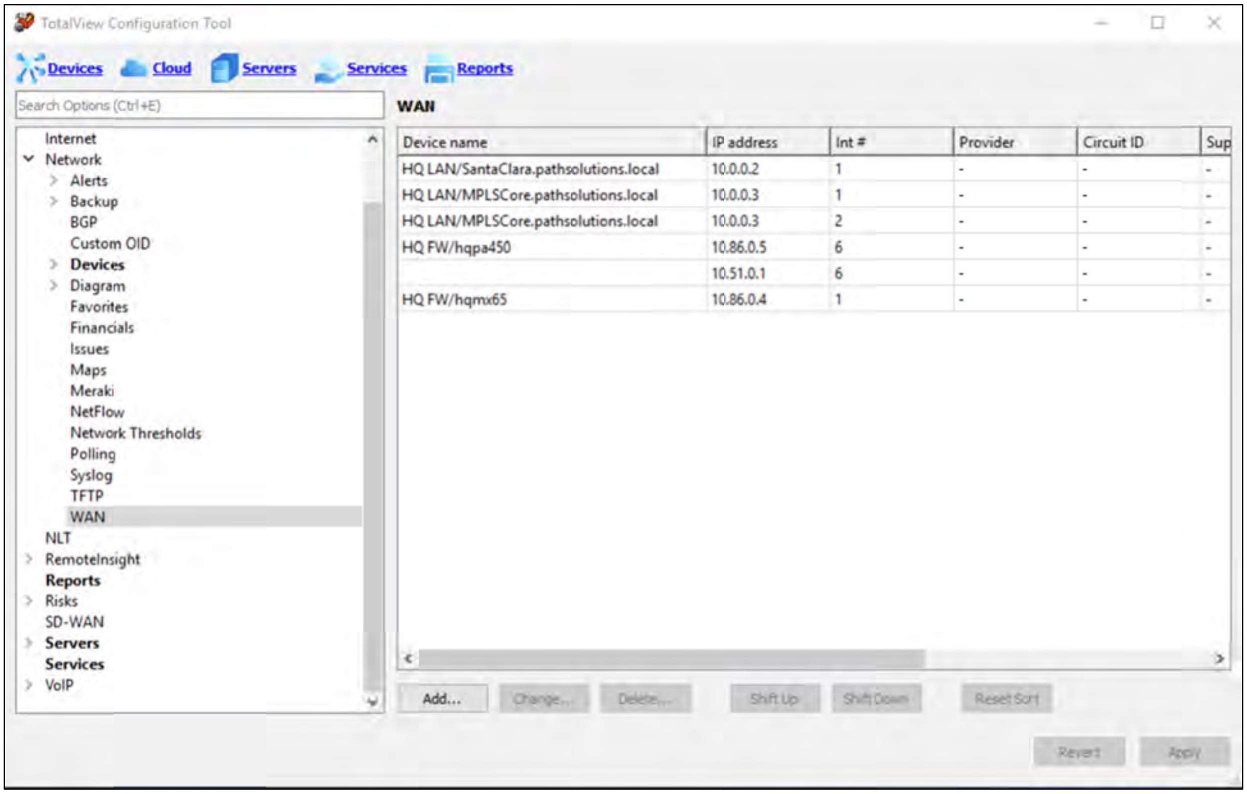
☑ Enable TFTP server

TFTP Directory: C:\Program Files (x86)\PathSolutions\TotalView\TFTP

Select the **Enable TFTP server** checkbox. If desired, select **Browse** to select a different directory where the TFTP files are saved/retrieved.

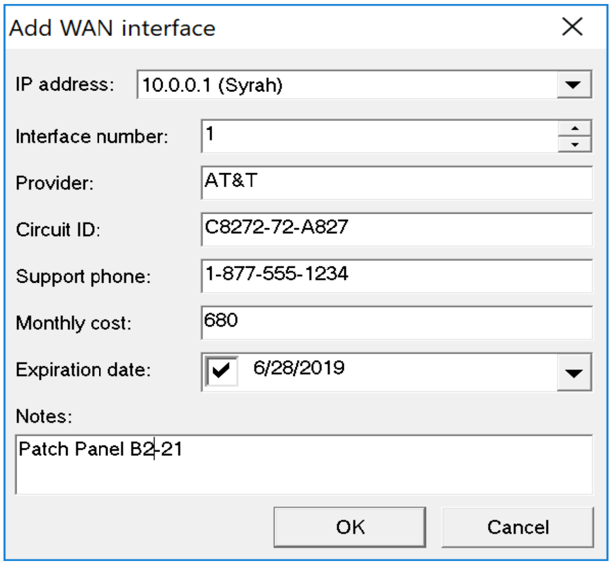
WAN Interfaces

Go to the **Network > WAN** section. The **WAN** tab of TotalView can include any interface desired. You can also include the **Provider**, **Circuit ID**, **Support Phone**, **Monthly Cost**, **Expiration Date** and Notes about a device to display on the **WAN** tab.



Device name	IP address	Int #	Provider	Circuit ID	Sup
HQ LAN/SantaClara.pathsolutions.local	10.0.0.2	1	-	-	-
HQ LAN/MPLSCore.pathsolutions.local	10.0.0.3	1	-	-	-
HQ LAN/MPLSCore.pathsolutions.local	10.0.0.3	2	-	-	-
HQ FW/hqpa450	10.86.0.5	6	-	-	-
	10.51.0.1	6	-	-	-
HQ FW/hqmx65	10.86.0.4	1	-	-	-

To add an interface, select the **Add** button and add the details, then select **OK**.



IP address: 10.0.0.1 (Syrah)

Interface number: 1

Provider: AT&T

Circuit ID: C8272-72-A827

Support phone: 1-877-555-1234

Monthly cost: 680

Expiration date: ☑ 6/28/2019

Notes:

Patch Panel B2-21

Use the **Change** or **Delete** buttons to change and delete WAN interfaces and the **Shift Up** or **Shift Down** buttons to sort the list in the order you would like to view them.

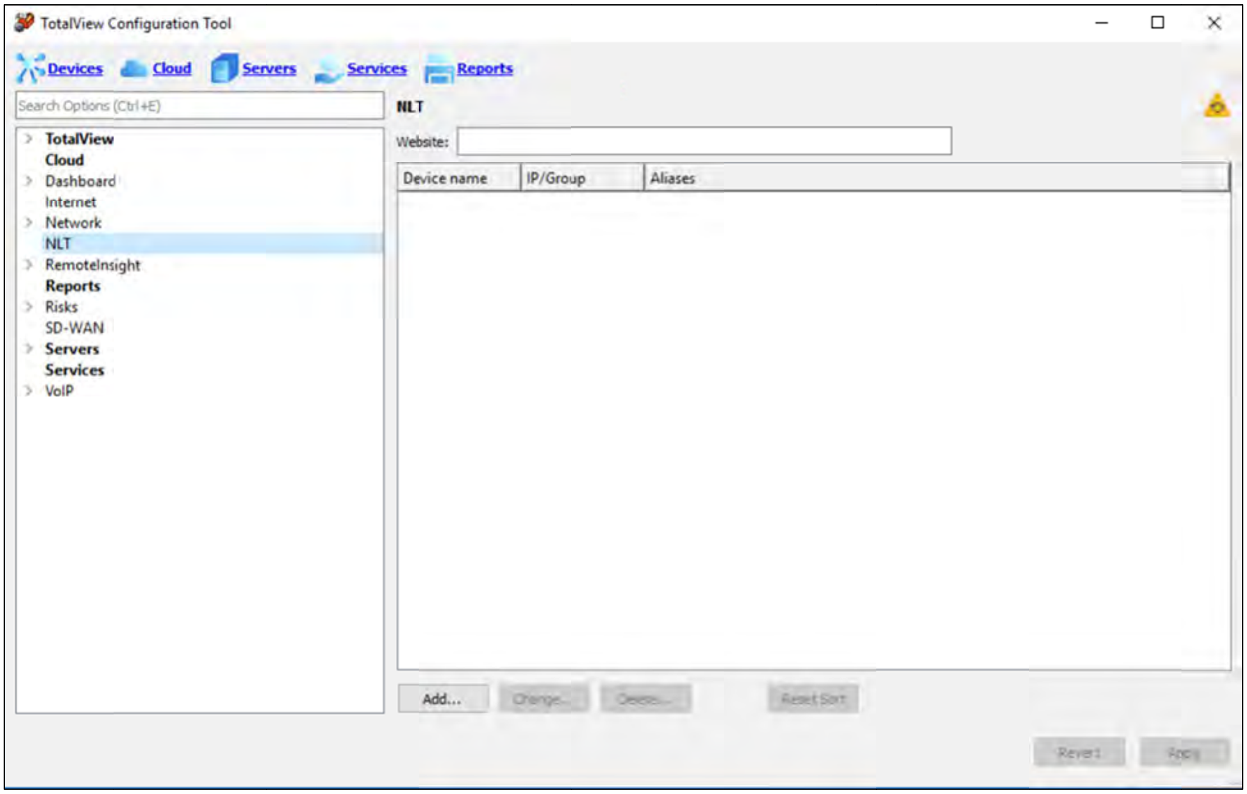
You can also configure it so that users can add WAN interfaces while in the TotalView web interface.

Note: The web server must be unlocked for the Favorites column to show up in TotalView. See the Section *Web Authentication* for how to lock and unlock the web server.

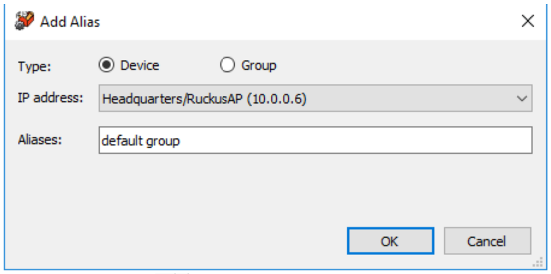
Note: Add WAN by editing the CFG text file. See *Appendix H. Changing the WAN Tab*.

NLT

NLT stands for Natural Language Troubleshooting. Go to the **NLT** section to add a website and to setup alias names. Aliases allow you to refer to devices and groups by aliases when asking questions on the TotalView **NLT** tab.



Use the **Add** and **Change** buttons to add and change aliases. For devices, select the **Device** radio button, then pick an IP address from the IP drop-down menu and give it an alias.

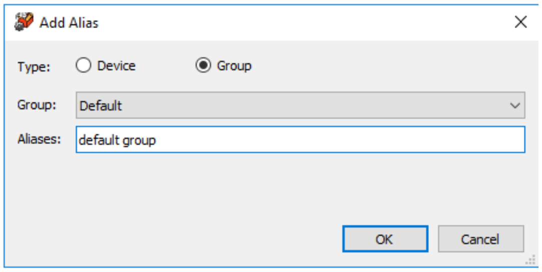


Type: ● Device ○ Group

IP address: Headquarters/RuckusAP (10.0.0.6)

Aliases: default group

For groups, select the type of **Group**. then pick a group from the drop-down menu and give it an alias.



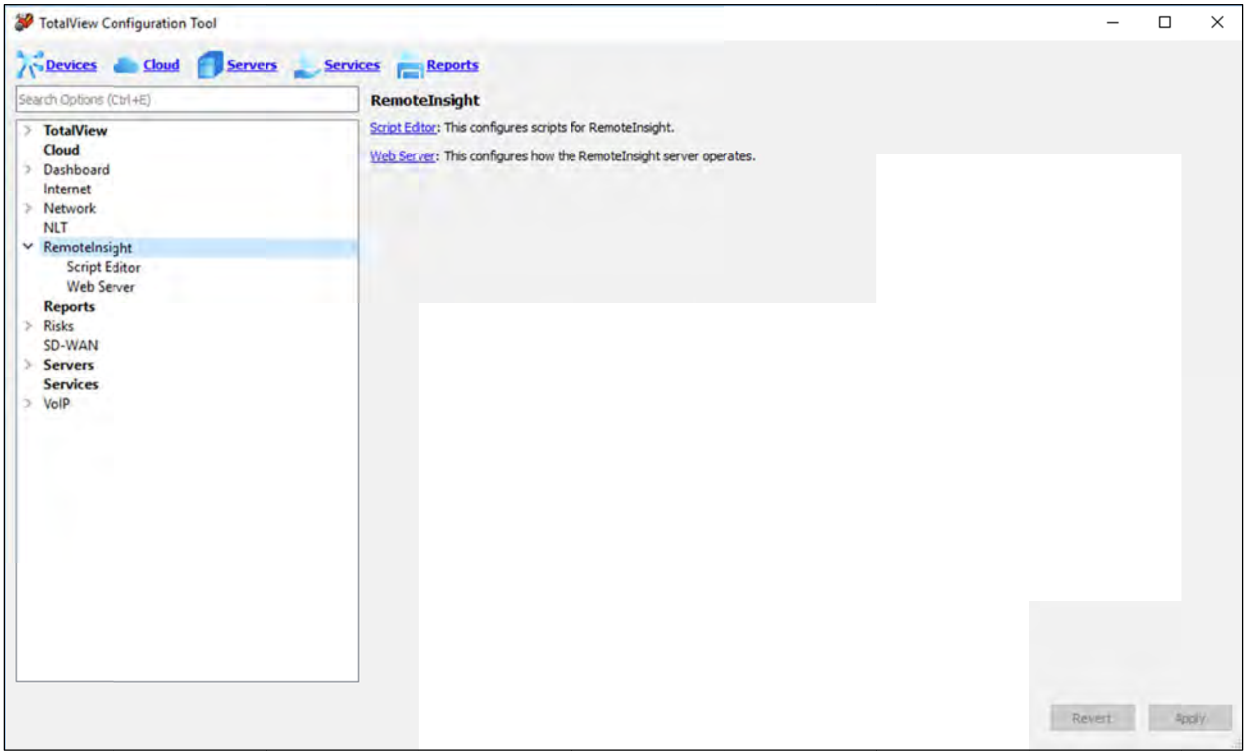
Type: ○ Device ● Group

Group: Default

Aliases: default group

Remote Insight

If you have the license to the optional **RemoteInsight** module, you will see **RemoteInsight** included in the left-hand menu. The first screen shows a short description and links to the Script Editor and Web Server subsections:



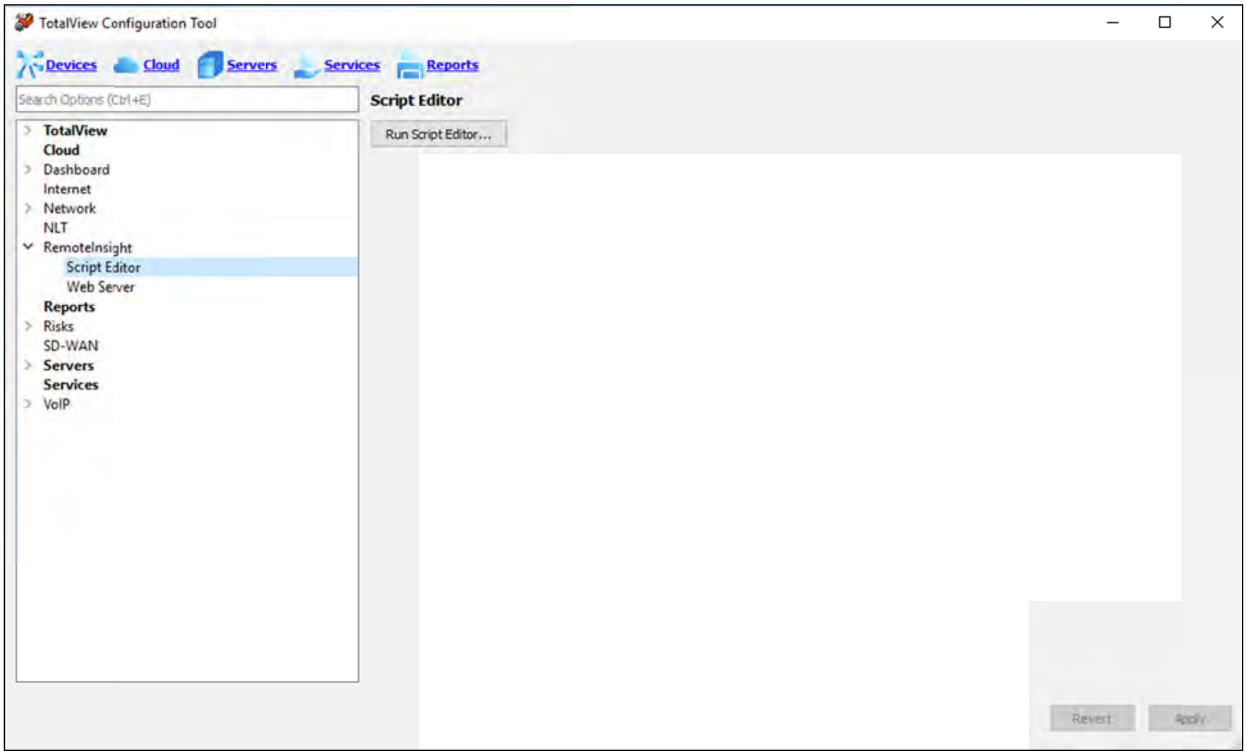
RemoteInsight

Script Editor: This configures scripts for RemoteInsight.

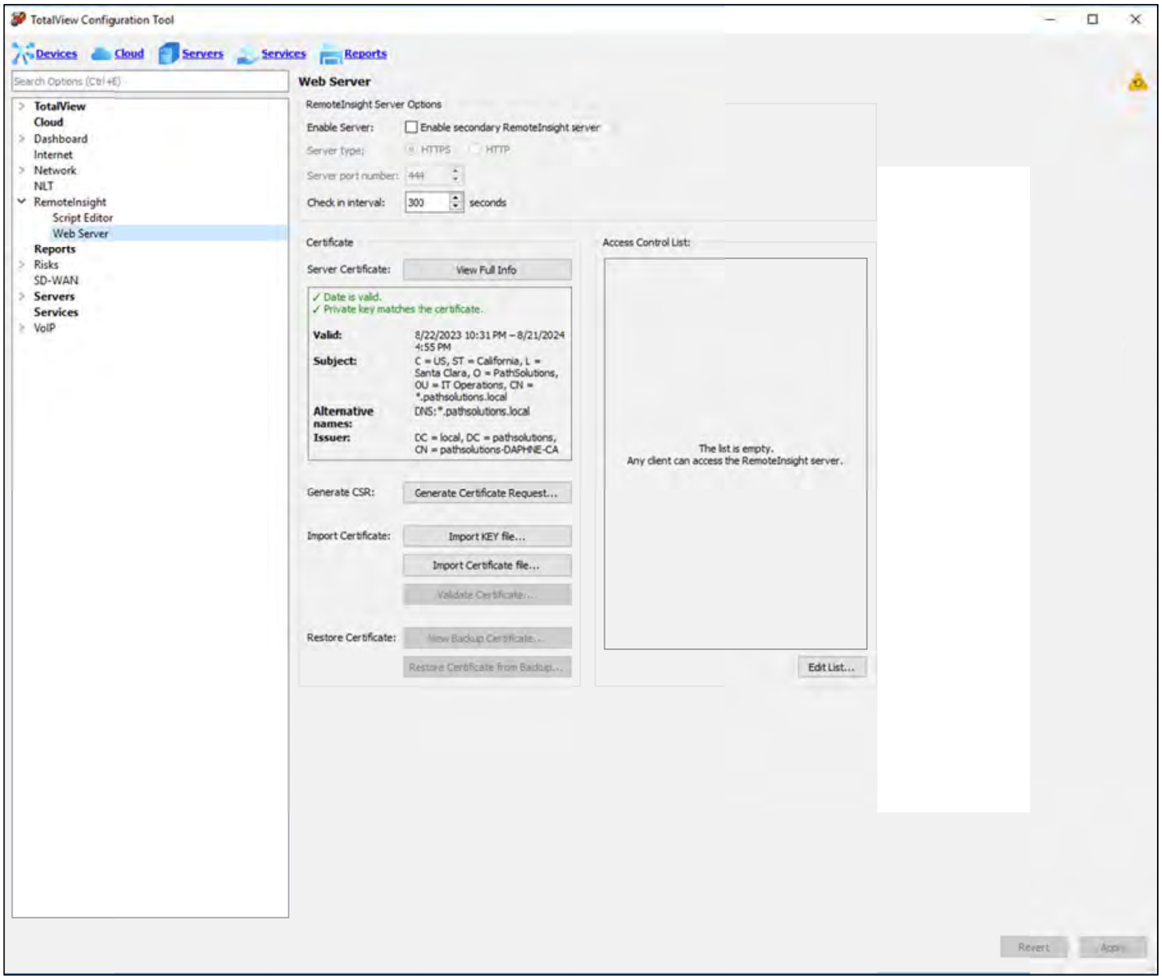
Web Server: This configures how the RemoteInsight server operates.

The **RemoteInsightt > Script Editor** section permits the launch of the **Script Editor** program. For this to work, a certificate must be added to this Web Server. The field descriptions should be the same as the main **TotalView > Web Server** fields.

The **Script Editor** configures scripts for **RemoteInsight**.



The **RemoteInsight > Web Server** section allows you to designate a separate listening webserver on a different port so it can be accessed via the Internet. This Web Server will only respond to RemoteInsight requests, so it will not permit access to the TotalView web UI.



Web Server

RemoteInsight Server Options

Enable Server: □ Enable secondary RemoteInsight server

Server type: ● HTTPS ○ HTTP

Server port number: 444

Check in interval: 300 seconds

Certificate

Server Certificate:

✓ Date is valid.
✓ Private key matches the certificate.

Valid:	8/22/2023 10:31 PM – 8/21/2024 4:55 PM
Subject:	C = US, ST = California, L = Santa Clara, O = PathSolutions, OU = IT Operations, CN = *.pathsolutions.local
Alternative names:	DNS:*.pathsolutions.local
Issuer:	DC = local, DC = pathsolutions, CN = pathsolutions-DAPHNE-CA

Generate CSR:

Import Certificate:

Restore Certificate:

Access Control List:

The list is empty.
Any client can access the RemoteInsight server.

Reports

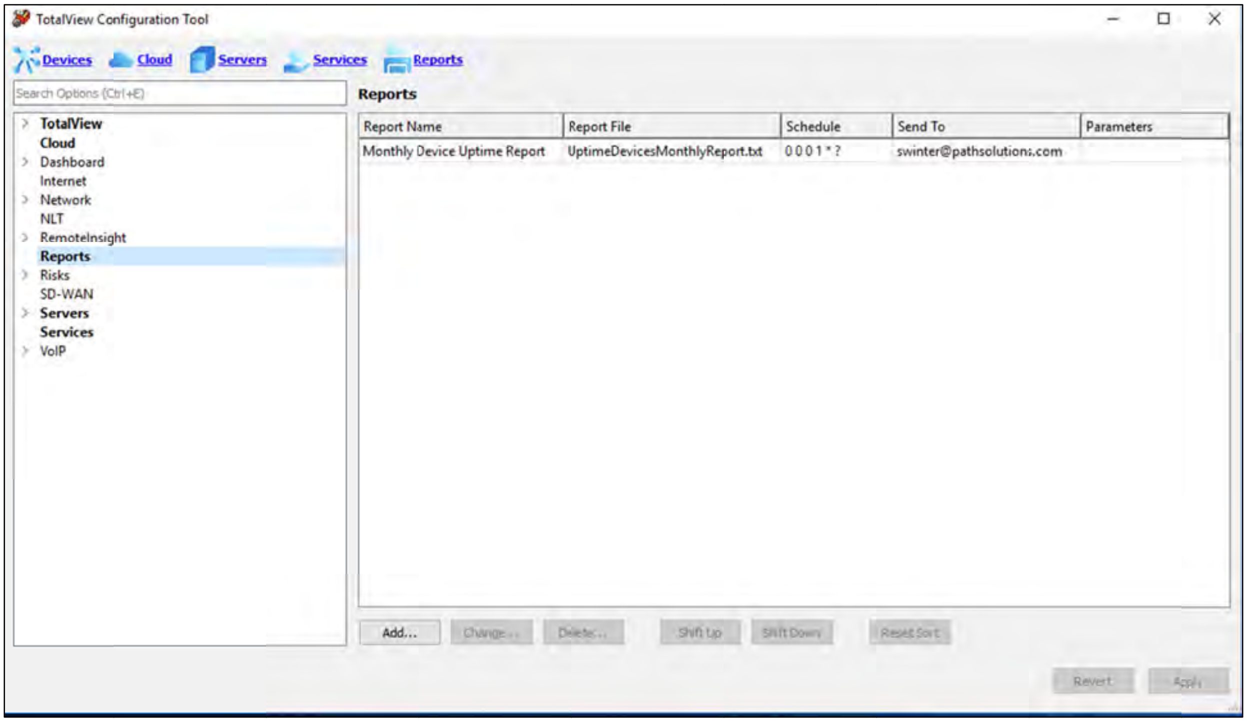
The **Reports** section allows you to configure scheduled email report sending.

Select **Add** to request a report name as well as a report template file. Select **Browse** to display report templates that can be selected, and a sample of the generated report will display on the right side.

The report can be scheduled to be sent on a regular basis. It uses Unix CRON formatting to define the report schedule. Select **Edit** for an easy way to enter the schedule for the report to be generated. The **Next launches** field for the dates and times when the report will go out. Once this is correct, you can select **OK** and it will generate the CRON formatting for that scheduled report to be sent.

The **Send to** field allows defines email recipients who should receive the report. Enter multiple names by using commas or semicolons to separate the recipients.

Some report templates require sending a device or an interface number. Those can be entered in the provided fields.

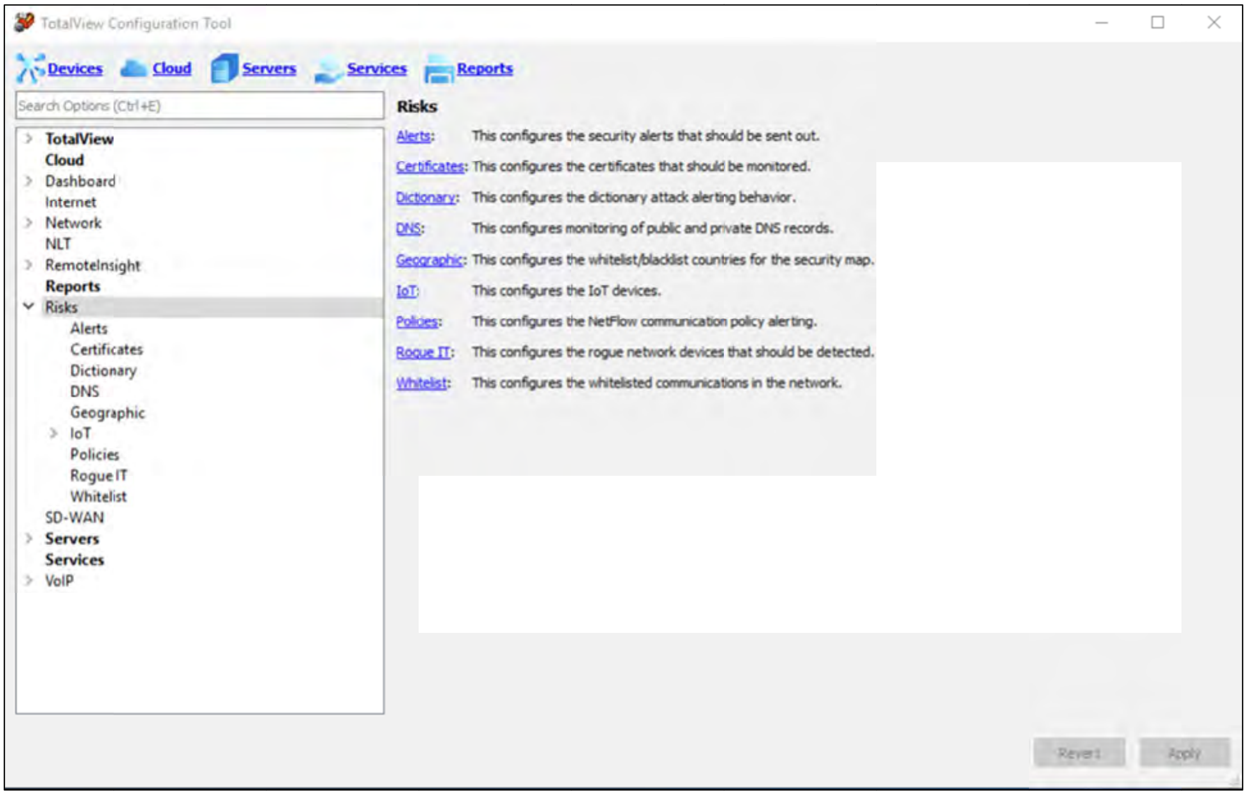


Reports

Report Name	Report File	Schedule	Send To	Parameters
Monthly Device Uptime Report	UptimeDevicesMonthlyReport.txt	0 0 0 1 * ?	swinter@pathsolutions.com	

Risks Monitoring

This section is part of the optional SecOps module. If you have the license to the SecOps module, you will see the **Risks** section included in the left-hand menu. It opens the **Risks** configuration menu with a short description of the various settings you can change: **Alerts**, **Certificates**, **Dictionary**, **DNS**, **Geographic** (security map), **IOT**, **Policies**, **Rogue IT**, and **Whitelist**.



Risks

Alerts: This configures the security alerts that should be sent out.

Certificates: This configures the certificates that should be monitored.

Dictionary: This configures the dictionary attack alerting behavior.

DNS: This configures monitoring of public and private DNS records.

Geographic: This configures the whitelist/blacklist countries for the security map.

IoT: This configures the IoT devices.

Policies: This configures the NetFlow communication policy alerting.

Rogue IT: This configures the rogue network devices that should be detected.

Whitelist: This configures the whitelisted communications in the network.

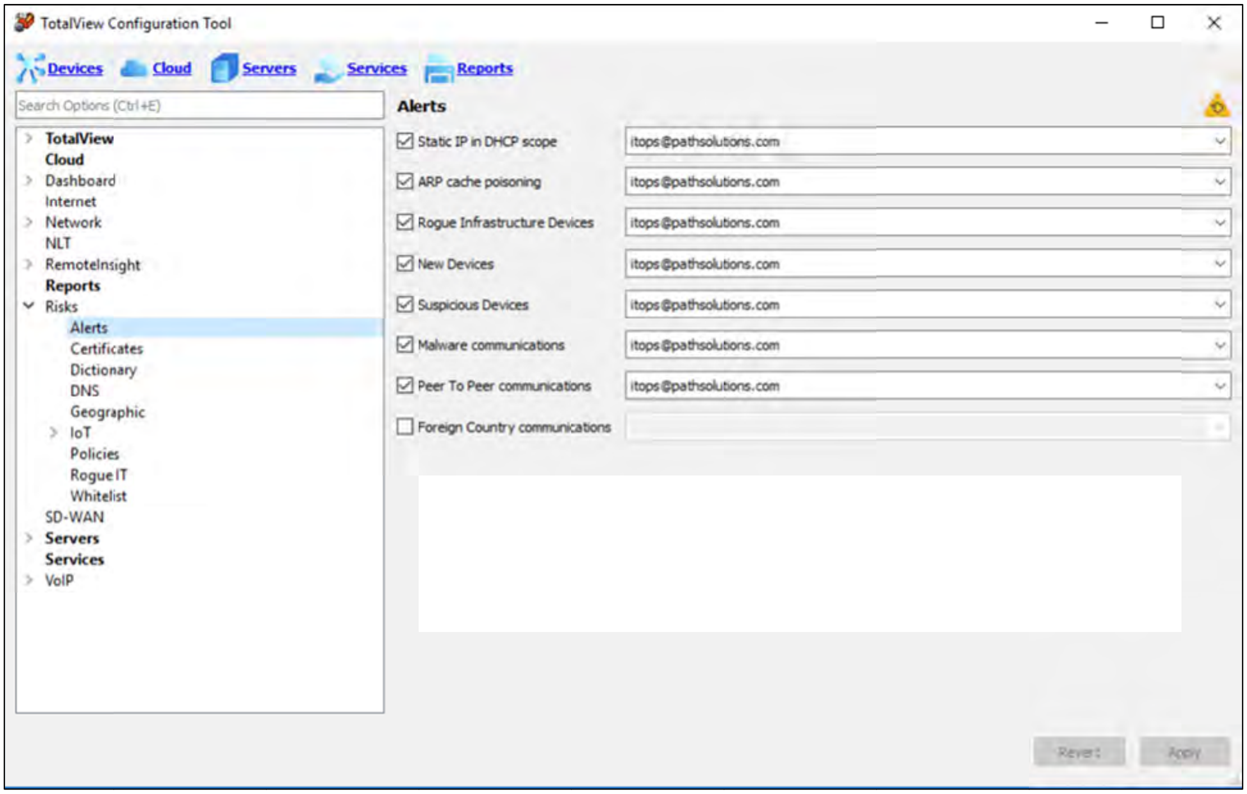
Risks Alerts

This section is to configure risk alerts that can be sent out on Risks via email. Select **Risks > Alerts** from the left-hand menu and select the type of alerts to receive.

- **Static IP in DHCP Scope**
- **ARP Cache Poisoning**
- **Rogue Infrastructure Devices**
- **New Devices**
- **Suspicious Devices**
- **Malware Communications**
- **Peer to Peer Communications**
- **Foreign Country Communications**

In addition, the alerts for SSL Certificates and DNS Records are covered in the Certificate and DNS sections.

Select the security alerts you want to get and specify the email recipient for security alerts in this menu.



TotalView Configuration Tool

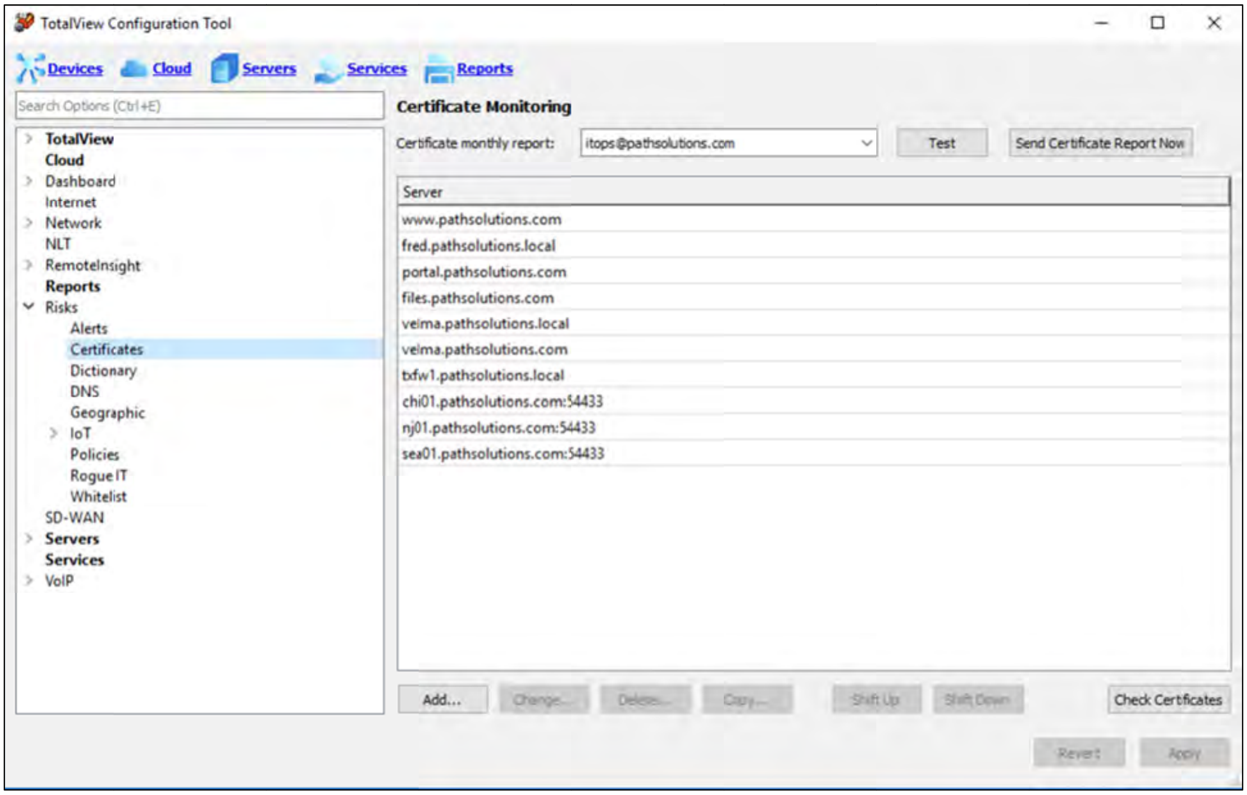
Alerts

☑ Static IP in DHCP scope	itops@pathsolutions.com
☑ ARP cache poisoning	itops@pathsolutions.com
☑ Rogue Infrastructure Devices	itops@pathsolutions.com
☑ New Devices	itops@pathsolutions.com
☑ Suspicious Devices	itops@pathsolutions.com
☑ Malware communications	itops@pathsolutions.com
☑ Peer To Peer communications	itops@pathsolutions.com
□ Foreign Country communications	

Certificates (SSL)

Go to the **Risks > Certificates** section to configure SSL Certificate monitoring. This is where you setup the email alert of expiring SSL Certificates.

At the top of the left-hand, enter the name of the person to get the email reports on certificate status. To make that easy, view commonly used email addresses in the drop-down menus.



Certificate Monitoring

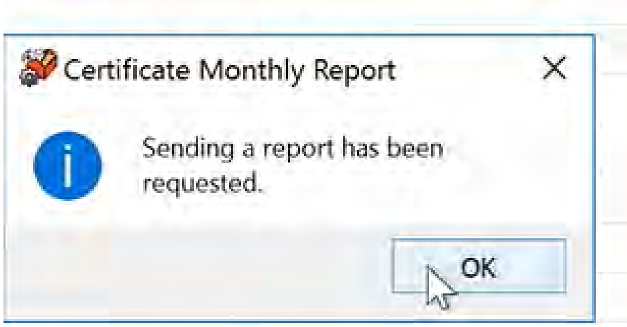
Certificate monthly report: itops@pathsolutions.com

Server
www.pathsolutions.com
fred.pathsolutions.local
portal.pathsolutions.com
files.pathsolutions.com
velma.pathsolutions.local
velma.pathsolutions.com
txfw1.pathsolutions.local
chi01.pathsolutions.com:54433
nj01.pathsolutions.com:54433
sea01.pathsolutions.com:54433

Add, change, and delete servers on the **Certificate Monitoring** list by using the buttons below the list.

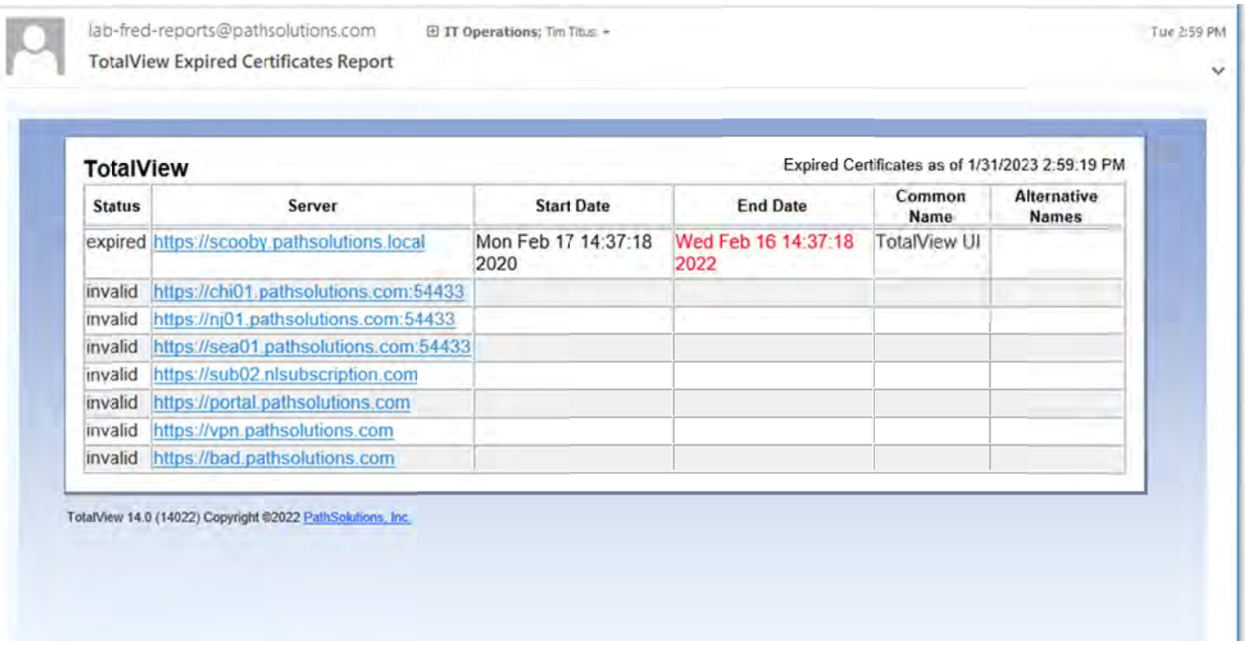
If you want to check certificates, use the **Check Certificates** button.

If you want to get an emailed report now, select the **Send Report Now** button. A small menu will confirm that you are going to send monthly reports. Select **OK**.



Sending a report has been requested.

Below is an example of the emailed report.



lab-fred-reports@pathsolutions.com

TotalView Expired Certificates Report

TotalView

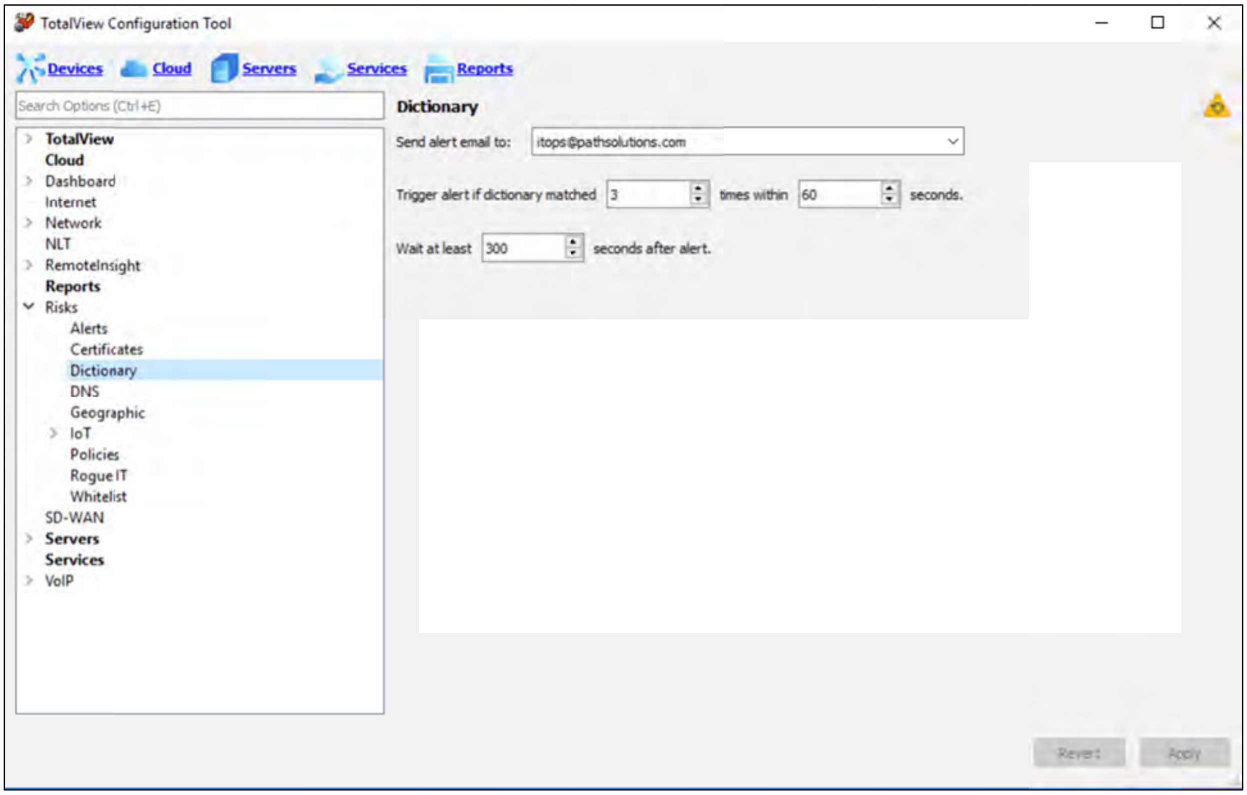
Expired Certificates as of 1/31/2023 2:59:19 PM

Status	Server	Start Date	End Date	Common Name	Alternative Names
expired	https://scooby.pathsolutions.local	Mon Feb 17 14:37:18 2020	Wed Feb 16 14:37:18 2022	TotalView UI	
invalid	https://chi01.pathsolutions.com:54433				
invalid	https://nj01.pathsolutions.com:54433				
invalid	https://sea01.pathsolutions.com:54433				
invalid	https://sub02.nlsubscription.com				
invalid	https://portal.pathsolutions.com				
invalid	https://vpn.pathsolutions.com				
invalid	https://bad.pathsolutions.com				

TotalView 14.0 (14022) Copyright ©2022 PathSolutions, Inc.

