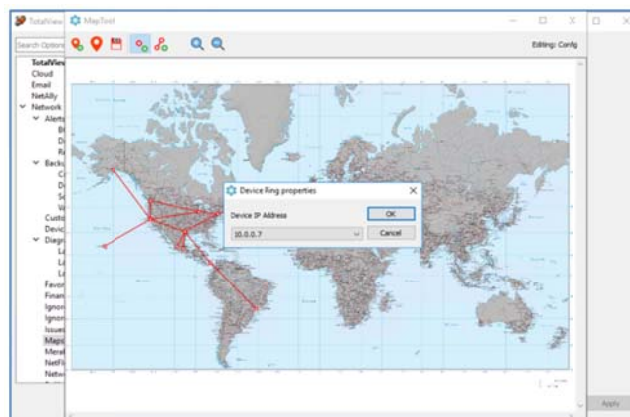




TotalView 14 Administration Guide

NetOps | SecOps | Telecom Ops | RemoteView



Produced by

PathSolutions, Inc.

3080 Olcott Street #A210

Santa Clara, CA 95054

www.PathSolutions.com

Support@PathSolutions.com

Sales@PathSolutions.com

Document and Software Copyrights

Copyright ©2023 by PathSolutions, Inc., Santa Clara, California, U.S.A. All rights reserved. Printed in the United States of America. Contents of this publication may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written authorization of PathSolutions, Inc.

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

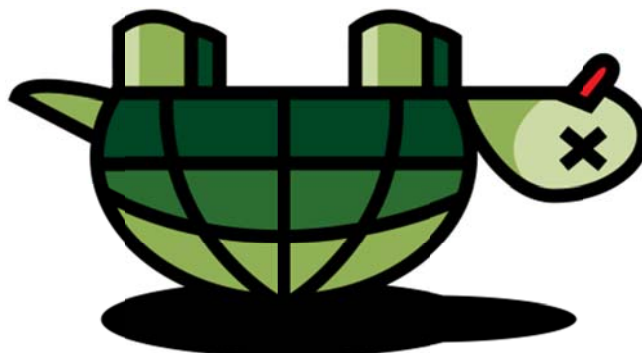
PathSolutions, TotalView, QueueVision, RemoteView, Total Cloud Visibility, Total Network Visibility, and Total VoIP Visibility are Registered Trademarks of PathSolutions, Inc. in the United States and/or other countries. Network Weather Report and Network Prescription are Trademarks of PathSolutions,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

Version Information

TotalView
Version: 14
Date: Feb. 14, 2023

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	5
Technical Support.....	5
Activation and Quick Config Wizard.....	6
Using the Configuration Tool.....	7
Running the Configuration Tool	7
TotalView License Window.....	7
Navigation	8
Buttons	8
Alert Options	10
Cloud Monitoring.....	12
Email Reports	13
Configuring Network Weather Report	13
Configuring Nightly Security Report	14
Additional Email Report Templates	15
NetAlly Settings.....	20
Network Monitoring.....	21
Alerts	22
Backup Configuration	29
Custom OID	37
Devices Configuration	38
Diagram (Interactive Diagrams)	42
Favorites.....	47
Financials	48
Ignored Interfaces.....	49
Ignored Types.....	51
Issues	52
Maps.....	53
Meraki.....	54
NetFlow	55
Network Thresholds.....	58
Polling Behavior.....	59
Syslog.....	61
TFTP Server.....	70
WAN Interfaces	71
NLT	73
Risk Monitoring	74
Alerts	75
Certificates/SSL <i>NEW</i>	76
Dictionary.....	78
DNS Record Monitoring <i>NEW</i>	79
Geographic.....	81
Policies	82
Rogue IT	84
Whitelist.....	85
SD-WAN	86
Servers and Operating Systems.....	87
Linux Servers Monitoring <i>NEW</i>	89
Windows Servers.....	97
Server Thresholds	102
Services	103
VoIP	104
VoIP Alerts.....	105
Phones	106
SIP-Trunks.....	107
Website Interface.....	108

Web Authentication	109
Web Server (Options).....	114
Using the Device Configuration Wizard	116
Re-Configuring TotalView When Your Network Changes	120
Automatic Re-Configuration	121
Other Network Program Configuration Tools.....	122
Interface Discovery Tool	122
Config Editor	125
Map Config Tool.....	126
How to Add Maps	128
How to Add Links.....	129
How to Add Ping Points.....	130
How to Change Items on the Map	130
How to Delete Items on the Map	130
How to Save the Map	131
MIB Browser	132
OID Lookups <i>NEW</i>	133
OID Monitoring <i>NEW</i>	134
OID Graphing	136
SNMP Trap Receiver Configuration	137
Poll Device Tool	140
Syslog Viewer Tool	141
RemoteView Script Editor Tool	142
Appendix A. Email Report Templates and Variables	147
Customizing Email Reports	151
Appendix B. SMTP Email Forwarding.....	152
Appendix C. Overriding Displayed Device Icons	153
Appendix D. Changing Interface Names and Speed	154
Appendix E. Configuring Multiple Locations	155
Appendix F. Custom OID Monitoring	157
Appendix G. Configuring Additional OUIs for Phones	158
Appendix H. Changing the WAN Tab	159
Appendix I. Adding a Static Route to the Call Path	160
Appendix J. Automatic Update Scheduling.....	161
Appendix K. Changing the Map Fetch Variables to Improve Map Stability	162
Glossary	163

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.

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 on how to activate and use the Quick Config Wizard.

The QuickConfig Wizard will auto-configure the PathSolutions TotalView for you and begin monitoring in just a few minutes.

Using the Configuration Tool

The Configuration Tool is used to 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 you can use 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 clicking "Start", choose "Programs", point to "PathSolutions", then choose "TotalView", and then select "Config Tool".

TotalView License Window

If you have not yet entered your subscription information, you may be presented with the following dialog upon starting the program:

The screenshot shows the 'TotalView Configuration Tool' window. On the left is a sidebar with a search bar and a tree view containing categories like TotalView, Alert Options, Cloud, Email, NetAlly, Network, Alerts, Backup, Custom OID, Devices, Diagram, Favorites, Financials, Ignored Interfaces, Ignored Types, Issues, Maps, Meraki, NetFlow, Network Thresholds, Polling, Syslog, TFTP, WAN, NLT, Risks, SD-WAN, Servers, Services, VoIP, and Web Interface. The main area is divided into sections: 'pathSolutions' logo, 'TotalView' and 'PathSolutions' text with the website URL, 'Total Network Visibility®', service versions, copyright, and a 'Copy version info to clipboard' button. The 'License Information' section contains fields for Customer Number, Location, Name, Phone, Email, and MAC Address, followed by a 'Change / Validate License' button. Below this is a 'License Count' table showing usage of interfaces, servers, services, cloud, SD-WAN, and SIP-Trunks. The 'Tech Support' section includes a service account field, a 'Change' button, and a 'Service Status' section indicating 'Service is running' with buttons to start, restart, or stop the service. At the bottom is an 'Event Log' section with a log level display and buttons for debugging.