Dictionary

Use the **Risks > Dictionary** section to setup alerts for dictionary attacks. Select the email recipients, the settings for what matches will trigger an alert, and how long to wait between sending alerts.



Dictionary

Send alert email to: itops@pathsolutions.com

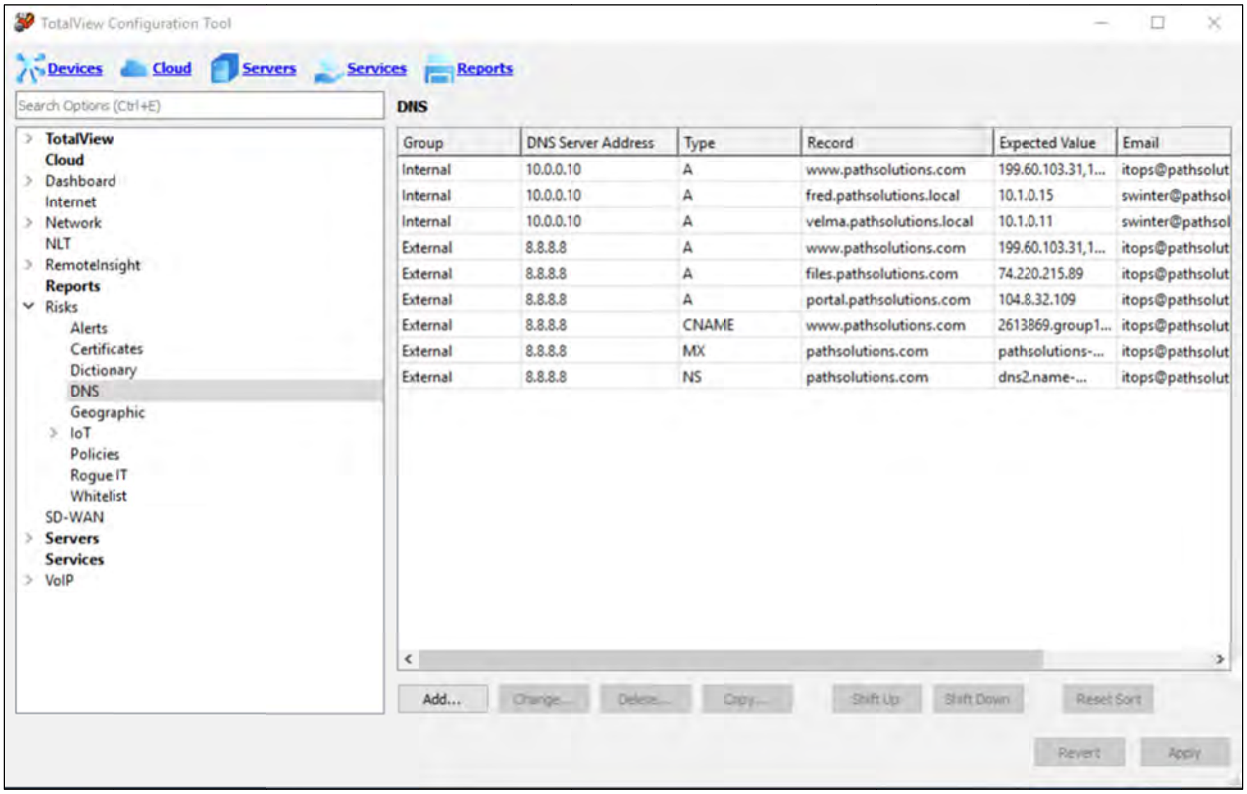
Trigger alert if dictionary matched 3 times within 60 seconds.

Wait at least 300 seconds after alert.

Note: Syslog must be set up for this feature to function.

DNS (DNS Record Monitoring)

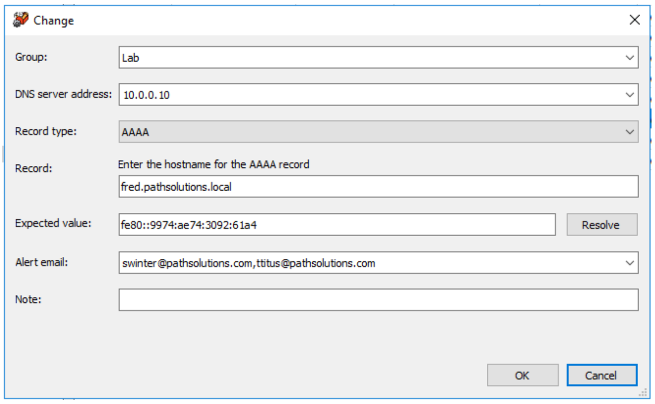
Go to the **Risks > DNS** section to monitor DNS records and receive an alert if a DNS record is changed.



DNS

Group	DNS Server Address	Type	Record	Expected Value	Email
Internal	10.0.0.10	A	www.pathsolutions.com	199.60.103.31,1...	itops@pathsolut
Internal	10.0.0.10	A	fred.pathsolutions.local	10.1.0.15	swinter@pathsol
Internal	10.0.0.10	A	velma.pathsolutions.local	10.1.0.11	swinter@pathsol
External	8.8.8.8	A	www.pathsolutions.com	199.60.103.31,1...	itops@pathsolut
External	8.8.8.8	A	files.pathsolutions.com	74.220.215.89	itops@pathsolut
External	8.8.8.8	A	portal.pathsolutions.com	104.8.32.109	itops@pathsolut
External	8.8.8.8	CNAME	www.pathsolutions.com	2613869.group1...	itops@pathsolut
External	8.8.8.8	MX	pathsolutions.com	pathsolutions-...	itops@pathsolut
External	8.8.8.8	NS	pathsolutions.com	dns2.name-...	itops@pathsolut

Add, change, and delete URLs on the DNS Monitoring list by using the buttons below the list. Below is an example of the **Change** dialog box.



Group: Lab

DNS server address: 10.0.0.10

Record type: AAAA

Record: Enter the hostname for the AAAA record

fred.pathsolutions.local

Expected value: fe80::9974:ae74:3092:61a4

Alert email: swinter@pathsolutions.com,ttitus@pathsolutions.com

Note:

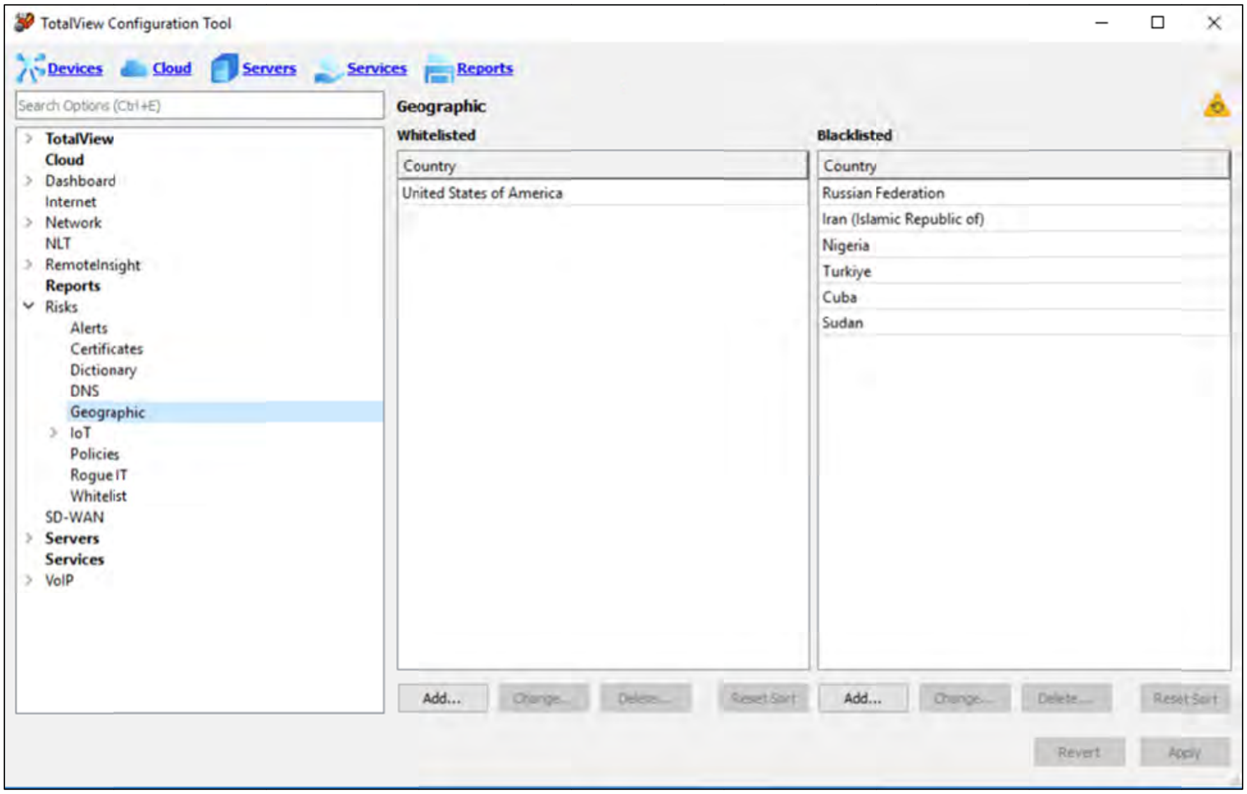
For the **Add** and **Change** dialog boxes, use the drop-down menus to select the group, DNS server address, and record type you want to monitor. Enter the hostname for the record, complete the **Expected Value** field, and the **Alert email** field.

If you do not know the value for the **Expected Value** field, select **Resolve** and it will fill in the field. Select **Resolve** to also check and correct this field.

Geographic

In the **Risks > Geographic** section, configure the Whitelisted and Blacklisted locations to monitoring communications by geographic location. These lists will allow you to filter the communications in the web interface and sort between Whitelisted (safer) communications and Blacklisted (riskier) communications.

The communications with countries you add to the Whitelisted are shaded light green on the web interface map. The communications with the countries you place on the Blacklisted are to be monitored and shaded red on the geographic map. Countries that are not whitelisted or blacklisted, will be grey on the map.



Geographic

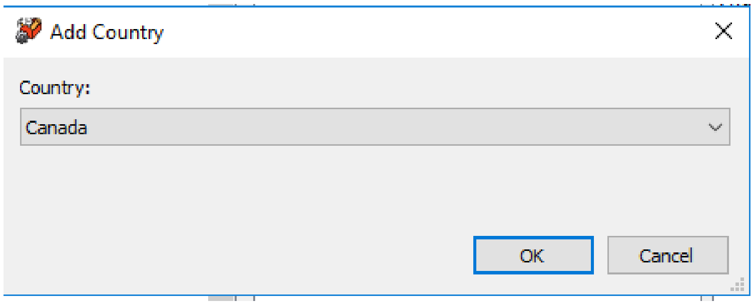
Whitelisted

Country
United States of America

Blacklisted

Country
Russian Federation
Iran (Islamic Republic of)
Nigeria
Turkiye
Cuba
Sudan

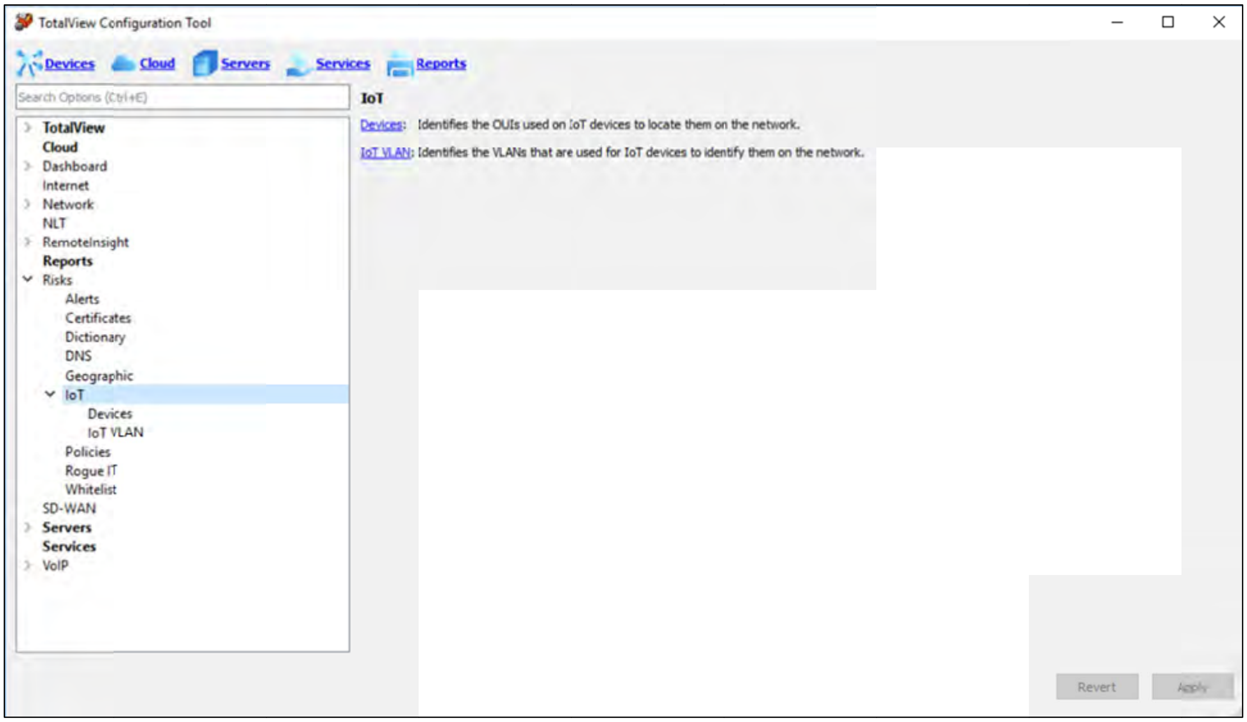
Use the **Add**, **Change** and **Delete** buttons to edit the Whitelist and Blacklist of countries. Below is a screenshot of the **Add Country** dialog box.



Country: Canada

IoT

In the **Risks > IoT** section, you can configure TotalView to find IoT devices by manufacturer or by VLAN name or number.



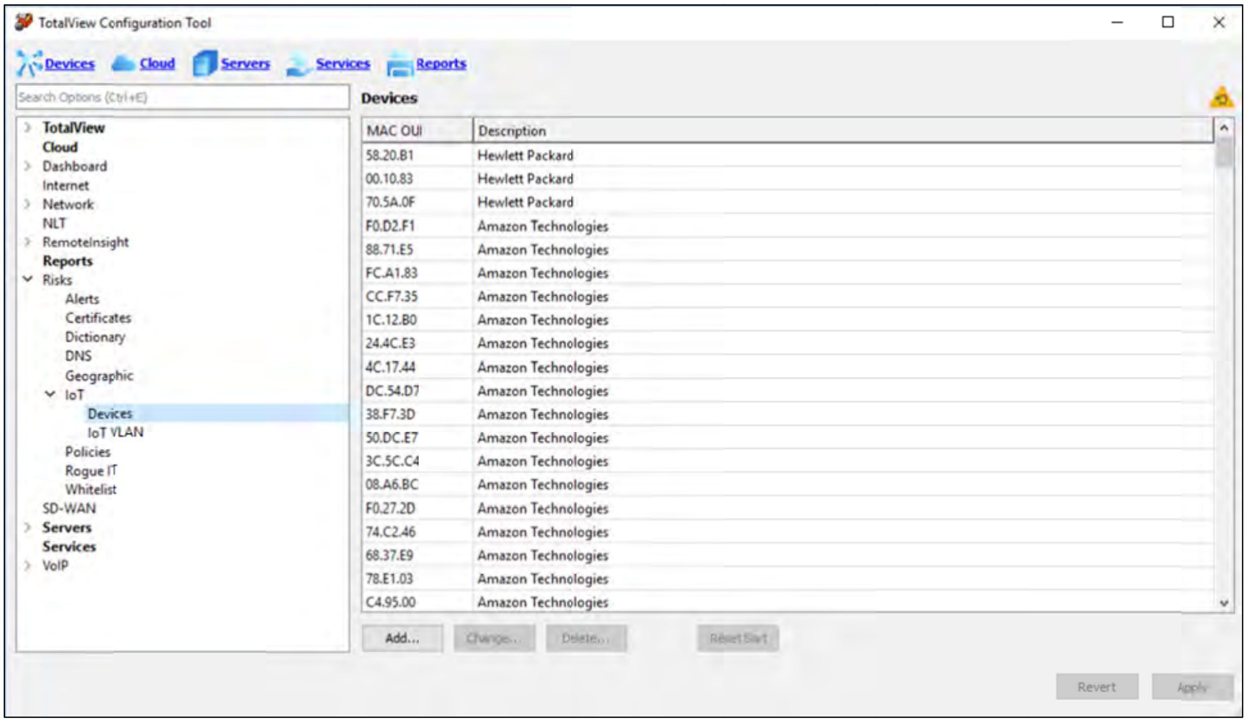
IoT

Devices: Identifies the OUIs used on IoT devices to locate them on the network.

IoT VLAN: Identifies the VLANs that are used for IoT devices to identify them on the network.

Devices

Devices identify the OUIs used on IoT devices to find their location on the network.

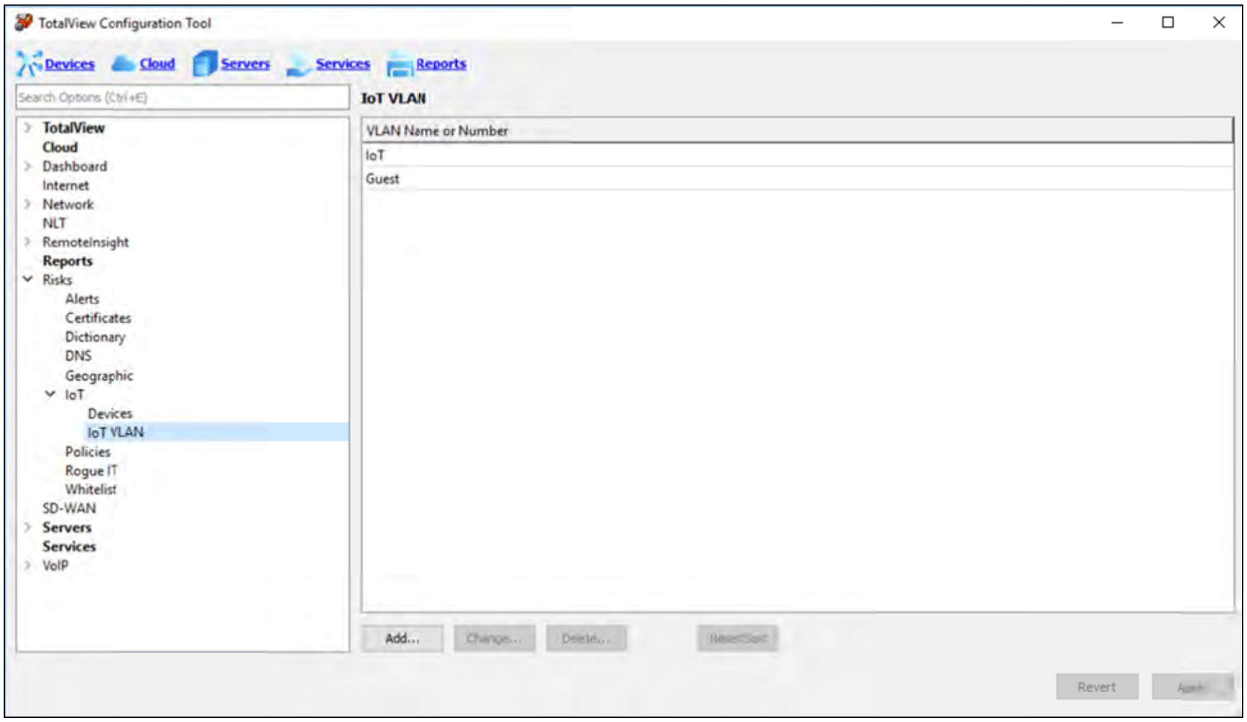


Devices

MAC OUI	Description
58.20.B1	Hewlett Packard
00.10.83	Hewlett Packard
70.5A.0F	Hewlett Packard
F0.D2.F1	Amazon Technologies
88.71.E5	Amazon Technologies
FC.A1.83	Amazon Technologies
CC.F7.35	Amazon Technologies
1C.12.B0	Amazon Technologies
24.4C.E3	Amazon Technologies
4C.17.44	Amazon Technologies
DC.54.D7	Amazon Technologies
38.F7.3D	Amazon Technologies
50.DC.E7	Amazon Technologies
3C.5C.C4	Amazon Technologies
08.A6.BC	Amazon Technologies
F0.27.2D	Amazon Technologies
74.C2.46	Amazon Technologies
68.37.E9	Amazon Technologies
78.E1.03	Amazon Technologies
C4.95.00	Amazon Technologies

IoT VLAN

IoT VLAN identify the VLANs that are used for IoT devices to find their location on the network.

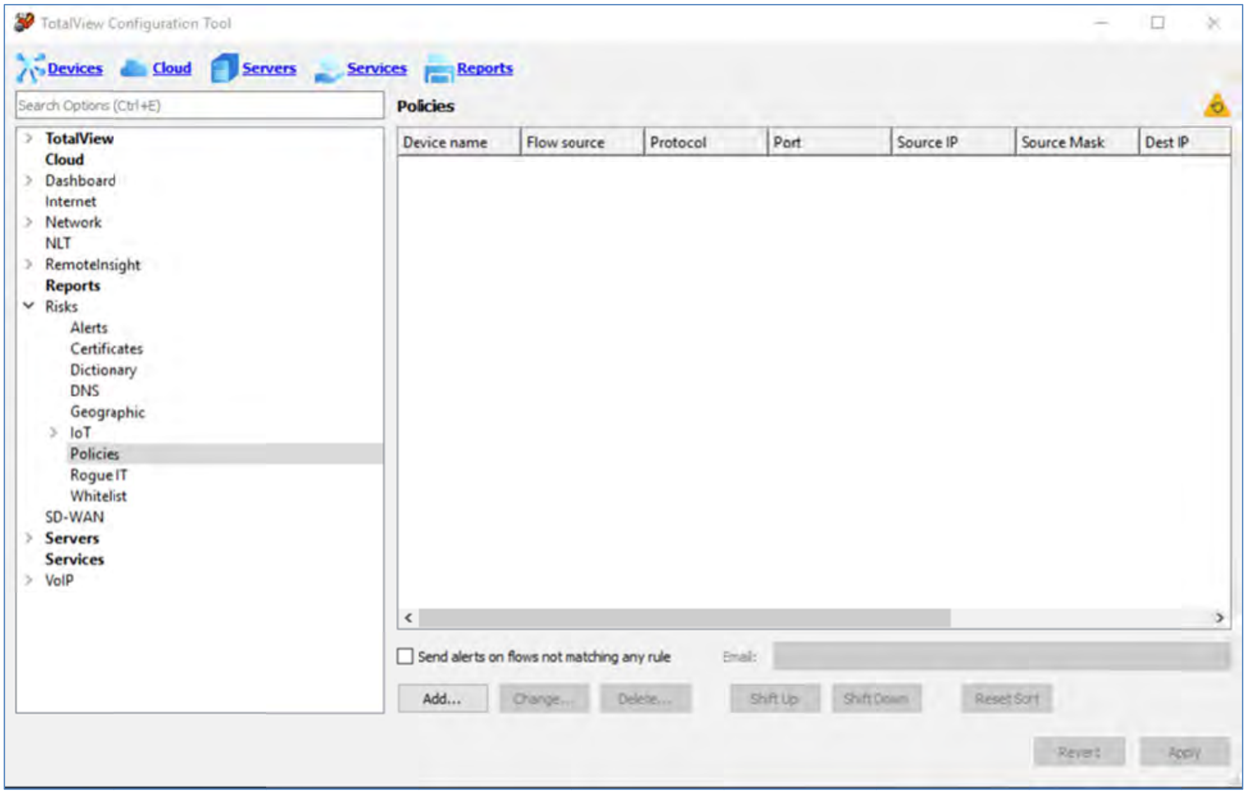


IoT VLAN

VLAN Name or Number
IoT
Guest

Policies

In the **Risks > Policies** section, Security Policy Alerting is performed by analyzing all collected flows and applying them to a security policy template. Alerts can be generated and sent to your e-mail if a policy is not followed.

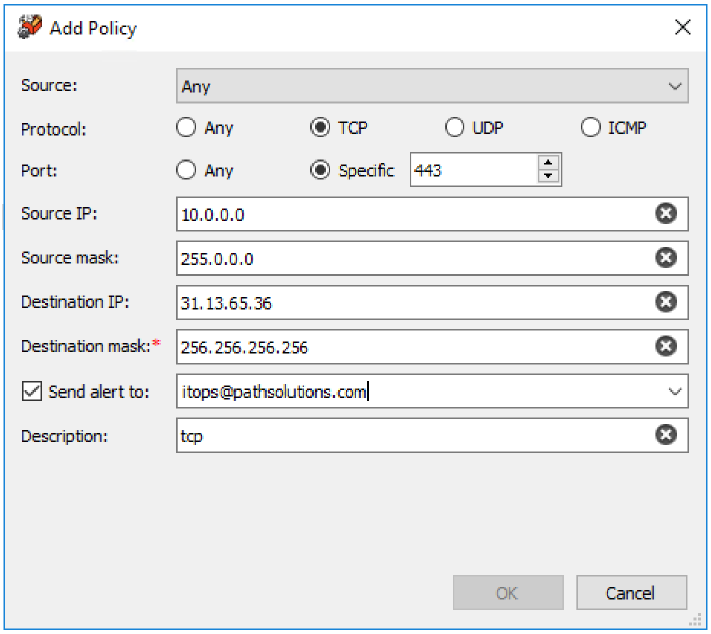


Device name	Flow source	Protocol	Port	Source IP	Source Mask	Dest IP

□ Send alerts on flows not matching any rule

Email:

To create a security policy, select **Add**, the **Add Policy** dialog will display.



Add Policy

Source: Any

Protocol: ○ Any ● TCP ○ UDP ○ ICMP

Port: ○ Any ● Specific 443

Source IP: 10.0.0.0

Source mask: 255.0.0.0

Destination IP: 31.13.65.36

Destination mask:* 256.256.256.256

☑ Send alert to: itops@pathsolutions.com

Description: tcp

A single policy match can be defined on this dialog.

The **Source** is the NetFlow flow generator for IP addresses. In most cases, this can be set to **Any** and the policy can be defined to match traffic flows no matter where the flow came from.

Choose the protocol and port number that should match the policy.

The **Source IP** and **Source Mask** define a subnet or host of the source of the flow.

The **Destination IP** and **Destination Mask** define a subnet or host of the destination of the flow.

Note: If the Source IP or Destination IP is a host, use the Mask of 255.255.255.255.

Note: Flow records are checked from Source to Destination as well as from Destination to Source.

A single policy match can be created that addresses any communications between two IP addresses.

If this communication occurs, choose to send an email alert to a destination.

Note: If **No alert** is selected and this flow is matched, it will immediately stop checking policies for this flow, as it is defined as an accepted policy on the network.

Define all the policy matches that are appropriate for your network and change the policy match order to generate alerts for policies that you deem unacceptable.

Below is an example of a policy list.

Flow Source	***Protocol***	***Port***	***Source IP***	***Source Mask***	***Destination IP***	***Destination Mask***	***Email***
Any	Any	Any	10.0.0.0	255.0.0.0	10.0.0.0	255.0.0.0	
Any	TCP	Any	10.0.0.0	255.0.0.0	10.0.12.42	255.255.255.255	noc@company.com
Any	TCP	443	10.0.1.0	255.255.255.0	10.8.2.0	255.255.255.0	noc@company.com
Any	TCP	443	10.0.0.0	255.0.0.0	45.8.0.0	255.255.0.0	

In the above example, the first policy will match any traffic from any internal source to any other internal source and stop checking after it finds match. If the Flow Source **Any** is going to Destination 255.0.0.0, the second and third policy will never be checked. If the first policy does not match, then the other policies will be checked in order.

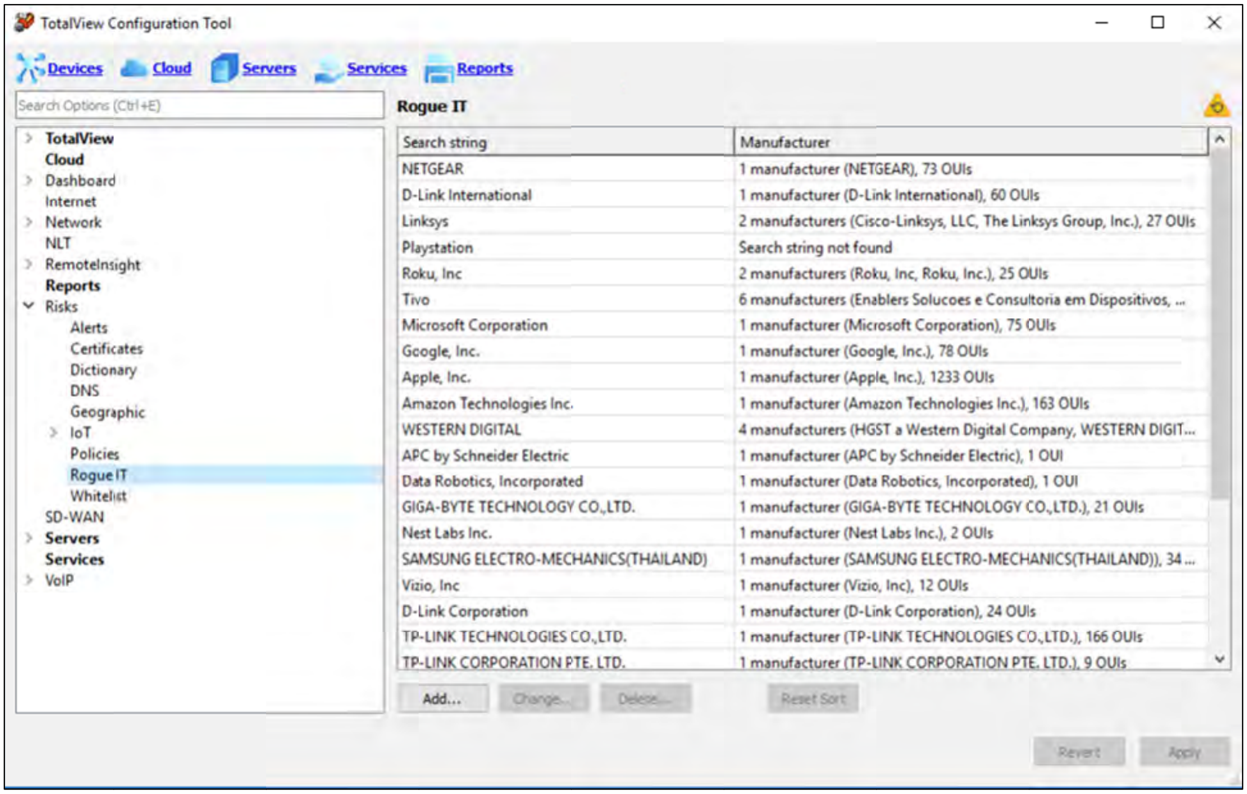
Note: Policy list ordering is important not only to make sure that alerts are generated correctly, but also to ensure that NetFlow record processing is not slowed down by excessive policy checking or a poorly ordered list.

Once you setup a security policy, e-mail alerts will be sent when communications occur outside of the policy.

Rogue IT

In the **Risks > Rogue IT** section, identify the things that are rogues in your network, by manufacturer name, OUI or Mac Addresses, and to configure the alerts to send if one is found. Rogue device manufacturers are devices that should not be found on the network.

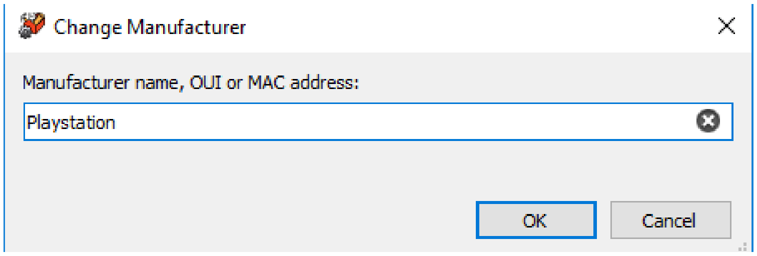
For example: If you run a network and all your network equipment is manufactured by Cisco, if a D-Link device shows up on the network, it is rogue and unapproved.



Rogue IT

Search string	Manufacturer
NETGEAR	1 manufacturer (NETGEAR), 73 OUIs
D-Link International	1 manufacturer (D-Link International), 60 OUIs
Linksys	2 manufacturers (Cisco-Linksys, LLC, The Linksys Group, Inc.), 27 OUIs
Playstation	Search string not found
Roku, Inc	2 manufacturers (Roku, Inc, Roku, Inc.), 25 OUIs
Tivo	6 manufacturers (Enablers Solucoes e Consultoria em Dispositivos, ...
Microsoft Corporation	1 manufacturer (Microsoft Corporation), 75 OUIs
Google, Inc.	1 manufacturer (Google, Inc.), 78 OUIs
Apple, Inc.	1 manufacturer (Apple, Inc.), 1233 OUIs
Amazon Technologies Inc.	1 manufacturer (Amazon Technologies Inc.), 163 OUIs
WESTERN DIGITAL	4 manufacturers (HGST a Western Digital Company, WESTERN DIGIT...
APC by Schneider Electric	1 manufacturer (APC by Schneider Electric), 1 OUI
Data Robotics, Incorporated	1 manufacturer (Data Robotics, Incorporated), 1 OUI
GIGA-BYTE TECHNOLOGY CO.,LTD.	1 manufacturer (GIGA-BYTE TECHNOLOGY CO.,LTD.), 21 OUIs
Nest Labs Inc.	1 manufacturer (Nest Labs Inc.), 2 OUIs
SAMSUNG ELECTRO-MECHANICS(THAILAND)	1 manufacturer (SAMSUNG ELECTRO-MECHANICS(THAILAND)), 34 ...
Vizio, Inc	1 manufacturer (Vizio, Inc), 12 OUIs
D-Link Corporation	1 manufacturer (D-Link Corporation), 24 OUIs
TP-LINK TECHNOLOGIES CO.,LTD.	1 manufacturer (TP-LINK TECHNOLOGIES CO.,LTD.), 166 OUIs
TP-LINK CORPORATION PTE. LTD.	1 manufacturer (TP-LINK CORPORATION PTE. LTD.), 9 OUIs

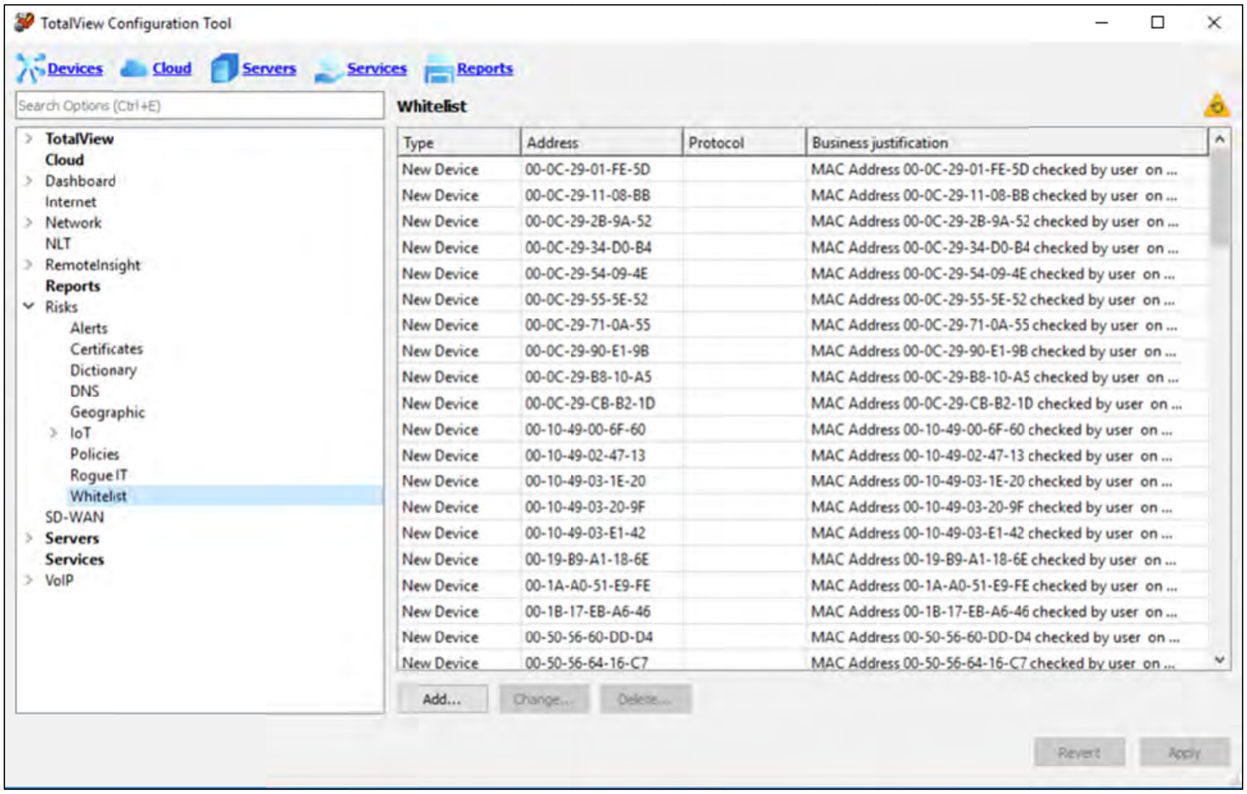
Use the **Add** or **Change** buttons to add or change manufacturer names, OUI and Mac Addresses on the Rogue IT list.



Manufacturer name, OUI or MAC address: Playstation

Whitelist

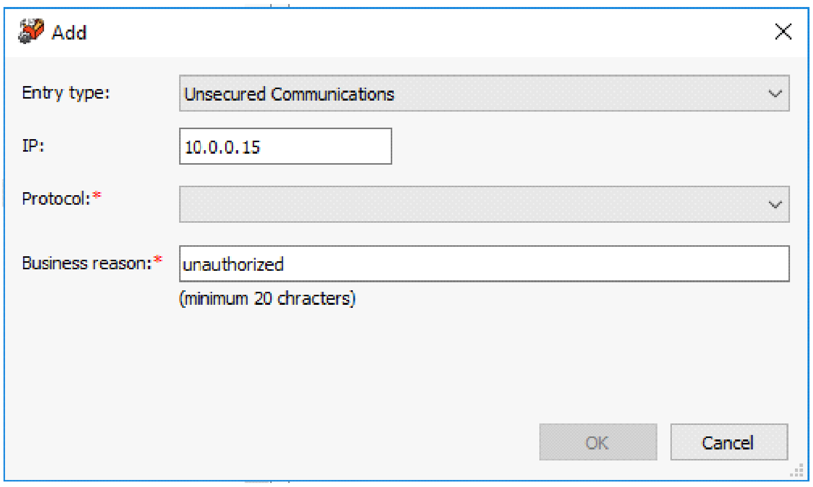
In the **Risks > Whitelist** section, list any devices that you do not need to monitor as a security risk.



Whitelist

Type	Address	Protocol	Business justification
New Device	00-0C-29-01-FE-5D		MAC Address 00-0C-29-01-FE-5D checked by user on ...
New Device	00-0C-29-11-08-BB		MAC Address 00-0C-29-11-08-BB checked by user on ...
New Device	00-0C-29-2B-9A-52		MAC Address 00-0C-29-2B-9A-52 checked by user on ...
New Device	00-0C-29-34-D0-B4		MAC Address 00-0C-29-34-D0-B4 checked by user on ...
New Device	00-0C-29-54-09-4E		MAC Address 00-0C-29-54-09-4E checked by user on ...
New Device	00-0C-29-55-5E-52		MAC Address 00-0C-29-55-5E-52 checked by user on ...
New Device	00-0C-29-71-0A-55		MAC Address 00-0C-29-71-0A-55 checked by user on ...
New Device	00-0C-29-90-E1-9B		MAC Address 00-0C-29-90-E1-9B checked by user on ...
New Device	00-0C-29-B8-10-A5		MAC Address 00-0C-29-B8-10-A5 checked by user on ...
New Device	00-0C-29-CB-B2-1D		MAC Address 00-0C-29-CB-B2-1D checked by user on ...
New Device	00-10-49-00-6F-60		MAC Address 00-10-49-00-6F-60 checked by user on ...
New Device	00-10-49-02-47-13		MAC Address 00-10-49-02-47-13 checked by user on ...
New Device	00-10-49-03-1E-20		MAC Address 00-10-49-03-1E-20 checked by user on ...
New Device	00-10-49-03-20-9F		MAC Address 00-10-49-03-20-9F checked by user on ...
New Device	00-10-49-03-E1-42		MAC Address 00-10-49-03-E1-42 checked by user on ...
New Device	00-19-B9-A1-18-6E		MAC Address 00-19-B9-A1-18-6E checked by user on ...
New Device	00-1A-A0-51-E9-FE		MAC Address 00-1A-A0-51-E9-FE checked by user on ...
New Device	00-1B-17-EB-A6-46		MAC Address 00-1B-17-EB-A6-46 checked by user on ...
New Device	00-50-56-60-DD-D4		MAC Address 00-50-56-60-DD-D4 checked by user on ...
New Device	00-50-56-64-16-C7		MAC Address 00-50-56-64-16-C7 checked by user on ...

To add or change items to the Whitelist, use the **Add** or **Change** buttons. The **Add** menu shows a list of entry types to Whitelist in the **Entry type** drop-down menu such as: Unsecured Communications, Unauthorized Static IP, New Devices and Rogues. It will ask you to specify the IP address or Mac Address, the protocol (DNS, NTP, or SMTP), and the business reason.



Entry type: Unsecured Communications

IP: 10.0.0.15

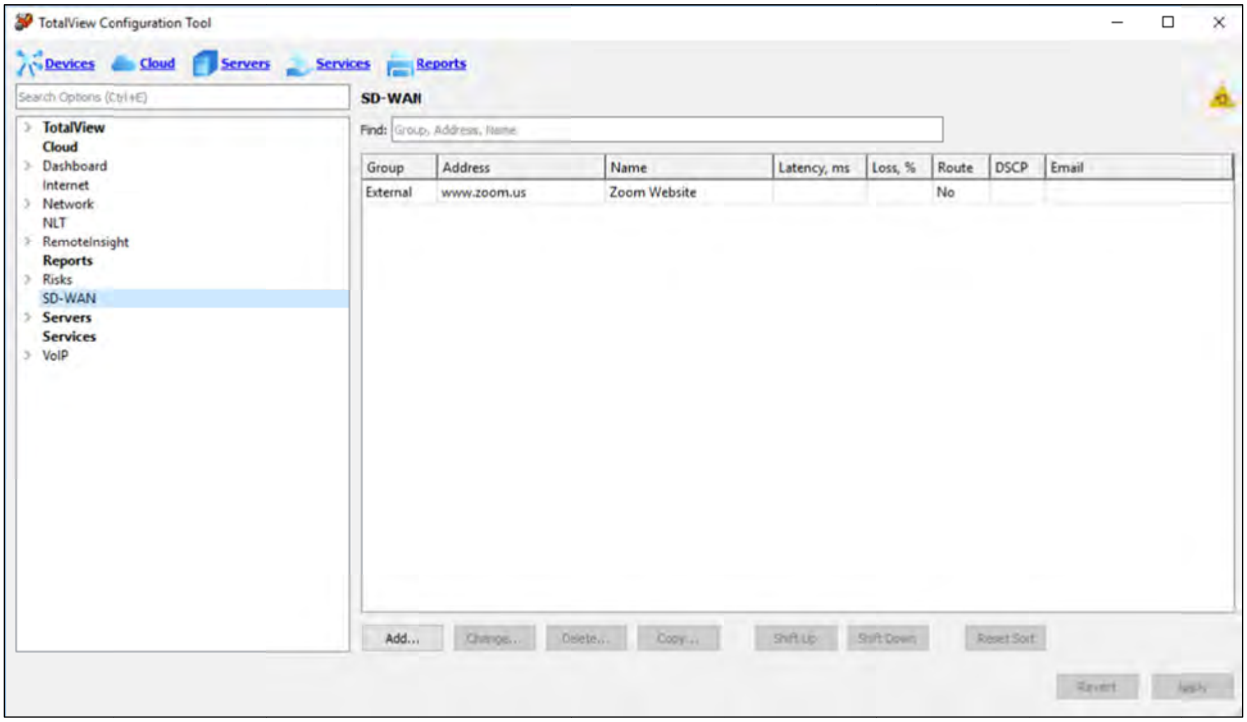
Protocol:*

Business reason:* unauthorized

(minimum 20 chracters)

SD-WAN

To configure **SD-WAN**, select the SD-WAN section from the left-hand menu. In this section you can add, change, or delete SD-WAN services by using the **Add**, **Change** and **Delete** buttons. Adding a Service Icon picture is optional.

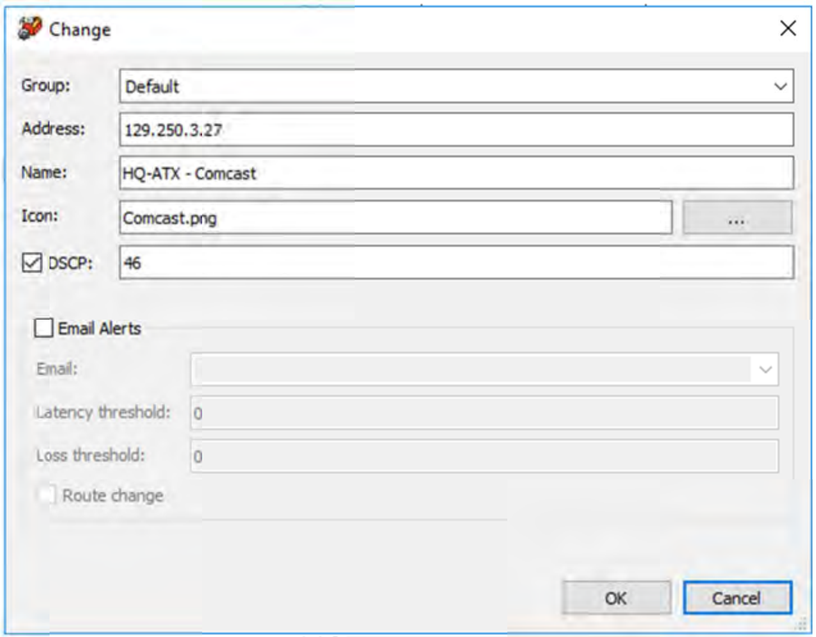


SD-WAN

Find: Group, Address, Name

Group	Address	Name	Latency, ms	Loss, %	Route	DSCP	Email
External	www.zoom.us	Zoom Website			No		

Setup email alerts for latency and loss thresholds on the submenu. You can also assign a sort order by using the **Shift Up** or **Shift Down** keys.



Group: Default

Address: 129.250.3.27

Name: HQ-ATX - Comcast

Icon: Comcast.png

☑ DSCP: 46

☐ Email Alerts

Email:

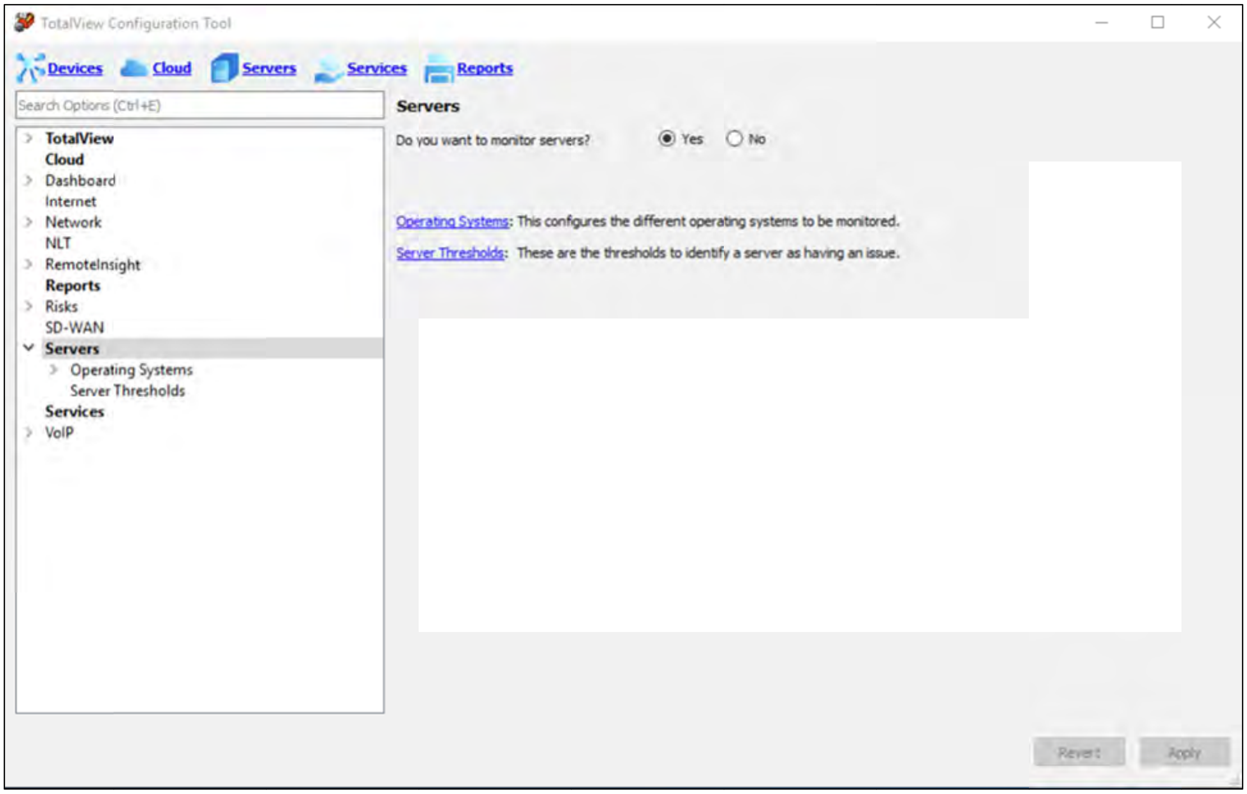
Latency threshold: 0

Loss threshold: 0

☐ Route change

Servers and Operating Systems

Select **Servers** from the left-hand menu. This section is to configure the different operating systems and to set server thresholds for identifying issues.



Servers

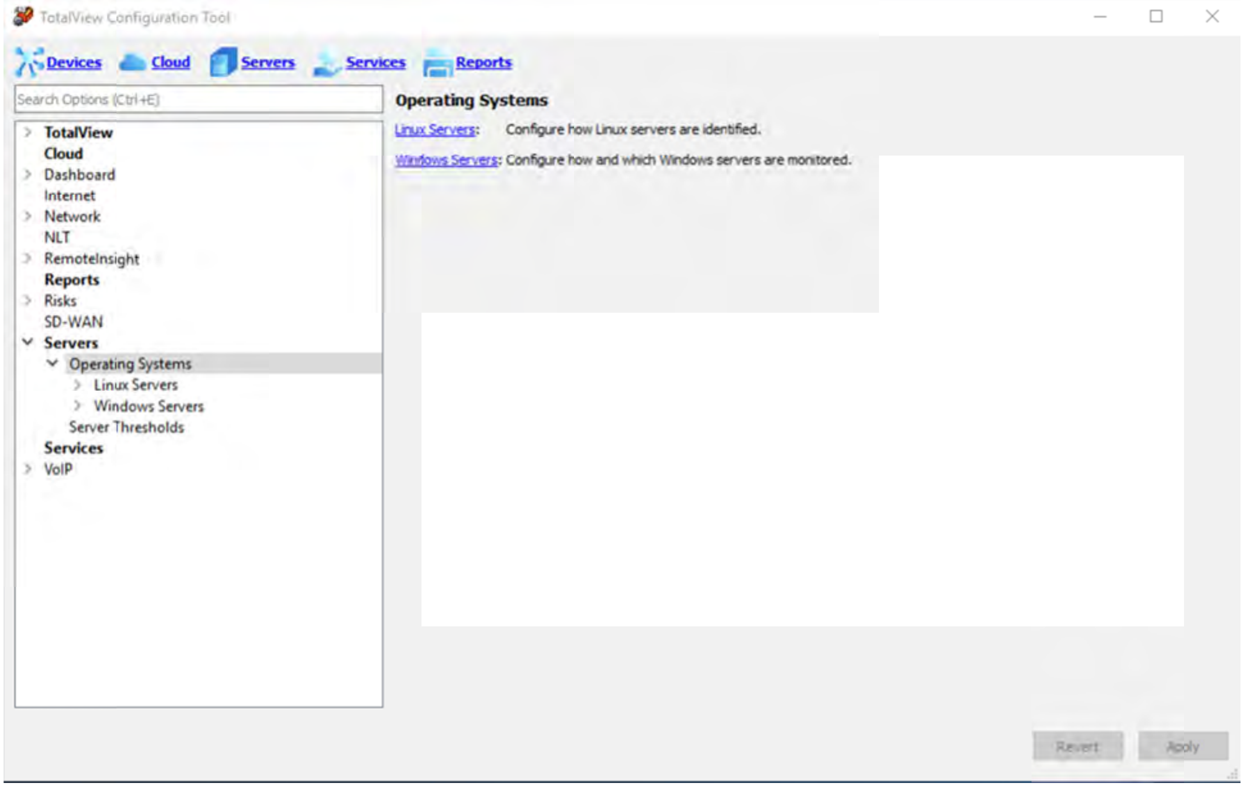
Do you want to monitor servers? ● Yes ○ No

Operating Systems: This configures the different operating systems to be monitored.

Server Thresholds: These are the thresholds to identify a server as having an issue.

Do you want to monitor servers? Select **Yes** or **No**.

The **Operating Systems** section links to Linux and Windows.



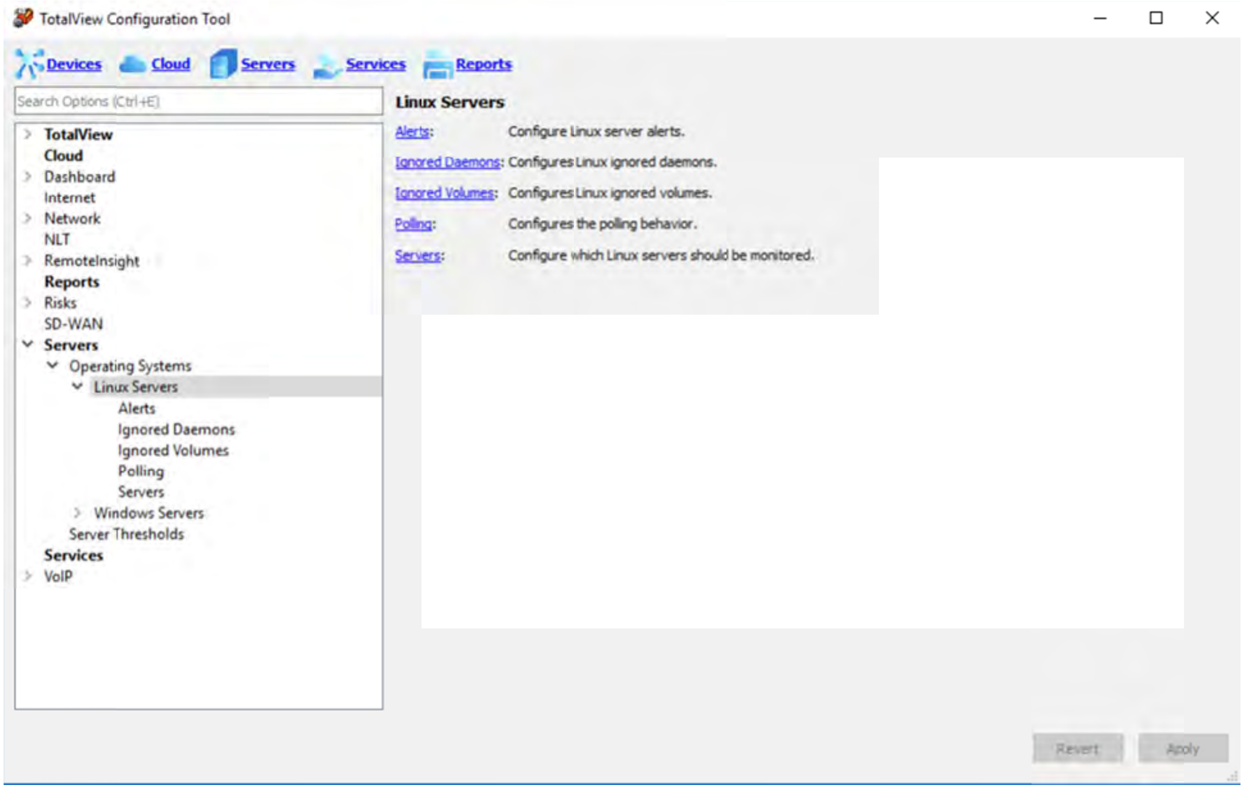
Operating Systems

Linux Servers: Configure how Linux servers are identified.

Windows Servers: Configure how and which Windows servers are monitored.

Linux Servers Monitoring

Navigate to the **Linux Servers** section from the left-hand menu. There are options to configure alerts, ignore Daemons, ignore volumes, polling and servers.



Linux Servers

Alerts: Configure Linux server alerts.

Ignored Daemons: Configures Linux ignored daemons.

Ignored Volumes: Configures Linux ignored volumes.

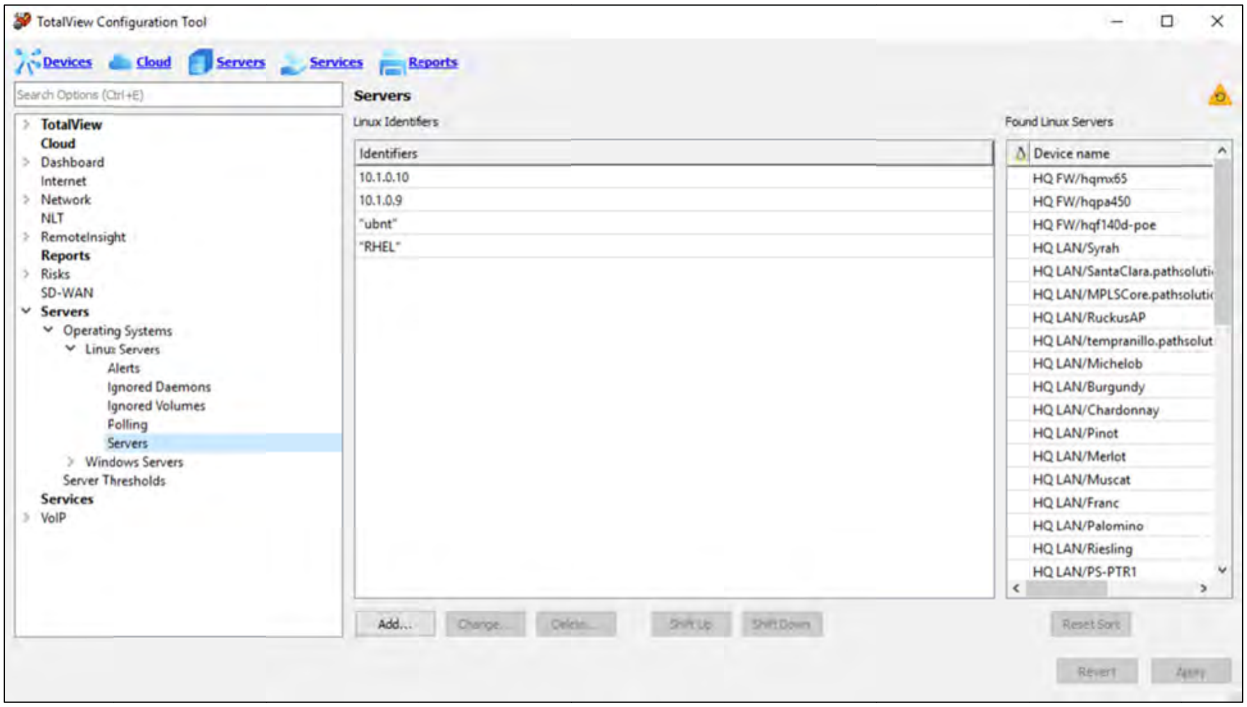
Polling: Configures the polling behavior.

Servers: Configure which Linux servers should be monitored.

How to Identify Linux Servers

TotalView will recognize anything with a system description for Linux, as well as any IPs you identify as Linux, by following the steps below. First, make sure the items you are going to monitor have already been added to the network devices (see the section under Network).

Navigate to **Servers > Operating Systems > Linux Servers > Servers** to designate the Linux Servers (identifiers) and build a list of Linux identifiers.



Servers

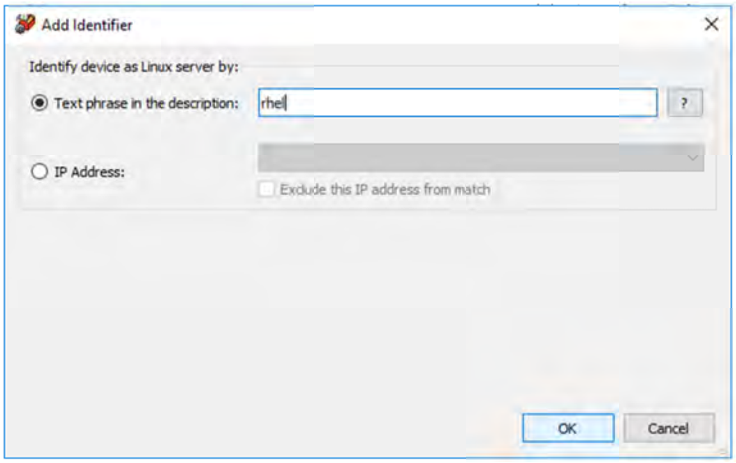
Linux Identifiers

Identifiers
10.1.0.10
10.1.0.9
"ubnt"
"RHEL"

Found Linux Servers

Device name
HQ FW/hqmx65
HQ FW/hqpa450
HQ FW/hqf140d-poe
HQ LAN/Syrah
HQ LAN/SantaClara.pathsoluti
HQ LAN/MPLSCore.pathsolutio
HQ LAN/RuckusAP
HQ LAN/tempranillo.pathsolut
HQ LAN/Michelob
HQ LAN/Burgundy
HQ LAN/Chardonnay
HQ LAN/Pinot
HQ LAN/Merlot
HQ LAN/Muscat
HQ LAN/Franc
HQ LAN/Palomino
HQ LAN/Riesling
HQ LAN/PS-PTR1

Under the middle column, select **Add**. The **Add Identifier** window will appear. In the **text phrase in the description** field for add the phrase of *rhel*, which stands for *Red Hat Enterprise License* (as a common identifier for a Linux server).



Identify device as Linux server by:

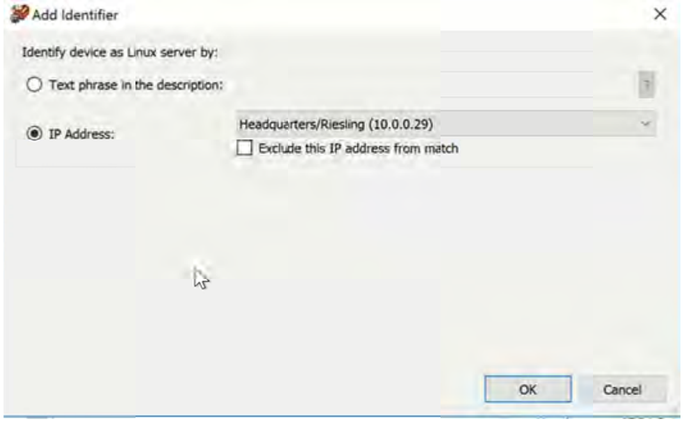
● Text phrase in the description: rhel

○ IP Address:

□ Exclude this IP address from match

Repeat this step and add the phrase of *Ubuntu* (another common identifier for a Linux server).

To enter specific Linux devices. select the **IP address** radio button, select devices from the drop-down menu, and then select **OK**.



Identify device as Linux server by:

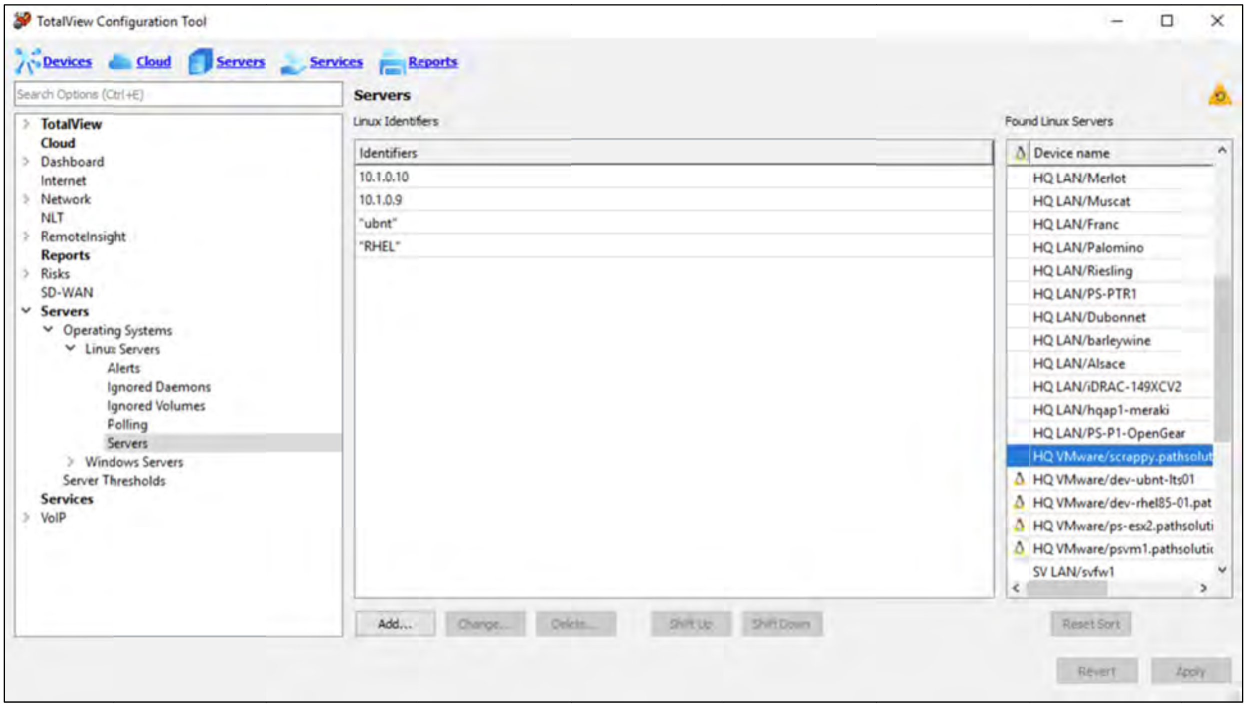
○ Text phrase in the description:

● IP Address: Headquarters/Riesling (10.0.0.29)

□ Exclude this IP address from match

Exclude devices by adding their IP addresses. Find the IP address, select the **Exclude this IP address from match** checkbox and select **OK**.

The Linux servers are identified in the list at the far right, with a small penguin. Edit the Linux identifiers, as needed using the **Add**, **Change** and **Delete** buttons.



Servers

Linux Identifiers

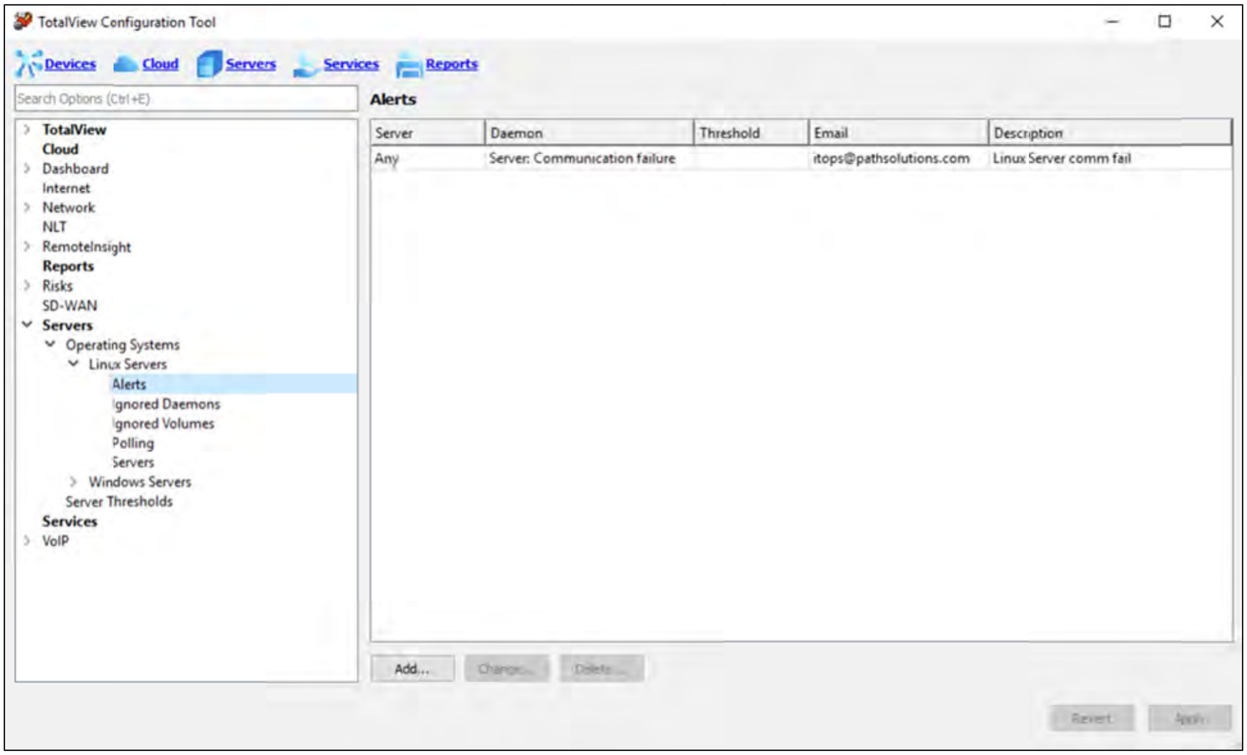
Identifiers
10.1.0.10
10.1.0.9
"ubnt"
"RHEL"

Found Linux Servers

	Device name
	HQ LAN/Merlot
	HQ LAN/Muscat
	HQ LAN/Franc
	HQ LAN/Palomino
	HQ LAN/Riesling
	HQ LAN/PS-PTR1
	HQ LAN/Dubonnet
	HQ LAN/barleywine
	HQ LAN/Alsace
	HQ LAN/iDRAC-149XCV2
	HQ LAN/hqap1-meraki
	HQ LAN/PS-P1-OpenGear
	HQ VMware/scrappy.pathsolut
🐧	HQ VMware/dev-ubnt-lts01
🐧	HQ VMware/dev-rhel85-01.pat
🐧	HQ VMware/ps-esx2.pathsoluti
🐧	HQ VMware/psvm1.pathsolutic
	SV LAN/svfw1

Linux - Alerts

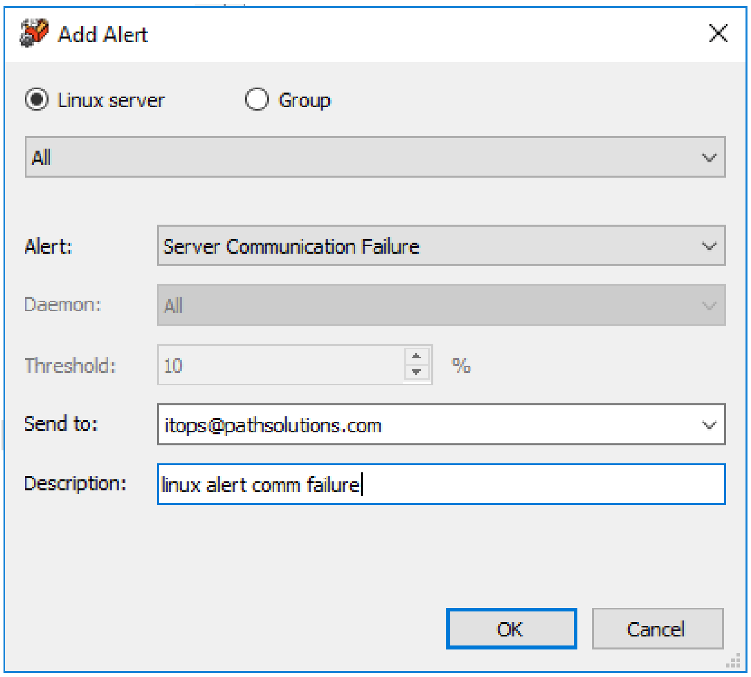
Go to the **Linux Servers > Alerts** section to set Linux alerts, the thresholds that trigger alerts, and the email recipients.



Alerts

Server	Daemon	Threshold	Email	Description
Any	Server: Communication failure		itops@pathsolutions.com	Linux Server comm fail

Use the **Add** and **Change** buttons to modify the alerts.



● Linux server ○ Group

All

Alert: Server Communication Failure

Daemon: All

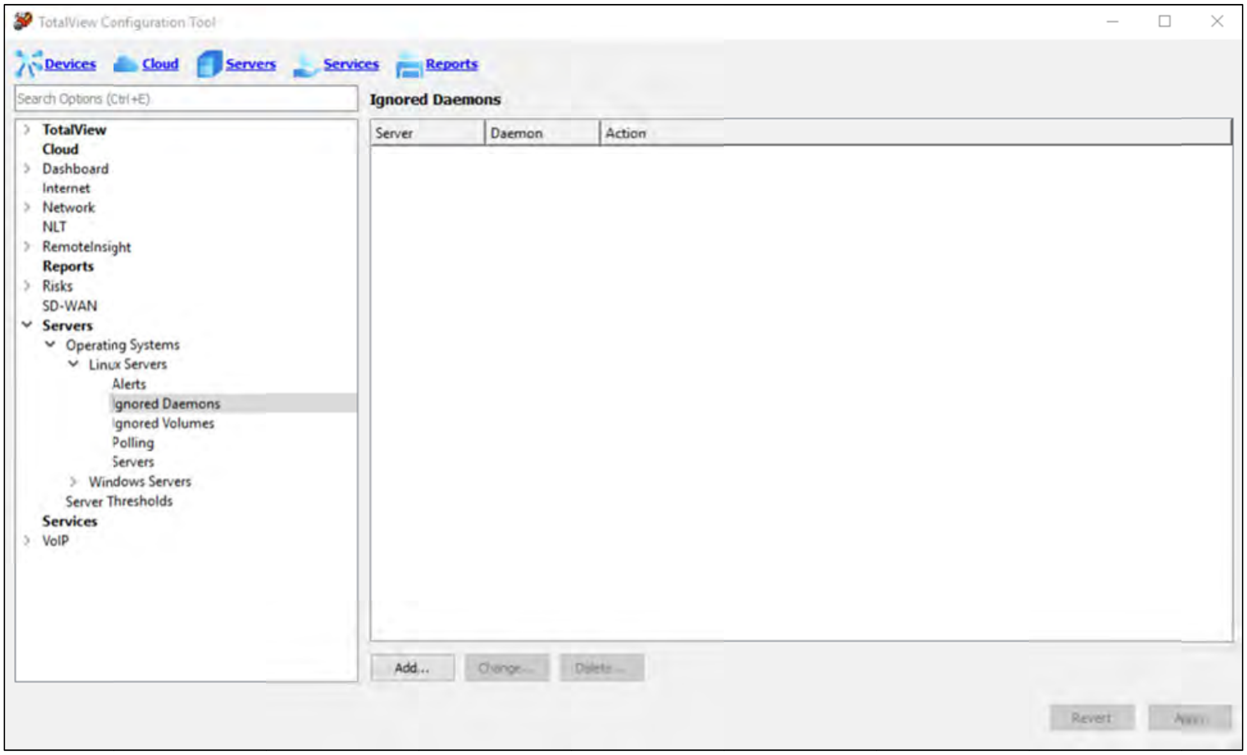
Threshold: 10 %

Send to: itops@pathsolutions.com

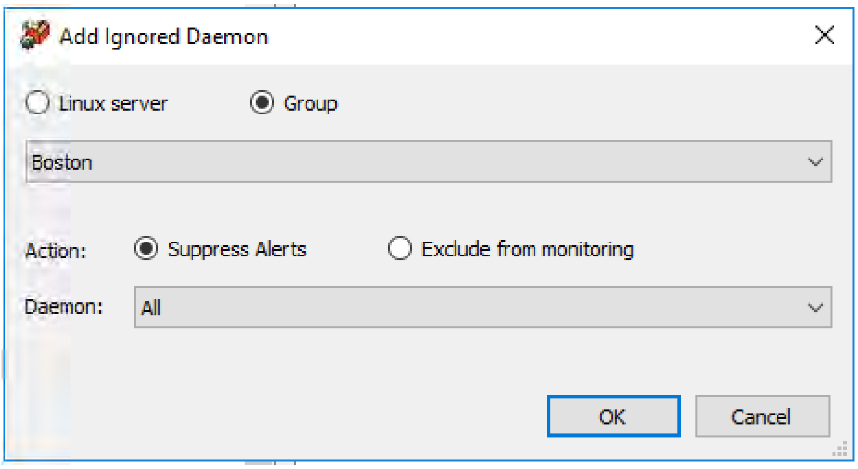
Description: linux alert comm failure

Linux - Ignored Daemons

Go to the **Linux Servers > Ignored Daemons** section to identify the Ignored Daemons.



Use the **Add** and **Change** buttons to edit the list of ignored Daemons, and whether to suppress alerts or exclude each one from monitoring altogether:



Add Ignored Daemon

○ Linux server ● Group

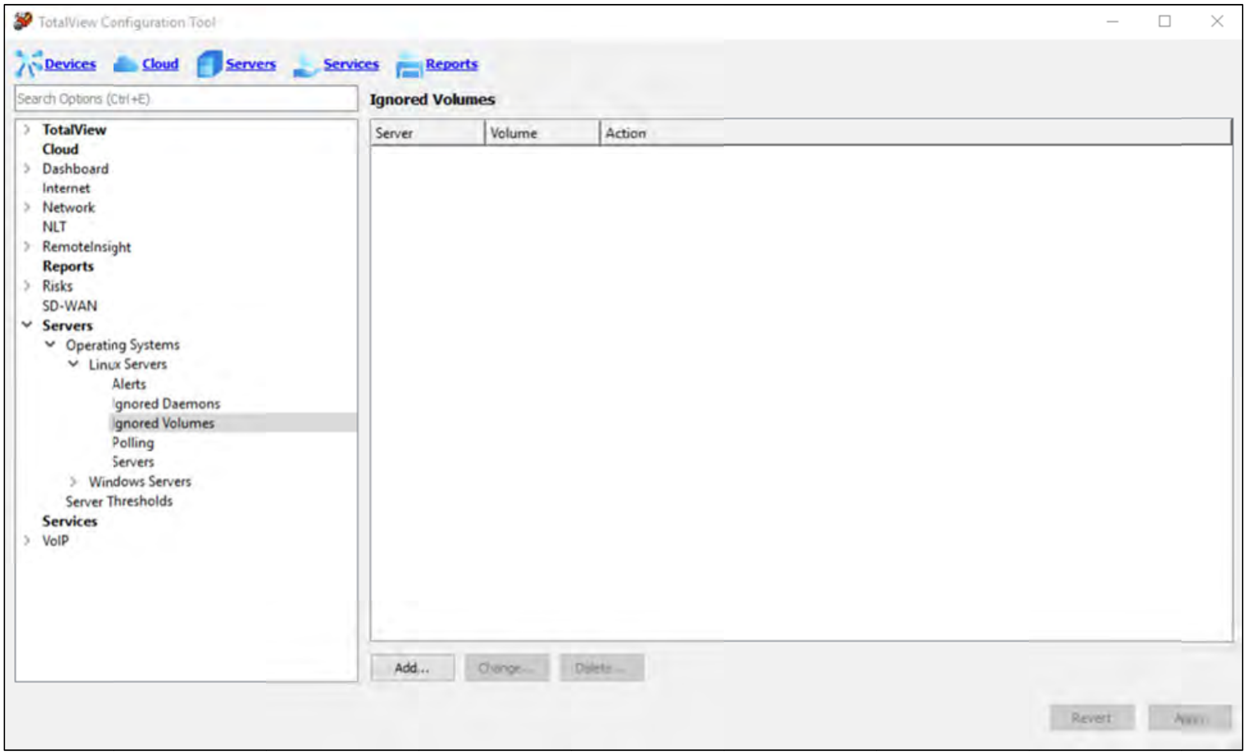
Boston

Action: ● Suppress Alerts ○ Exclude from monitoring

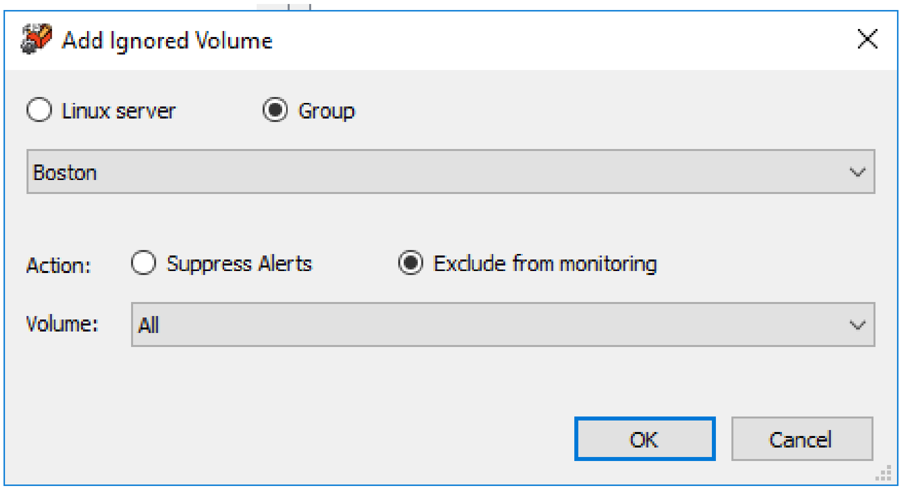
Daemon: All

Linux - Ignored Volumes

Go to the Linux **Servers > Ignored Volumes** section to identify the Linux Ignored Volumes.



Use the **Add** and **Change** buttons to edit the list of ignored Volumes and to suppress alerts or exclude each one monitoring them.



○ Linux server ● Group

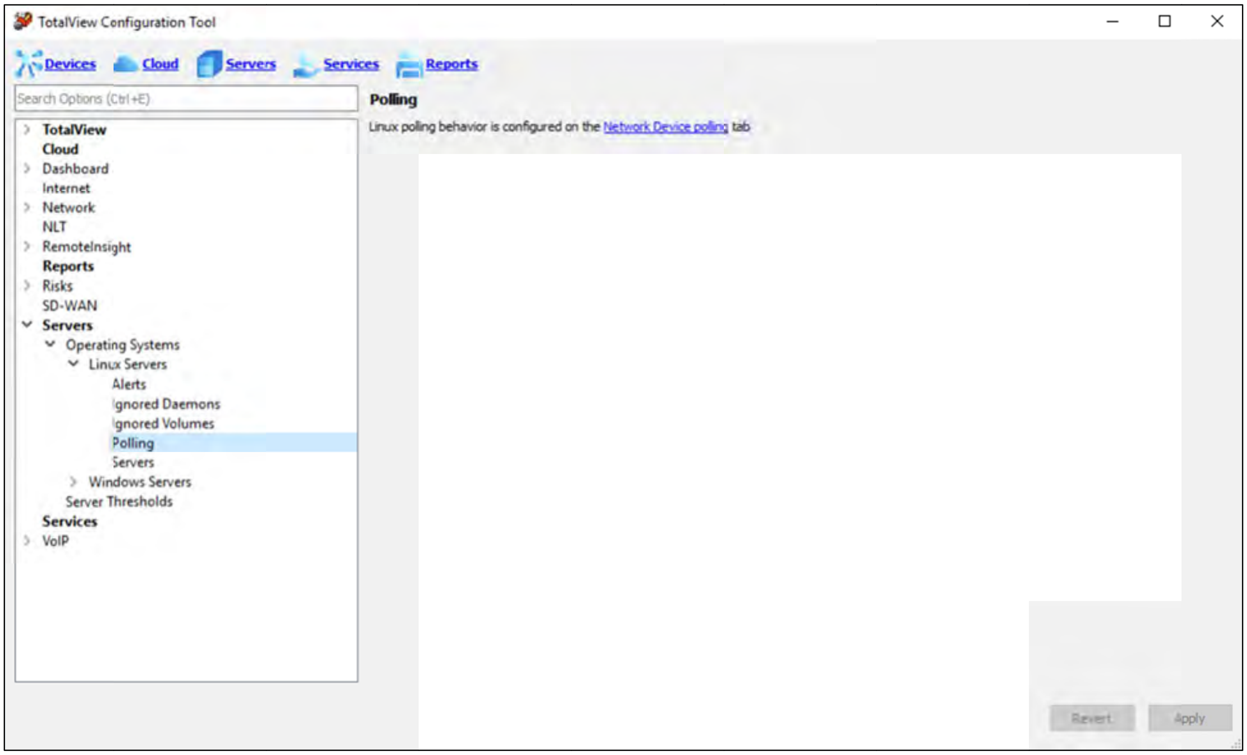
Boston

Action: ○ Suppress Alerts ● Exclude from monitoring

Volume: All

Linux - Polling

The **Linux Server > Polling** section, states that polling is configured on the **Network Device Polling** tab and provides a link. Set up polling there.

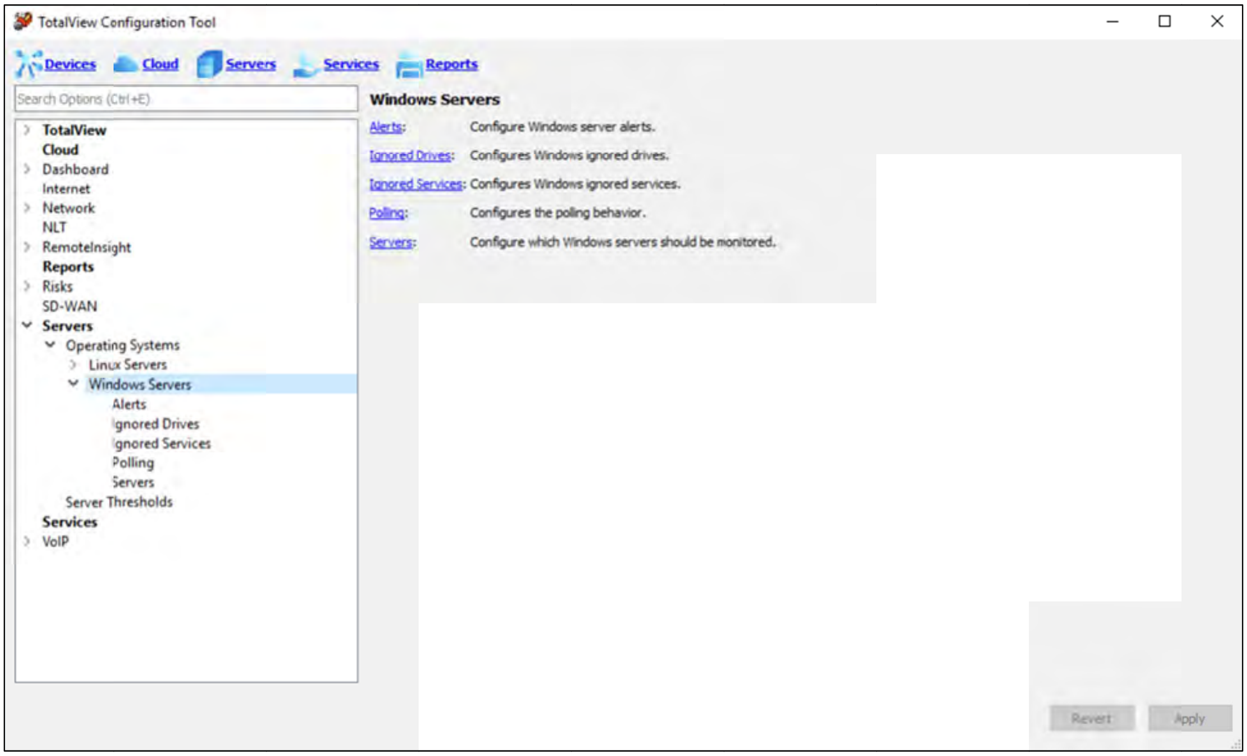


Polling

Linux polling behavior is configured on the Network Device polling tab

Windows Servers

Go to the **Servers > Operating Systems > Windows Servers** section. You will see the options to configure Window Server alerts, ignore drives, ignore services, polling and servers.



Windows Servers

Alerts: Configure Windows server alerts.

Ignored Drives: Configures Windows ignored drives.