1094	Licensed interfaces	x 1	1094
14	Servers	x 5	70
23	Services	x 1	23
1999	Cloud	x 3	5997
3	SD-WAN	x 3	9
1	SIP-Trunks	x 3	3
Total used			7196
Licensed			20000

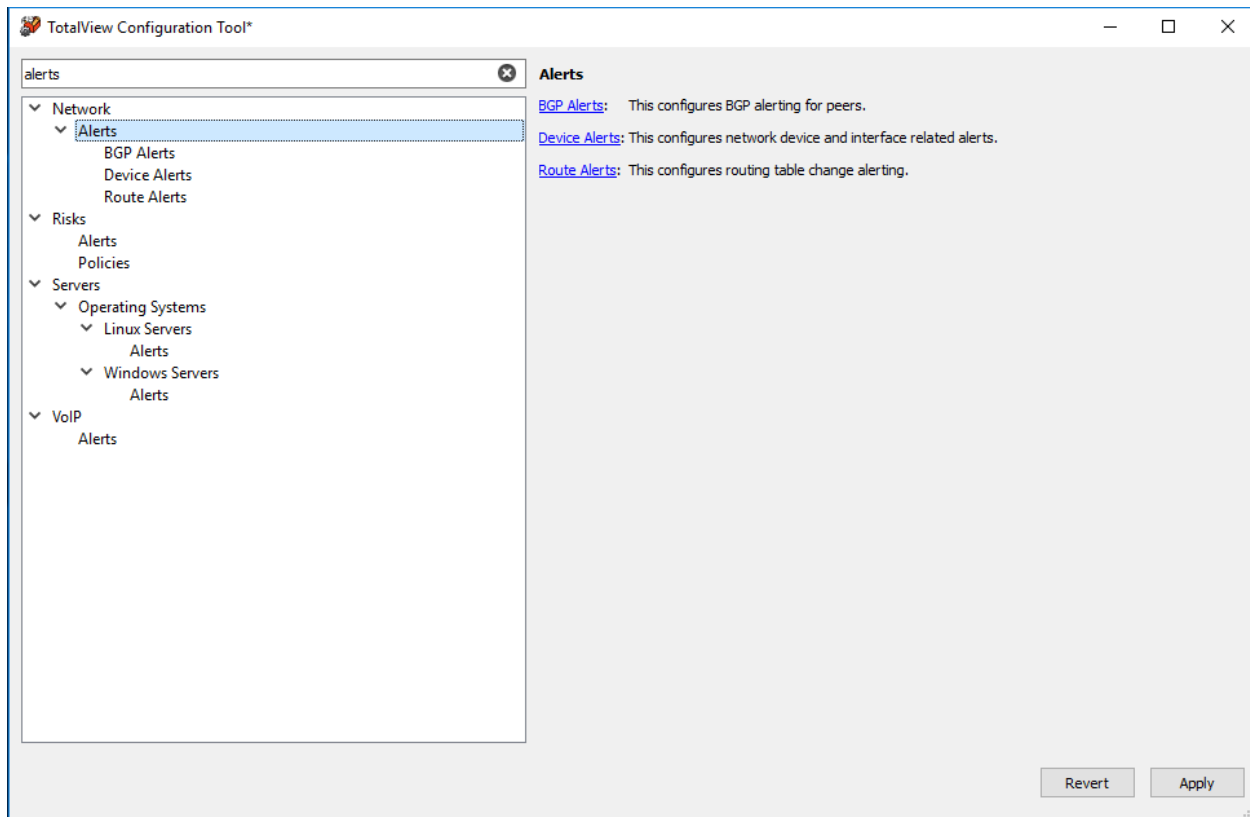
Use this page to validate and/or change your subscription information on your License

Enter your subscription information and then click "Change/Validate License" to validate the license and continue.

If you purchase additional interfaces for your growing network, just give us a call or email and you come back here to Check/Validate license and it will show your new license count!

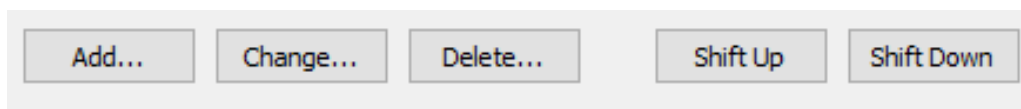
Navigation

There is a menu down the left hand side that shows all the categories you can configure in alphabetical order. You can expand or contract the sections on the list. You can also filter the list by adding words to the filter field at top left. For example, here is a view of filtering on the word “Alerts”:



Buttons

For many sections there are buttons along the bottom to make changes to settings with, and to organize the display:



- Use the “Add” button to add new items like device config and alerts into 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 asking you to confirm you want to delete it.
- Use the “Shift UP” and “Shift Down” buttons to shift the order of items in list up and down.

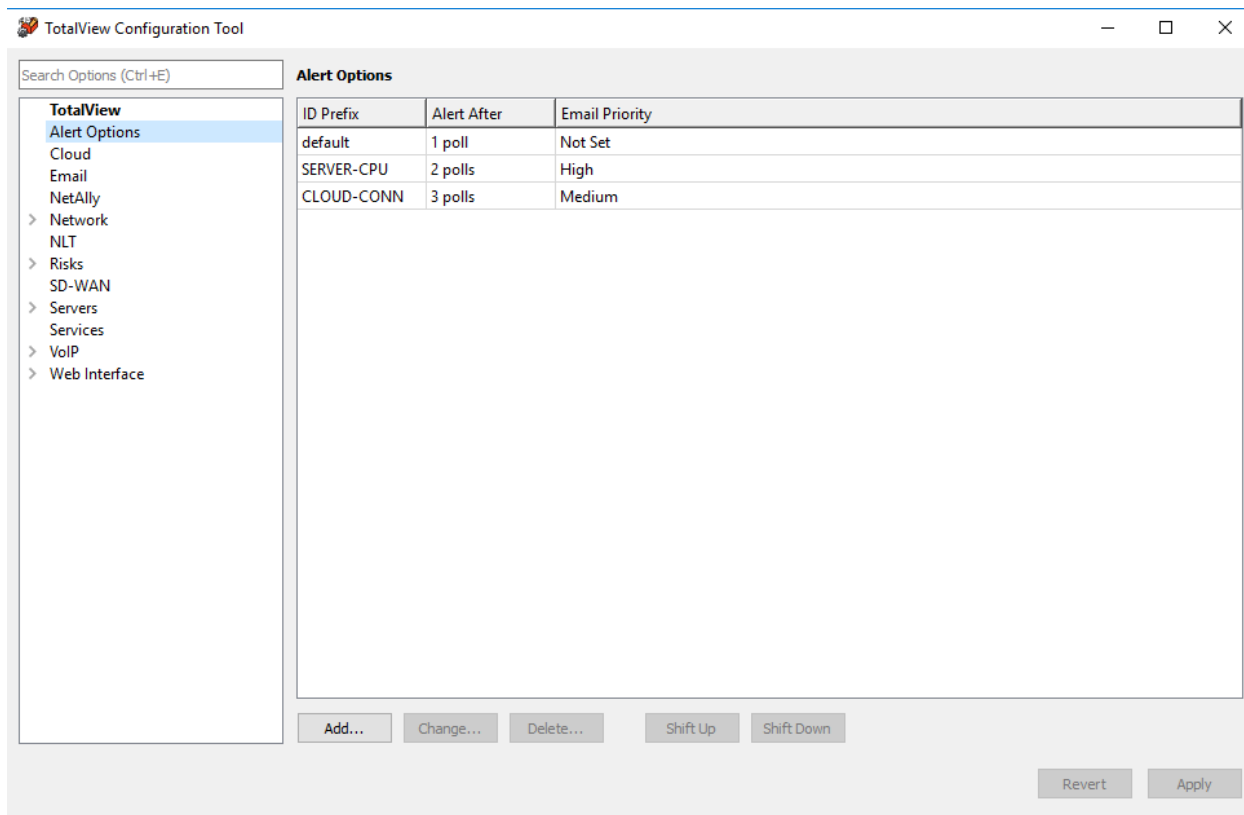
At the very bottom right of all screens, there are also “Revert” and “Apply” buttons that will be available if you have made any edits:



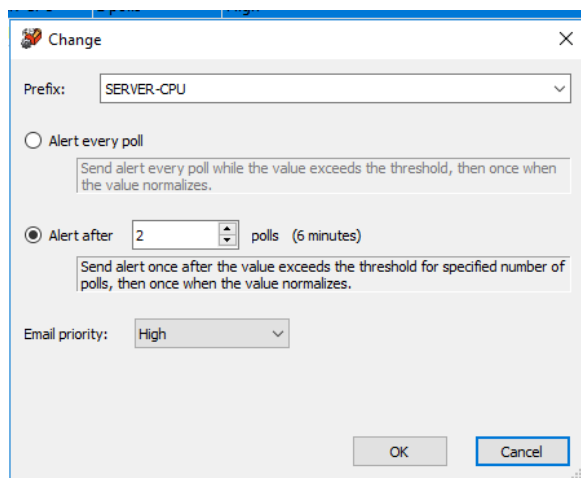
- Use the “Apply” button to apply all the settings you’ve configured during this session. By clicking “Apply”, it will stop and restart the TotalView service. This could take up to 5 minutes.
- Use the “Revert” button to revert to the last saved configuration.