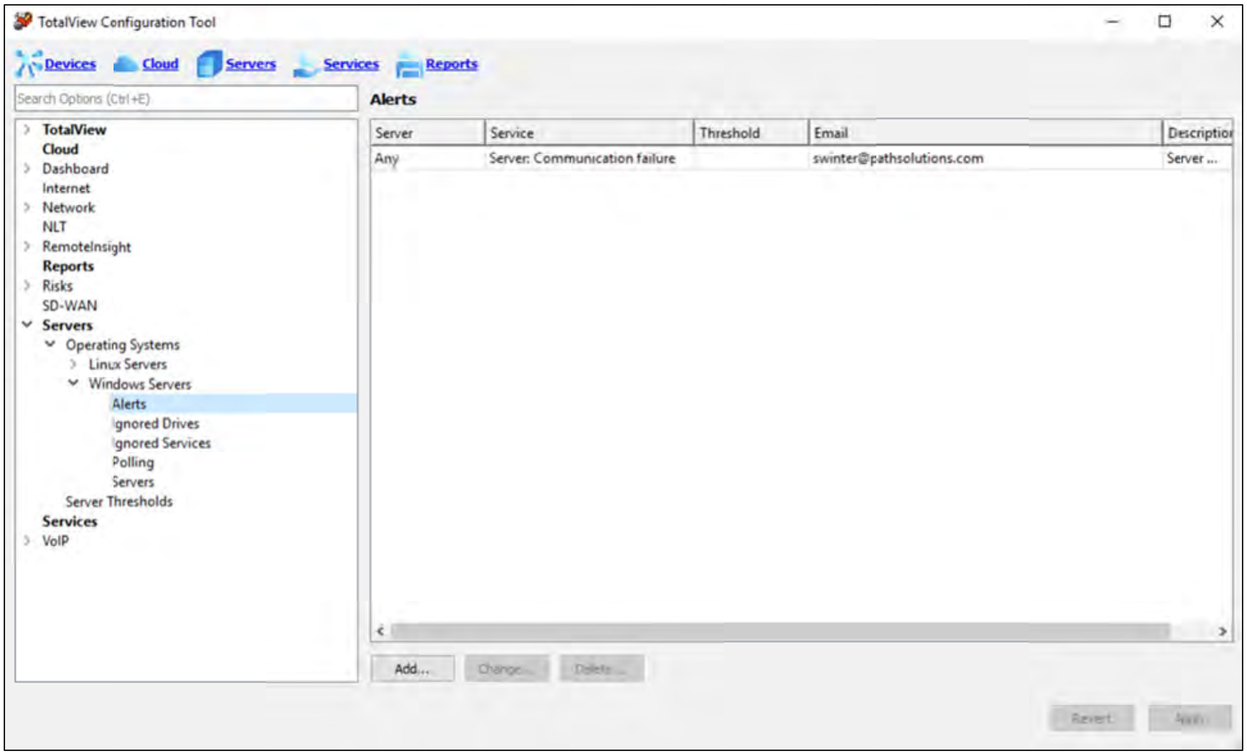
Ignored Services: Configures Windows ignored services.

Polling: Configures the polling behavior.

Servers: Configure which Windows servers should be monitored.

Windows - Alerts

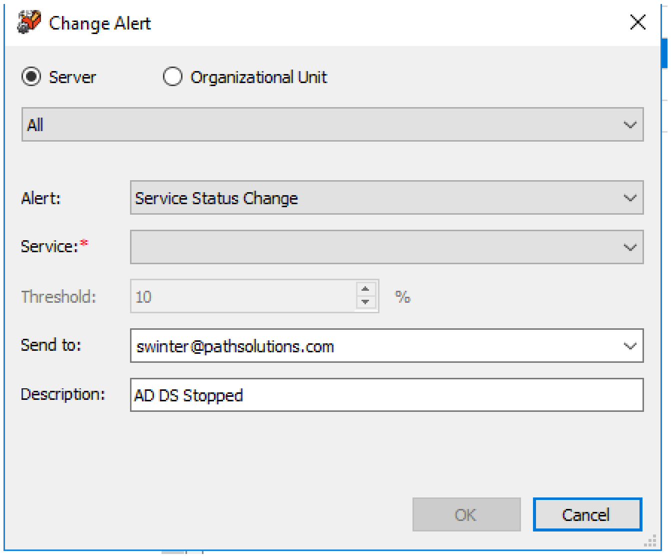
Go to **Windows Servers > Alerts** section to set Windows alerts, the thresholds that trigger alerts, and the email recipients.



Alerts

Server	Service	Threshold	Email	Descriptio
Any	Server: Communication failure		swinter@pathsolutions.com	Server ...

Use the **Add**, **Change**, and **Delete** buttons to set up Window Server alerts and designate the email where the alerts will go to:



● Server ○ Organizational Unit

All

Alert: Service Status Change

Service:*

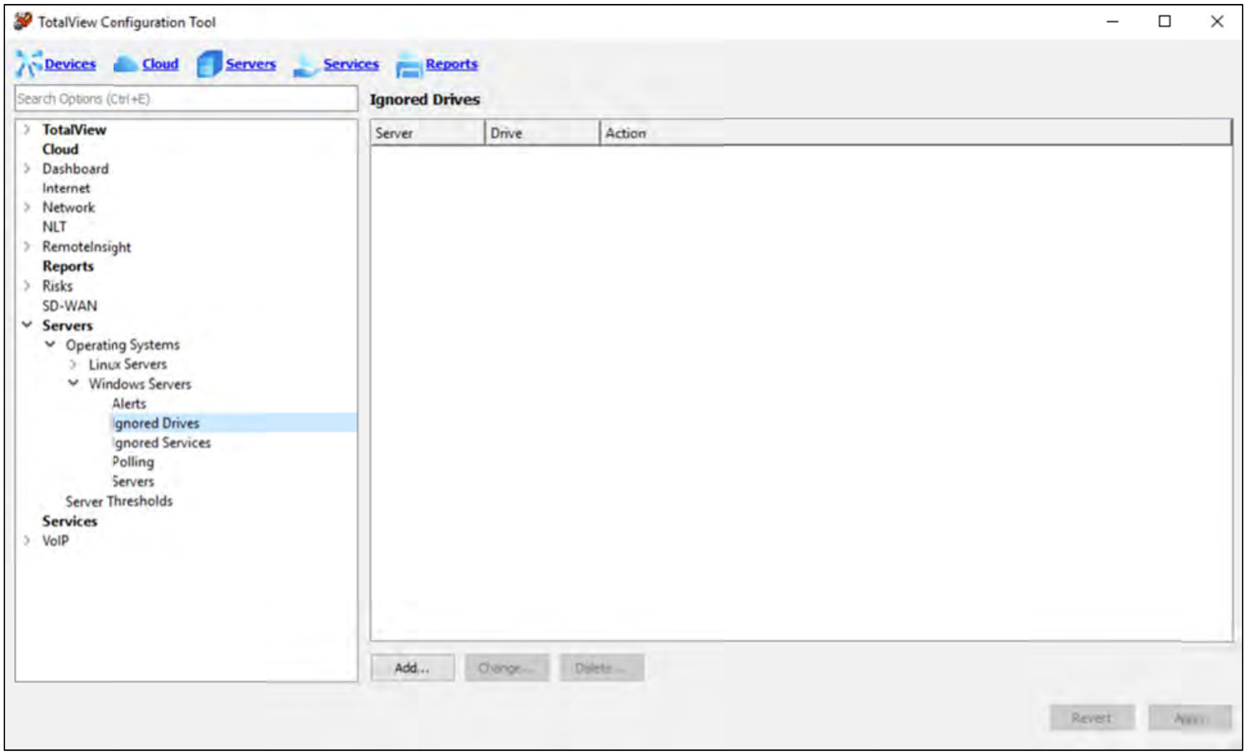
Threshold: 10 %

Send to: swinter@pathsolutions.com

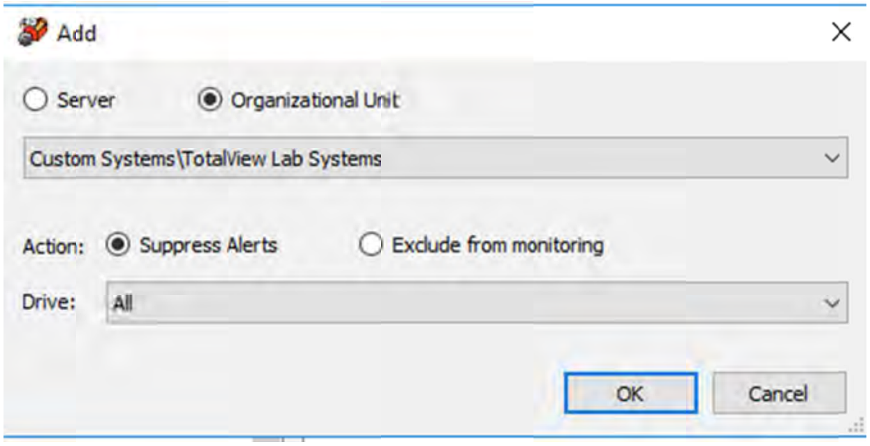
Description: AD DS Stopped

Windows - Ignored Drives

Go to the **Windows > Ignored Drives** section to identify the Windows Volumes to ignore.



Use the **Add** and **Change** buttons to modify the Windows Drives on the **Ignored Drives** list and to suppress alerts or exclude each one from monitoring altogether.


Add

○ Server ● Organizational Unit

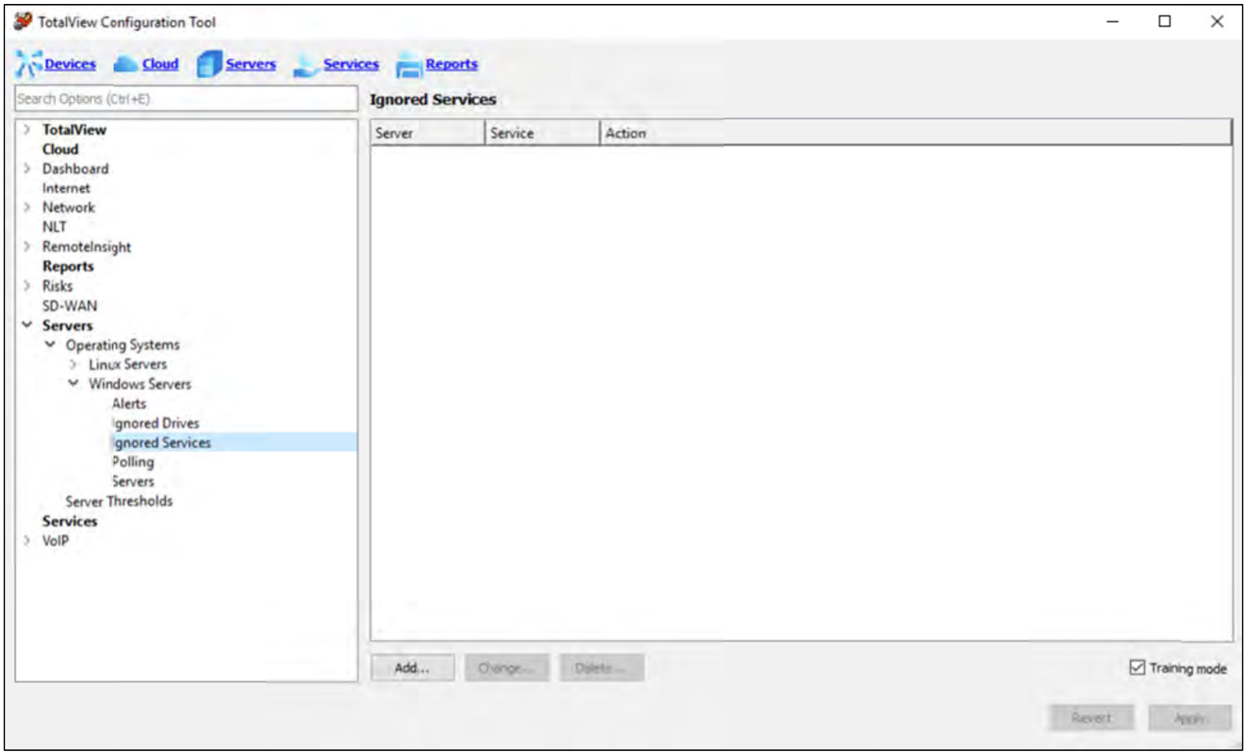
Custom Systems\TotalView Lab Systems

Action: ● Suppress Alerts ○ Exclude from monitoring

Drive: All

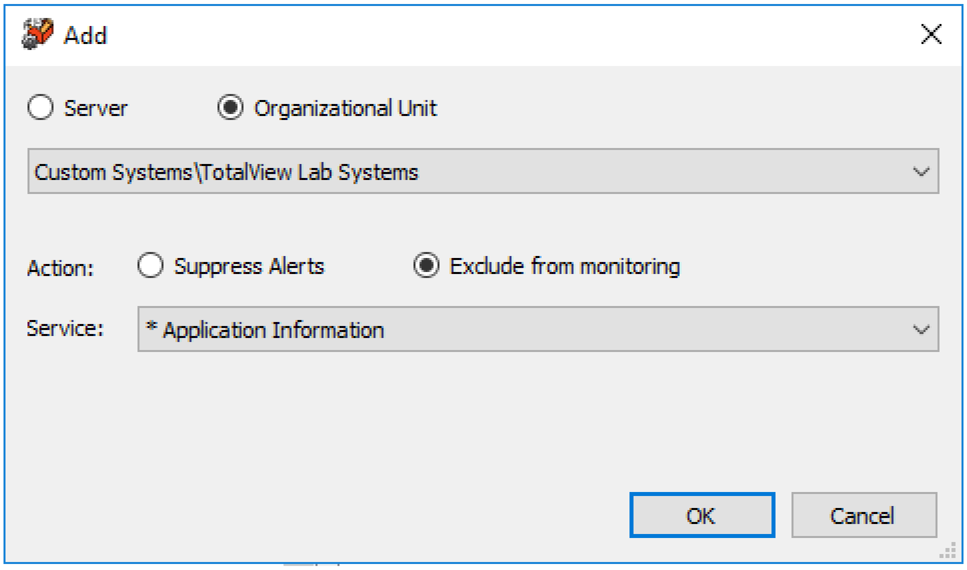
Windows - Ignored Services

Go to the **Windows > Ignored Services** section to identify the Windows Services to ignore.



☑ Training mode

Use the **Add** and **Change** buttons to modify the Windows Services on the Ignored Services list and to suppress alerts or exclude each one from monitoring altogether.



○ Server ● Organizational Unit

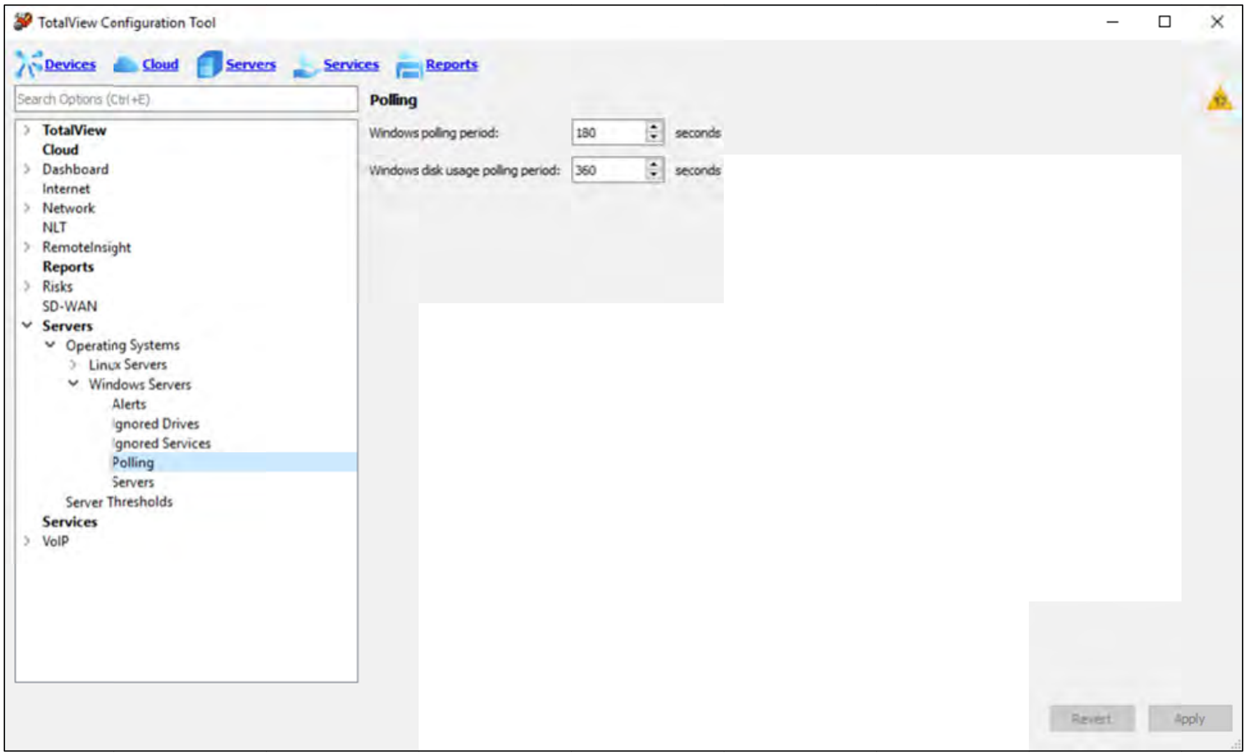
Custom Systems\TotalView Lab Systems

Action: ○ Suppress Alerts ● Exclude from monitoring

Service: * Application Information

Windows - Polling

The **Windows Server > Polling** section, lets you configure the windows per poll period in seconds, and the windows disks usage poll period in seconds. Enter values and either select **Apply** to save or **Revert** to cancel your changes.



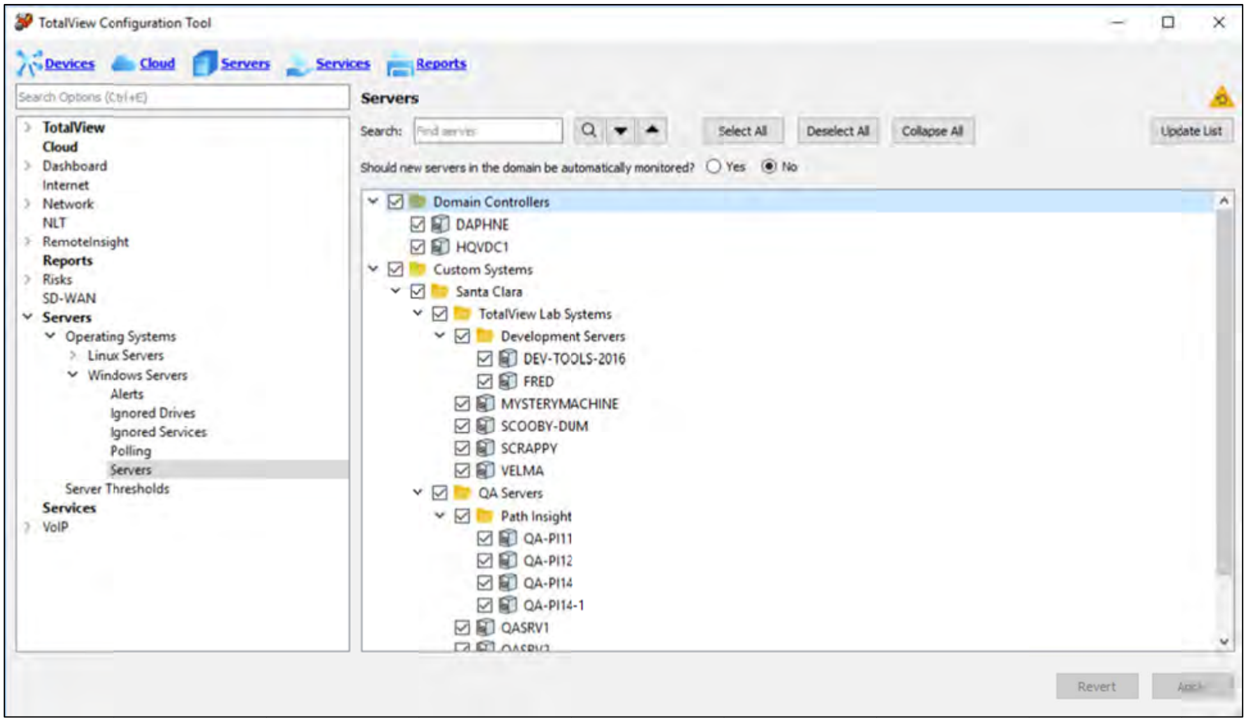
Polling

Windows polling period: 180 seconds

Windows disk usage polling period: 360 seconds

Servers

The **Windows Servers > Servers** section it will allow you to select or deselect servers that should be monitored.

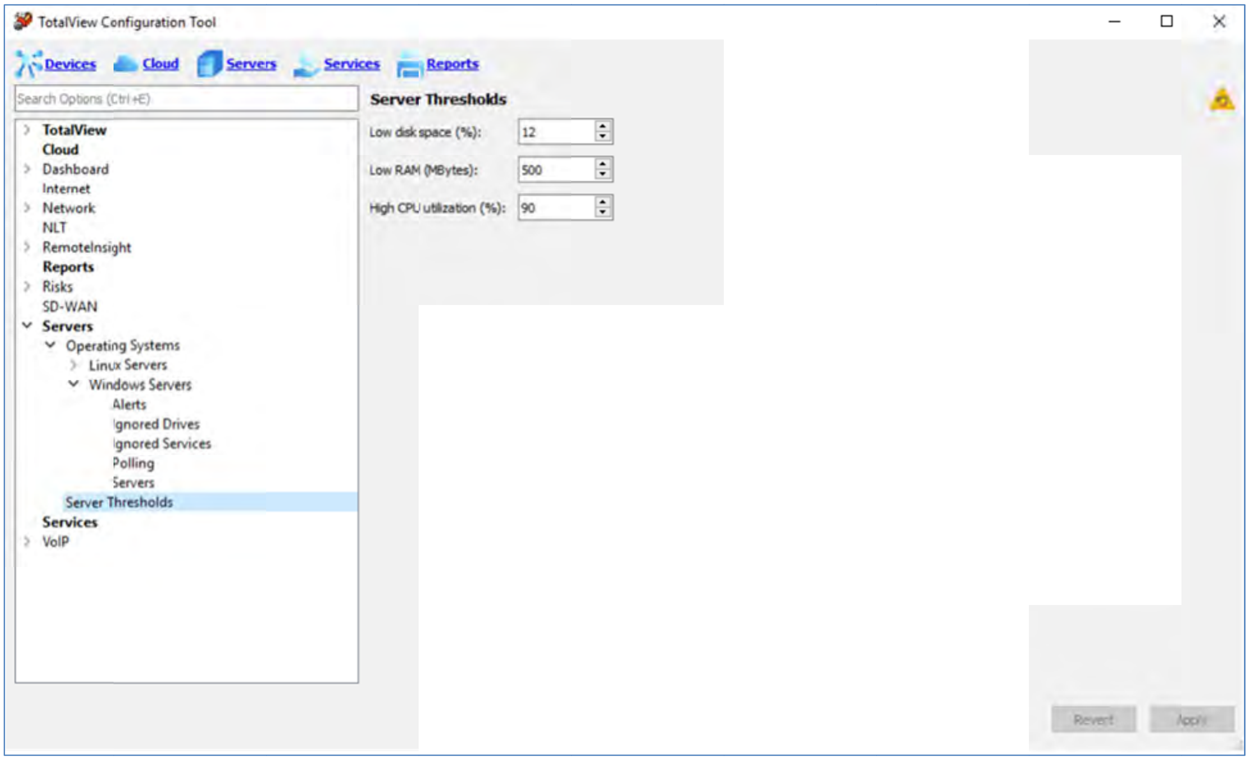


Should new servers in the domain be automatically monitored? ○ Yes ● No

- ☑ Domain Controllers
  - ☑ DAPHNE
  - ☑ HQVDC1
- ☑ Custom Systems
  - ☑ Santa Clara
    - ☑ TotalView Lab Systems
      - ☑ Development Servers
        - ☑ DEV-TOOLS-2016
        - ☑ FRED
      - ☑ MYSTERYMACHINE
      - ☑ SCOOBY-DUM
      - ☑ SCRAPPY
      - ☑ VELMA
    - ☑ QA Servers
      - ☑ Path Insight
        - ☑ QA-PI11
        - ☑ QA-PI12
        - ☑ QA-PI14
        - ☑ QA-PI14-1
      - ☑ QASRV1
      - ☑ QASRV2

Server Thresholds

Go to the **Server Thresholds** section to set server thresholds for Low disk space, Low RAM, and High CPU utilization.



Server Thresholds

Low disk space (%): 12

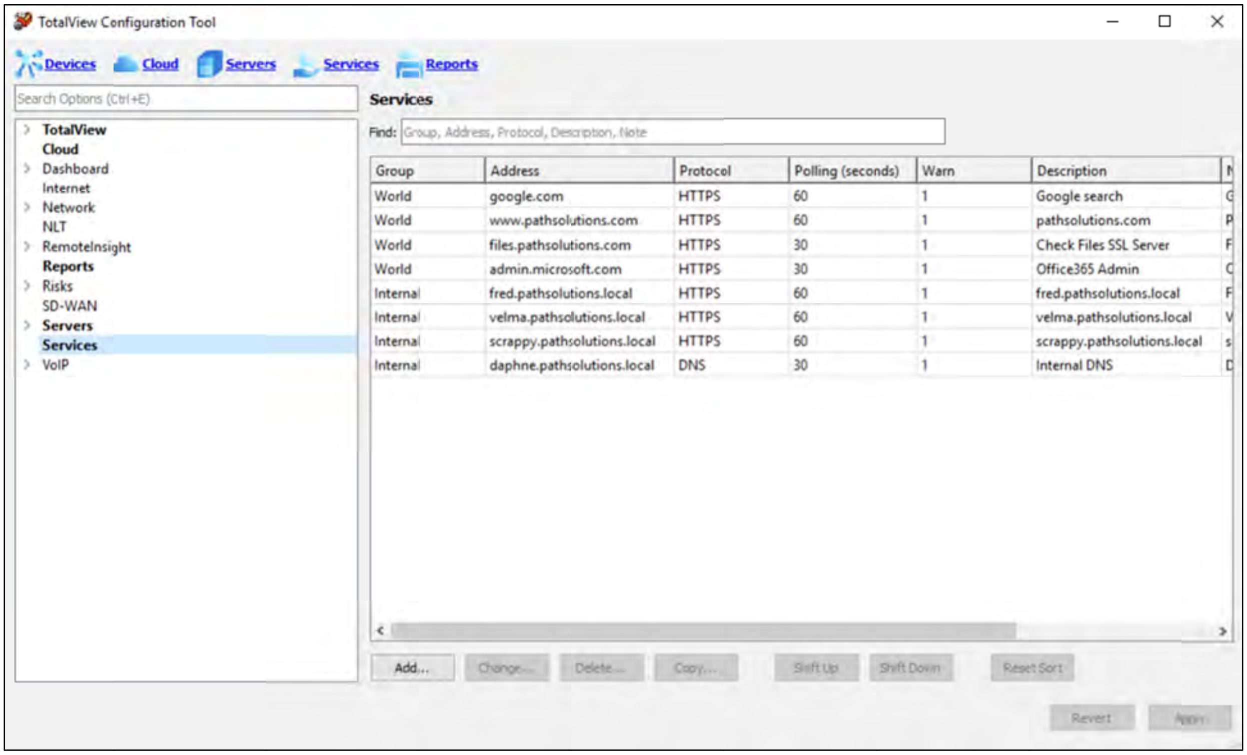
Low RAM (MBytes): 500

High CPU utilization (%): 90

Enter threshold values and then either select **Apply** to save or **Revert** to cancel your changes.

Services

Go to the **Services** section to configure the list of Services. Note there is a **Find** field at the top to filter the list. Find and filter services by group, address, protocol, description and by notes through this field.

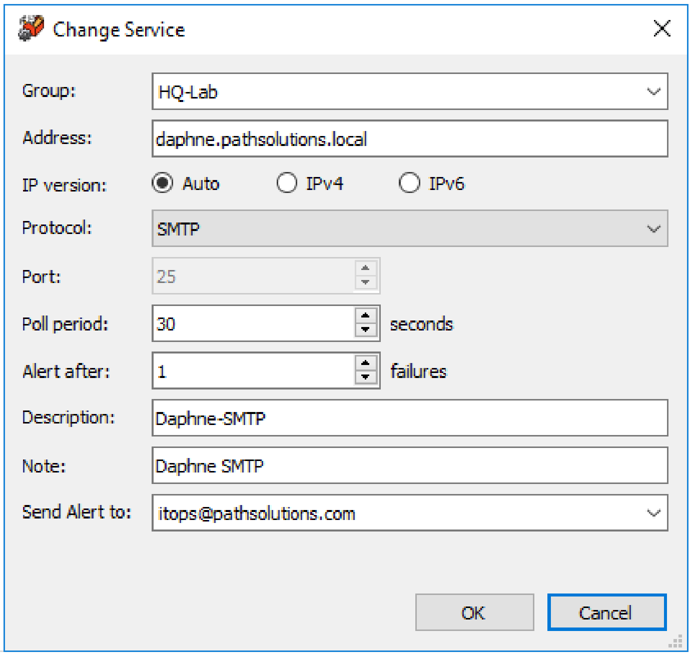


Services

Find: Group, Address, Protocol, Description, Note

Group	Address	Protocol	Polling (seconds)	Warn	Description	N
World	google.com	HTTPS	60	1	Google search	G
World	www.pathsolutions.com	HTTPS	60	1	pathsolutions.com	P
World	files.pathsolutions.com	HTTPS	30	1	Check Files SSL Server	F
World	admin.microsoft.com	HTTPS	30	1	Office365 Admin	O
Internal	fred.pathsolutions.local	HTTPS	60	1	fred.pathsolutions.local	F
Internal	velma.pathsolutions.local	HTTPS	60	1	velma.pathsolutions.local	V
Internal	scrappy.pathsolutions.local	HTTPS	60	1	scrappy.pathsolutions.local	s
Internal	daphne.pathsolutions.local	DNS	30	1	Internal DNS	D

Use the **Add** or **Change** buttons to modify services on the list. Fill out the information about the group, protocol, poll period, and email alerts in the **Change Service** window.



Group: HQ-Lab

Address: daphne.pathsolutions.local

IP version: ● Auto ○ IPv4 ○ IPv6

Protocol: SMTP

Port: 25

Poll period: 30 seconds

Alert after: 1 failures

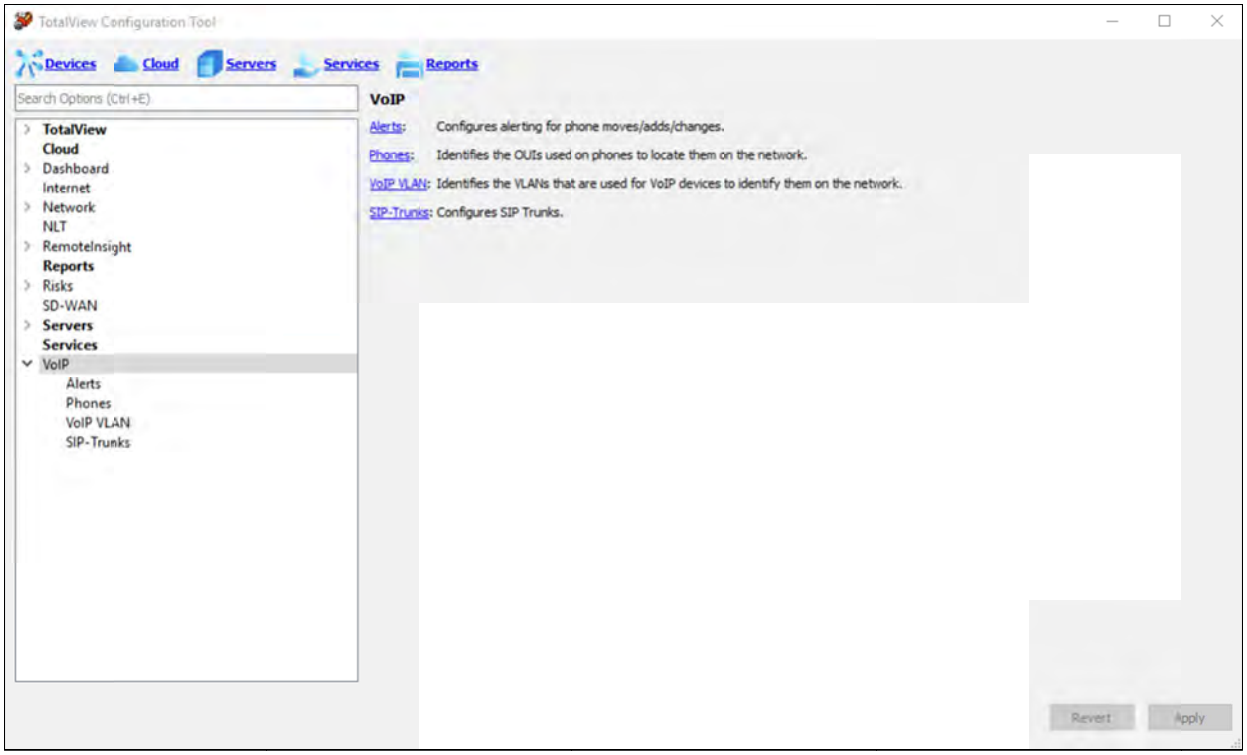
Description: Daphne-SMTP

Note: Daphne SMTP

Send Alert to: itops@pathsolutions.com

VoIP

This section will appear if you have the VoIP module license. To configure VoIP/Telecom settings, select **VoIP** in the left-hand menu. You will see options to configure **Alerts**, **Phones, VoIP VLAN**, and **SIP-Trunks**.



VoIP

Alerts: Configures alerting for phone moves/adds/changes.

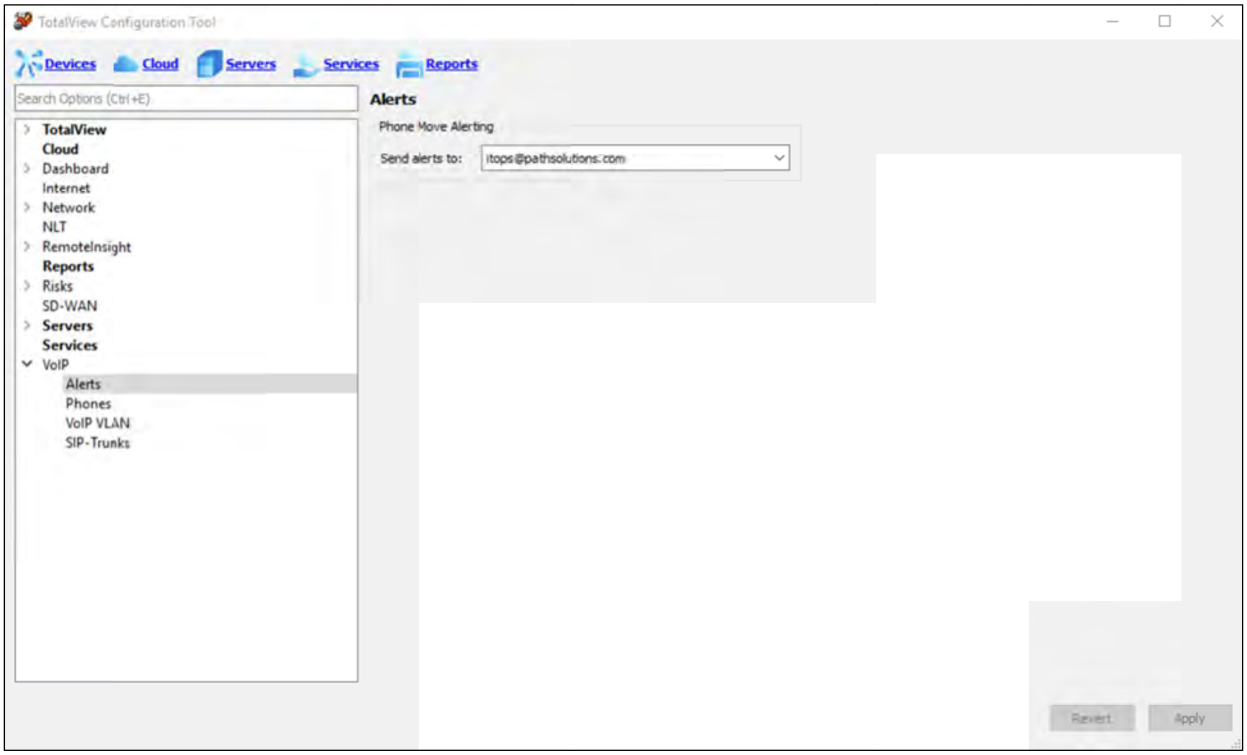
Phones: Identifies the OUIs used on phones to locate them on the network.

VoIP VLAN: Identifies the VLANs that are used for VoIP devices to identify them on the network.

SIP-Trunks: Configures SIP Trunks.

VoIP Alerts

On the **VoIP > Alerts** section, chose where to send email alerts for **Phone Move Alerting**.



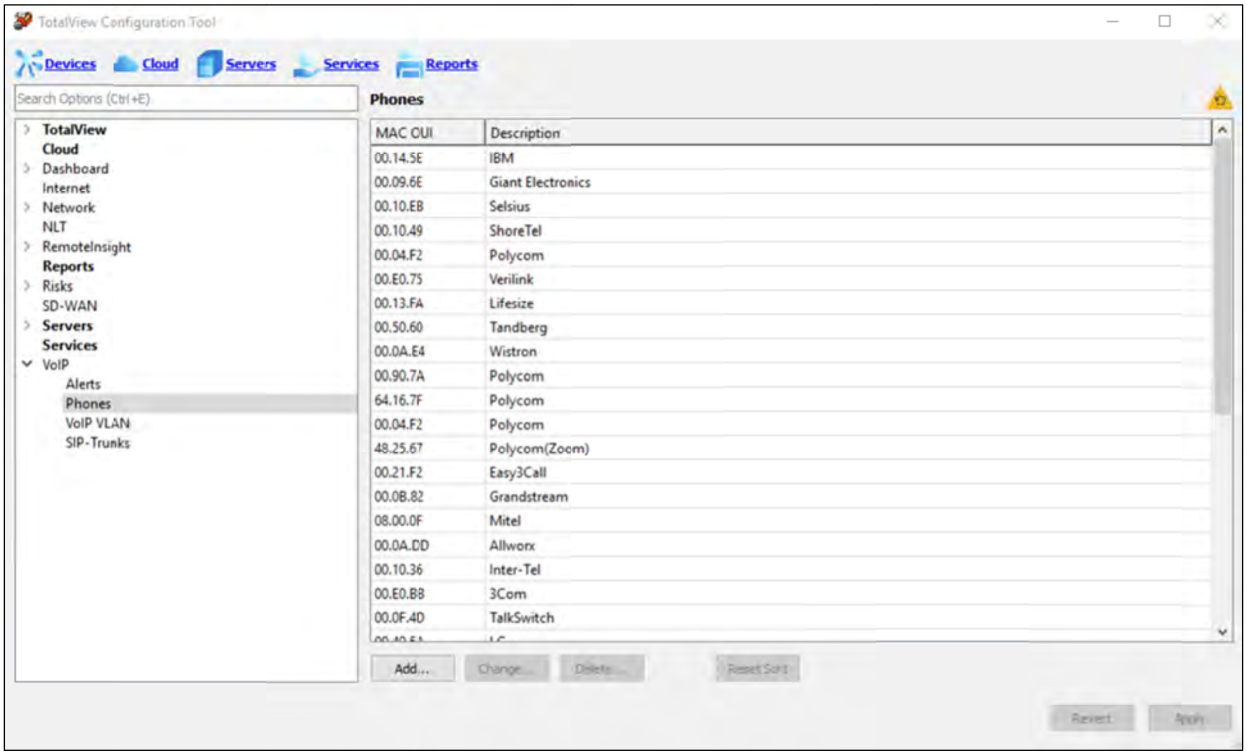
Alerts

Phone Move Alerting

Send alerts to: itops@pathsolutions.com

Phones

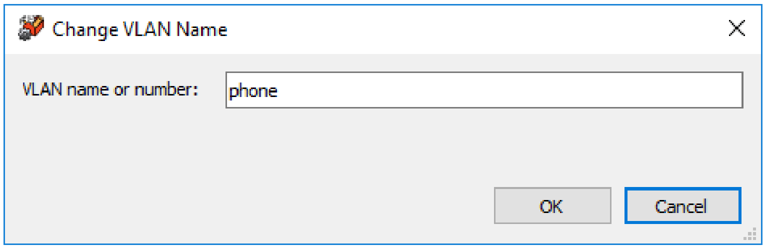
In the **VoIP > Phones** section, enter the VLAN name and/or number.



Phones

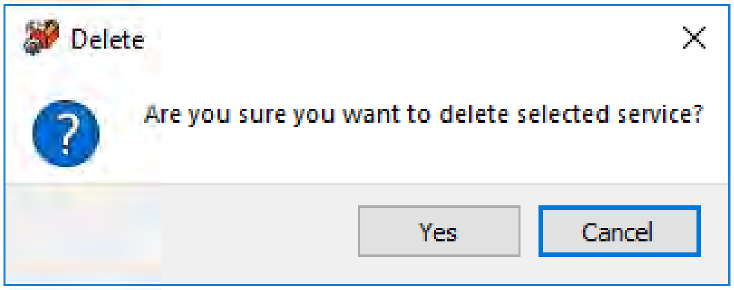
MAC OUI	Description
00.14.5E	IBM
00.09.6E	Giant Electronics
00.10.EB	Selsius
00.10.49	ShoreTel
00.04.F2	Polycom
00.E0.75	Verilink
00.13.FA	Lifesize
00.50.60	Tandberg
00.0A.E4	Wistron
00.90.7A	Polycom
64.16.7F	Polycom
00.04.F2	Polycom
48.25.67	Polycom(Zoom)
00.21.F2	Easy3Call
00.0B.82	Grandstream
08.00.0F	Mitel
00.0A.DD	Allworx
00.10.36	Inter-Tel
00.E0.BB	3Com
00.0F.4D	TalkSwitch

Use the **Add** and **Change** buttons to add and edit VLAN names or numbers.



VLAN name or number: phone

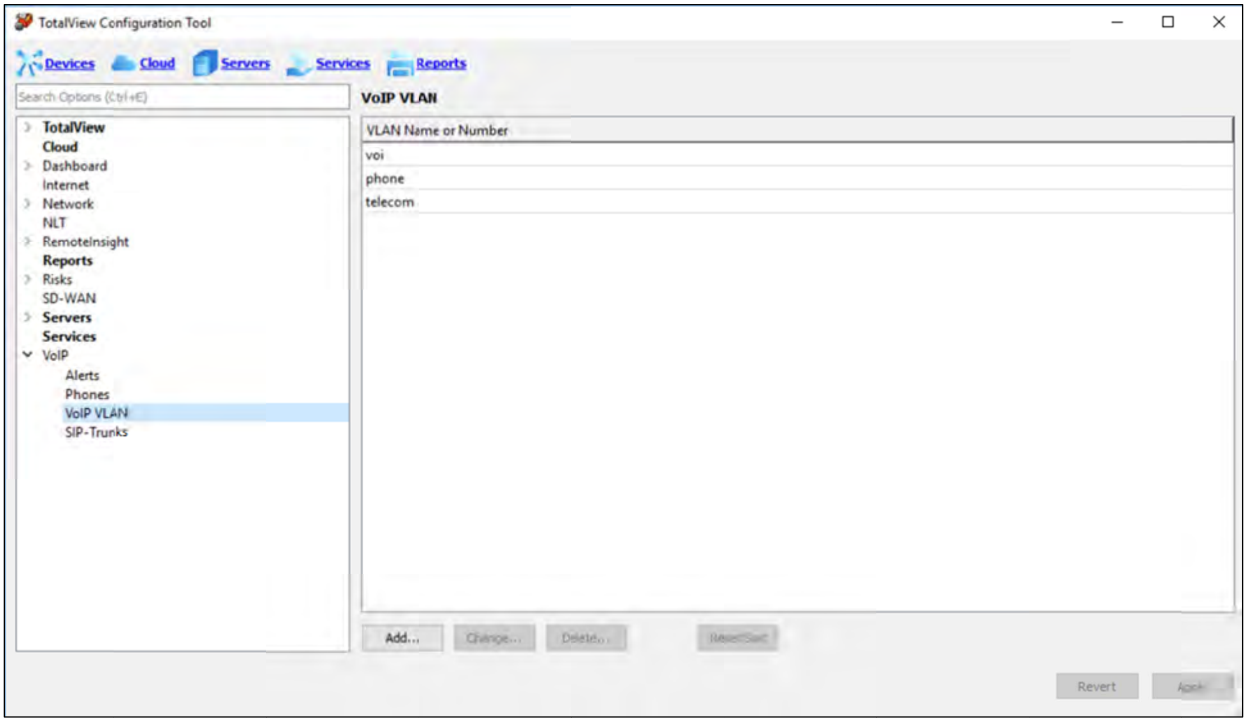
Use the delete button to delete one.