Alert Options

The Alert Options section allows you to change how alerts work. For example, if you want an alert to trigger the first time it happens (the default), you can create it here. However, if you want the alert to trigger only the 3rd time it happens, you may want to add an alert option to configure how a specific alert triggers.



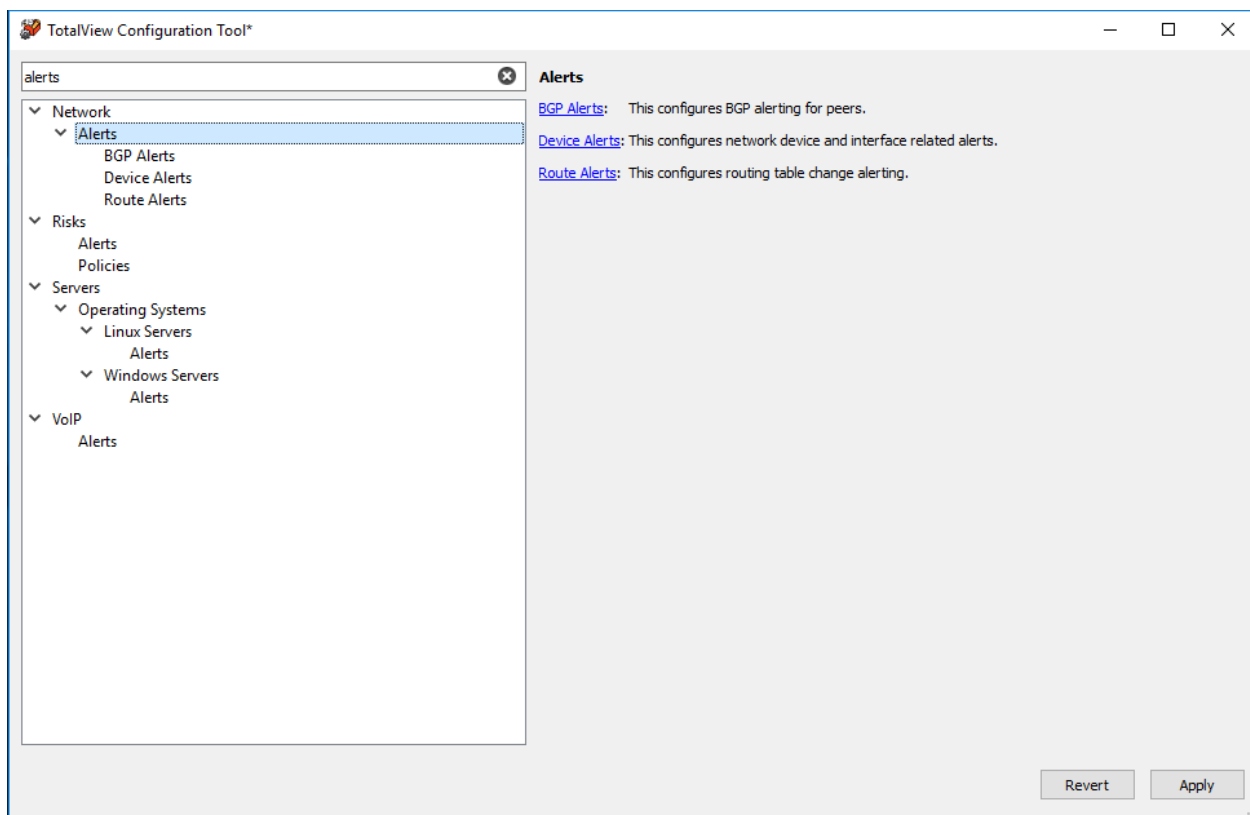
To add and change alert options, use the “Add” and “Change” buttons:



You can also set alerts to trigger each time the event occurs, or only when the alert happens get an initial alert, and then a second alert when the event recovers.

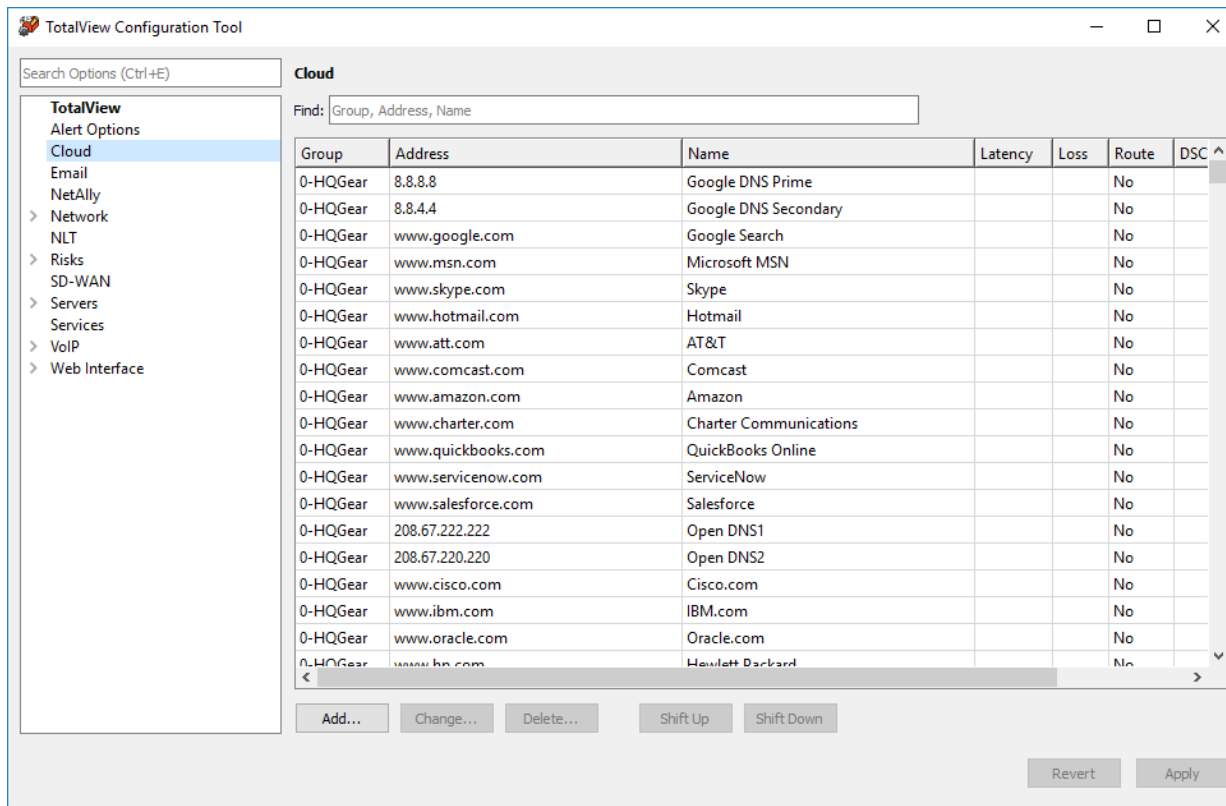
For example, if every 5 minutes an alert is sent on low disk space on one drive, the frequency of the alerting can be irritating, as it will fill your mailbox with alerts. In that case, set it to send just one threshold alert: *“Low disk space on Fred drive C”*, and then it will be quiet until the disk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

Note: There are also many other alerts you can set up for different conditions and events, available to you when you start to navigate the sections. You can do a filter on the word *alerts* to quickly get to the sections for setting Network alerts, Risk alerts, Server Alerts, and VoIP alerts. Here is a filter on the word *alerts*:

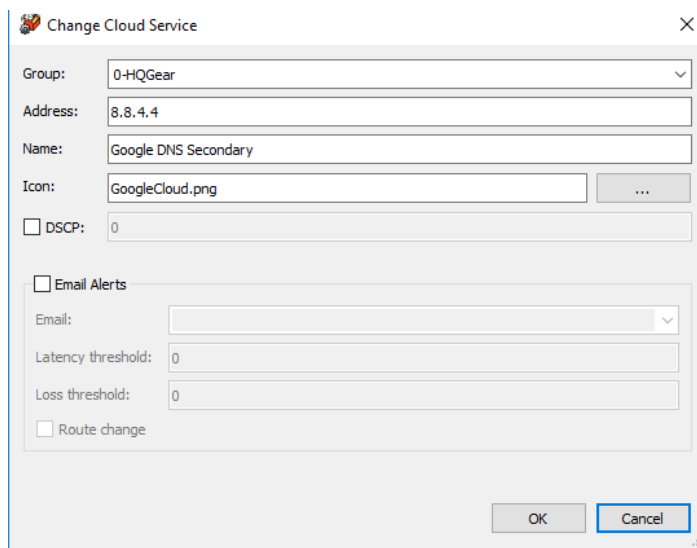


Cloud Monitoring

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



You can also setup email alerts for latency and loss thresholds when you add or change addressed on the cloud list: Select an address on the Cloud list, then select “Change”. If you want email alerts, checkmark “email alerts” and fill out those fields. Press “Ok” to save it.