Are you sure you want to delete selected service?

VoIP VLAN

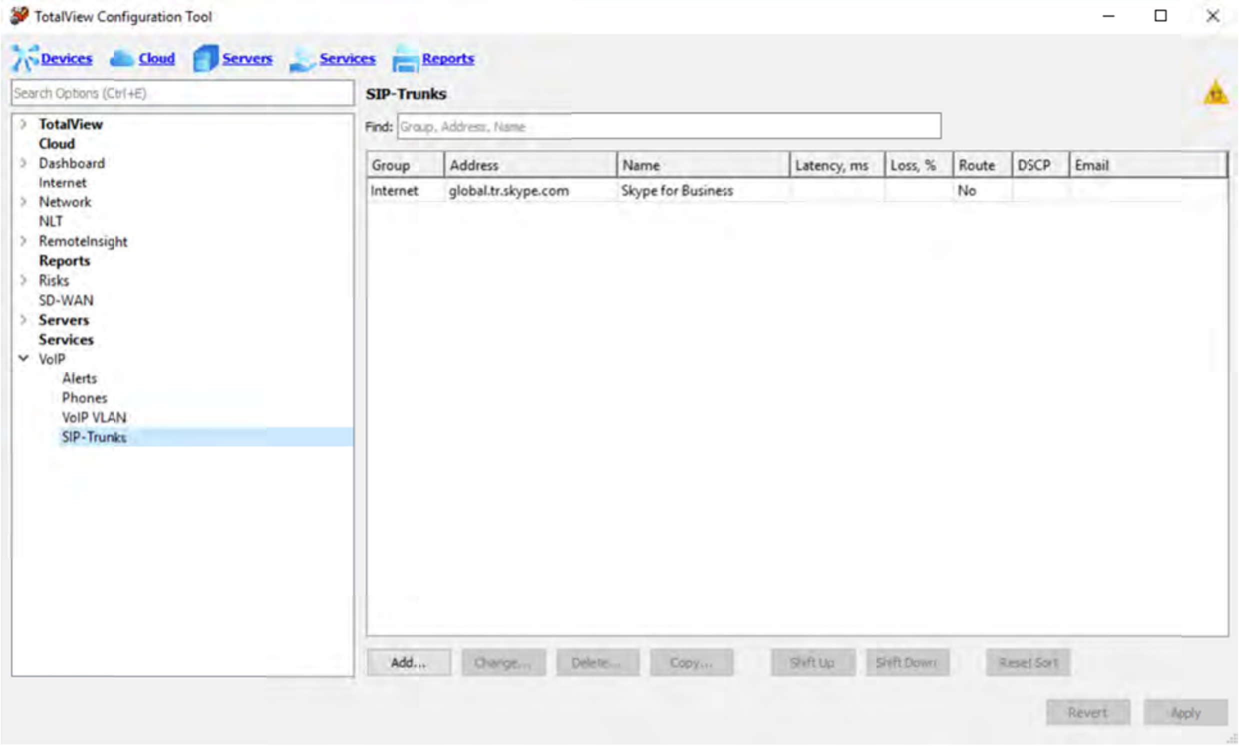
The VoIP VLAN section allows you to add, update, or delete a VLAN name or number.



VLAN Name or Number
voi
phone
telecom

SIP-Trunks

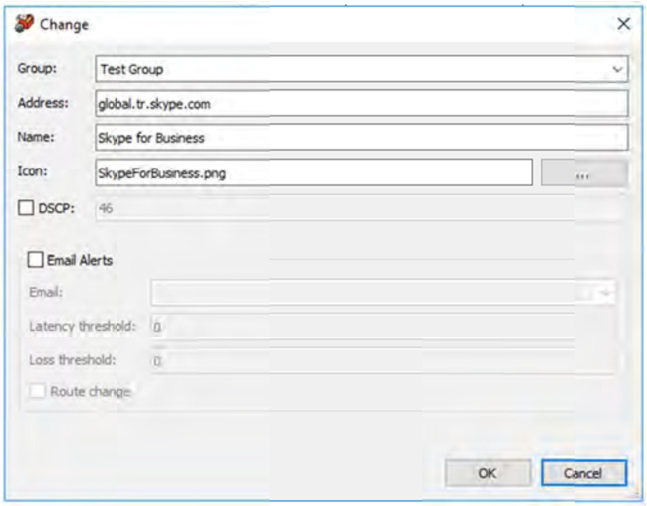
To configure SIP-Trunk interfaces, select **SIP-Trunks** from the left-hand menu.



Group	Address	Name	Latency, ms	Loss, %	Route	DSCP	Email
Internet	global.tr.skype.com	Skype for Business			No		

You can add, change, or delete any service by using the **Add**, **Change**, and **Delete** buttons and entering the group, address and name. Adding an **Icon** (a service picture) is optional.

When you add or change the devices, you can also setup email alerts for latency and loss thresholds, by checking the **Email Alerts** button and filling out those fields:



Change

Group: Test Group

Address: global.tr.skype.com

Name: Skype for Business

Icon: SkypeForBusiness.png

□ DSCP: 46

□ Email Alerts

Email:

Latency threshold: 0

Loss threshold: 0

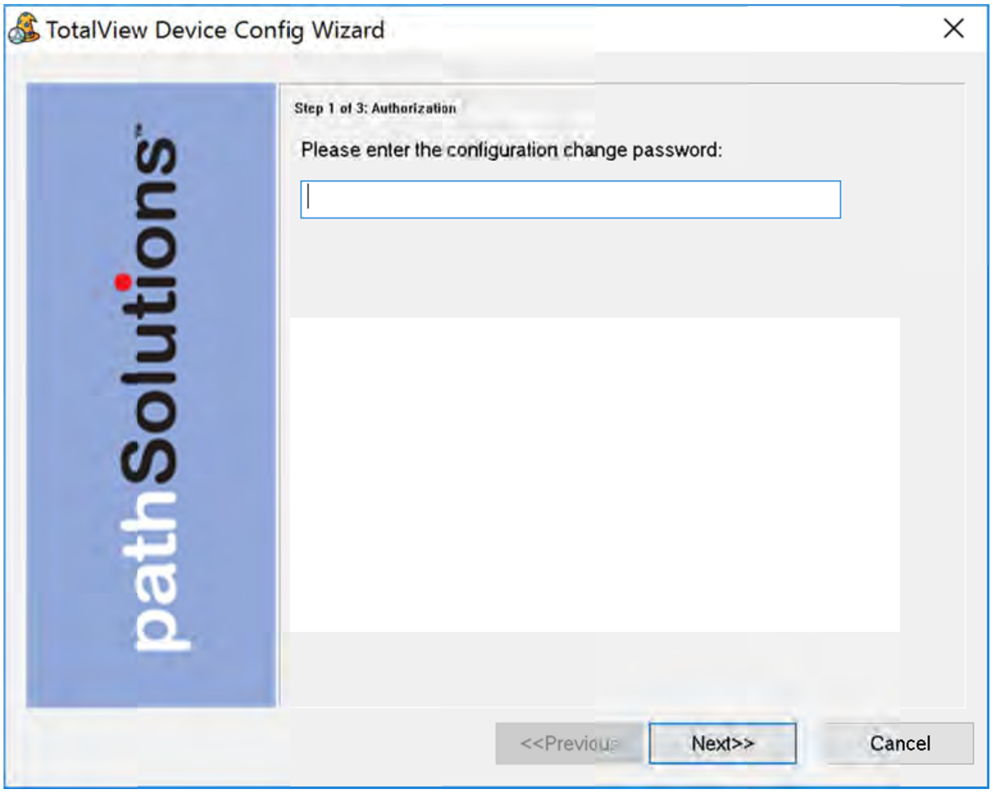
□ Route change

Using the Device Configuration Wizard

The Device Configuration Wizard is a 3-step wizard designed to make it quick and easy to change network equipment configurations on a large number of network devices, or extract operational information from multiple network devices.

The program can be launched on the server's console by selecting **Start**, choosing **PathSolutions > TotalView > TotalView Device Config Wizard**.

The wizard will launch and show you the first step. This step will ask you to enter the configuration change password. This password is set in the Config Tool on the Backup section.



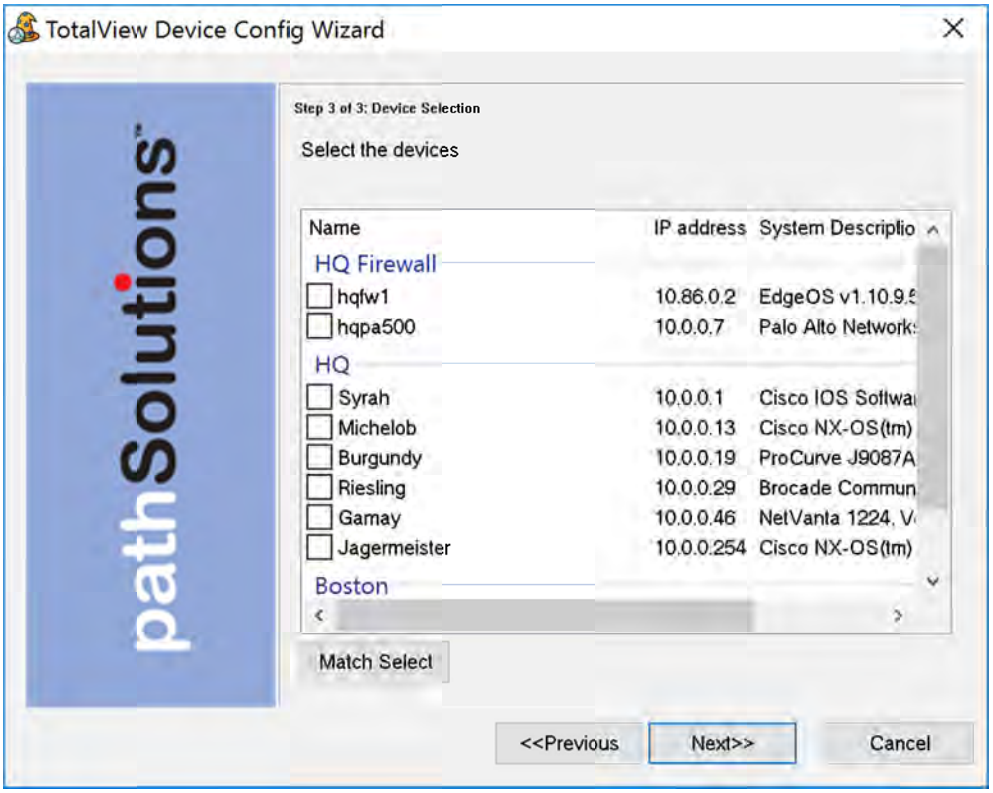
TotalView Device Config Wizard

Step 1 of 3: Authorization

Please enter the configuration change password:

Select **Next** to continue.

Step 2 will permit you to select devices. Check the appropriate device or devices that you want the configuration to apply to.

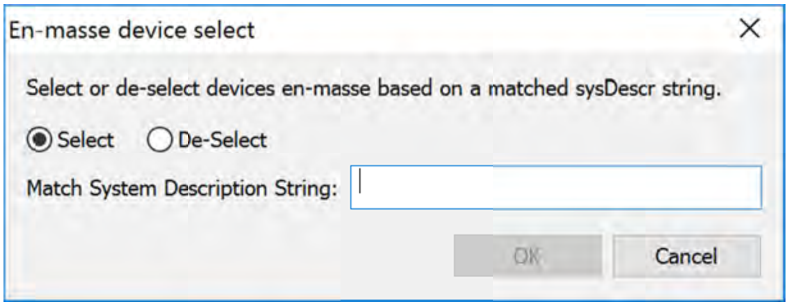


Step 3 of 3: Device Selection

Select the devices

Name	IP address	System Descriptio
HQ Firewall		
☐ hqfw1	10.86.0.2	EdgeOS v1.10.9.5
☐ hqpa500	10.0.0.7	Palo Alto Network:
HQ		
☐ Syrah	10.0.0.1	Cisco IOS Softwa
☐ Michelob	10.0.0.13	Cisco NX-OS(tm)
☐ Burgundy	10.0.0.19	ProCurve J9087A
☐ Riesling	10.0.0.29	Brocade Commun
☐ Gamay	10.0.0.46	NetVanta 1224, V
☐ Jagermeister	10.0.0.254	Cisco NX-OS(tm)
Boston		

If you want to do global selects, this can be done with the **Match Select** option. For example, you can select **Match Select** and choose all devices that have **Cisco** in the system description. Then you can do another match select and choose **De-select** to remove all references to Nexus. At this point, it will have all Cisco devices that are Not Nexus selected.

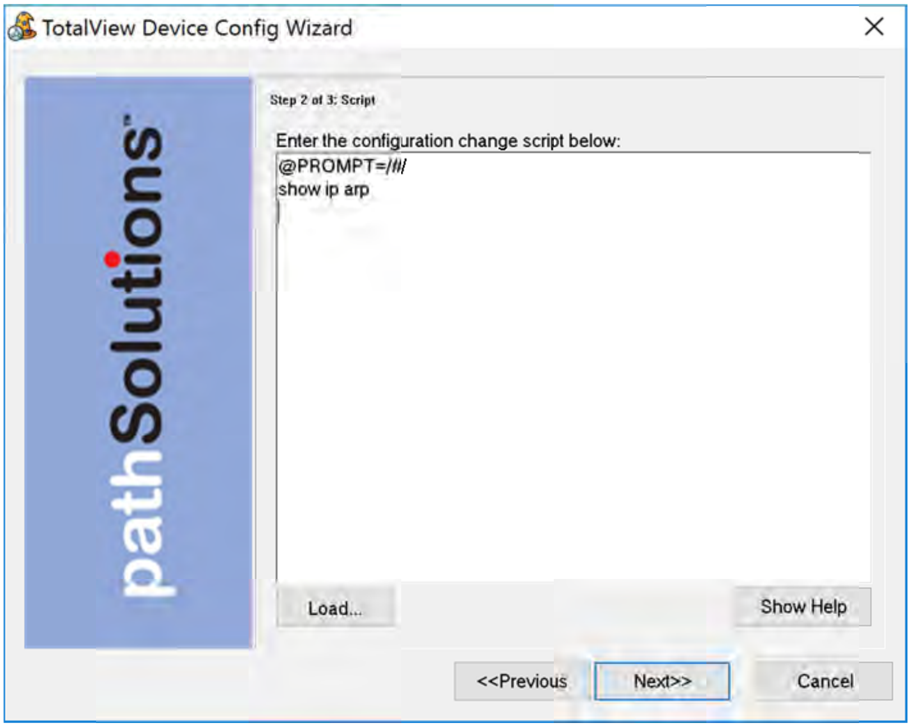


Select or de-select devices en-masse based on a matched sysDescr string.

● Select ○ De-Select

Match System Description String:

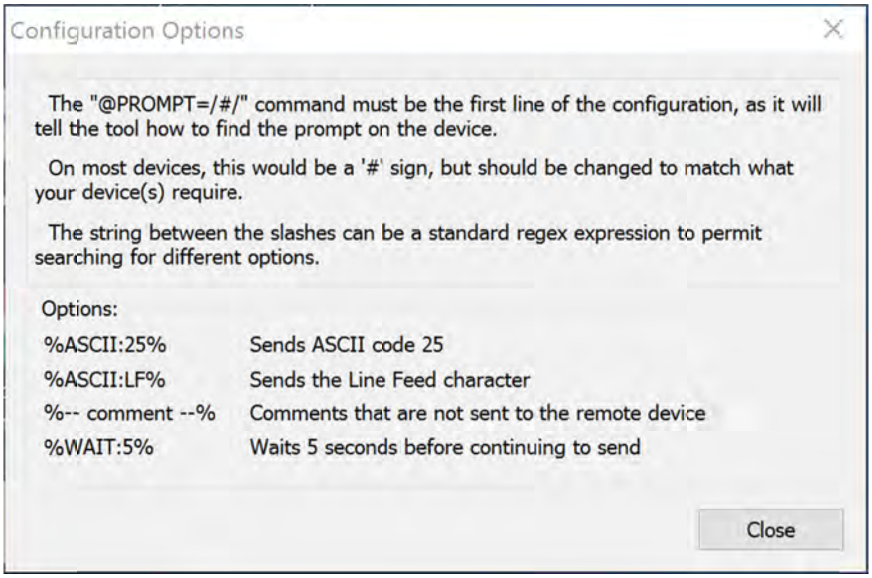
Then in step 3, enter the configuration change script. If needed select **Load** or **Show Help**. When finished, select **Next**.


TotalView Device Config Wizard
pathSolutions
Step 2 of 3: Script
Enter the configuration change script below:
Load...
Show Help
<<Previous
Next>>
Cancel

```
@PROMPT=/#/
show ip arp
```

Note: The “@PROMPT=/#/” must be the first or second line, as this tells the program how to identify that the console is ready to accept input. This may be different depending on the device being connected to.

Additional options can be entered in the configuration. Select **Show Help** to open a non-modal dialog box that can help with the configuration input.



The "@PROMPT=/#/" command must be the first line of the configuration, as it will tell the tool how to find the prompt on the device.

On most devices, this would be a '#' sign, but should be changed to match what your device(s) require.

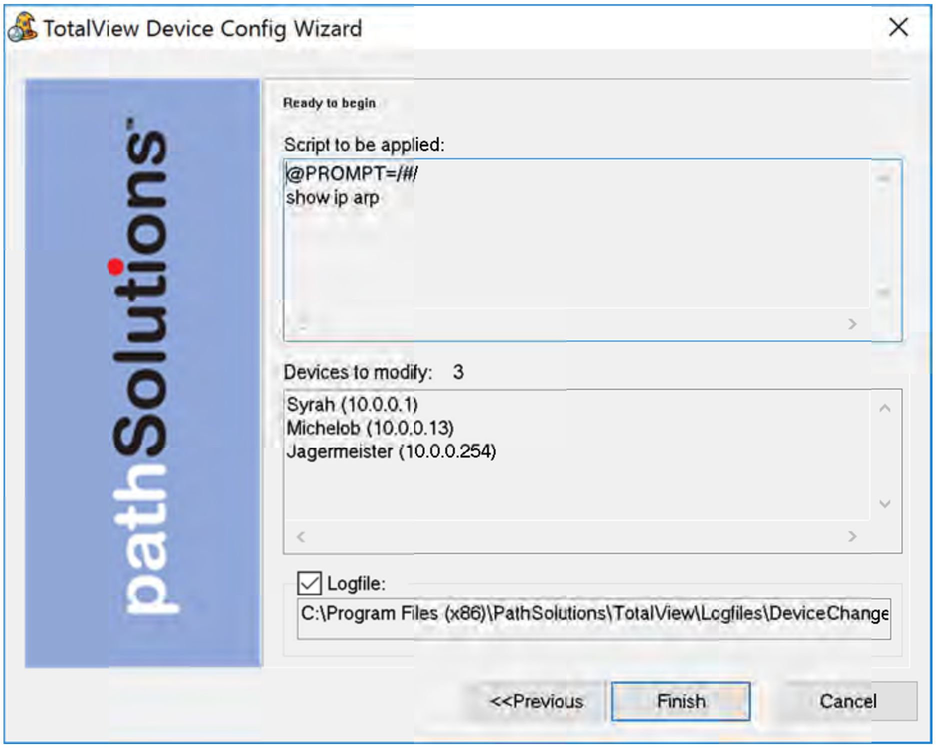
The string between the slashes can be a standard regex expression to permit searching for different options.

Options:

%ASCII:25%	Sends ASCII code 25
%ASCII:LF%	Sends the Line Feed character
%-- comment --%	Comments that are not sent to the remote device
%WAIT:5%	Waits 5 seconds before continuing to send

Select **Next** to continue.

A final confirmation will appear. Select **Finish** if everything looks correct.



Script to be applied:

```
@PROMPT=/#/
show ip arp
```

Devices to modify: 3

Syrah (10.0.0.1)
Michelob (10.0.0.13)
Jagermeister (10.0.0.254)

☑ Logfile: C:\Program Files (x86)\PathSolutions\TotalView\Logfiles\DeviceChange

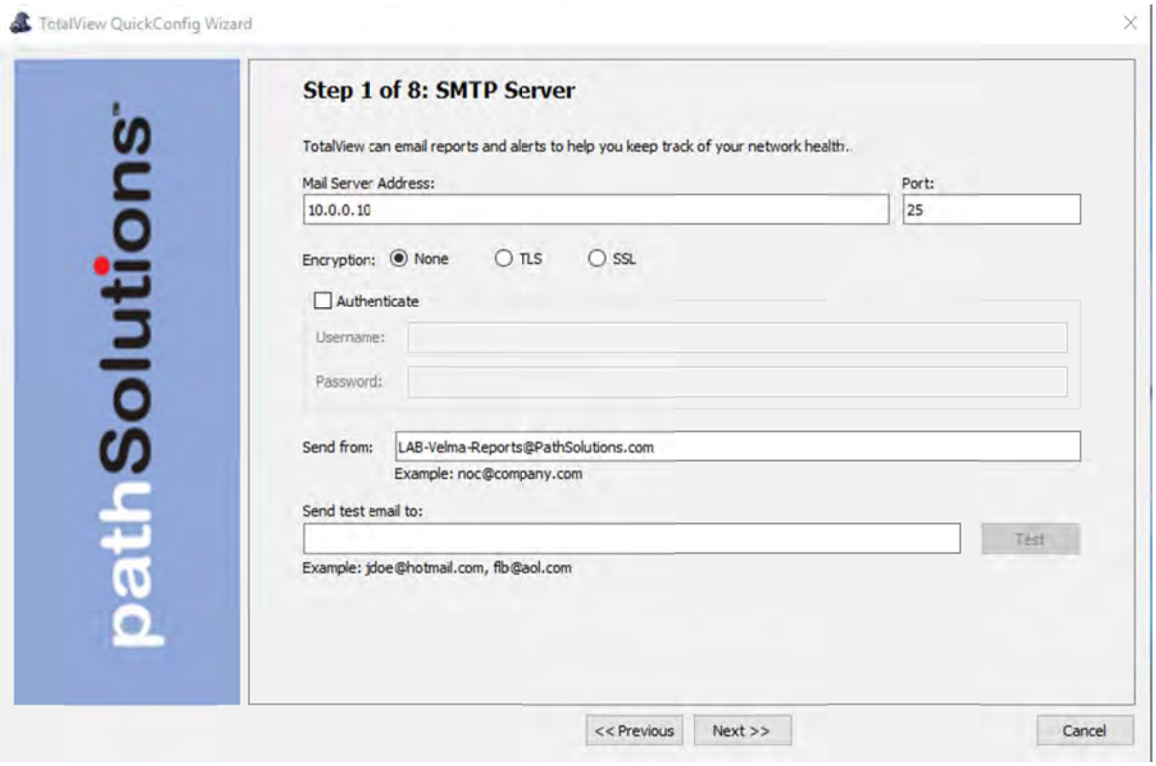
The wizard will then start applying the configuration query to the devices and show a status of each. When completed, it will open the device change log to show the results of each communication.

Re-Configuring TotalView When Your Network Changes

If you have new interfaces on your network, you can re-run the QuickConfig Wizard to scan your network and determine what changes have occurred.

To re-run the QuickConfig Wizard, select **Start**. Then choose **Programs > PathSolutions > TotalView > QuickConfig Wizard**.

You don't have to change any configurations already set with the QuickConfig Wizard. Select **Next** on every screen and the network will be scanned for new devices.



Step 1 of 8: SMTP Server

TotalView can email reports and alerts to help you keep track of your network health.

Mail Server Address: 10.0.0.10

Port: 25

Encryption: ● None ○ TLS ○ SSL

□ Authenticate

Username:

Password:

Send from: LAB-Velma-Reports@PathSolutions.com

Example: noc@company.com

Send test email to:

Example: jdoe@hotmail.com, flb@aol.com

Automatic Re-Configuration

The QuickConfig wizard can be run in automatic mode from a scheduled task if it is desired for new devices to be automatically discovered on a regular basis.

```
MonitorWizard.exe /a
```

When run in automatic mode, the program will not ask any questions but will scan the previous IP address ranges, will use the previous SNMP community strings, and add any new devices to the service. The service will then be stopped and then re-started to have the new devices added.

To change what IP address ranges and SNMP community strings are used in the automatic scan, edit the wizard.ini file:

```
/#10.100.47.1 - 10.100.47.254 [Default]/
/#10.100.56.1 - 10.100.56.254 [Default]/
/#192.168.136.1 - 192.168.136.10 [Edge Network]/
/#192.168.110.1 - 192.168.110.10 [Edge Network]/
/public/
```

Make sure all slashes '/' and pound signs '#' are maintained.

Other Network Program Configuration Tools

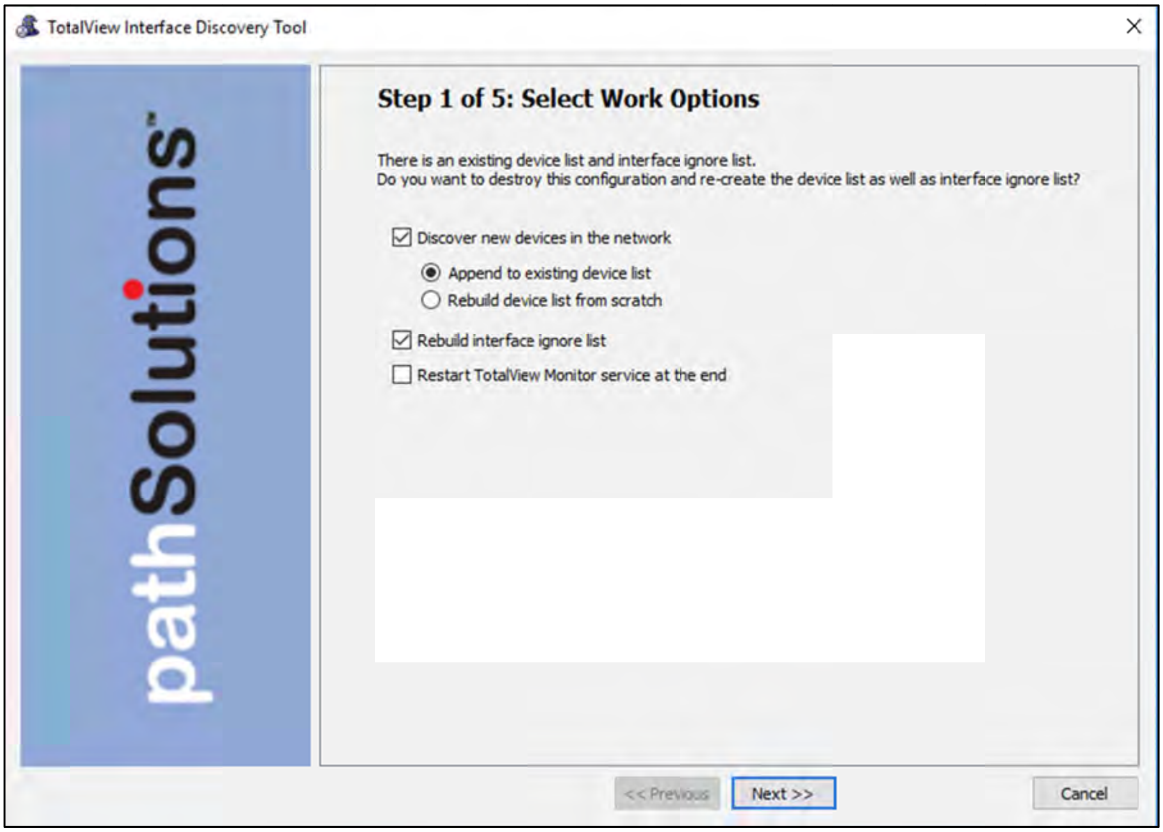
These are the config tools for TotalView deployment and use: In TotalView 14, the config tool has been completely re-designed to be faster and easier to navigate. It also includes configuration options. It also has been changed to make it faster/easier to set up SSH device backups on multiple devices faster.

Interface Discovery Tool

The Interface Discovery Tool is a three-step wizard designed to find new devices on the network and fine-tune which interfaces are monitored. This can help reduce the number of monitored interfaces to fix license limitation problems.

Go to **C:\Program Files (x86)\PathSolutions\TotalView** and select **IntDiscoveryTool** to launch the Interface Discovery Tool on the server's console.

It will launch and show the first step.



Step 1 of 5: Select Work Options

There is an existing device list and interface ignore list.
Do you want to destroy this configuration and re-create the device list as well as interface ignore list?

☑ Discover new devices in the network

● Append to existing device list

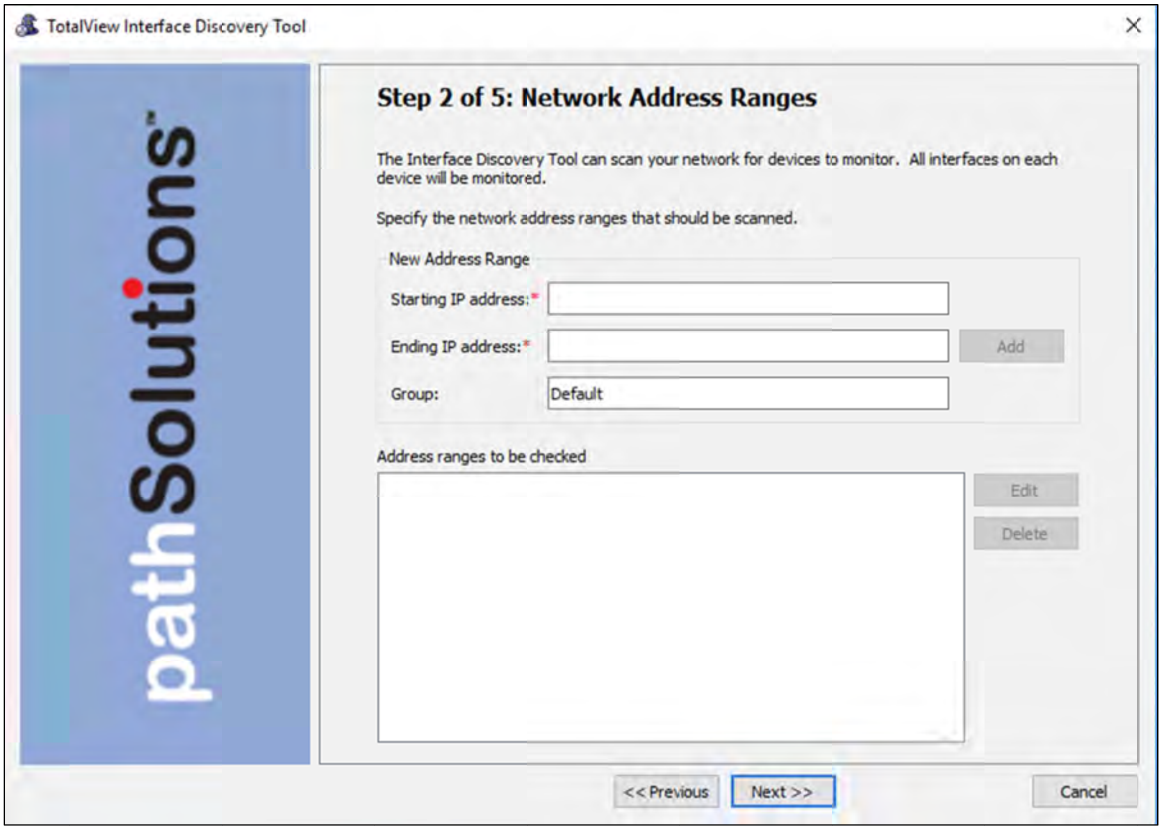
○ Rebuild device list from scratch

☑ Rebuild interface ignore list

□ Restart TotalView Monitor service at the end

This step will allow you to select work options.

The second step allows you to enter network address ranges.



Step 2 of 5: Network Address Ranges

The Interface Discovery Tool can scan your network for devices to monitor. All interfaces on each device will be monitored.

Specify the network address ranges that should be scanned.

New Address Range

Starting IP address:*

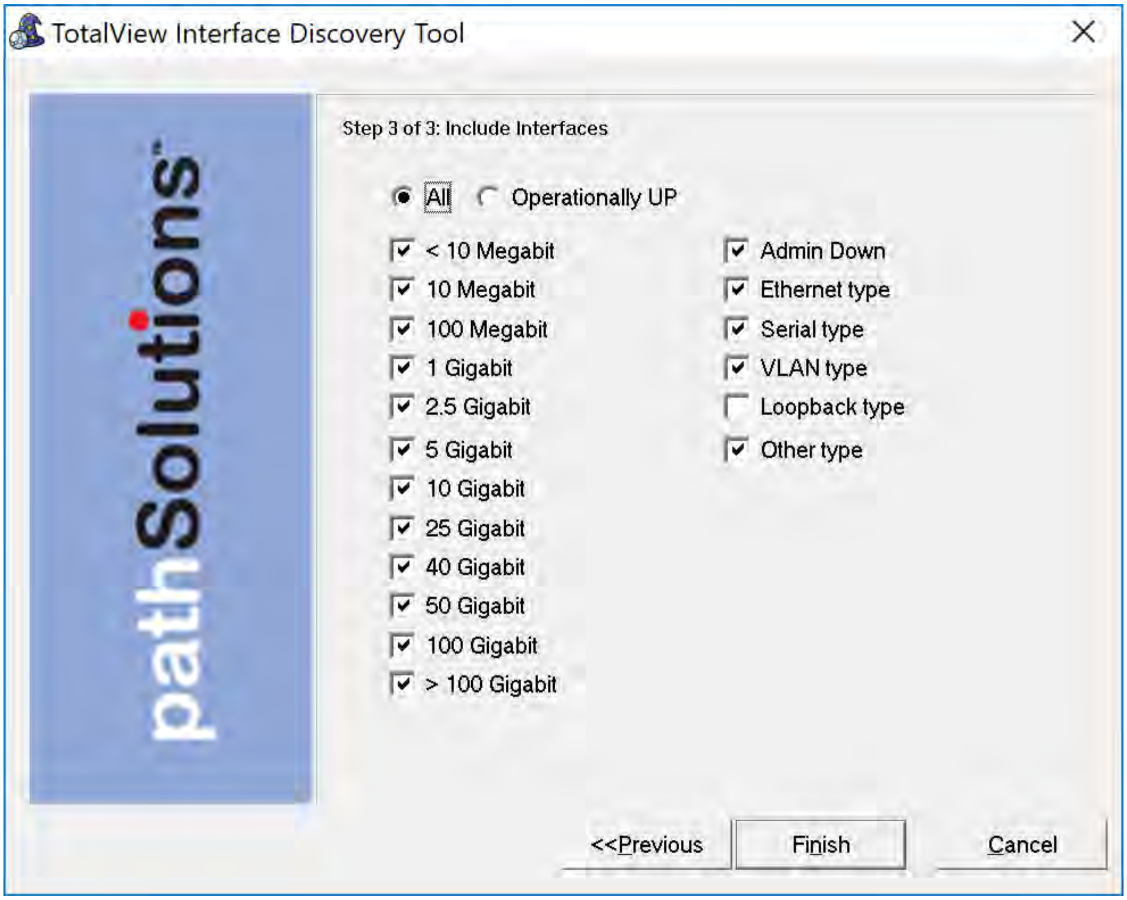
Ending IP address:*

Group: Default

Address ranges to be checked

Enter the appropriate IP addresses and select **Next** to continue.

The third step permits selecting which types of interfaces should be included in monitoring.



Step 3 of 3: Include Interfaces

● All ○ Operationally UP

☑ < 10 Megabit
☑ 10 Megabit
☑ 100 Megabit
☑ 1 Gigabit
☑ 2.5 Gigabit
☑ 5 Gigabit
☑ 10 Gigabit
☑ 25 Gigabit
☑ 40 Gigabit
☑ 50 Gigabit
☑ 100 Gigabit
☑ > 100 Gigabit

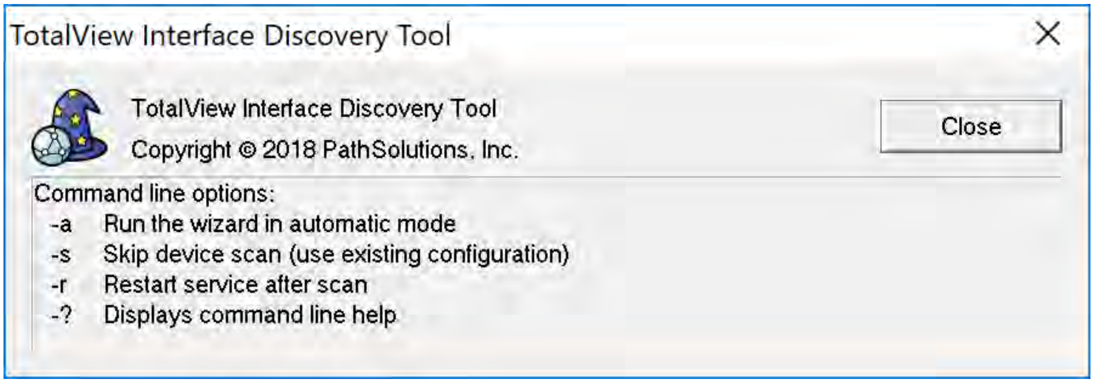
☑ Admin Down
☑ Ethernet type
☑ Serial type
☑ VLAN type
□ Loopback type
☑ Other type

If an interface type is not checked, it will not be included in TotalView's configuration.

When you select **Finish**, it will scan the network for new devices, add them to monitoring, and then remove interfaces that don't match the interface types.

The service will then be restarted.

This tool is designed to also run from and command-line as a nightly task if desired. It includes the following command-line options.

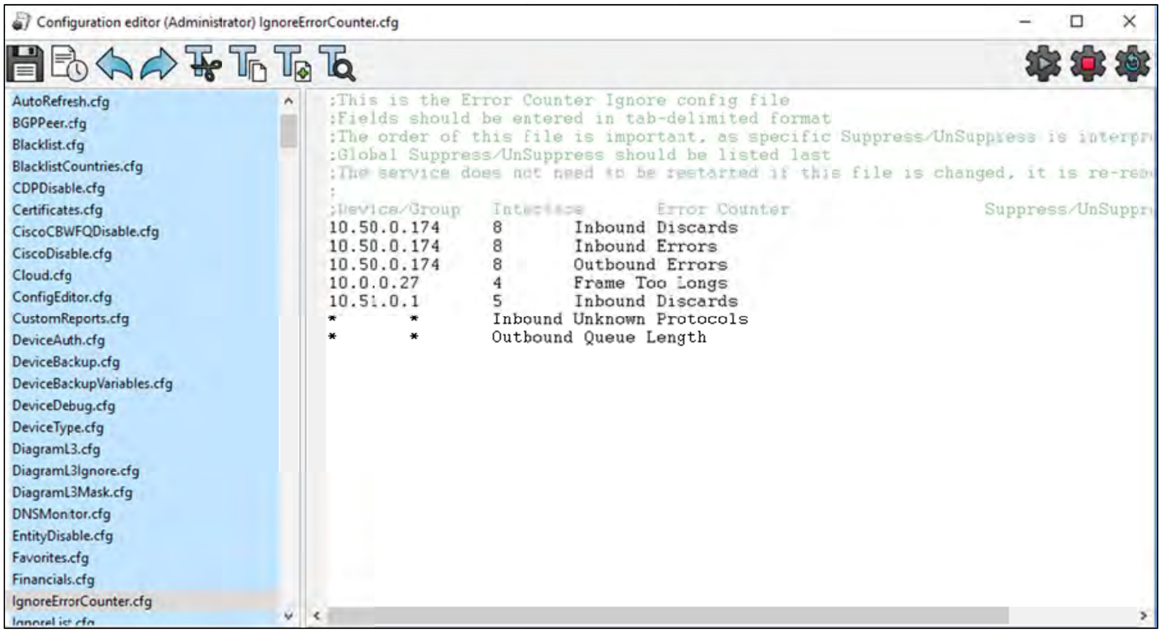


TotalView Interface Discovery Tool
Copyright © 2018 PathSolutions, Inc.

```
Command line options:
  -a    Run the wizard in automatic mode
  -s    Skip device scan (use existing configuration)
  -r    Restart service after scan
  -?    Displays command line help
```

Config Editor

This tool can be used to free-form update configuration files. It can be launched by selecting **Start/Programs/PathSolutions/TotalView** and choosing **Config Editor**. It will show the default screen.



```
;This is the Error Counter Ignore config file
;Fields should be entered in tab-delimited format
;The order of this file is important, as specific Suppress/UnSuppress is interpr
;Global Suppress/UnSuppress should be listed last
;The service does not need to be restarted if this file is changed, it is re-rea
;
;Device/Group   Interface       Error Counter                           Suppress/UnSuppr
10.50.0.174     8       Inbound Discards
10.50.0.174     8       Inbound Errors
10.50.0.174     8       Outbound Errors
10.0.0.27       4       Frame Too Longs
10.51.0.1       5       Inbound Discards
*       *       Inbound Unknown Protocols
*       *       Outbound Queue Length
```

Choose a config file in the left column and it will show the contents of the file in the main window.

The file can be edited and saved by selecting the disk icon in the toolbar.

The service can be restarted by selecting the far-right toolbar icon.

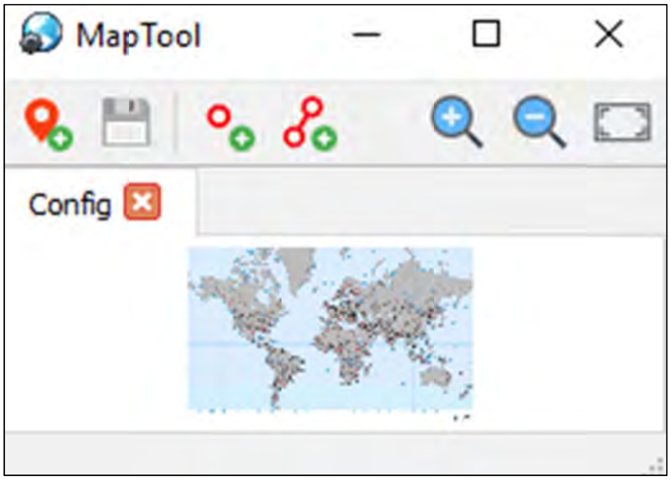
Note: Some configuration files will take immediate effect and do not require a service restart.

Map Config Tool

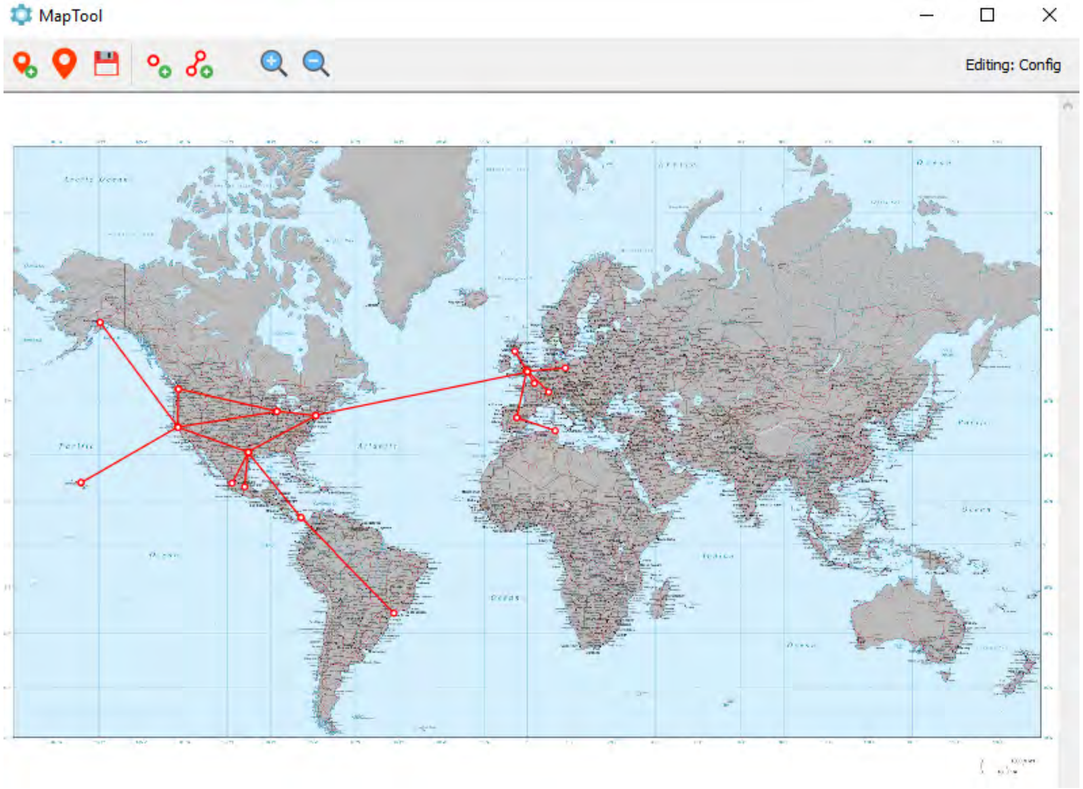
The Map Config Tool can be used to create and update the **Map** tab on the web user interface. It can be launched from the Configuration Tool. It can also be run from the console where TotalView is installed.

To run from the console, go to **Start/Programs/PathSolutions/Map Tool.**

When you first start the app, it will ask you to select a map. Select from the drop-down menu then select **OK**. The default map is **Config** but others may be available if they were created and saved.



After the map is chosen, the Map Tool will load the map and show any previously configured ping points and links.



A ping point or link can be added by right-clicking anywhere on the map and choosing the element type you want to add.

The toolbar across the top contains these tools:

The pointer with a plus sign allows you to add and name a new map:

Select this pointer symbol top select and open a map:

Select the floppy disk symbol to update the dynamic map:

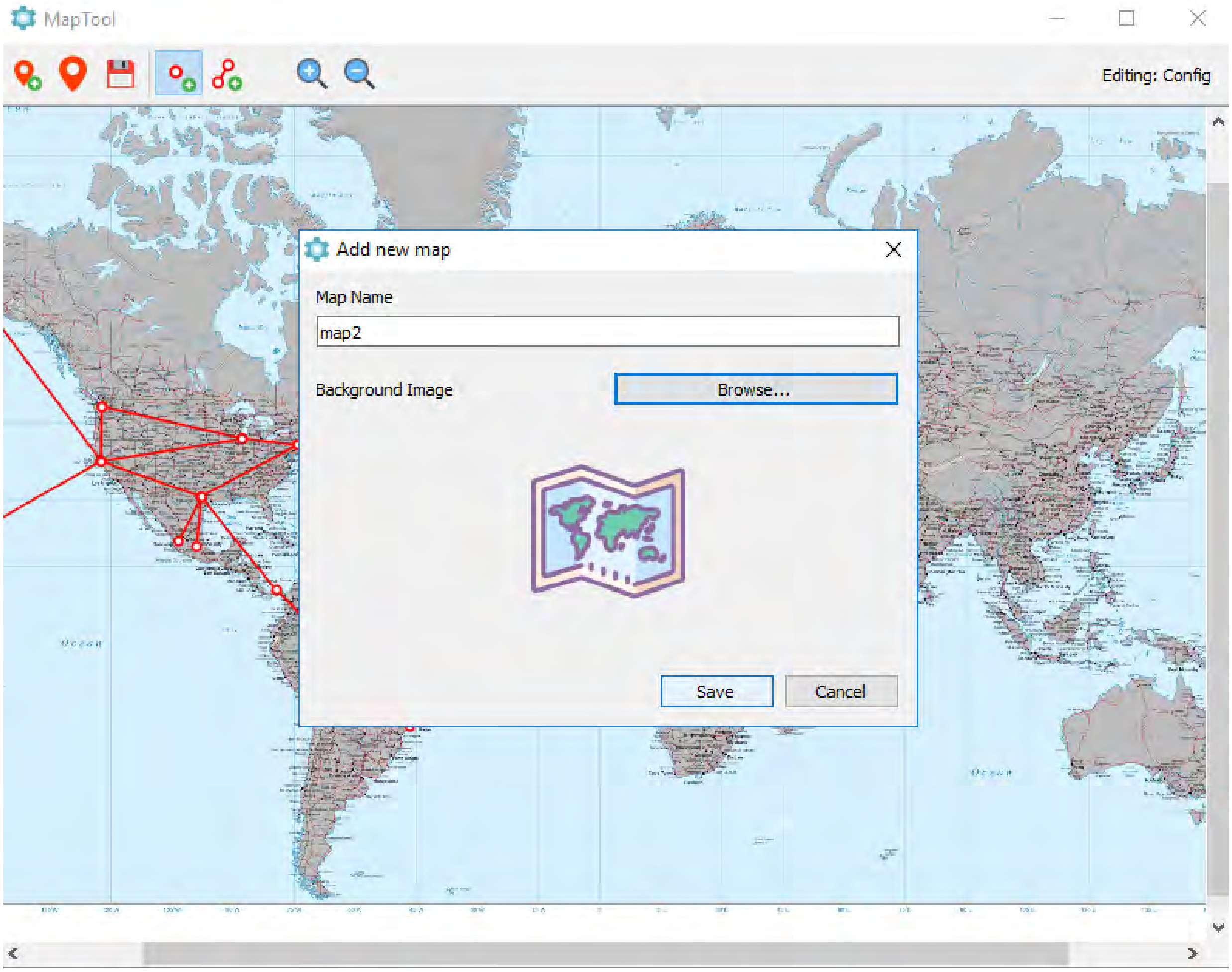
To add a device ping, use the **Add Device Ping** symbol:

To add a link, use the **Add Link** symbol:

To change magnification up or down, clock on the magnifying icons:

How to Add Maps

Select the **Add Map** icon and this popup menu will ask you to name the map and select a map background image from computer files. Select a map from your TotalView Graphics folder. Multiple Maps can be created this way.

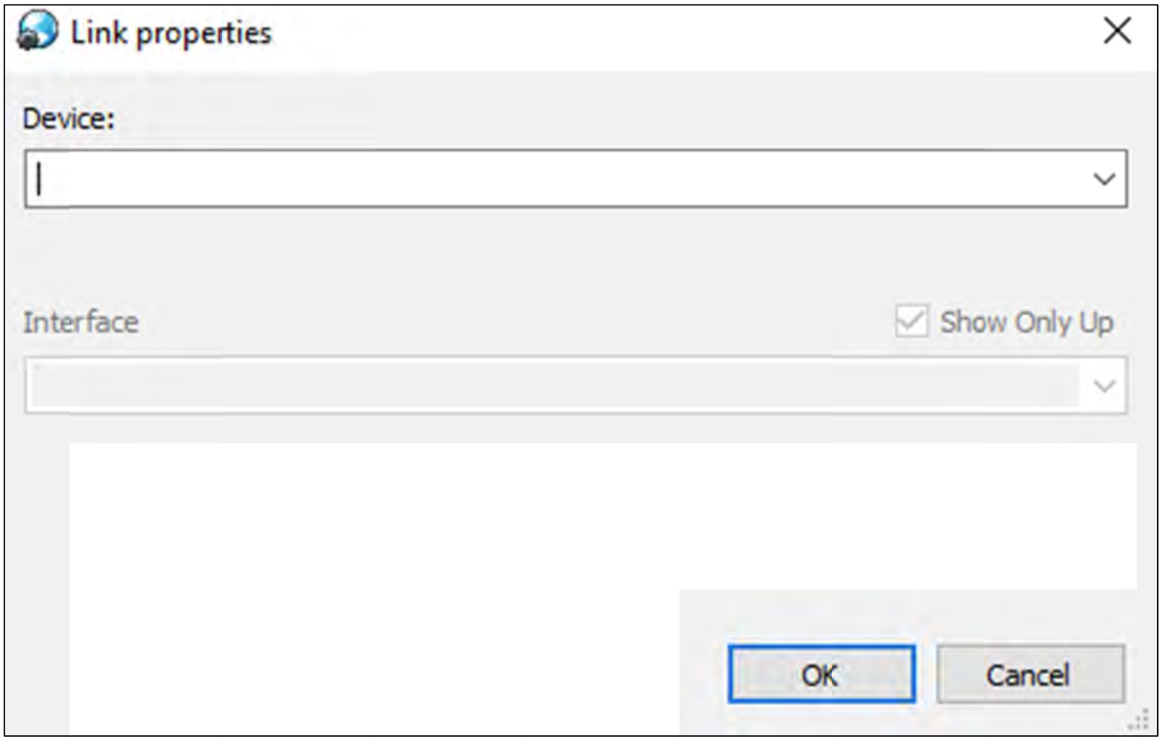


Map Name: map2

Background Image

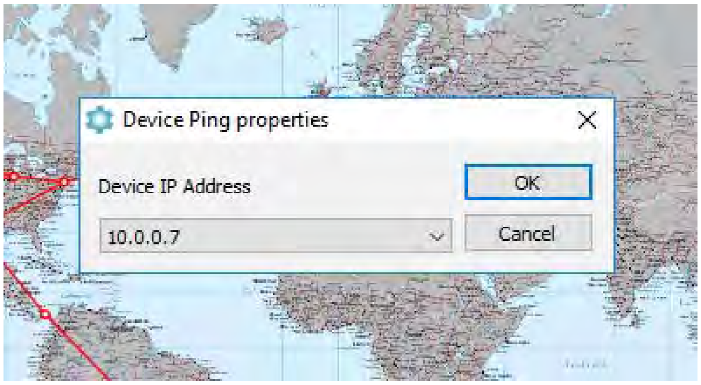
How to Add Links

To add a link connection between coordinates, select the **Add Link** icon. It will ask you to select the device IP address and interface that should be associated with the link:



After selecting the device and interface, it will start a line draw that will allow you to position the remote endpoint of the link. Position it with a select.

Then, it will ask you to select the device IP address for that ping point.

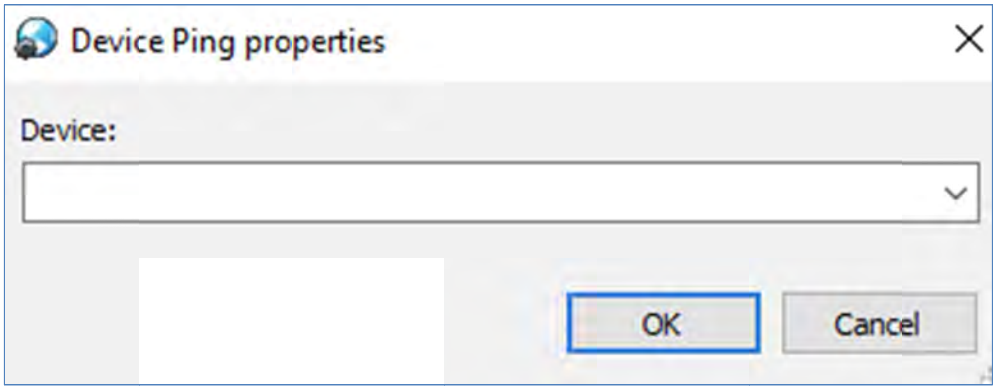


Device IP Address: 10.0.0.7

If you save the map, you can immediately check the web page’s map to see the change automatically updated. (There’s no need to restart the service or refresh the browser window).

How to Add Ping Points

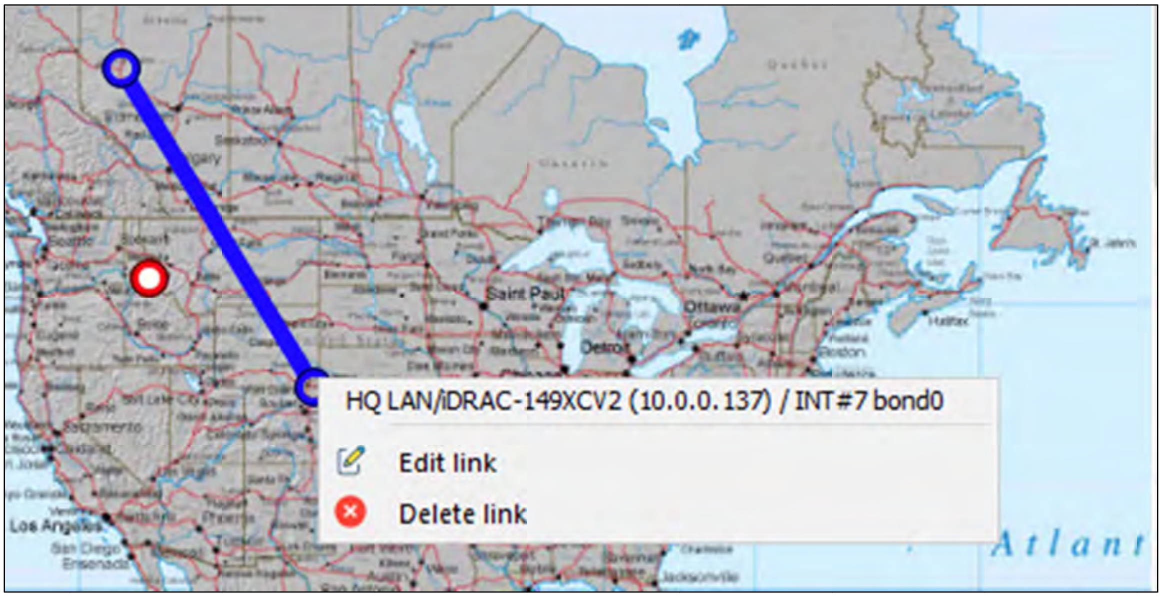
For a Ping point, select the **Ping Point** icon, and then enter the Device's IP address. This represents that the Device can be pinged. In TotalView, the point will display as a green dot (can ping), a red dot (cannot ping), or a black dot (device is down).


Device Ping properties

Device:

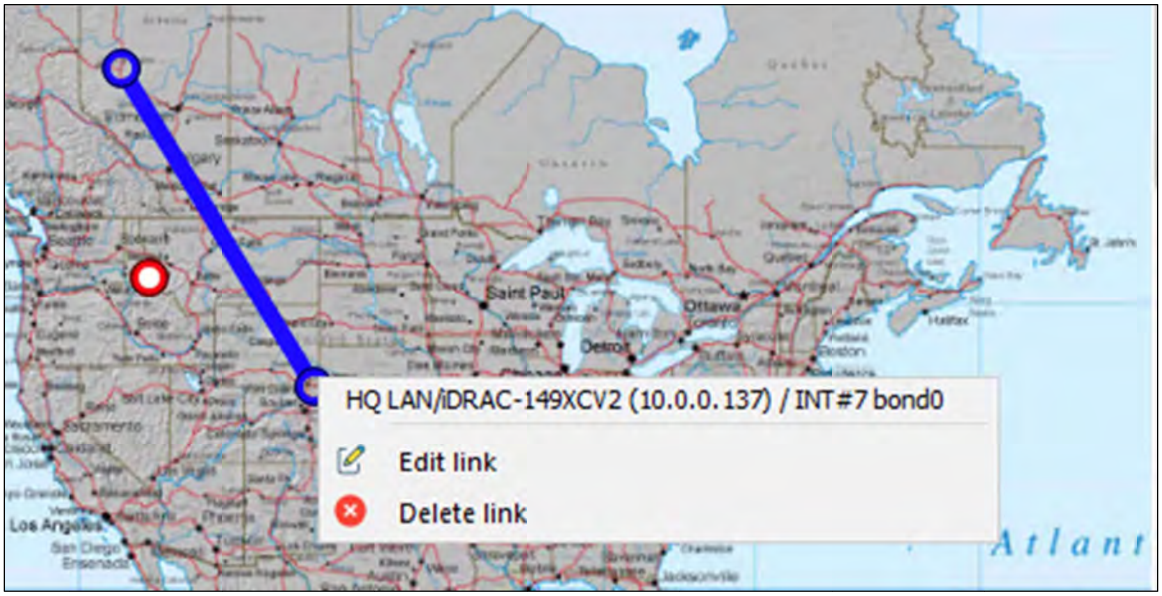
How to Change Items on the Map

Hover your mouse over one of the endpoint dots of a link. The element will turn from red to blue.
Right-click on the element, then select **Edit** from the pop-up menu.
It will allow you to choose a new IP address and move the point.


HQ LAN/iDRAC-149XCV2 (10.0.0.137) / INT#7 bond0

How to Delete Items on the Map

Hover your mouse over one of the endpoint dots of a link. The element will turn from red to blue. Right-click on the element, then select **Delete** from the pop-up menu.



How to Save the Map

When finished adding Links and Ping Points, select the **Save** icon to save the changes in the map. If you save the map, immediately check the web page's map to see the change automatically update (no need to restart the service or refresh the browser window).

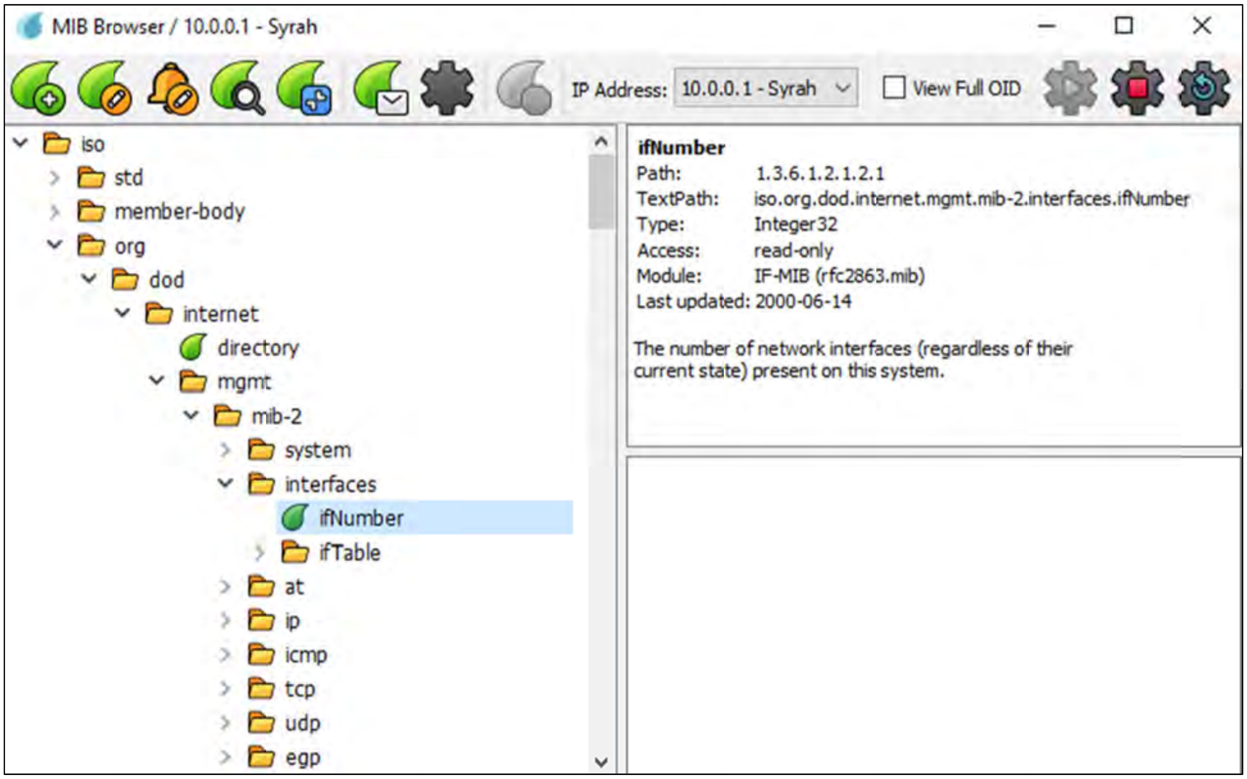
After saving, close the **Map Tool**.

MIB Browser

A full-featured MIB Browser is included for easily finding and selecting SNMP variables from devices. It can easily be launched from the Configuration Tool. It can also be run from the console where TotalView was installed.

To launch the MIB browser from the console, select **Start/Programs/PathSolutions/MIB Browser** (MIBBrowser.exe).

The first time it launches, it will download the latest MIB database from the PathSolutions website.



ifNumber
Path: 1.3.6.1.2.1.2.1
TextPath: iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber
Type: Integer32
Access: read-only
Module: IF-MIB (rfc2863.mib)
Last updated: 2000-06-14

The number of network interfaces (regardless of their current state) present on this system.

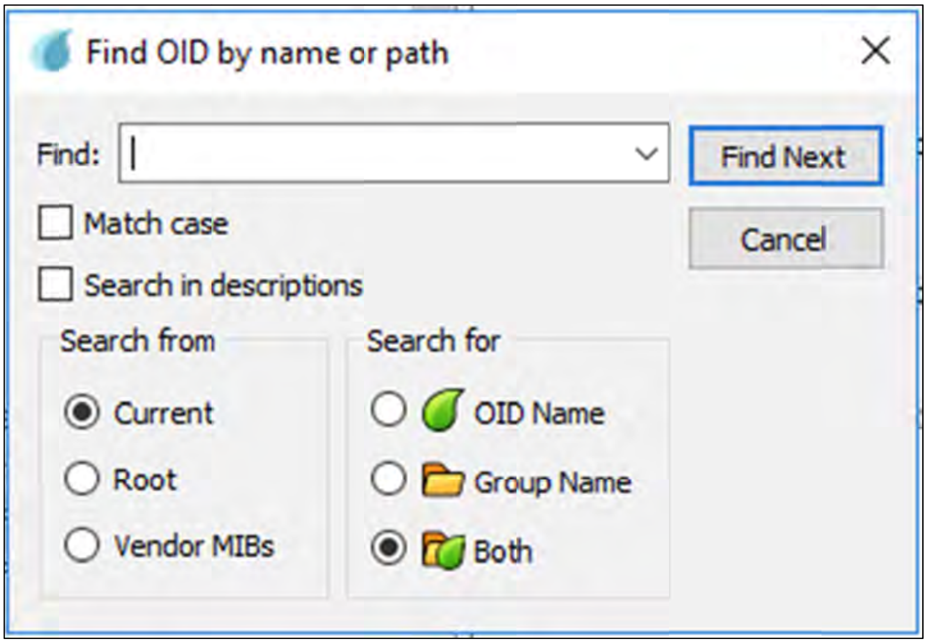
Most all manufacturer's MIBs have been automatically added into the database so variables can be immediately queried without the need to find and compile MIBs. Live and historic graphing and tracking of variables are also available to see inflection changes.

If you right-click on a variable, it shows information about the variables in the top right panel, and offers the following options from a drop-down menu:

Add OID:	Add this OID to TotalView to monitor and alert continuously.
Get:	Get the variable (one fetch)
GetNext	Get all of these variables until it reaches the end
GetBulk	Get all of these variables using a bulk request until it reaches the end
Monitor…	Monitor this variable live (updates every 5 seconds to every 5 minutes)

If you need to search for items by OID name or path, select on this search symbol in the top menu.

If you select it, the search menu will popup. Enter a search string, then select **Find Next**.



Find OID by name or path

Find:

□ Match case

□ Search in descriptions

Search from

● Current

○ Root

○ Vendor MIBs

Search for

○ OID Name

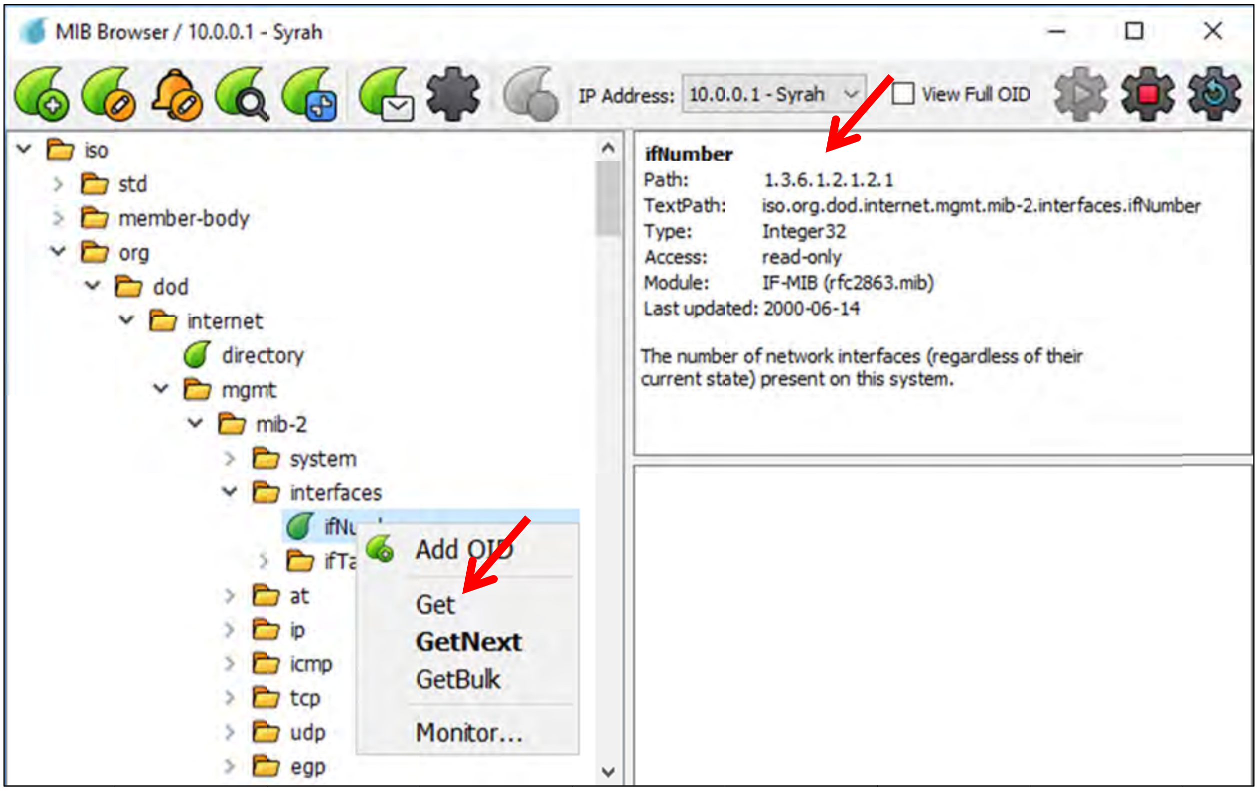
○ Group Name

● Both

OID Lookups

The left navigation panel allows you to navigate and choose an OID variable. Once you select a variable, the description of the OID is displayed in the upper right panel.

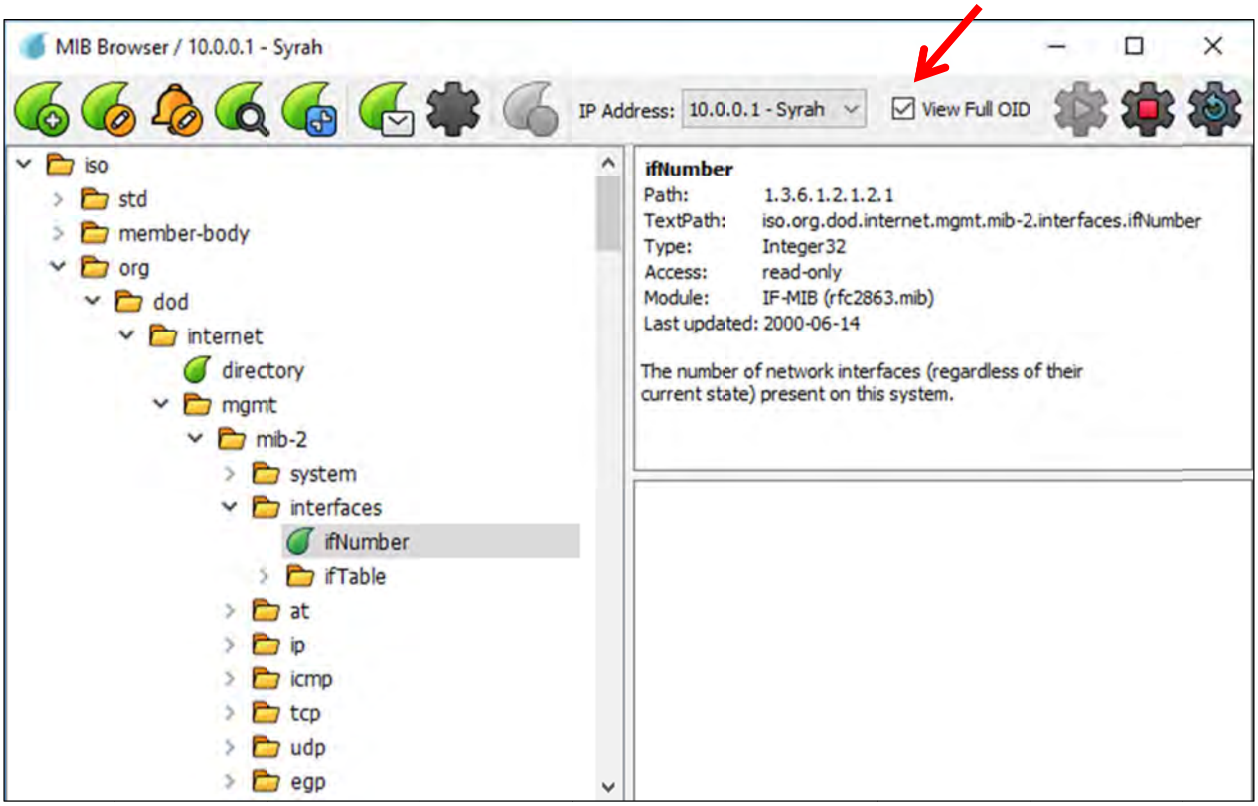
If you right double-click on the variable in the left panel and select **Get**. it will fetch that variable and display the name of it in the lower right panel.



ifNumber
Path: 1.3.6.1.2.1.2.1
TextPath: iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber
Type: Integer32
Access: read-only
Module: IF-MIB (rfc2863.mib)
Last updated: 2000-06-14

The number of network interfaces (regardless of their current state) present on this system.

View the full OUI value in the lower right panel by selecting **View Full OID**.

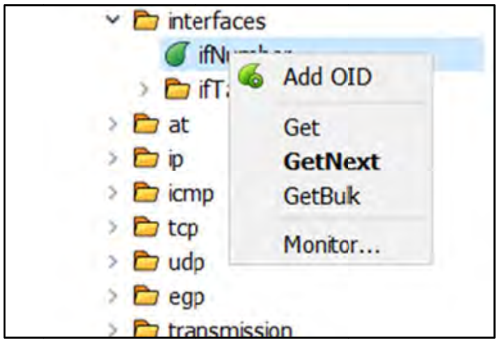


ifNumber
Path: 1.3.6.1.2.1.2.1
TextPath: iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber
Type: Integer32
Access: read-only
Module: IF-MIB (rfc2863.mib)
Last updated: 2000-06-14

The number of network interfaces (regardless of their current state) present on this system.

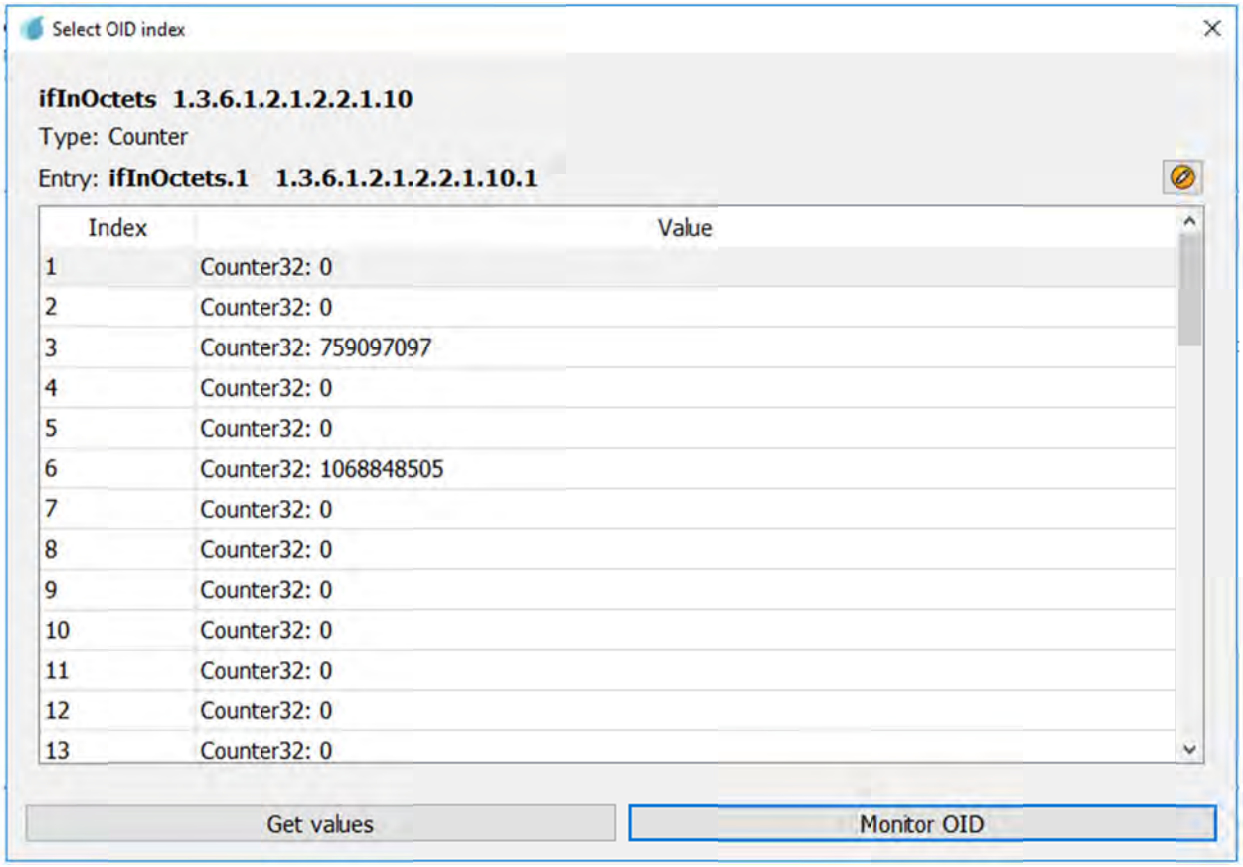
OID Monitoring

When you right-click on an OID, it has a drop-down menu that allows you to choose **Monitor…**



Select **Monitor…** and the dialog box for the selected Interface’s OID Index will popup.

If you select **Get values**, it will refresh the values on screen, to show any updated information since the last query.



ifInOctets 1.3.6.1.2.1.2.2.1.10

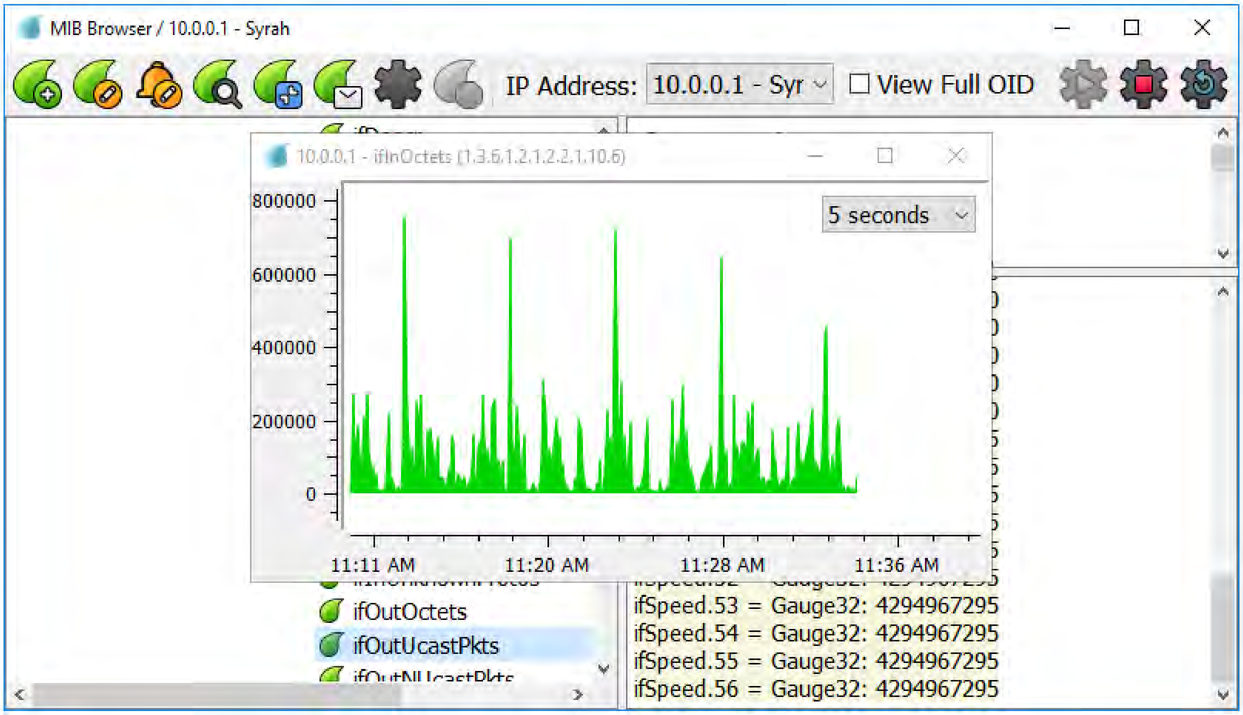
Type: Counter

Entry: **ifInOctets.1 1.3.6.1.2.1.2.2.1.10.1**

Index	Value
1	Counter32: 0
2	Counter32: 0
3	Counter32: 759097097
4	Counter32: 0
5	Counter32: 0
6	Counter32: 1068848505
7	Counter32: 0
8	Counter32: 0
9	Counter32: 0
10	Counter32: 0
11	Counter32: 0
12	Counter32: 0
13	Counter32: 0

If you select **Monitor OID**, a window opens that charts the current values on the device over time. The chart is updated at set intervals. You can set the intervals from every 5 seconds to every 5 minutes.

Tip: We recommend setting intervals to monitor less frequently, if your device does not update its SNMP counters as often.

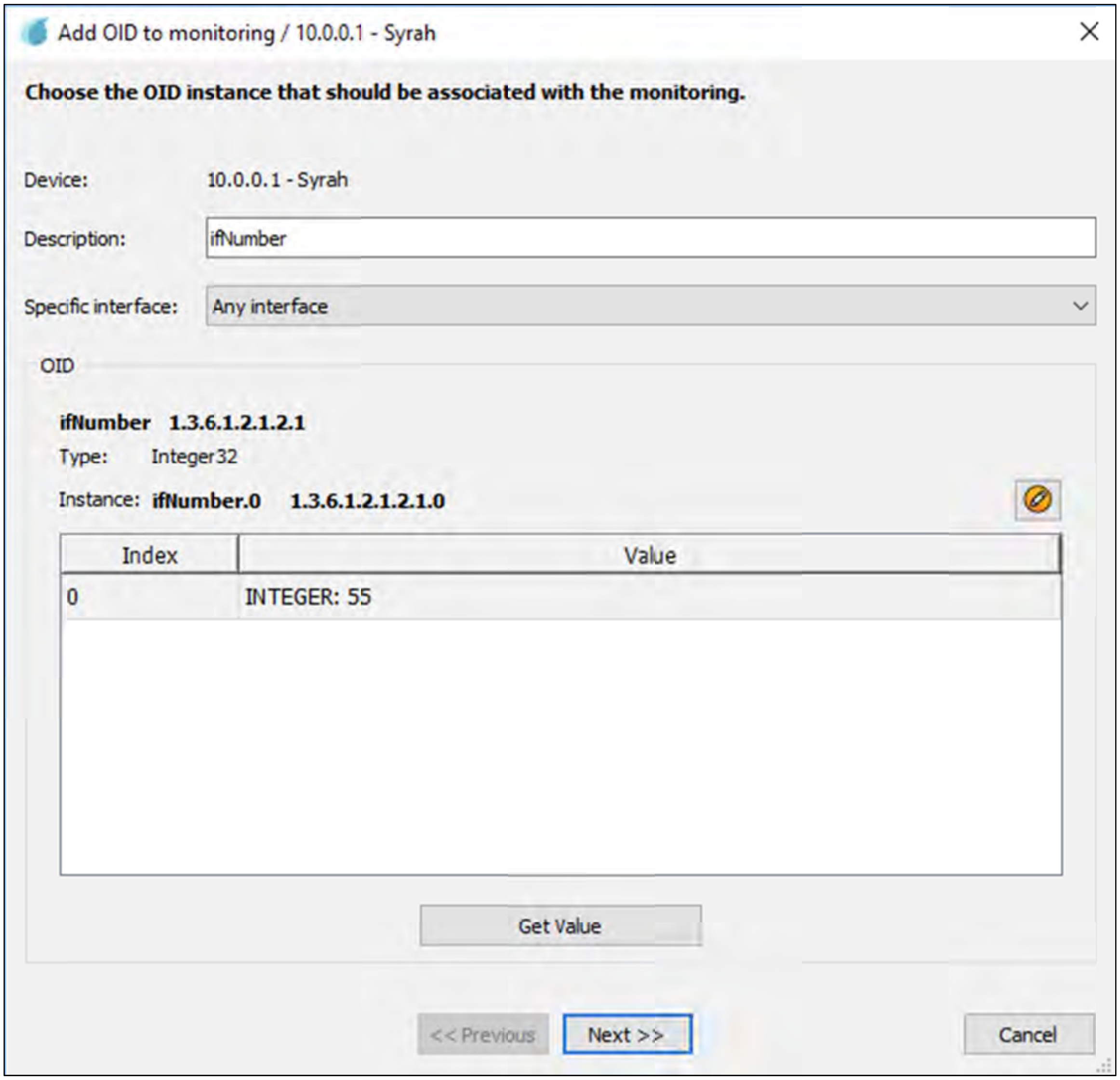


ifSpeed.53 = Gauge32: 4294967295
ifSpeed.54 = Gauge32: 4294967295
ifSpeed.55 = Gauge32: 4294967295
ifSpeed.56 = Gauge32: 4294967295

OID Graphing

Run the **MIB Browser** and select a variable in the lists on the left to monitor and graph.
When you right-click on the variable, it has a drop-down menu that allows you to select **Add OID.**

The **Add OID** wizard will appear. In the first dialog, add the specific interface or index to monitor.



Add OID to monitoring / 10.0.0.1 - Syrah

Choose the OID instance that should be associated with the monitoring.

Device: 10.0.0.1 - Syrah

Description: ifNumber

Specific interface: Any interface

OID

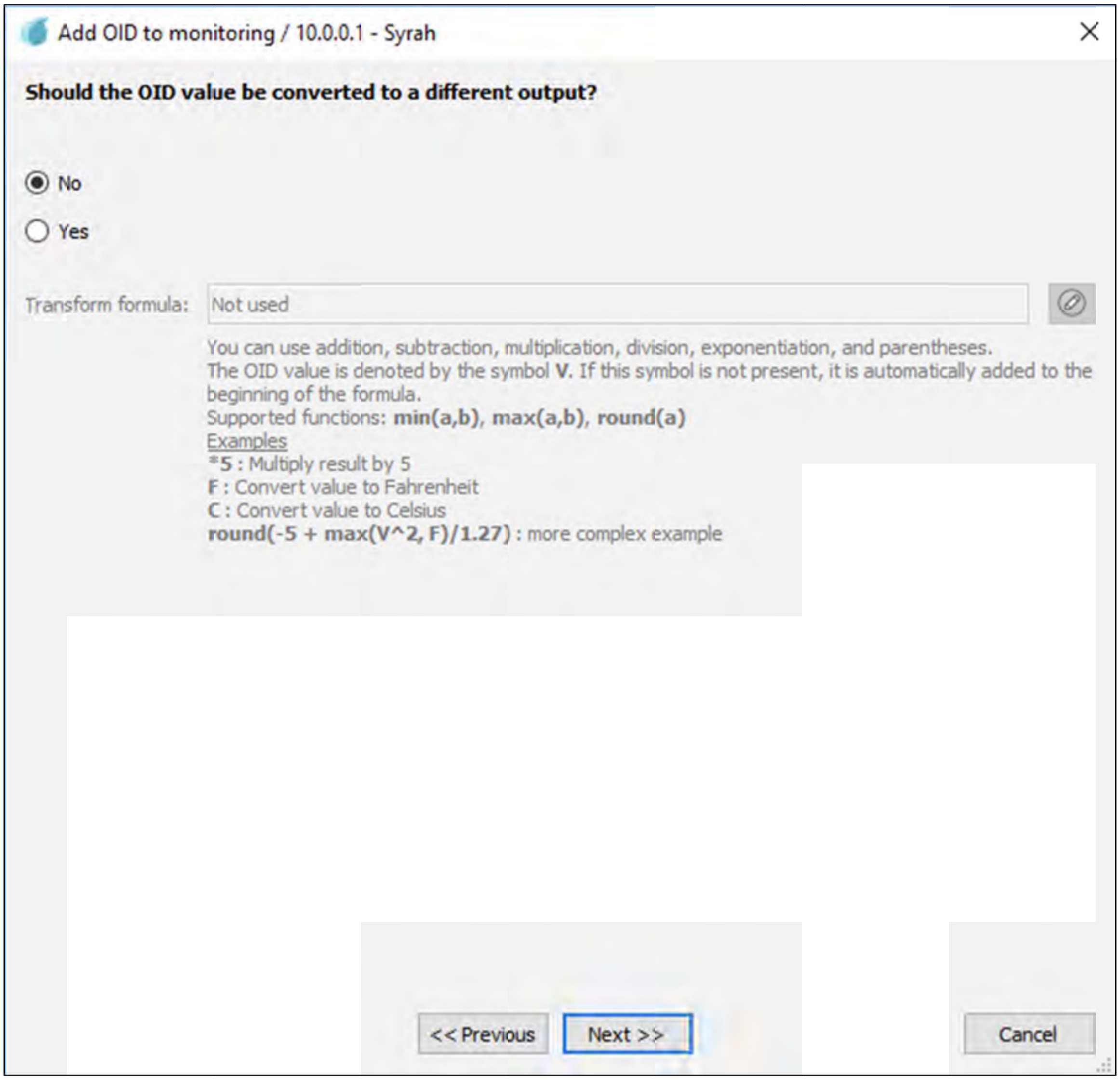
ifNumber 1.3.6.1.2.1.2.1

Type: Integer32

Instance: **ifNumber.0 1.3.6.1.2.1.2.1.0**

Index	Value
0	INTEGER: 55

The second step is to decide whether to transform the returned value to a different result.
For example: if the device returns Fahrenheit values but you want the results to be converted to Celsius, you can enter the conversion formula in the **Transform formula** field.