Email Reports

For all email reports, you can select from your commonly used email addresses in the drop-down menus. Select the "Email" section to enable and configure the email reports.

Configuring Network Weather Report

If you want to receive a daily network Weather Report, put a checkmark in the box next to "Send daily network Weather Report".

The screenshot shows the 'Email' configuration window in the TotalView Configuration Tool. On the left is a sidebar with a search bar and a tree view containing: TotalView, Alert Options, Cloud, Email (selected), NetAlly, Network, NLT, Risks, SD-WAN, Servers, Services, VoIP, and Web Interface. The main panel is titled 'Email' and contains the following fields and options:

- Mail Server Address:** 10.0.0.10
- Port:** 25
- Encryption:** Radio buttons for None (selected), TLS, and SSL.
- Send from:** lab-fred-reports@pathsolutions.com (with an example: noc@company.com)
- Authenticate:** A checkbox that is currently unchecked, with fields for Username and Password.
- Send daily network "Weather Report":** A checked checkbox. Below it, a text box explains: "The 'Weather Report' can help you keep track of your network health on a daily basis." To the right of this text are buttons for "Send Weather Report Now" and "Test".
- Send to:** itops@pathsolutions.com (with an example: jdoe@hotmail.com, flb@aol.com)
- Customization:** A text box stating "This report can be customized to include specific information, or simply provide an overview of general health." with an "Edit Report" button.
- Send Nightly Security Report:** An unchecked checkbox. Below it, a text box explains: "A nightly security report showing footprint, exposures and vulnerabilities in the environment." To the right are buttons for "Send Security Report Now" and "Test".
- Send to (Security Report):** itops@pathsolutions.com, ttitus@pathsolutions.com (with an example: jdoe@hotmail.com, flb@aol.com)
- Buttons:** "Revert" and "Apply" buttons are at the bottom right.

You must enter an Internet SMTP email address that the report should be sent from and an Internet SMTP email address that the report should be sent to. If you want reports to be sent to multiple users on the network, enter the user names here separated by a semicolon, comma, or space.

You must also 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.

Click "Test" to send a test email to all users listed.

If you want to modify the network Weather Report, click "Edit Report". You will be able to modify the default report to include your company logo, custom information, or shrink the email to display only the information you are interested in. 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.

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

Configuring Nightly Security Report

If you have the Security Operations Manager module, you can get a nightly security report sent to your mailbox. If you want to receive the Nightly Security Report, put a checkmark in the box next to “Send Nightly Security Report”:

The screenshot shows the 'Email' configuration window of the TotalView Configuration Tool. On the left is a tree view with categories: TotalView, Alert Options, Cloud, Email (selected), NetAlly, Network, NLT, Risks, SD-WAN, Servers, Services, VoIP, and Web Interface. The main area is titled 'Email' and contains the following fields and options:

- Mail Server Address:** 10.0.0.10
- Port:** 25
- Encryption:** Radio buttons for None (selected), TLS, and SSL.
- Authenticate:** A checkbox that is currently unchecked, with fields for Username and Password below it.
- Send from:** lab-fred-reports@pathsolutions.com (with an example: noc@company.com).
- Send daily network "Weather Report":** A checked checkbox. Below it is a description: "The 'Weather Report' can help you keep track of your network health on a daily basis." and a 'Send Weather Report Now' button. There is also a 'Send to:' field with the value itops@pathsolutions.com (example: jdoe@hotmail.com, flb@aol.com) and a 'Test' button. Below this is a note: "This report can be customized to include specific information, or simply provide an overview of general health." with an 'Edit Report' button.
- Send Nightly Security Report:** A checked checkbox, highlighted with a yellow background. Below it is a description: "A nightly security report showing footprint, exposures and vulnerabilities in the environment." and a 'Send Security Report Now' button. There is also a 'Send to:' field with the value itops@pathsolutions.com, ttitus@pathsolutions.com (example: jdoe@hotmail.com, flb@aol.com) and a 'Test' button.

At the bottom right are 'Revert' and 'Apply' buttons.

If you want to receive this report, check the Send Nightly Security Report box.

You must enter an Internet SMTP email address that the report should be sent from and an Internet SMTP email address that the report should be sent to. (If so, the previous section tells how to fill out 'send to' and 'send from' fields, and how to test emails.)

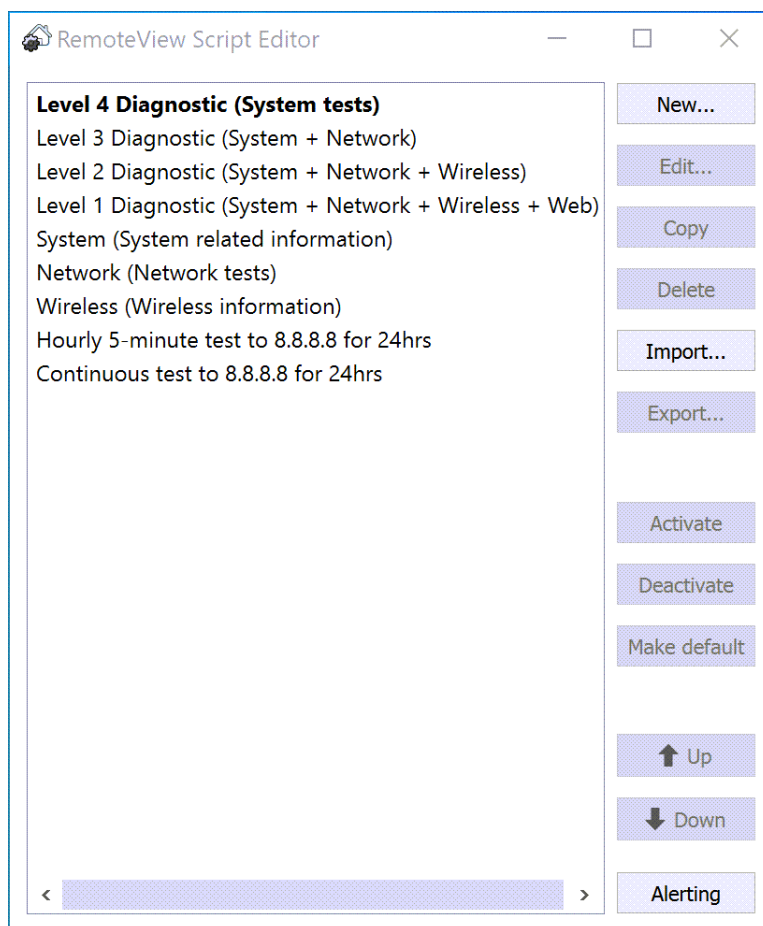
Additional Email Report Templates

Most of the Config Wizard sections have places you can setup email alerts, beside the two we mentioned in this section. Go to the subjects you are interested in, and look at the email fields.

We also provide many other email report templates outside of the Config Tool, and instructions on how to create your own customized email alerts. See [RemoteView Script Editor Tool](#). You have the ability to configure and create your own RemoteView batch scripts using this tool. To open the tool, click on "Start". Then choose "Programs", "PathSolutions", "TotalView", and "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.