Add OID to monitoring / 10.0.0.1 - Syrah

Should the OID value be converted to a different output?

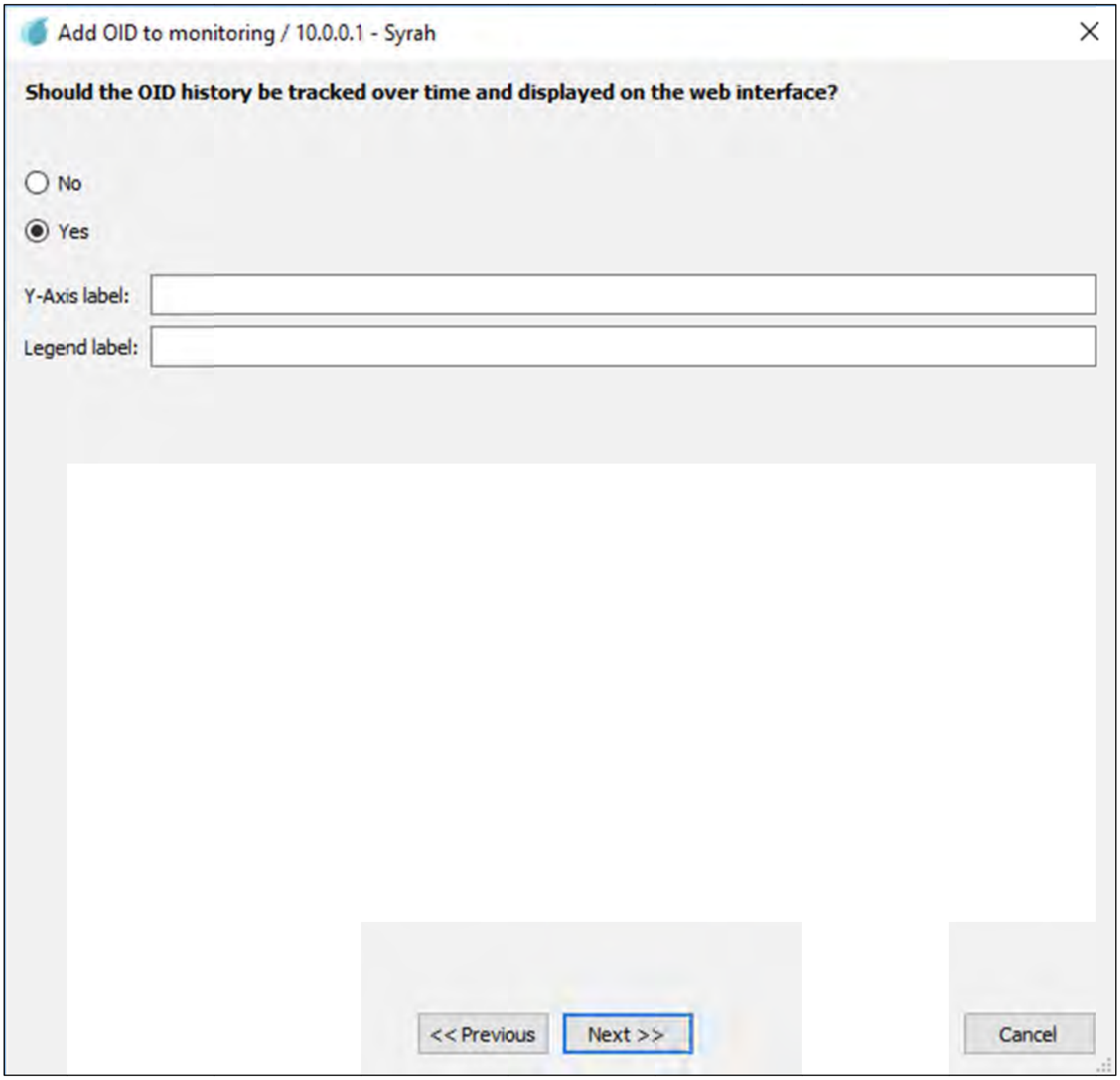
● No

○ Yes

Transform formula: Not used

You can use addition, subtraction, multiplication, division, exponentiation, and parentheses.
The OID value is denoted by the symbol **V.** If this symbol is not present, it is automatically added to the beginning of the formula.
Supported functions: **min(a,b), max(a,b), round(a)**
Examples
***5** : Multiply result by 5
F : Convert value to Fahrenheit
C : Convert value to Celsius
round(-5 + max(V^2, F)/1.27) : more complex example

The next step is to determine if you want to track the history of this value over time and present the graph on the web UI. This is normally recommended, but for certain queried values you might only want to generate an alert and not display the values.



Should the OID history be tracked over time and displayed on the web interface?

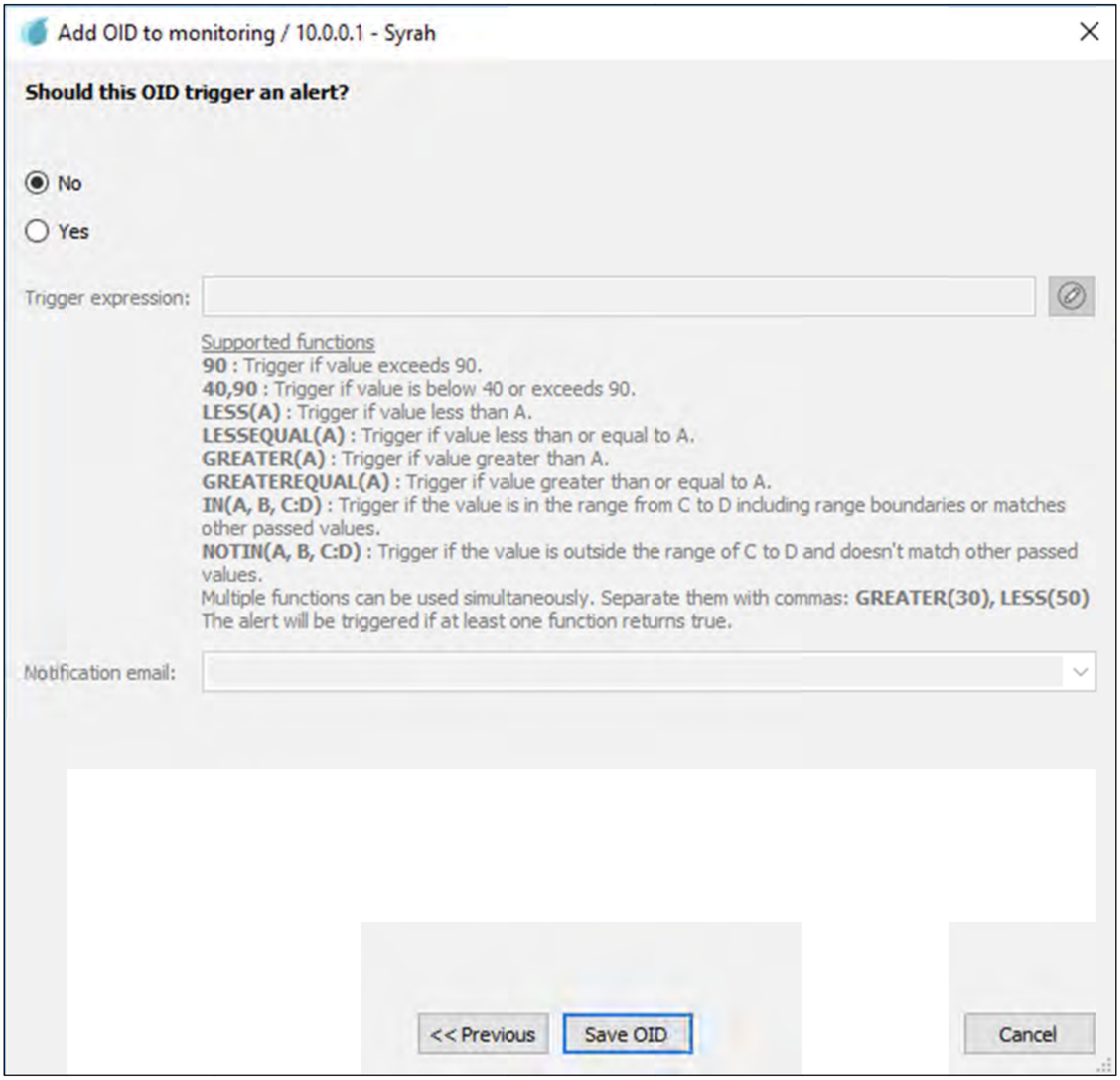
○ No

● Yes

Y-Axis label:

Legend label:

Define the triggers for the custom OID alert. You can enter thresholds high as well as low and a range that it should exist in.



Should this OID trigger an alert?

● No

○ Yes

Trigger expression:

Supported functions
90 : Trigger if value exceeds 90.
40,90 : Trigger if value is below 40 or exceeds 90.
LESS(A) : Trigger if value less than A.
LESSEQUAL(A) : Trigger if value less than or equal to A.
GREATER(A) : Trigger if value greater than A.
GREATEREQUAL(A) : Trigger if value greater than or equal to A.
IN(A, B, C:D) : Trigger if the value is in the range from C to D including range boundaries or matches other passed values.
NOTIN(A, B, C:D) : Trigger if the value is outside the range of C to D and doesn't match other passed values.
Multiple functions can be used simultaneously. Separate them with commas: **GREATER(30), LESS(50)**
The alert will be triggered if at least one function returns true.

Notification email:

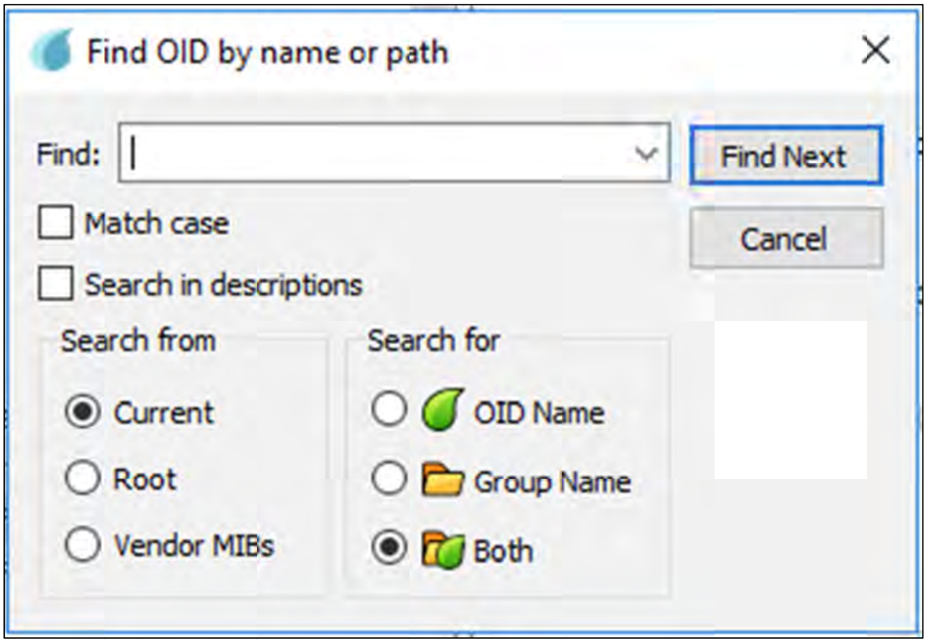
SNMP Trap Receiver Configuration

The MIB browser includes a SNMP Trap receiver to trigger alerts for received event traps. Simply select the device, specific trap, variable that will trigger the alert, and who to receive the notification, as described here.

Note: The SNMP Trap Receiver service must be installed before it can be used. To install the SNMP Trap Receiver service, refer to the following KB entry: https://support.pathsolutions.com/support/solutions/articles/14000128376-totalview-12-installing-totalview-snmp-trap-service

Alerting on a Specific Trap

Find the SNMP trap that you want to monitor in the MIB Browser. For example, the search for **dsx1LineStatusChange** then select **Find Next** several times to see all the instances of that string.



Find OID by name or path

Find:

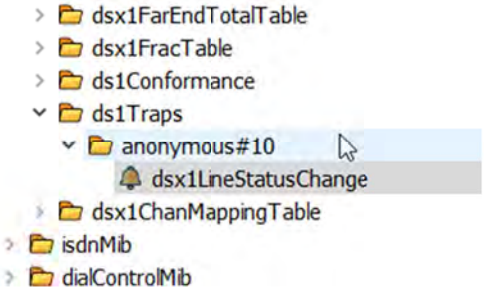
□ Match case

□ Search in descriptions

Search from
- ● Current
- ○ Root
- ○ Vendor MIBs

Search for
- ○ OID Name
- ○ Group Name
- ● Both

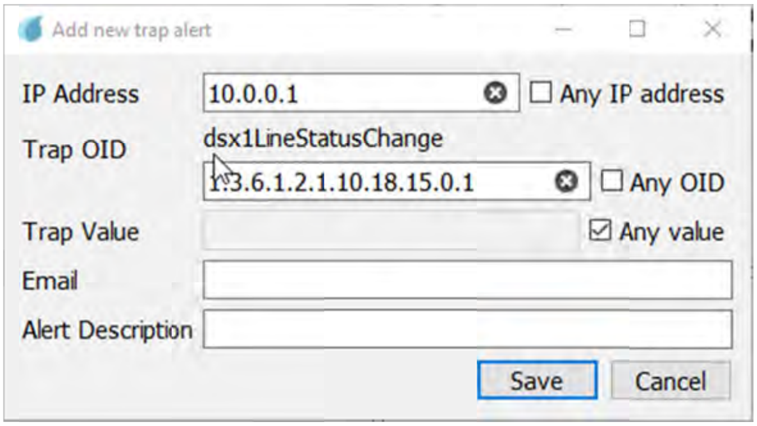
On the second instance, in this example, a bell icon next to the line item indicated it has a trap.



```
> dsx1FarEndTotalTable
> dsx1FracTable
> ds1Conformance
v ds1Traps
  v anonymous#10
      dsx1LineStatusChange
> dsx1ChanMappingTable
> isdnMib
> dialControlMib
```

Right-click on the trap (the line item with the bell icon) and select **Add Trap Alert**. Alternatively, select the line item, then select this bell-and-plus-sign symbol in the top navigational bar:

This will allow you to add a trap for this SNMP Trap on this device.


Add new trap alert

IP Address: 10.0.0.1 ☐ Any IP address

Trap OID: dsx1LineStatusChange 1.3.6.1.2.1.10.18.15.0.1 ☐ Any OID

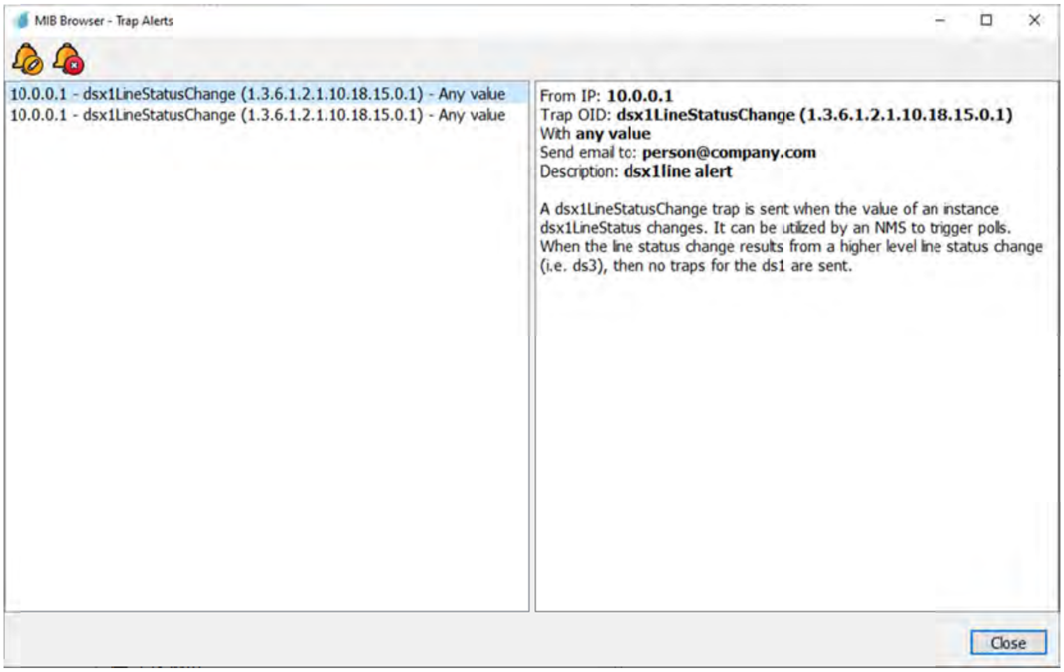
Trap Value: ☑ Any value

Email:

Alert Description:

Modifying Trap Alerts
First select a line item with a trap alert you wish to modify. Then select this bell-and-pencil symbol in the top navigational bar.

A submenu of trap alerts will display as shown in the screenshot below.

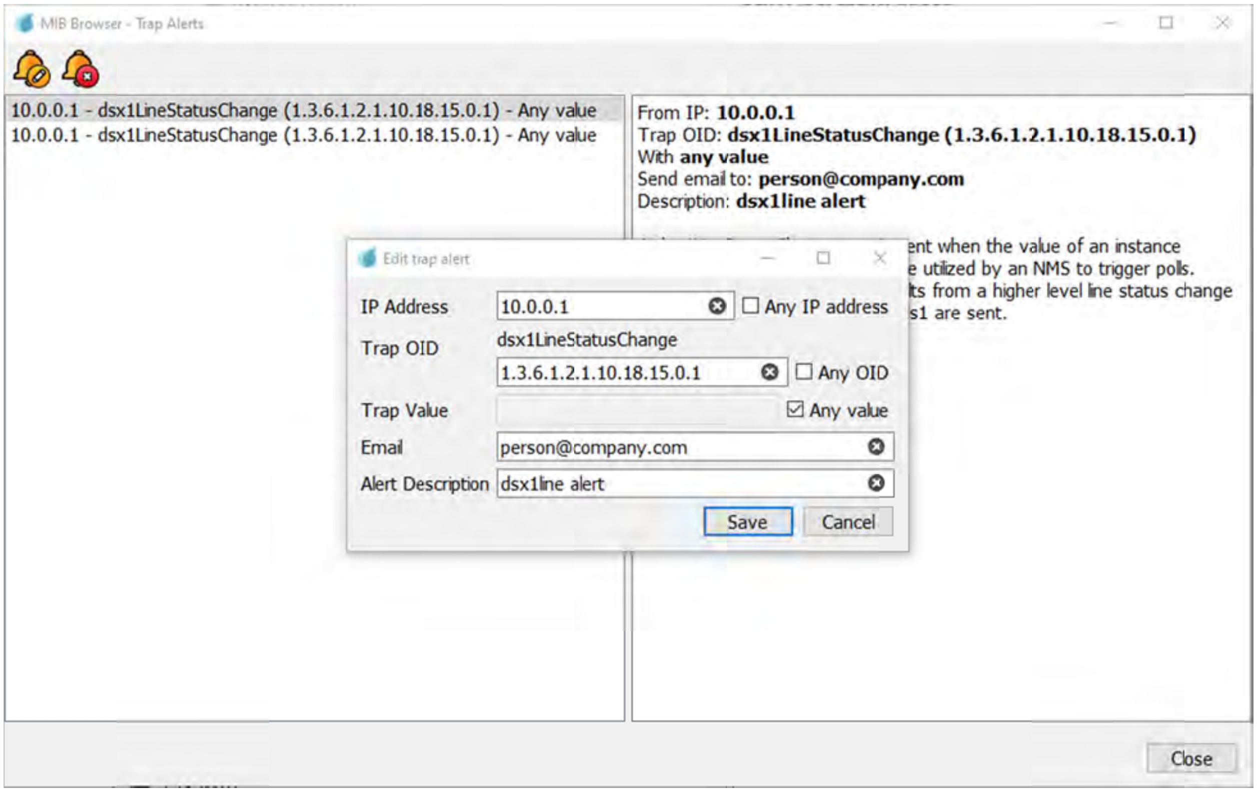

MIB Browser - Trap Alerts

10.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value
10.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value

From IP: **10.0.0.1**
Trap OID: **dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1)**
With **any value**
Send email to: **person@company.com**
Description: **dsx1line alert**

A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes. It can be utilized by an NMS to trigger polls. When the line status change results from a higher level line status change (i.e. ds3), then no traps for the ds1 are sent.

Select the line item you wish to edit and select the bell-and-pencil symbol to modify it.



10.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value
10.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value

From IP: **10.0.0.1**
Trap OID: **dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1)**
With **any value**
Send email to: **person@company.com**
Description: **dsx1line alert**

ent when the value of an instance
e utilized by an NMS to trigger polls.
ts from a higher level line status change
s1 are sent.

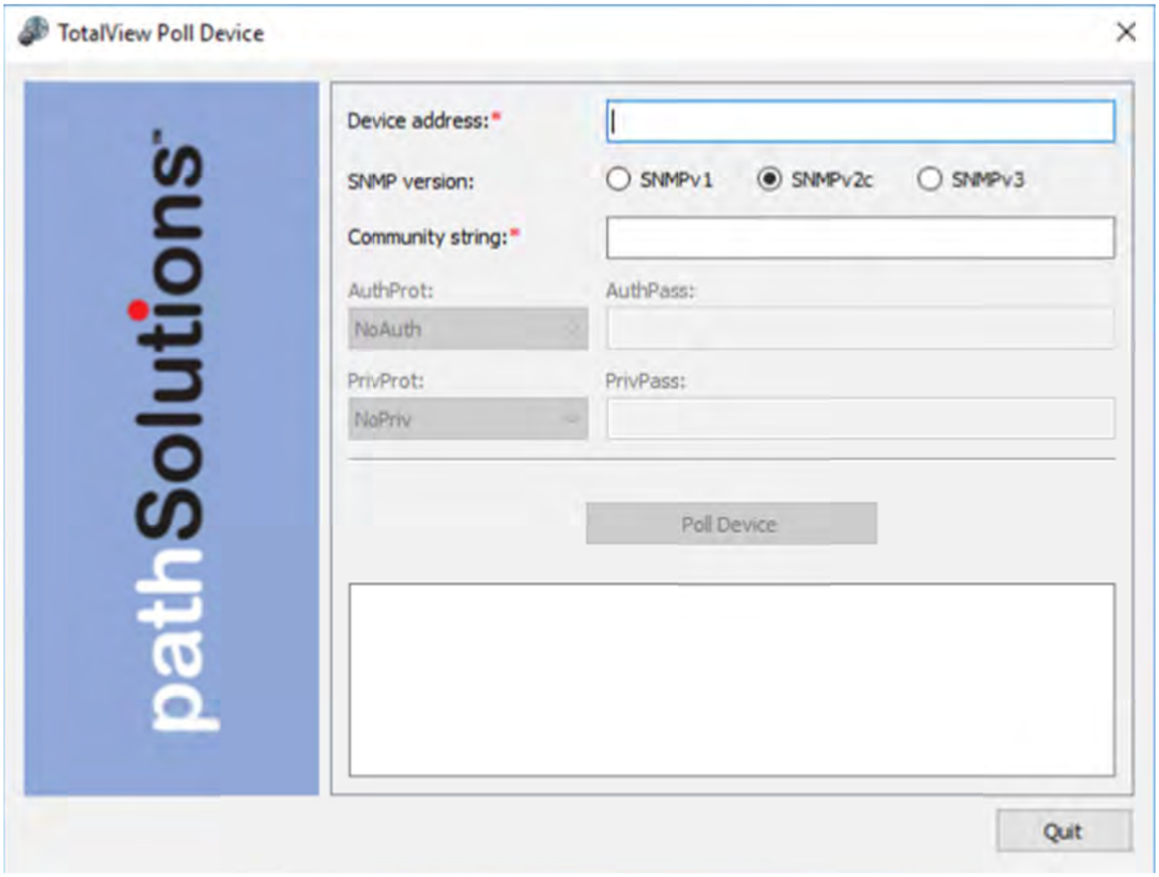
IP Address: 10.0.0.1 □ Any IP address
Trap OID: dsx1LineStatusChange 1.3.6.1.2.1.10.18.15.0.1 □ Any OID
Trap Value: ☑ Any value
Email: person@company.com
Alert Description: dsx1line alert

You may also delete any trap alert previously set up, in this submenu.

Contact support@pathsolutions.com for assistance with setting up SNMP Traps.

Poll Device Tool

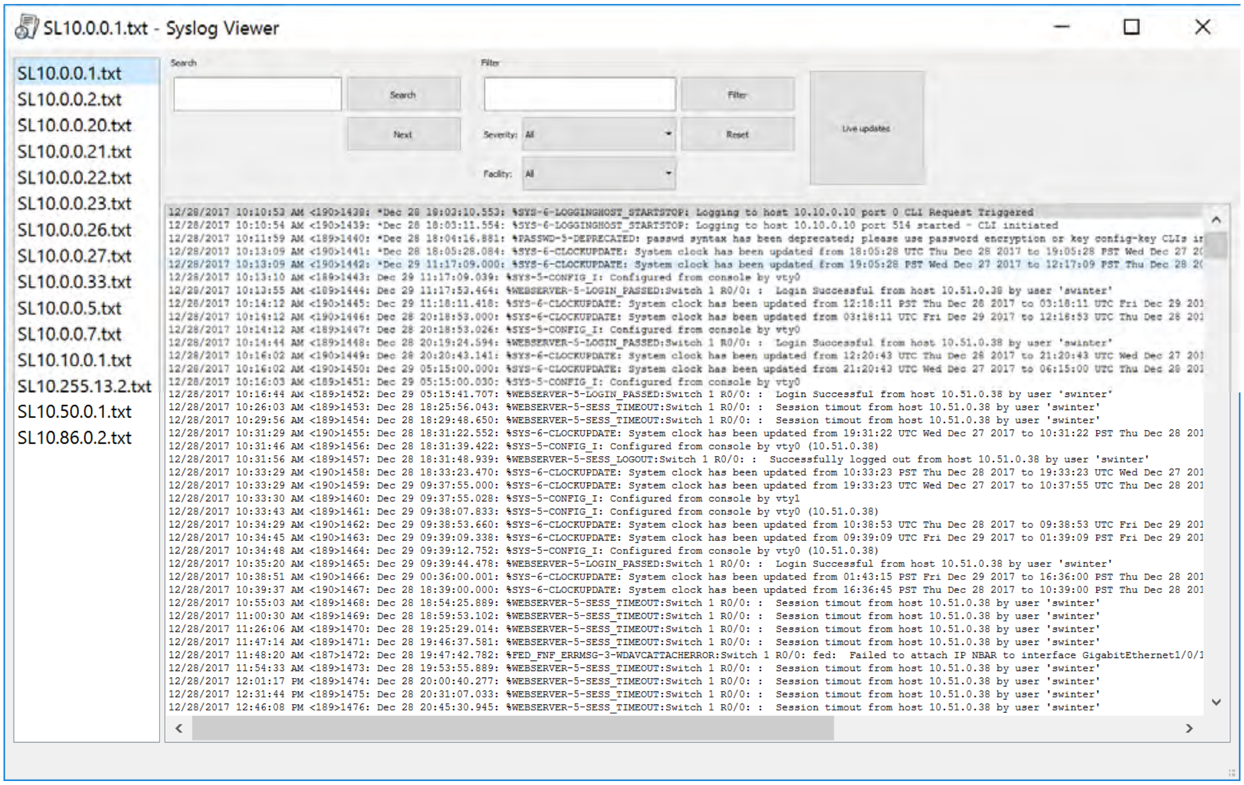
This is a simple test tool to verify that SNMP is communicating correctly. It is a stand-alone program and is run from the **Start/Programs/PathSolutions/TotalView/Poll Device** menu.



Enter a device IP address and SNMP credentials and select **Submit** to test communications. The tool will attempt to ping the remote device to see if it responds to a ping before doing the SNMP query.

Syslog Viewer Tool

This is a file viewer for syslog files that includes filtering and search capabilities. It is a stand-alone program and available to run from the **Start/Programs/PathSolutions/TotalView/Syslog Viewer** menu.



Severity: All

Facility: All

```
12/28/2017 10:10:53 AM <190>1438: *Dec 28 18:03:10.553: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.0.10 port 0 CLI Request Triggered
12/28/2017 10:10:54 AM <190>1439: *Dec 28 18:03:11.554: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.0.10 port 514 started - CLI initiated
12/28/2017 10:11:59 AM <189>1440: *Dec 28 18:04:16.881: %PASSWD-5-DEPRECATED: passwd syntax has been deprecated; please use password encryption or key config-key CLIs ir
12/28/2017 10:13:09 AM <190>1441: *Dec 28 18:05:28.084: %SYS-6-CLOCKUPDATE: System clock has been updated from 18:05:28 UTC Thu Dec 28 2017 to 19:05:28 PST Wed Dec 27 20
12/28/2017 10:13:09 AM <190>1442: *Dec 29 11:17:09.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 19:05:28 PST Wed Dec 27 2017 to 12:17:09 PST Thu Dec 28 20
12/28/2017 10:13:10 AM <189>1443: Dec 29 11:17:09.039: %SYS-5-CONFIG_I: Configured from console by vty0
12/28/2017 10:13:55 AM <189>1444: Dec 29 11:17:53.464: %WEBSERVER-5-LOGIN_PASSED:Switch 1 R0/0: :  Login Successful from host 10.51.0.38 by user 'swinter'
12/28/2017 10:14:12 AM <190>1445: Dec 29 11:18:11.418: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:18:11 PST Thu Dec 28 2017 to 03:18:11 UTC Fri Dec 29 201
12/28/2017 10:14:12 AM <190>1446: Dec 28 20:18:53.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 03:18:11 UTC Fri Dec 29 2017 to 12:18:53 UTC Thu Dec 28 201
12/28/2017 10:14:12 AM <189>1447: Dec 28 20:18:53.026: %SYS-5-CONFIG_I: Configured from console by vty0
12/28/2017 10:14:44 AM <189>1448: Dec 28 20:19:24.594: %WEBSERVER-5-LOGIN_PASSED:Switch 1 R0/0: :  Login Successful from host 10.51.0.38 by user 'swinter'
12/28/2017 10:16:02 AM <190>1449: Dec 28 20:20:43.141: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:20:43 UTC Thu Dec 28 2017 to 21:20:43 UTC Wed Dec 27 201
12/28/2017 10:16:02 AM <190>1450: Dec 29 05:15:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 21:20:43 UTC Wed Dec 27 2017 to 06:15:00 UTC Thu Dec 28 201
12/28/2017 10:16:03 AM <189>1451: Dec 29 05:15:00.030: %SYS-5-CONFIG_I: Configured from console by vty0
12/28/2017 10:16:44 AM <189>1452: Dec 29 05:15:41.707: %WEBSERVER-5-LOGIN_PASSED:Switch 1 R0/0: :  Login Successful from host 10.51.0.38 by user 'swinter'
12/28/2017 10:26:03 AM <189>1453: Dec 28 18:25:56.043: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 10:29:56 AM <189>1454: Dec 28 18:29:48.650: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 10:31:29 AM <190>1455: Dec 28 18:31:22.552: %SYS-6-CLOCKUPDATE: System clock has been updated from 19:31:22 UTC Wed Dec 27 2017 to 10:31:22 PST Thu Dec 28 201
12/28/2017 10:31:46 AM <189>1456: Dec 28 18:31:39.422: %SYS-5-CONFIG_I: Configured from console by vty0 (10.51.0.38)
12/28/2017 10:31:56 AM <189>1457: Dec 28 18:31:48.939: %WEBSERVER-5-SESS_LOGOUT:Switch 1 R0/0: :  Successfully logged out from host 10.51.0.38 by user 'swinter'
12/28/2017 10:33:29 AM <190>1458: Dec 28 18:33:23.470: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:33:23 PST Thu Dec 28 2017 to 19:33:23 UTC Wed Dec 27 201
12/28/2017 10:33:29 AM <190>1459: Dec 29 09:37:55.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 19:33:23 UTC Wed Dec 27 2017 to 10:37:55 UTC Thu Dec 28 201
12/28/2017 10:33:30 AM <189>1460: Dec 29 09:37:55.028: %SYS-5-CONFIG_I: Configured from console by vty1
12/28/2017 10:33:43 AM <189>1461: Dec 29 09:38:07.833: %SYS-5-CONFIG_I: Configured from console by vty0 (10.51.0.38)
12/28/2017 10:34:29 AM <190>1462: Dec 29 09:38:53.660: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:38:53 UTC Thu Dec 28 2017 to 09:38:53 UTC Fri Dec 29 201
12/28/2017 10:34:45 AM <190>1463: Dec 29 09:39:09.338: %SYS-6-CLOCKUPDATE: System clock has been updated from 09:39:09 UTC Fri Dec 29 2017 to 01:39:09 PST Fri Dec 29 201
12/28/2017 10:34:48 AM <189>1464: Dec 29 09:39:12.752: %SYS-5-CONFIG_I: Configured from console by vty0 (10.51.0.38)
12/28/2017 10:35:20 AM <189>1465: Dec 29 09:39:44.478: %WEBSERVER-5-LOGIN_PASSED:Switch 1 R0/0: :  Login Successful from host 10.51.0.38 by user 'swinter'
12/28/2017 10:38:51 AM <190>1466: Dec 29 00:36:00.001: %SYS-6-CLOCKUPDATE: System clock has been updated from 01:43:15 PST Fri Dec 29 2017 to 16:36:00 PST Thu Dec 28 201
12/28/2017 10:39:37 AM <190>1467: Dec 28 18:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 16:36:45 PST Thu Dec 28 2017 to 10:39:00 PST Thu Dec 28 201
12/28/2017 10:55:03 AM <189>1468: Dec 28 18:54:25.889: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 11:00:30 AM <189>1469: Dec 28 18:59:53.102: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 11:26:06 AM <189>1470: Dec 28 19:25:29.014: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 11:47:14 AM <189>1471: Dec 28 19:46:37.581: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 11:48:20 AM <187>1472: Dec 28 19:47:42.782: %FED_FNF_ERRMSG-3-WDAVCATTACHERROR:Switch 1 R0/0: fed:  Failed to attach IP NBAR to interface GigabitEthernet1/0/1
12/28/2017 11:54:33 AM <189>1473: Dec 28 19:53:55.889: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 12:01:17 PM <189>1474: Dec 28 20:00:40.277: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 12:31:44 PM <189>1475: Dec 28 20:31:07.033: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
12/28/2017 12:46:08 PM <189>1476: Dec 28 20:45:30.945: %WEBSERVER-5-SESS_TIMEOUT:Switch 1 R0/0: :  Session timout from host 10.51.0.38 by user 'swinter'
```

The viewer allows you to select a logfile from the left column and review the received syslog messages contained.

Filtering can be performed by entering the information into the filter and selecting **Filter**.

Searching for text can be performed by entering text in the search field and selecting **Search** or **Next**.

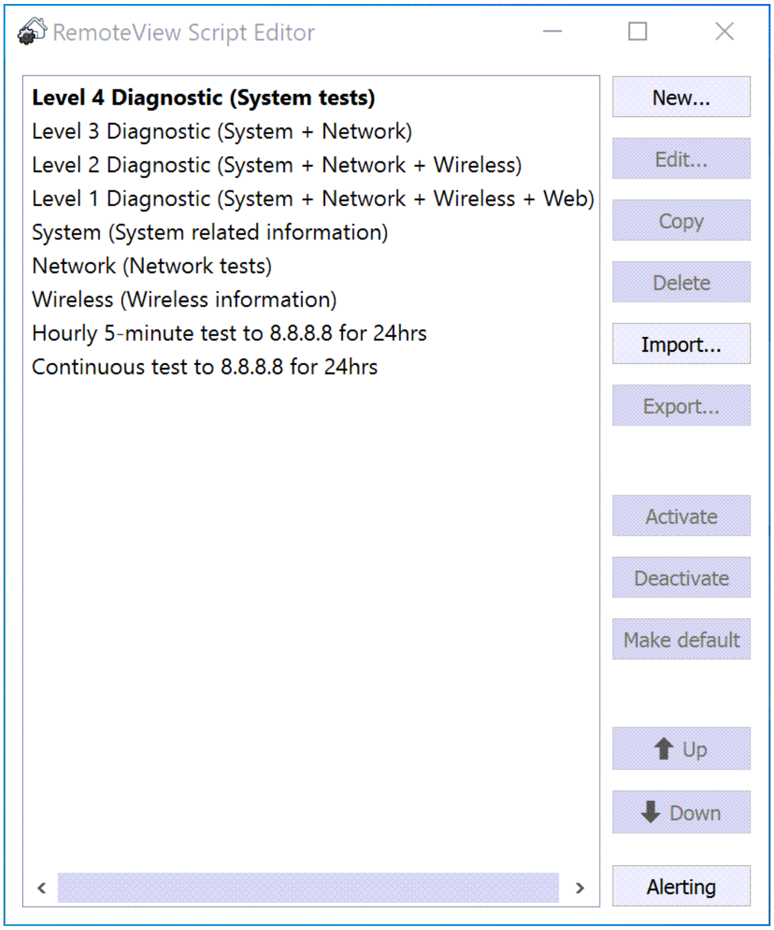
If you want to view newly received syslog messages from a device, select **Live update** to turn this feature on or off.

RemoteInsight Script Editor Tool

You can configure and create your own RemoteInsight batch scripts using this tool. To open the tool, select **Start** and then choose **Programs > PathSolutions > TotalView > SOMETHING**.

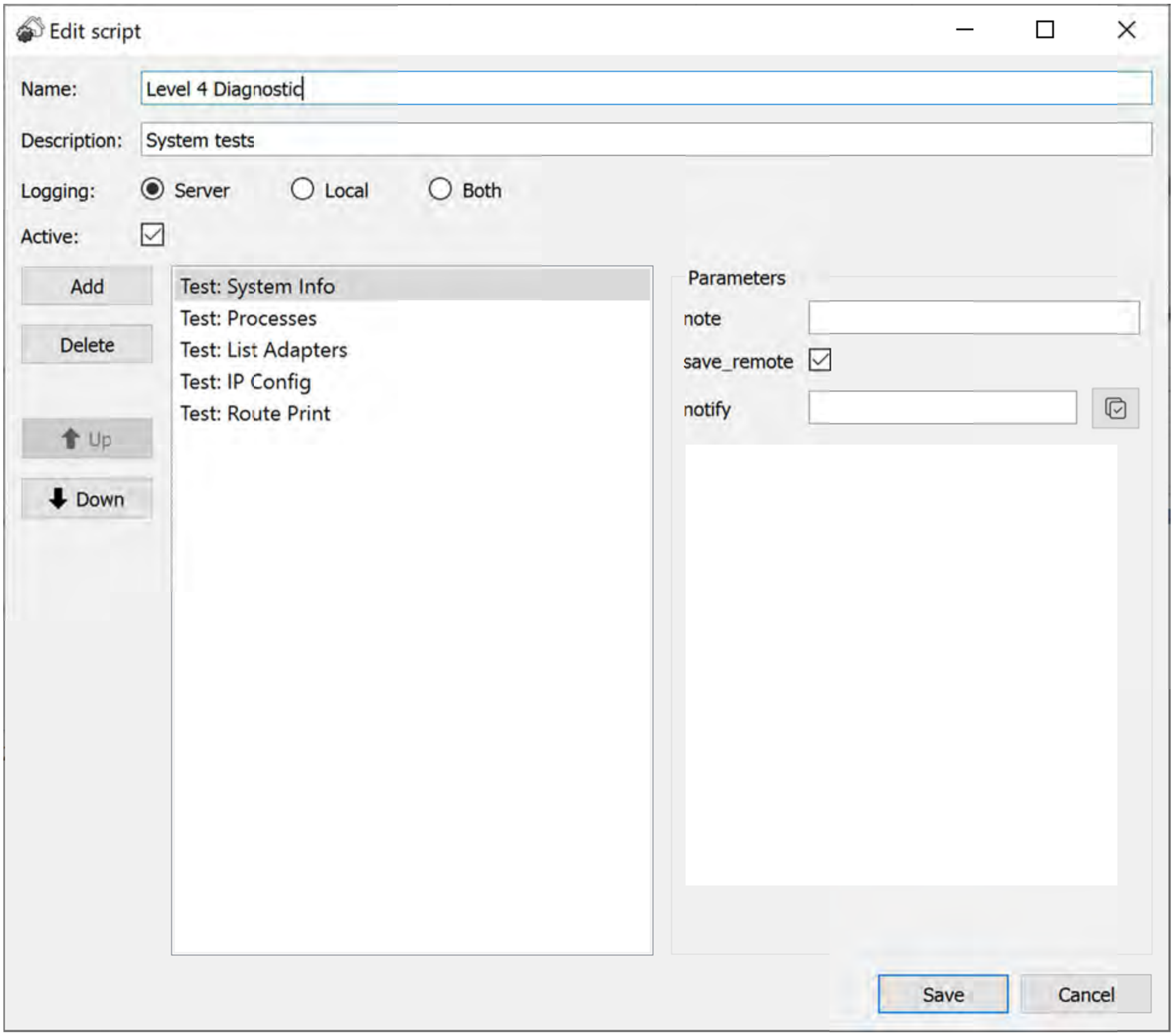
The Script Editor dialog box will open. Note the available pre-written scripts, and on the right, the buttons to create new scripts, edit an existing script, copy, and delete scripts. The scripts will appear in the left pane.

Use the buttons to select scripts and activate or deactivate scripts, and to make one default.



Level 4 Diagnostic (System tests)
Level 3 Diagnostic (System + Network)
Level 2 Diagnostic (System + Network + Wireless)
Level 1 Diagnostic (System + Network + Wireless + Web)
System (System related information)
Network (Network tests)
Wireless (Wireless information)
Hourly 5-minute test to 8.8.8.8 for 24hrs
Continuous test to 8.8.8.8 for 24hrs

To edit a script, select the script (the Level 4 Diagnostic is shown below), and select **Edit**. A dialog box will appear that allows you to name and describe scripts, the place that script results are logged, and what tests the script performs.   You can also setup notes and notifications.