Notice also you have buttons to select scripts and activate or deactivate them, and to make one a default:



To edit a script, select the script (the Level 4 Diagnostic is shown below), and select “Edit”. A dialog box will appear that gives you the ability 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:

Edit script

Name:

Description:

Logging: ☒ Server ☐ Local ☐ Both

Active: ☒

Test List:

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

Parameters:

note:

save_remote: ☒

notify:

You can add new commands to a script using the “Add” button. Then select a new command from the drop-down menu that will appear, then click “OK”.

Here is adding an end-to-end test:

The screenshot shows a 'Create new script' dialog box with the following fields and options:

- Name:** Call quality test script
- Description:** Script that tests for various call quality performance metrics
- Logging:** ☒ Server ☐ Local ☐ Both
- Active:** ☒

On the left side of the dialog, there are buttons for **Add**, **Copy**, **Delete**, **Up**, and **Down**. The main area is divided into **Parameters** and **Script** sections. An 'Add new command' sub-dialog is open, showing:

- Command:** Test: End To End (selected from a dropdown menu)
- Buttons:** OK, Cancel

At the bottom right of the main dialog, there are **Save** and **Cancel** buttons.

Here is 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: ☒

Add

Copy

Delete

↑ Up

↓ Down

Test: End To End

Parameters

duration60

address*

codecG.711(64)

calls10

dscp46

failed_if*...

note

save_remote☒

save_local...

notify☐

Save

Cancel

Here is setting the fail parameters on an end-to-end test:

The screenshot shows the 'Create new script' dialog box with the following fields and options:

- Name:** Call quality test script
- Description:** Script that tests for various call quality performance metrics
- Logging:** ☒ Server ☐ Local ☐ Both
- Active:** ☒

On the left side of the dialog, there are buttons: Add, Copy, Delete, Up, and Down.

The 'Test: End To End' tab is selected. An 'Edit parameter' sub-dialog is open, showing the 'failed_if' section with the following parameters:

Parameter	Operator	Value
<input checked="" type="checkbox"/> QOS	<	4.0
<input type="checkbox"/> LOSS	>	0.5
<input type="checkbox"/> LATENCY	>	50
<input type="checkbox"/> JITTER	>	110

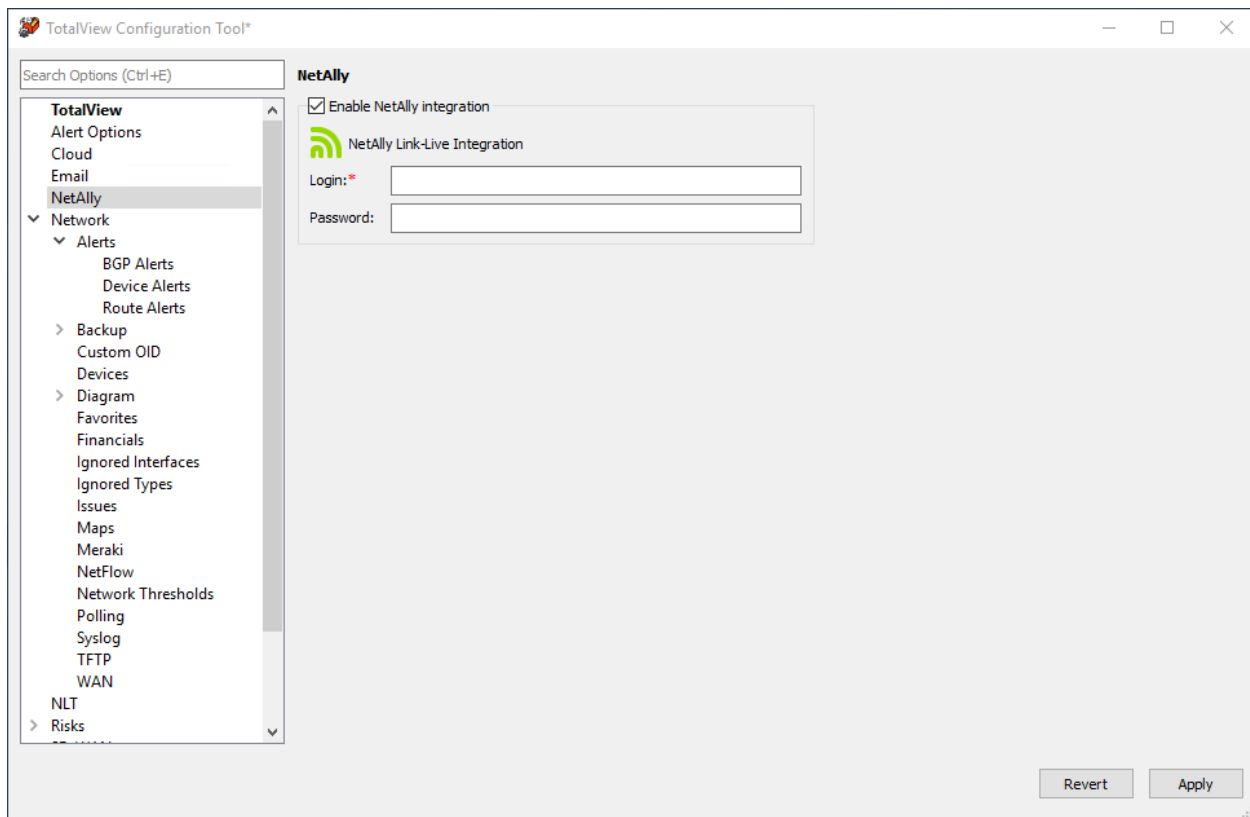
At the bottom of the 'Edit parameter' dialog are 'OK' and 'Cancel' buttons. At the bottom of the main 'Create new script' dialog are 'Save' and 'Cancel' buttons.

Appendix A. Email Report Templates and Variables

NetAlly Settings

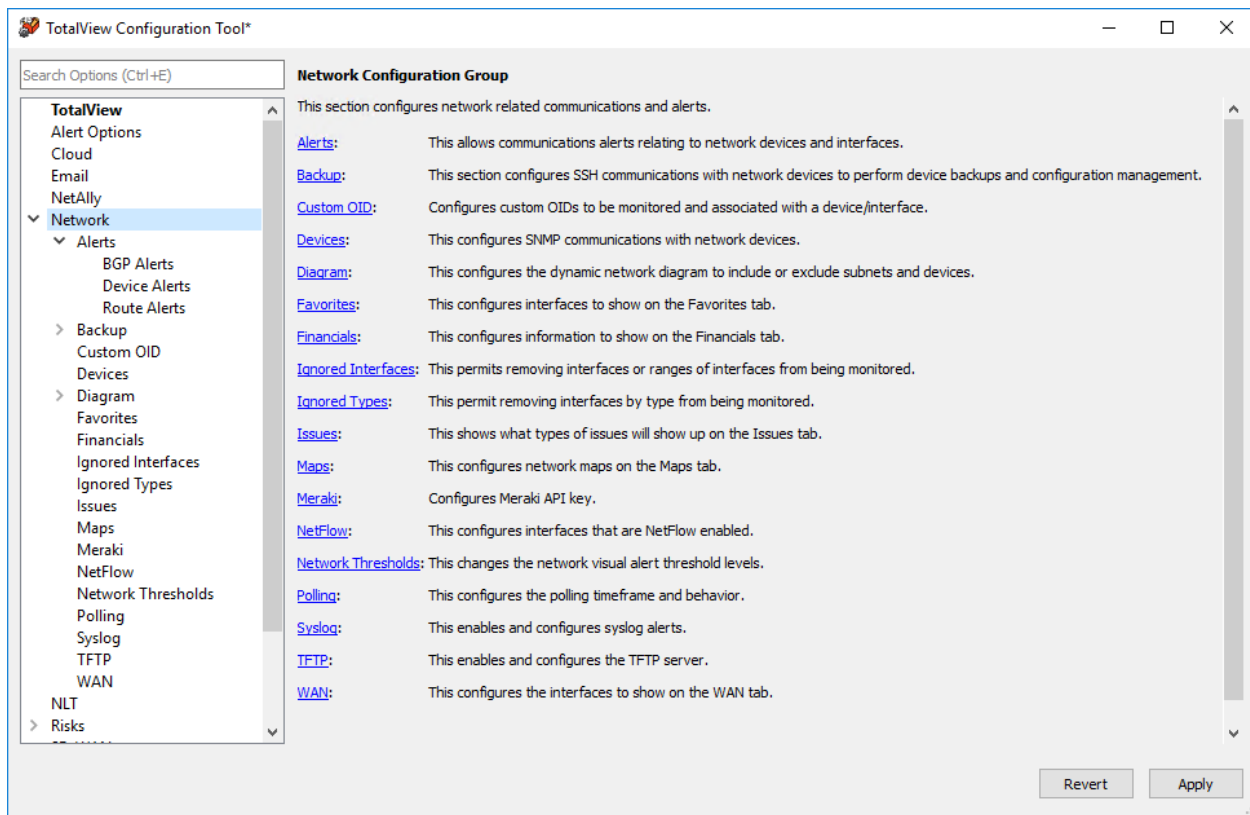
Select NetAlly from the left-hand menu, then checkmark next to “Enable NetAlly Integration” and the section on NetAlly link-Live Integration will become available to fill out:

Then enter your NetAlly login and Password here:



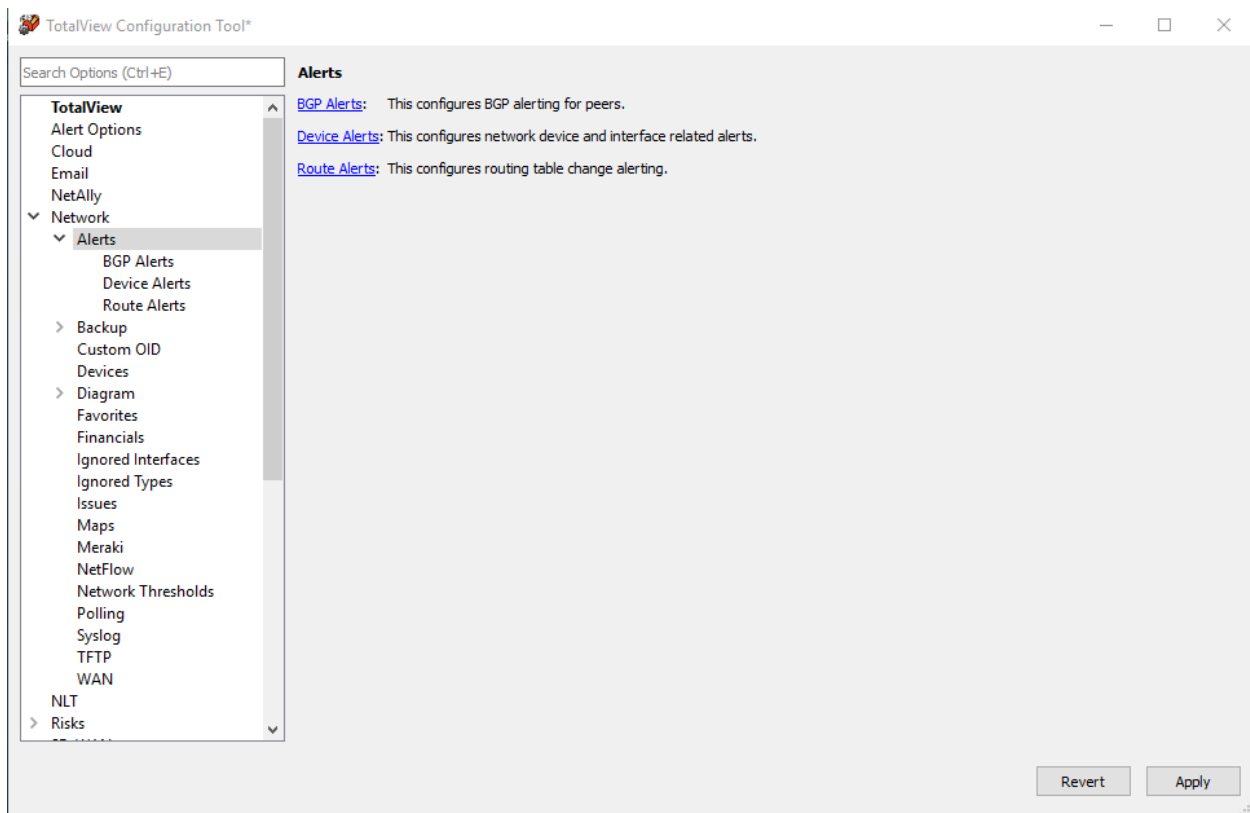
Network Monitoring

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



Alerts

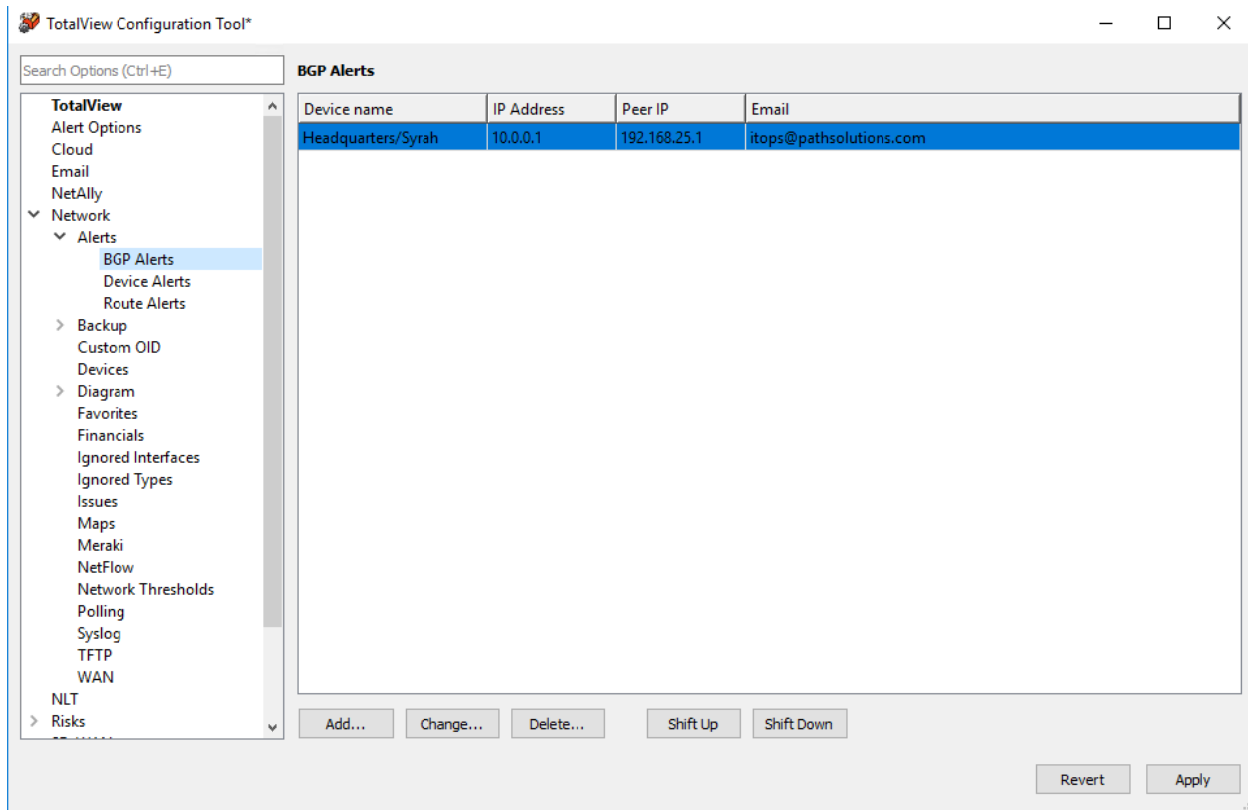
Select Network > Alerts from the left-hand menu. This section allows for you to configure: BGP Alerts, Device Alerts, and Route Alerts:



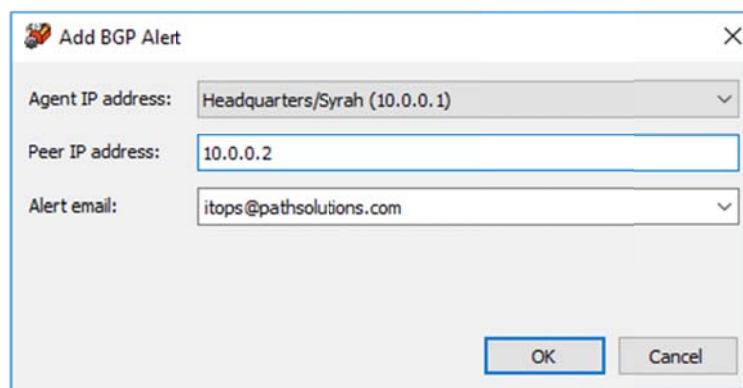
Note: There are also many other network alerts you can set up for different conditions and events, available to you when you start to navigate the sections.