Name: Level 4 Diagnostic

Description: System tests

Logging: ● Server ○ Local ○ Both

Active: ☑

Test: System Info
Test: Processes
Test: List Adapters
Test: IP Config
Test: Route Print

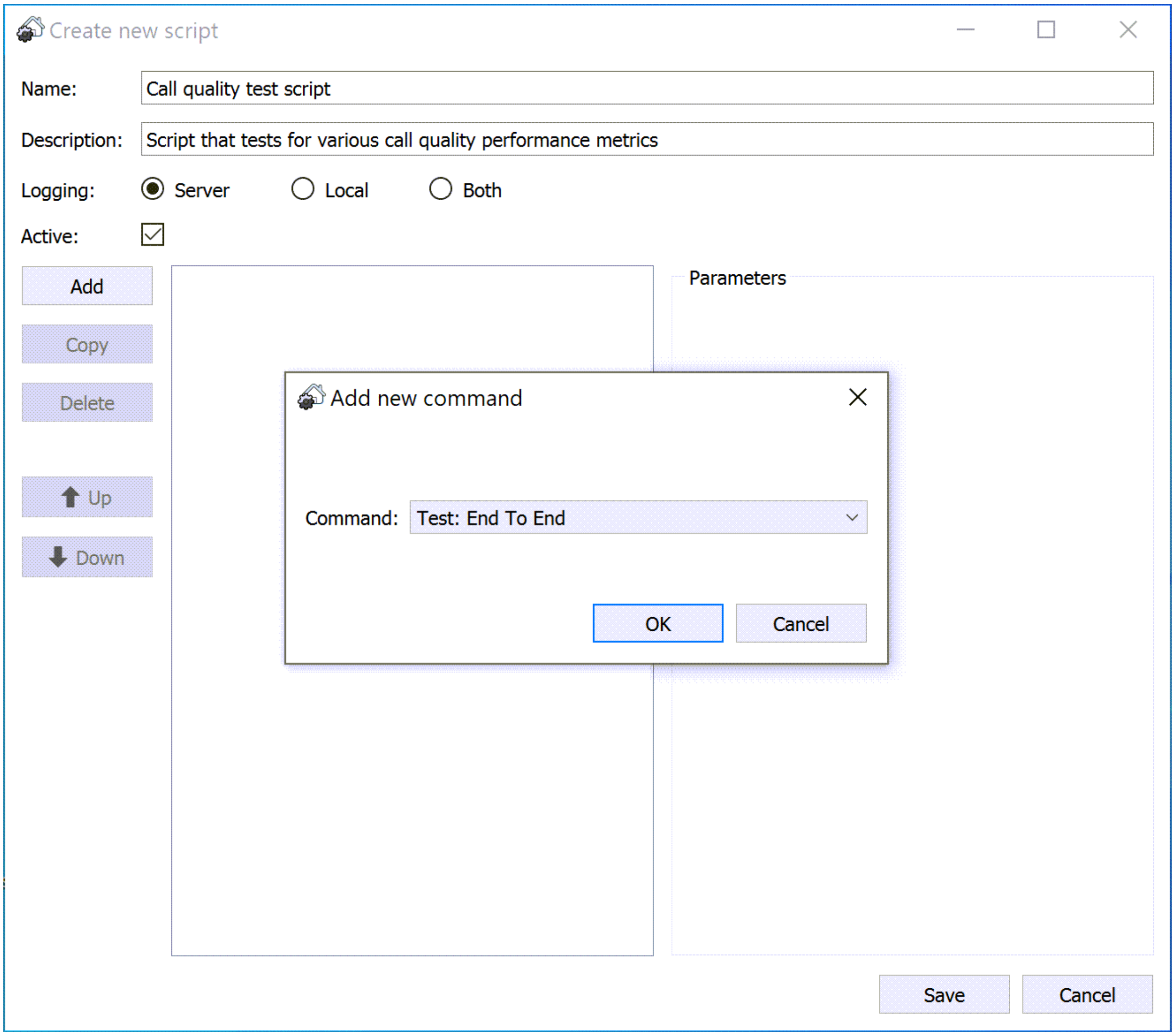
note

save_remote ☑

notify

Add new commands to a script using the **Add** button, then select a new command from the drop-down menu that will appear and select **OK**.

The screenshot below shows an example of adding an end-to-end test.



Create new script

Name: Call quality test script

Description: Script that tests for various call quality performance metrics

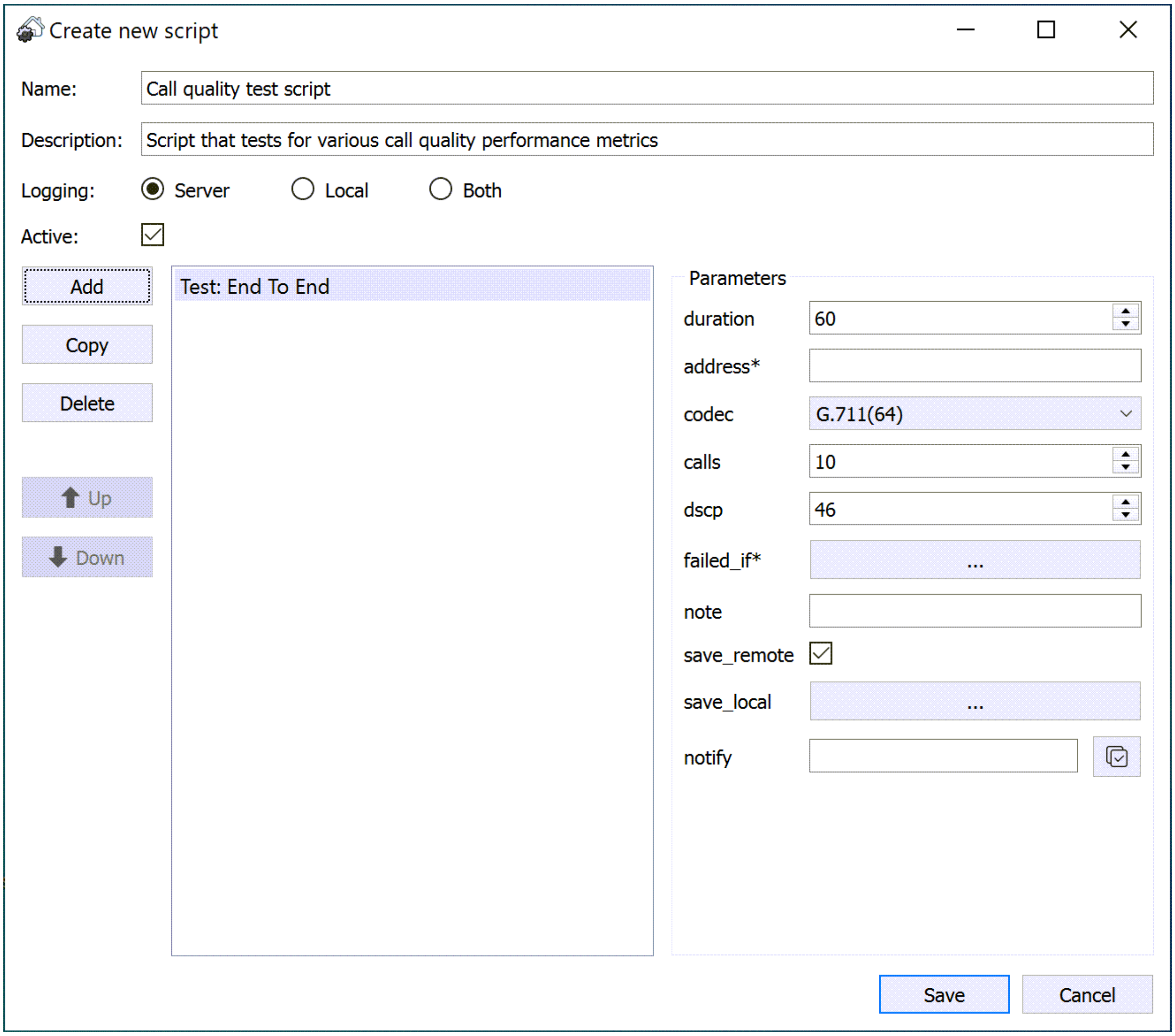
Logging: ● Server ○ Local ○ Both

Active: ☑

Add new command

Command: Test: End To End

The screenshot below shows an example of setting the parameters for the end-to-end test.



Create new script

Name: Call quality test script

Description: Script that tests for various call quality performance metrics

Logging: ● Server ○ Local ○ Both

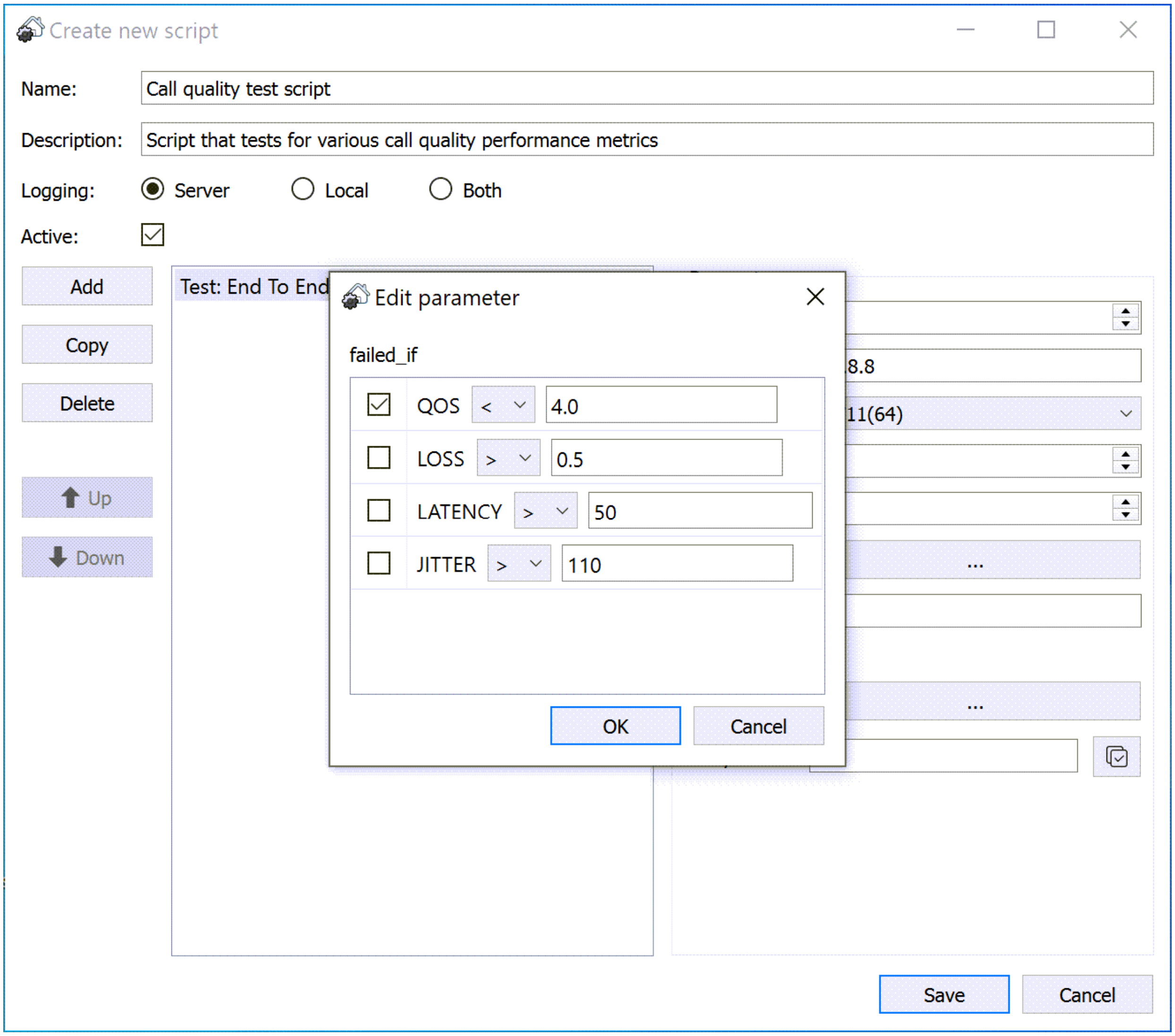
Active: ☑

Test: End To End

Parameters

duration	60
address*	
codec	G.711(64)
calls	10
dscp	46
failed_if*	...
note	
save_remote	☑
save_local	...
notify	

The screenshot below shows an example of setting the fail parameters on an end-to-end test.



Create new script

Name: Call quality test script

Description: Script that tests for various call quality performance metrics

Logging: ● Server ○ Local ○ Both

Active: ☑

Test: End To End

Edit parameter

failed_if

☑	QOS	<	4.0
□	LOSS	>	0.5
□	LATENCY	>	50
□	JITTER	>	110

Appendix A. Email Report Templates and Variables

Existing email report templates are in the **MailTemplates** directory. They can be edited with a text editor and copied to create new templates. The format of the templates includes standard MIME encapsulation headers and definitions for multipart messages (HTML and embedded graphics).

PathSolutions TotalView will pre-process the template and add data elements using the %ELEMENT% replacement strings.

Available replacement strings are as follows:

Server Variables (new in TotalView 12):

%% Prints percent sign	
%ADMINDOWN#%	Prints the number of admin down interfaces
%ADMINDOWN%	Prints a text table of admin down interfaces
%ADMINDOWN*%	Prints an HTML table of admin down interfaces
%ANALYZETICKCOUNT%	Prints the number of ticks (ms) required during the last poll to analyze all data
%ANALYZETICKCOUNTAVG%	Prints the average number of ticks (ms) required to analyze all data
%BACKUP-STATUS%	Status of Last backup
%CAPTURE-FULL%"	device backup
%CAPTURE-SHORT%	first 5 lines of capture-full
%CLOUD-PATH-DETAILS-LINK%	
%CLOUD-PATH-HOPS%	
%CLOUD-PATH-LATENCY%	
%CLOUD-PATH-LOSS%	
%CLOUD-SERVICE-DNS%	
%CLOUD-SERVICE-IP%	
%CLOUD-SERVICE-LATENCY-THRESHOLD%	
%CLOUD-SERVICE-LOSS-THRESHOLD%	
%CLOUD-SERVICE-NAME%	
%CLOUD-SERVICE-PORT%	
%COMMENT-END%	Ends a comment area
%COMMENT-START%	Starts a comment area that won't be sent in the email
%COMPANYNAME%	Prints the company name
%CUSTOMERLOCATION%	Prints the licensed customer location
%CUSTOMERNUMBER%	Prints the licensed customer number
%DATE%	Prints current date
%DEVICE-ADMINDOWN%	Prints the number of admin down interfaces on the device
%DEVICE-AGENT%	Prints the device agent (IP address)
%DEVICE-CONTACT%	Prints the device configured contact (sysContact)
%DEVICE-CONTRACT-DATE%	Prints the configured device service contract date
%DEVICE-CONTRACT-ID%	Prints the configured device ID number associated with the service contract
%DEVICE-CONTRACT-PHONE%	Prints the configured device service contract phone number
%DEVICE-CPU%	Prints the device current CPU utilization graph (Cisco IOS only)
%DEVICE-DAILY-CPU%	Prints base64 encoding of the daily CPU utilization graph (Cisco IOS only)
%DEVICE-DAILY-JITTER%	Prints base64 encoding of the daily jitter graph (VoIP only)
%DEVICE-DAILY-LATENCY%	Prints base64 encoding of the daily latency graph (VoIP only)
%DEVICE-DAILY-LOSS%	Prints base64 encoding of the daily loss graph (VoIP only)
%DEVICE-DAILY-MOS%	Prints base64 encoding of the daily MOS graph (VoIP only)
%DEVICE-DAILY-RAM%	Prints base64 encoding of the daily RAM utilization graph (Cisco IOS only)
%DEVICE-DAILY-UTIL%	Prints base64 encoding of the daily device overall utilization graph
%DEVICE-DESCRIPTION%	Prints the configured device description
%DEVICE-DIFF-FROM-LAST-BACKUP*%	Diff from Last Backup
%DEVICE-GROUP%	Prints the configured group for the device
%DEVICE-INT-DESCRIPTION%	Prints the device internal description (sysDescr)
%DEVICE-INTERFACES%	Prints the number of interfaces for the device
%DEVICE-LOCATION%	Prints the device configured location (sysLocation)
%DEVICE-MONTHLY-CPU%	Prints base64 encoding of the monthly CPU utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-JITTER%	Prints base64 encoding of the monthly jitter graph (VoIP only)

%DEVICE-MONTHLY-LATENCY%	Prints base64 encoding of the monthly latency graph (VoIP only)
%DEVICE-MONTHLY-LOSS%	Prints base64 encoding of the monthly loss graph (VoIP only)
%DEVICE-MONTHLY-MOS%	Prints base64 encoding of the monthly MOS graph (VoIP only)
%DEVICE-MONTHLY-RAM%	Prints base64 encoding of the monthly RAM utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-UTIL%	Prints base64 encoding of the monthly device overall utilization graph
%DEVICE-NAME%	Prints the device configured name (sysName)
%DEVICE-NUMBER%	Prints the device number
%DEVICE-OPERDOWN%	Prints the number of oper down interfaces on the device
%DEVICE-RAM%	Prints the device current RAM utilization graph (Cisco IOS only)
%DEVICE-SERIALNO%	Prints the device serial number (Cisco IOS only)
%DEVICE-WEEKLY-CPU%	Prints base64 encoding of the weekly CPU utilization graph (Cisco IOS only)
%DEVICE-WEEKLY-JITTER%	Prints base64 encoding of the weekly jitter graph (VoIP only)
%DEVICE-WEEKLY-LATENCY%	Prints base64 encoding of the weekly latency graph (VoIP only)
%DEVICE-WEEKLY-LOSS%	Prints base64 encoding of the weekly loss graph (VoIP only)
%DEVICE-WEEKLY-MOS%	Prints base64 encoding of the weekly MOS graph (VoIP only)
%DEVICE-WEEKLY-RAM%	Prints base64 encoding of the weekly RAM utilization graph (Cisco IOS only)
%DEVICE-WEEKLY-UTIL%	Prints base64 encoding of the weekly device overall utilization graph
%DEVICE-YEARLY-CPU%	Prints base64 encoding of the yearly CPU utilization graph (Cisco IOS only)
%DEVICE-YEARLY-JITTER%	Prints base64 encoding of the yearly jitter graph (VoIP only)
%DEVICE-YEARLY-LATENCY%	Prints base64 encoding of the yearly latency graph (VoIP only)
%DEVICE-YEARLY-LOSS%	Prints base64 encoding of the yearly loss graph (VoIP only)
%DEVICE-YEARLY-MOS%	Prints base64 encoding of the yearly MOS graph (VoIP only)
%DEVICE-YEARLY-RAM%	Prints base64 encoding of the yearly RAM utilization graph (Cisco IOS only)
%DEVICE-YEARLY-UTIL%	Prints base64 encoding of the yearly device overall utilization graph
%EMAILADDRESS%	Prints the email address(es) that this email will be sent to
%ENDIF%	Ends a conditional IFSTATUS section
%ENDIF-CISCO%	Ends conditional for Cisco device
%ENDIF-VOIP%	Ends conditional for VoIP License
%ENTITY-NAME%	The name of the device, interface that is generating the alert. This can be used to correlate multiple alerts together that are all associated with a single problem.
%FAVORITES%	Prints a text table of favorite interfaces
%FAVORITES*%	Prints an HTML table of favorite interfaces
%GUID%	A unique identifier for this specific alert. This can be used to de-duplicate alerts.
%IFDEVICE-CISCO%	Prints the following if it is a Cisco device
%IFLICENSE-VOIP%	Prints the following if the system is licensed for VoIP
%IFSTATUS-DEGRADED%	Prints the following if there are issues
%IFSTATUS-GOOD%	Prints the following if there are no issues
%INT-ADMINSTATUS%	Prints the current admin status of the interface
%INT-ADMINSTATUSLAST%	Prints the last admin status of the interface
%INT-ALIAS%	Prints the interface alias
%INT-CURRERRPCT%	Prints the current (last poll) error rate of the interface
%INT-CURRRXUTIL%	Prints the current (last poll) receive rate of the interface
%INT-CURRTXUTIL%	Prints the current (last poll) transmit rate of the interface
%INT-DAILY-BCSTS%	Prints base64 encoding of the daily broadcasts graph
%INT-DAILY-BPS%	Prints base64 encoding of the daily bits per second graph
%INT-DAILYERRORRATE%	Prints the daily peak error rate
%INT-DAILYERRORRATECOLOR%	Prints the daily peak error rate color
%INT-DAILY-ERRORS%	Prints base64 encoding of the daily errors graph
%INT-DAILY-PCT%	Prints base64 encoding of the daily percentage graph
%INT-DAILY-PKTS%	Prints base64 encoding of the daily packets graph
%INT-DAILY-PPCT%	Prints base64 encoding of the daily peak percentage graph
%INT-DAILYRXRATE%	Prints the peak daily receive rate
%INT-DAILYRXRATECOLOR%	Prints the peak daily receive rate color
%INT-DAILYTXRATE%	Prints the peak daily transmit rate
%INT-DAILYTXRATECOLOR%	Prints the peak daily transmit rate color
%INT-DESCRIPTION%	Prints the interface description
%INT-DUPLEX%	Prints the interface duplex of the interface
%INTERFACES%	Prints the number of monitored interfaces
%INT-MONTHLY-BCSTS%	Prints base64 encoding of the monthly broadcasts graph
%INT-MONTHLY-BPS%	Prints base64 encoding of the monthly bits per second graph
%INT-MONTHLY-ERRORS%	Prints base64 encoding of the monthly errors graph
%INT-MONTHLY-PCT%	Prints base64 encoding of the monthly percentage graph
%INT-MONTHLY-PKTS%	Prints base64 encoding of the monthly packets graph

%INT-MONTHLY-PPCT%	Prints base64 encoding of the monthly peak percentage graph
%INT-NAME%	Prints the interface name
%INT-NUMBER%	Prints the interface number
%INT-OPERSTATUS%	Prints the current oper status of the interface
%INT-OPERSTATUSLAST%	Prints the last oper status of the interface
%INT-POEMAXDRAW%	Maximum power draw of an interface
%INT-POESTATE%	Current PoE state
%INT-POESTATELAST%	Last PoE state
%INT-RXBROADCAST%	Prints the receive broadcast rate of the interface
%INT-SPEED%	Prints the interface speed of the interface
%INT-TXBROADCAST%	Prints the transmit broadcast rate of the interface
%INT-WEEKLY-BCSTS%	Prints base64 encoding of the weekly broadcasts graph
%INT-WEEKLY-BPS%	Prints base64 encoding of the weekly bits per second graph
%INT-WEEKLY-ERRORS%	Prints base64 encoding of the weekly errors graph
%INT-WEEKLY-PCT%	Prints base64 encoding of the weekly percentage graph
%INT-WEEKLY-PKTS%	Prints base64 encoding of the weekly packets graph
%INT-WEEKLY-PPCT%	Prints base64 encoding of the weekly peak percentage graph
%INT-YEARLY-BCSTS%	Prints base64 encoding of the yearly broadcasts graph
%INT-YEARLY-BPS%	Prints base64 encoding of the yearly bits per second graph
%INT-YEARLY-ERRORS%	Prints base64 encoding of the yearly errors graph
%INT-YEARLY-PCT%	Prints base64 encoding of the yearly percentage graph
%INT-YEARLY-PKTS%	Prints base64 encoding of the yearly packets graph
%INT-YEARLY-PPCT%	Prints base64 encoding of the yearly peak percentage graph
%ISSUES#%	Prints the current number of issues
%ISSUES%	Prints a text table of current issues
%ISSUES*%	Prints an HTML table of current issues
%LICENSEDAYSLEFT%	Prints the number of licensed days remaining
%LICENSEDINTERFACES%	Prints the licensed interface count
%LICENSEEXPIRATION%	Prints the license expiration
%NETWORK-SERVICE-DESCRIPTION%	Service Description
%NETWORK-SERVICE-GROUP%	Service Group Name
%NETWORK-SERVICE-NOTE%	Service Note
%NETWORK-SERVICE-NOTIFY%	Service Monitor Email Recipient
%NETWORK-SERVICE-PORT%	Service Monitored Port
%NETWORK-SERVICE-PROTOCOL%	Service Protocol
%OID-DESCR%	OID Description
%OID-DEVICE-IP%	OID Device IP address
%OID-DEVICE-NAME%	OID Device name
%OID-INTERFACE%	OID Interface number
%OID-NOTE%	OID Note
%OID-THRESHOLD%	OID Threshold
%OID-VALUE%	OID Value
%OPERDOWN#%	Prints the number of oper down interfaces
%OPERDOWN%	Prints a text table of oper down interfaces
%OPERDOWN*%	Prints an HTML table of oper down interfaces
%OUTPUTTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to write output information
%OUTPUTTICKCOUNTAVG%	Prints the average number of ticks (ms) required to write output information
%POLLDELAY%	Prints the current configured poll delay
%POLLFAILSECONDS%	Prints the number of seconds that the last poll failed by
%POLLFAILTABLE%	Prints the text version of the poll fail table
%POLLFAILTABLE*%	Prints the HTML version of the poll fail table
%POLLHOURS%	Prints the configured poll delay hours
%POLLMINUTES%	Prints the configured poll delay minutes
%POLLSECONDS%	Prints the configured poll delay seconds
%POLLTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to collect SNMP information from all devices
%POLLTICKCOUNTAVG%	Prints the average number of ticks (ms) required to collect SNMP information from all devices
%PRODNAME%	Prints the product name
%PRODNUMBER%	Prints the product license number
%RESELLERNUMBER%	Prints the reseller number
%REVISION%	Prints the revision of the program

%SAVESTATSTICKCOUNT%	Prints the number of ticks (ms) required during the last poll to save statistics to disk
%SAVESTATSTICKCOUNTAVG%	Prints the average number of ticks (ms) required to save statistics to disk
%SERVER-AGENT%	Server Agent Name
%SERVER-NAME%	Server Name
%SERVER-OU%	Server OU name
%SERVER-SERVICE-DESCRIPTION%	Server Service Description
%SERVER-SERVICE-DISPLAY-NAME%	Server Service Display Name
%SERVER-URL%	- direct link to individual sever page
%SESSION-OUTPUT%	- all terminal output
%SSH-LOG%	- libssh library log
%STATUS-COLOR%	Prints “#008000” or “#FF0000” depending if there are any issues
%STATUS-ERR%	Prints the configured error threshold level
%STATUS-PERCENT%	Prints the current health percentage
%STATUS-RESULT%	Prints “Good” or “Degraded” depending if there are any issues
%STATUS-UTIL%	Prints the configured utilization threshold level
%SYSTEM-DAILY-ERRORS%	Prints base64 encoding of the daily overall errors graph
%SYSTEM-DAILY-INTERFACES%	Prints base64 encoding of the daily interfaces graph
%SYSTEM-DAILY-ISSUES%	Prints base64 encoding of the daily overall issues graph
%SYSTEM-DAILY-UTIL%	Prints base64 encoding of the daily aggregate utilization graph
%SYSTEM-MONTHLY-ERRORS%	Prints base64 encoding of the monthly overall errors graph
%SYSTEM-MONTHLY-INTERFACES%	Prints base64 encoding of the monthly interfaces graph
%SYSTEM-MONTHLY-ISSUES%	Prints base64 encoding of the monthly overall issues graph
%SYSTEM-MONTHLY-UTIL%	Prints base64 encoding of the monthly aggregate utilization graph
%SYSTEM-WEEKLY-INTERFACES%	Prints base64 encoding of the weekly interfaces graph
%SYSTEM-WEEKLY-ISSUES%	Prints base64 encoding of the weekly overall issues graph
%SYSTEM-WEEKLY-UTIL%	Prints base64 encoding of the weekly aggregate utilization graph
%SYSTEM-WEEKLY-UTIL%	Prints base64 encoding of the weekly overall errors graph
%SYSTEM-YEARLY-ERRORS%	Prints base64 encoding of the yearly overall errors graph
%SYSTEM-YEARLY-INTERFACES%	Prints base64 encoding of the yearly interfaces graph
%SYSTEM-YEARLY-ISSUES%	Prints base64 encoding of the yearly overall issues graph
%SYSTEM-YEARLY-UTIL%	Prints base64 encoding of the yearly aggregate utilization graph
%TIME%	Prints current time
%TOPCOUNT%	Prints the number of interfaces configured for the Top list
%TOPERRORS%	Prints a text table of top interfaces with errors
%TOPERRORS*%	Prints an HTML table of top interfaces with errors
%TOPJITTER%	Prints a text table of the top devices with the highest daily jitter sorted by jitter
%TOPJITTER*%	Prints an HTML table showing top devices with the highest daily jitter sorted by jitter
%TOPLATENCY%	Prints a text table of the top devices with the highest daily latency sorted by latency
%TOPLATENCY*%	Prints an HTML table showing top devices with the highest daily latency sorted by latency
%TOPLISTENERS%	Prints a text table of top listeners
%TOPLISTENERS*%	Prints an HTML table of top listeners
%TOPLOSS%	Prints a text table to the top devices with the highest daily loss sorted by loss
%TOPLOSS*%	Prints an HTML table showing top devices with the highest daily loss sorted by loss
%TOPRECEIVERS%	Prints a text table of the top Interfaces with highest daily received rates
%TOPRECEIVERS*%	Prints an HTML table showing the top Interfaces with highest daily received
%TOPTALKERS%	Prints a text table of top talkers
%TOPTALKERS*%	Prints an HTML table of top talkers
%TOPTRANSMITTERS%	Prints a text table of the top interfaces with the most data transmitted by utilization
%TOPTRANSMITTERS*%	Prints an HTML table showing the top interfaces with the most data
%URL-ADMINDOWN%	Prints the full URL to the admin down page
%URL-DEVICE%	Prints the full URL to the specified device page
%URL-FAVORITES%	Prints the full URL to the favorites page
%URL-GRAPHICS%	Prints the full URL to the graphics directory
%URL-HEALTH%	Prints the full URL to the health page
%URL-HOME%	Prints the full URL to the home page
%URL-INT%	Prints the full URL to the specified interface page
%URL-ISSUES%	Prints the full URL to the issues page

%URL-OPERDOWN%	Prints the full URL to the oper down page
%URL-TOPERRORS%	Prints the full URL to the top errors page
%URL-TOPJITTER%	Prints the full URL to the current top devices with the highest daily jitter
%URL-TOPLATENCY%	Prints the full URL to the current top devices with the highest daily latency
%URL-TOPLISTENERS%	Prints the full URL to the top listeners page
%URL-TOPLOSS%	Prints the full URL to the current top devices with the highest daily loss
%URL-TOPRECEIVERS%	Prints the full URL to the current top receivers web page
%URL-TOPTALKERS%	Prints the full URL to the top talkers page
%URL-TOPTRANSMITTERS%	Prints the full URL to the current top transmitters web page
%VERSION%	Prints the version of the program

Customizing Email Reports

Reports can be emailed to users whenever desired or on regular schedules.

To set up a report to be sent, create a text file with a text editor such as Notepad. This file should contain four fields, separated by at least one <TAB> character:

```
;Email Address    Template File                 Device       Interface
;---------------- ----------------------------  ------------ ---------
jdoe@company.com  IntMailDetailDaily.txt        192.168.1.1  1
jdoe@company.com  IntMailSummartyDaily.txt      192.168.6.12 14
jdoe@company.com  SystemMailDaily.txt           /            /
```

The first field is the email address where the report should be sent.

The second field is the email template file to use to send the report. Templates can be found in the **MailTemplates** subdirectory.

The third field references a monitored device. This field may or may not be required depending on the template used. If a system-wide report is used it does not need a specific device to be referenced and a slash '/' should be used instead.

The fourth field references a specific interface on the specified device. If the report is a system-wide report or a device report no interface needs to be specified and a slash '/' can be used instead.

Save this file with any filename that ends in **.cfg** in the **ReportSend** subdirectory and the report(s) will be sent during the next polling period and the file deleted.

Note: It's valuable to save this file in an alternate directory first and then copy it to the **ReportSend** directory when you want it to be sent.

Note: This process can be automated via the Windows Task manager to schedule reports to be sent on a regular basis.

Note: All files in the **ReportSend** directory with the extension .cfg will be processed and deleted every poll period.

Appendix B. SMTP Email Forwarding

Most companies use SMTP gateways to allow email from the Internet to reach internal users.

This gateway is typically set up to receive emails that are destined for mailboxes on the company's system.

If you configure the PathSolutions TotalView to use your company's SMTP mail gateway, the gateway should accept SMTP messages destined for internal users, but should not accept SMTP messages destined for outside addresses.

For example:

If you configured TotalView to use "mail.company.com " as the SMTP mail gateway, and set the **Globally send to** field to `jdoe@company.com`, the mail gateway would accept emails sent to this address because it exists on the same domain. If the **Globally send to** field was set to `jdoe@outside.com`, then the gateway would refuse this request because most mail systems do not allow relaying of messages from one to another.

This is done by mail administrators to prevent abuse by spammers. Email spammers will search the Internet for anonymous SMTP mail forwarders that they can use to send their emails out.

This allows them to send untraceable emails.

To allow the PathSolutions TotalView to send emails to different domains, there are a number of solutions:

- Ask your ISP if they have an SMTP relay server that can be used by your machines. They may have a server set up that will relay only your messages. In this case, you would configure TotalView to use their SMTP relay server.
- Ask your email administrator to configure the SMTP gateway to allow relaying from the server that TotalView is installed on.

Create a mail alias on your email system (for example: `jdoe@company.com`) that forwards to an outside address (`jdoe@outside.com`).

A free SMTP mail relay agent (SMTP forwarder) is included with many Windows server's IIS implementation.

Appendix C. Overriding Displayed Device Icons

The automatically determined device icon may display incorrectly with certain devices. This can be overridden by modifying **DeviceType.cfg** file:

```
C:\Program Files (x86)\PathSolutions\TotalView\DeviceType.cfg
```

This file requires entering two fields, each separated by one or more <TAB> characters.

```
;This is the device icon configuration override file.  It can be used
;to change the displayed icon in front of a device.
;
;IP Address
;Enter the IP address of the device
;
;DeviceType
;Enter the number associated with the device type that should be
;displayed:
;
; 1 = Layer-2 Switch
; 2 = Layer-3 Switch (Multilayer switch)
; 3 = Router
; 4 = WiFi AP
; 5 = Server
; 6 = Cloud
; 7 = Firewall
;
;IP Address                        DeviceType
;---------------                   ----------
```

Enter the IP address of the device and a <TAB> character and the numeric that refers to the type of device icon to use. After the file has been modified and saved, stop and restart the PathSolutions TotalView service to have the changes take effect.

Appendix D. Changing Interface Names and Speed

Many device manufacturers do not allow interface names to be changed to a descriptive name to help document the network. In this case, PathSolutions' TotalView can be configured to ignore the interface description in the device and use information from a Config file.

Use a text editor such as Notepad to open the **IntDescription.cfg** file in the directory where the PathSolutions TotalView is installed.

You should see a document with a description of how to enter the switch interfaces and descriptions.

The file is composed of a number of columns or fields; each separated by one or more <TAB> characters.

Note: The fields in the configuration file need to be separated by at least one <TAB> character, not spaces.

Here is an example of a configuration file:

```
;This line is commented out
;
;IPAddress              Interface   Speed       Description
;-----------            ---------   ------      ---------------
192.168.1.10            1           /           Internet connection
calvin.company.com      156         1544000     FE0/6
192.168.2.2             3           /           Connection to New York
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

IP Addresses

The IP address of the switch must be entered to identify the device. If the Config file has a DNS name, then that identical name should be used here to identify the same device.

Interface

The interface number (as listed in the web reports) should be entered here. If you are unsure of the exact number to use, reference your device manufacturer's documentation to map the SNMP interface numbers to the physical addresses on the device. Then use your network documentation to determine what device is physically connected to the interface on the device.

Speed

To override the reported interface speed, enter the speed in bits per second here. For example: To change the reported interface speed of a router interface connected to the Internet from 100 Mbps to the actual capacity of the link it is connected to (1.544 Mbps for a T1 connection). This will help to determine when the link utilization is exceeded. If you do not want to override this information, enter a slash "/" to skip this field.

Description

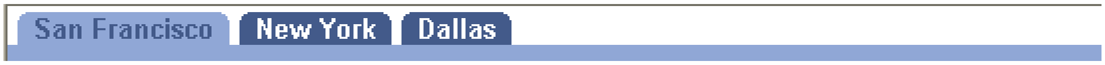
Enter the description here. The description field should not contain a semicolon character.

Note: The service must be stopped and re-started after this file is modified in order to have the descriptions take effect.

Appendix E. Configuring Multiple Locations

If you have multiple PathSolutions TotalView implementations, TotalView can be configured to make it easy to navigate between the sites.

Each web page will display tabs across the top of the web page indicating the site that you are viewing:



To configure multiple sites, use a text editor like Notepad to open the **MultiSite.cfg** file in the directory where you installed the program:

```
C:\Program Files (x86)\PathSolutions\TotalView\MultiSite.cfg
```

You should see a document with a description of how to enter the site names and URLs.

The file is composed of several columns or fields; each separated by one or more <TAB> characters.

Note: The fields in the configuration file need to be separated by at least one <TAB> character, not spaces.

Here is an example of a configuration file:

```
;Example for the San Francisco server:
;
;Current   Site Name        URL
;-------   --------------   ------------------------------------------
YES        San Francisco    http://sfserver.company.com:8084
NO         New York         http://nyserver.company.com:8084
NO         Chicago          http://chicago.company.com:8084

;Example for the New York server:
;
;Current   Site Name        URL
;-------   --------------   ------------------------------------------
NO         San Francisco    http://sfserver.company.com:8084
YES        New York         http://nyserver.company.com:8084
NO         Chicago          http://chicago.company.com:8084
```

Semicolons can be used anywhere in the file to indicate that the rest of the line is a comment.

Current

This field identifies which site should be highlighted. Only one site should be highlighted per Config file. The Config file on the New York server should have **Yes** for the New York entry.

Site Name

This is the name that is displayed in the tab.

URL

Enter the server's full URL and port here. This will allow linking from the other PathSolutions TotalView servers.

Note: The service must be stopped and re-started after this file is modified to have the links work.

The order of the listed sites should be similar for each deployed site so the tabs will display correctly for each site.

Appendix F. Custom OID Monitoring

*The user-friendly graphical method is with our MIB Browser, but this is how to do it by editing the **OIDEntry.cfg** file:*

PathSolutions TotalView can monitor custom OIDs such as CPU utilization, memory usage, and temperature if the device provides this information via SNMP.

The configuration file **OIDEntry.cfg** is used to configure custom OID monitoring. This file is found in the directory where the program was installed.

```
C:\Program Files (x86)\PathSolutions\TotalView\OIDEntry.cfg
```

Edit this file with a text editor like Notepad.

You will need to enter the following information to be able to set up monitoring of a custom OID:

- IP address of the device (“10.0.1.16”)
- Interface to be associated with or “/” if you want to associate it with the device instead of an interface (“23”)
- Unique filename for storing the data collected for this OID (“FRAMERELAY”)
- Description of this graph (“Frame Relay FECN & BECN”)
- Y Axis description (“Packets”)
- OID #1 Description (“FECN”)
- OID #1 (“GAUGE:1.3.6.1.2.1.2.2.1.17.1”)
- TRANSFORM field (math to be applied to convert numbers)
- Alert threshold (number to not exceed)
- Alert notification (“jdoe@company.com”)

Note: When entering the OID value, enter the prefix **GAUGE**:, **COUNTER:**, or **COUNTER:8** in front of the OID to identify how the OID should be tracked.

Note: After saving this file, stop and restart the TotalView service for the changes to take effect.

Appendix G. Configuring Additional OUIs for Phones

Several OUIs (Organizationally Unique Identifiers) for various VoIP equipment manufacturers have been added to the **OUIFilter.cfg** file. This file can be edited with a text editor (like Notepad) to add additional OUIs. It is located in the program files:

```
      C:\Program Files (x86)\PathSolutions\TotalView\OUIFilter.cfg
```

An OUI is the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.

The **OUIFilter.cfg** file will require you to enter the OUI (each byte separated by a period "."), then a <TAB>, then the name of the manufacturer.

Note: After saving this file, stop and restart the PathSolutions TotalView service for the changes to take effect.

Appendix H. Changing the WAN Tab

*The user-friendly graphical method is in the Config Tool, but this is how to do it by editing the **WAN.cfg** file.*

The **WAN** tab can include any interface desired. This involves changing the **WAN.cfg** file with a text editor (like Notepad). It is located in the program files:

```
      C:\Program Files (x86)\PathSolutions\TotalView\wan.cfg
```

This file requires entering two fields, each separated by one or more <TAB> characters.

```
;This is a list of WAN interfaces to display on the
;"WAN" tab.
;
;Interface numbers are entered in the following format:
;
;IP Address<TAB>Interface number
;
;For example:
;
;IPAddress                         Interface #
;-----------                       ---------------
;192.168.12.15                     43

;
;Enter your IP addresses and interface numbers below.
;IPAddress                         Interface #
;-----------                       ---------------
```

After the WAN.cfg file has been modified and saved, stop and restart the PathSolutions TotalView service to have the changes take effect.

Appendix I. Adding a Static Route to the Call Path

If there is an unmanaged device (or set of devices) in the network, a static route can be added to allow the Call Path mapping to ignore these devices and show a continuous map through the network.

Many times, this may be required if a network provider does not permit SNMP access to their routers.

Adding a static route involves changing the **StaticRoute.cfg** file with a text editor (like Notepad). It is located in the program files:

```
C:\Program Files (x86)\PathSolutions\TotalView\StaticRoute.cfg
```

This file requires entering five fields, each separated by one or more <TAB> characters.

```
;Router Address    Router Subnet    Route            Mask            NextHop
;--------------    ---------------  ---------------  --------------- ---------------
10.0.1.254         255.255.255.0    44.44.44.44      255.255.255.255 38.102.148.163
10.100.36.60       255.255.255.0    10.100.37.1      255.255.255.0   10.100.37.1
10.100.37.1        255.255.255.0    10.100.36.1      255.255.255.0   10.100.36.60
```

The first and second fields reference the router's IP address and subnet that should be used for the static route. This is typically the unmanaged router's IP address where packets are sent.

The third and fourth fields reference the route and subnet mask for that route.

Note: Enter a default route by using the route of 0.0.0.0 and mask of 0.0.0.0.

Note: Static routes take priority over any actual routes that exist on the network.

The fifth field references where the call path mapping should continue. This is typically the far-end router's LAN IP address.

Once the file is saved, the static route takes effect immediately. This will help speed up troubleshooting and debugging of static routes in the environment. No need to stop and restart the service or re-collect information from switches & routers.

Note: Two static routes will likely need to be created. One static route will need to be created for the outbound traffic and one for the return traffic.

Appendix J. Automatic Update Scheduling

Updating the bridge table, ARP cache, and routing table information can be automated to occur on a regular frequency. The following registry entry can be used to update the bridge table.

UpdateAutoFrequency=0

By default, this entry is 0 (zero). This means that the information is not collected on any schedule.

The variable can be changed to any of the following recommended intervals:
300000 (decimal) = 5 minutes
600000 (decimal) = 10 minutes
1800000 (decimal) = 30 minutes
3600000 (decimal) = 1 hour
86400000 (decimal) = 1 day

Other intervals can be used, as the number is the number of milliseconds to wait between automatic updates.

Note: The service must be stopped and restarted for this variable to take effect.

Appendix K. Changing the Map Fetch Variables to Improve Map Stability

You may be seeing white lines going from white to green to white or red dots going from red to green to red. White lines mean there was no SNMP response from the device. The red dots mean there was no response from the ping. There may be a problem with packet loss to/from the device or the device may have a small CPU that causes the 2 pings to fail.

We have 5 seconds to respond to the web browser's request for information. If a device is up, we would send a ping and receive a response within 5 seconds so it's easy to show that it's green.

If we send a ping, we must wait for a response. If we wait 2 seconds and don't receive a response, we can send a second ping and then wait 2 seconds to get a response. If we don't get a response from the second ping, then assume it is down.

TotalView's default performs 1 ping and then waits 2500ms (2.5 seconds) for a response. If it does not see a response, then it assumes it is down.

TotalView' s default performs 2 pings and then waits 1500 (1.5 seconds) for a response. If it does not see a response, then it assumes it is down.

This can be adjusted in the registry with the following variables to help improve the stability of the map.

Example of Variable Entry change in Bold below

Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Mode > Netlatency > SwitchMonitor

```
DestWebMapPingRetries = 1
DestWebMapPingDelay = 2500
```

In this case, set the following:

```
DestWebMapPingRetries = 2
DestWebMapPingDelay = 1500
```

It should improve the reliability/stability of the pings on the network.

For fetching the SNMP information, the following registry variables can be adjusted:

```
DestWebMapSNMPRetries = 1
DestWebMapSNMPTimeout = 1000
```

In this case, set the following:

```
DestWebMapSNMPRetries = 2
DestWebMapSNMPTimeout = 1000
```

The service should be stopped and restarted for these variables to take effect.

Glossary

IETF – This acronym stands for the Internet Engineering Task Force and is the governing body for all standards that relate to Internet and associated communications technologies. Website: www.ietf.org

MAC – Media Access Control: This is a unique address that is used by Ethernet adapters to transmit and receive frames on the network. They are only used for conveying layer 2 frames between nodes on a LAN.

MIME – Multi-Purpose Internet Mail Extensions: This is an email standard that defines how different content is handled inside email messages. This allows graphics, audio, HTML text, formatted text, and video to be displayed correctly inside email messages. MIME is defined by the IETF's RFC1521 document, and is available on the IETF's website: http://www.ietf.org/rfc/rfc1521.txt?number=1521

Network Weather Report – System Monitor can email network reports to you daily. The network Weather Report helps to keep you informed of the overall health of your network.

OSI – Open Systems Interconnect: This is a standard description or "reference model" for how services are provided on a network.

OUI – Organizationally Unique Identifier: This is the identification of the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.

SNMP read-only community string – This is an SNMP password with the rights to be able to read statistical information from a device.

SNMP – Simple Network Management Protocol. This protocol allows network management software (like System Monitor) to communicate with network devices to read statistical information.

SMTP email address – This is a standard Internet email address. For example: `jdoe@company.com`.

SMTP Simple Mail Transport Protocol. This protocol allows email clients and servers to communicate over the Internet.