BGP Peer alerting

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

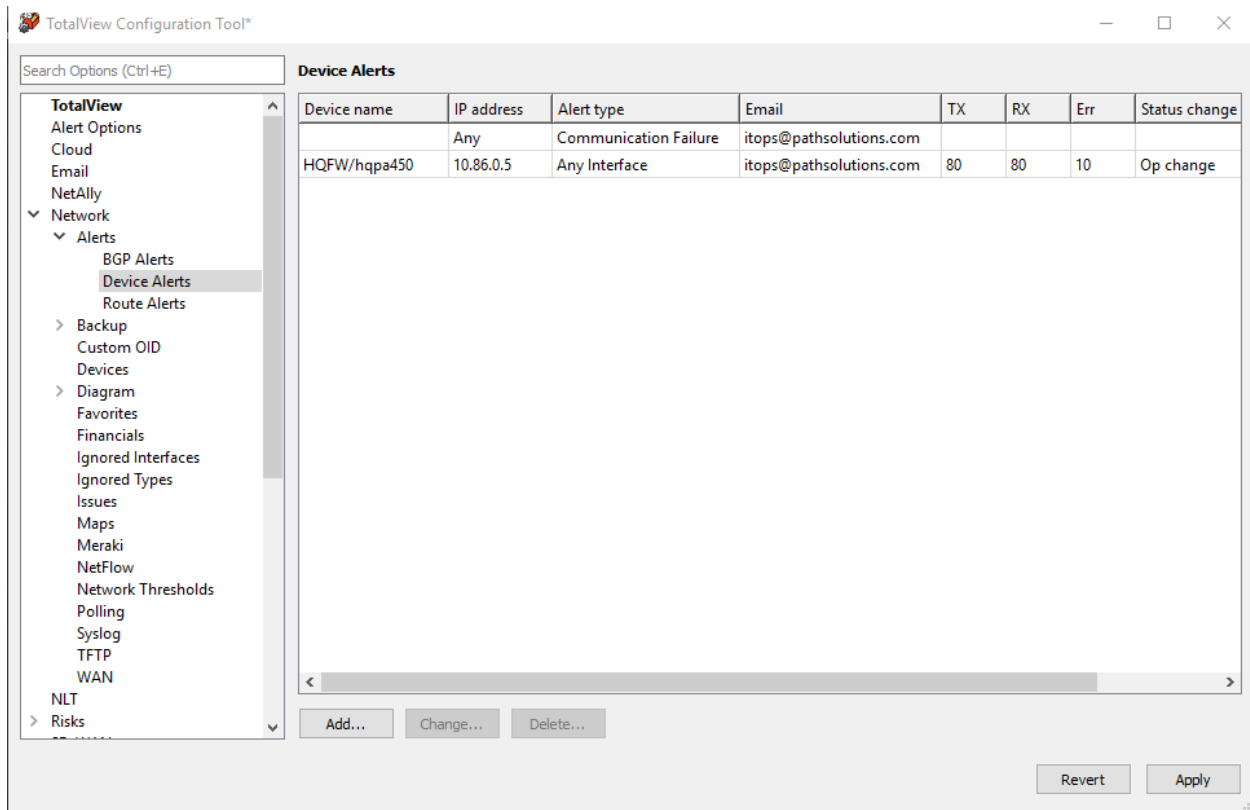


Use the “Add” or “Change” buttons to add or modify agents and peers on the list, and email for the alert:



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.



You can add or change alerting for interfaces or devices on the Alerts section.

For Device Alerts, if you click the “Add” button, you should see the following alert configuration dialog:

The 'Add Alert' dialog box contains the following fields and options:

- 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
- Buttons:** OK, Cancel

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

Enter the IP address of the device, or “Any” to match any device, or a device group to match any IP address in a device group.

You can then 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.

You may also 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

You can setup an alert for devices in a group. For example, if you want to know when any devices in the “Chicago” group have an interface with high utilization. Setup an email address from the drop-down menu. In the IP address field, select a group from the drop-down menu. 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

OK Cancel

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 click on “Add”.

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

Add a concise description, such as *PoE alert*, and then specify Alert Types and the settings that will trigger the alerts.

Then in the “Status Change” field, select “PoE change” from the drop-down menu.

Then press “OK”.

Note: You must first select an “Alert Type” before the “Status Change” field will be usable.

Add Alert

Email address:

Description:

IP address:

Alert type:

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

☐ Tx Utilization: percent utilized

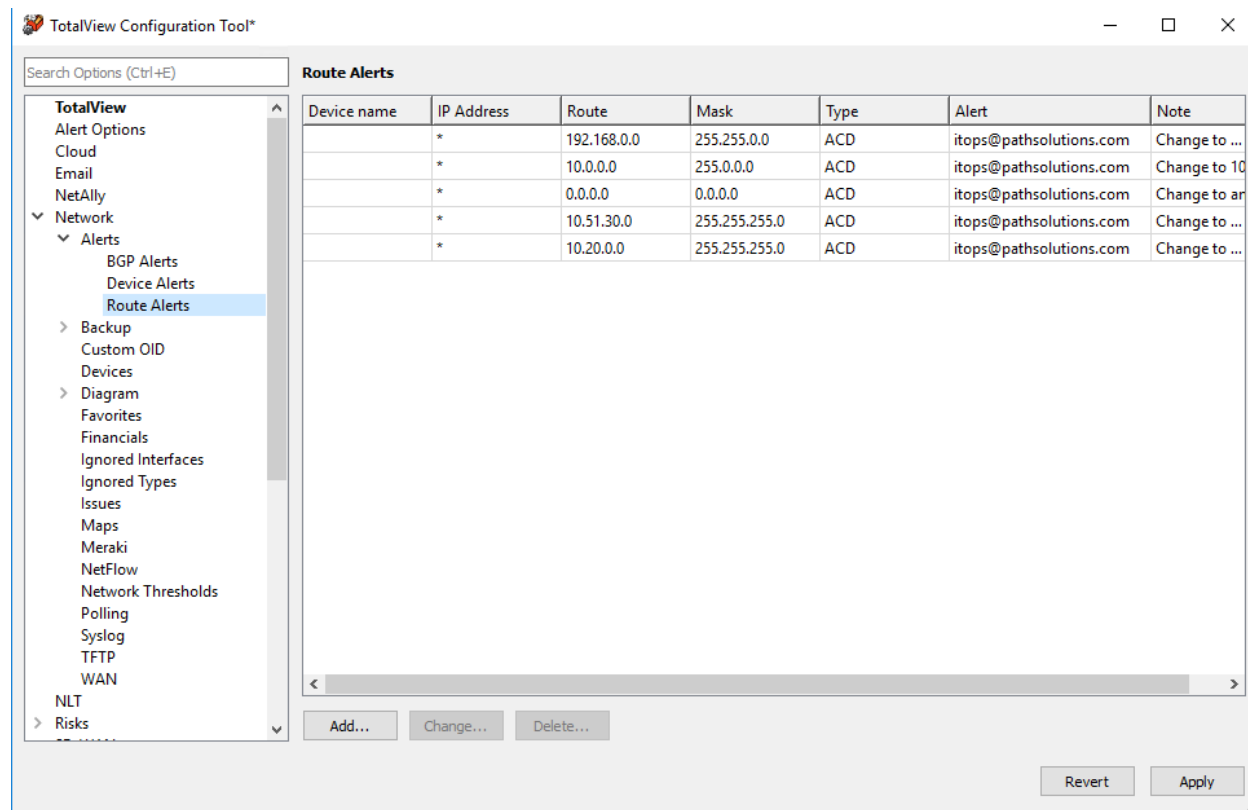
☐ Rx Utilization: percent utilized

☐ Error percentage: percent packet lost

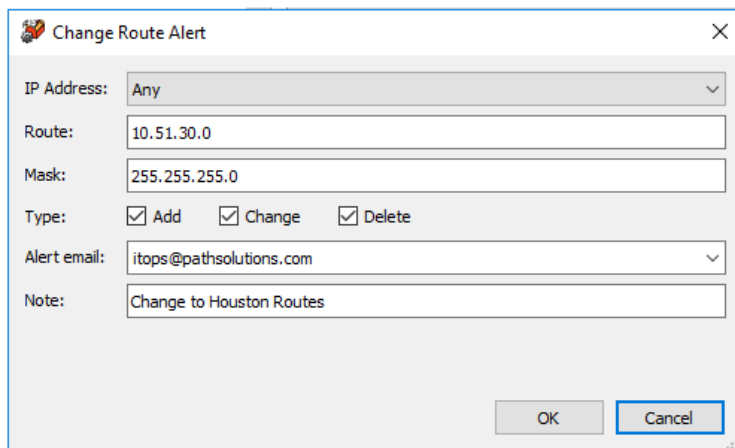
Status change:

Route Alerts

Go to the section Network > Alerts > Route Alerts to configure route alerts. This calls up the list of configured Route Alerts:

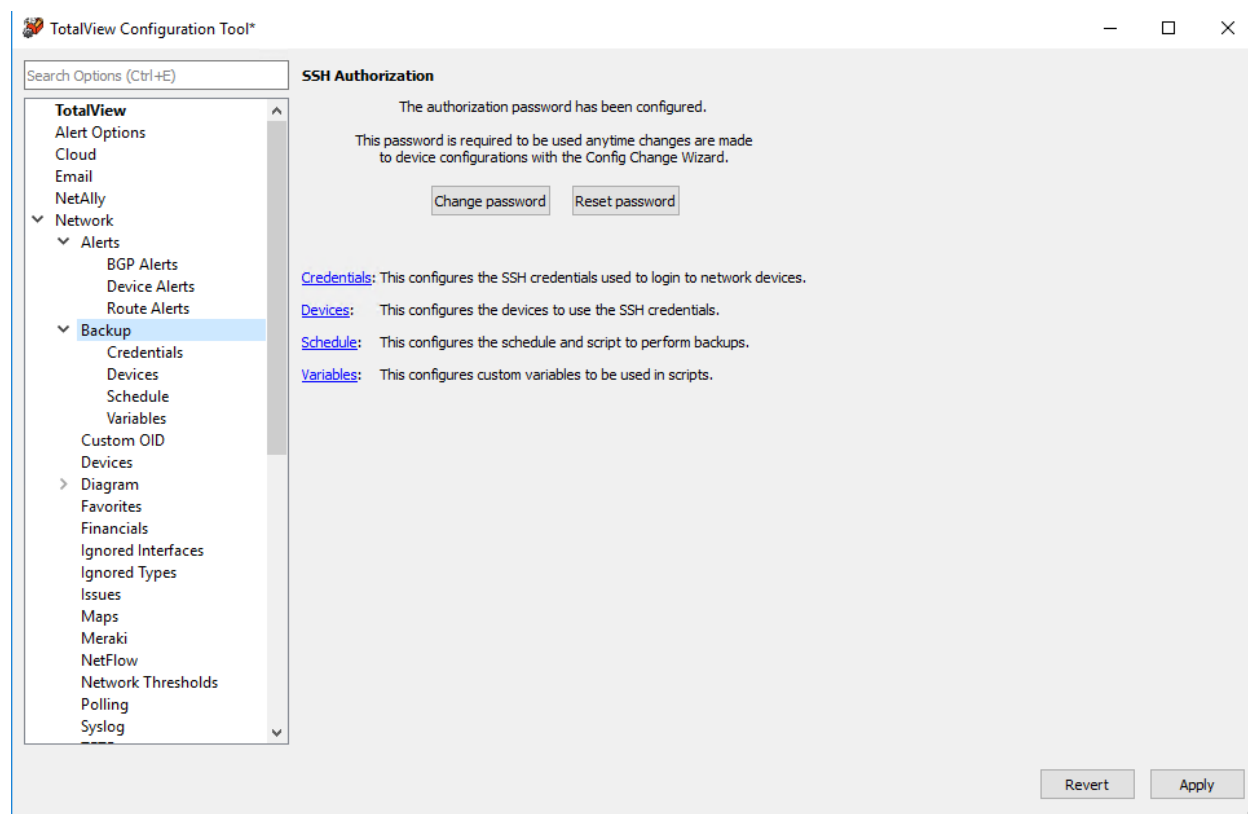


Use the “Add” and “Change” buttons to add and change the route alerts (IP address and mask), the type of alerts to send, and the email to send the alerts to.



Backup Configuration

Go to the section Network > Backups. This section permits network equipment configurations to be backed up on a scheduled basis. TotalView shows backup configurations as well as has the ability to do a diff against previous versions to see what has changed. You can also see the logfile of backups as well as initiate a manual backup from the web interface.



In order to use the device configuration backup capability, a master password must be created. This master password is used to protect the device login credentials to prevent them from being used illicitly.

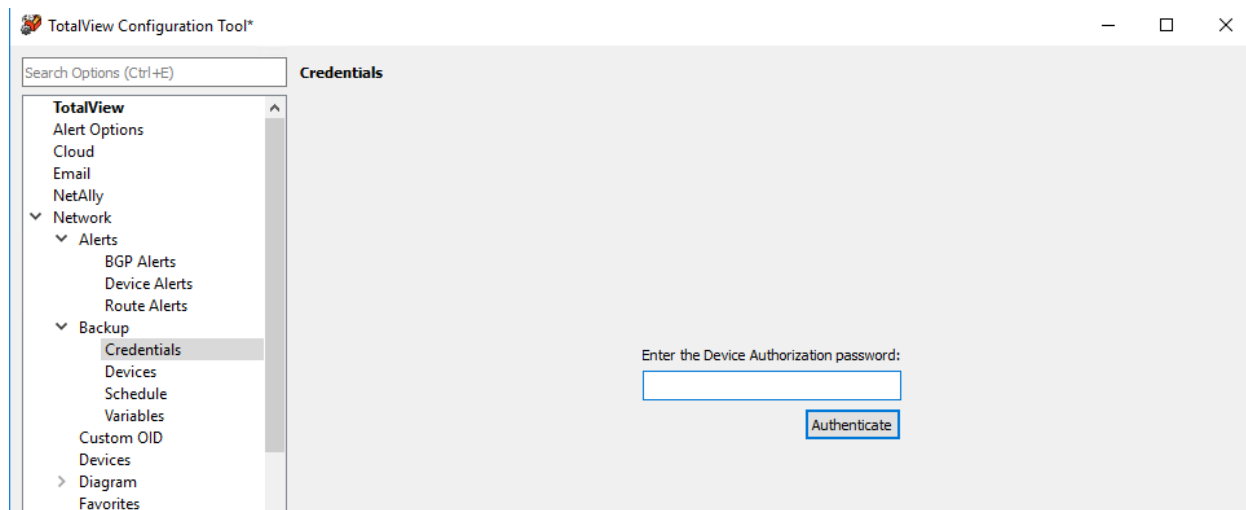
Once the master password has been set, it must be used for any changes made to the configuration, or anytime that the Device Configuration Wizard is used.

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

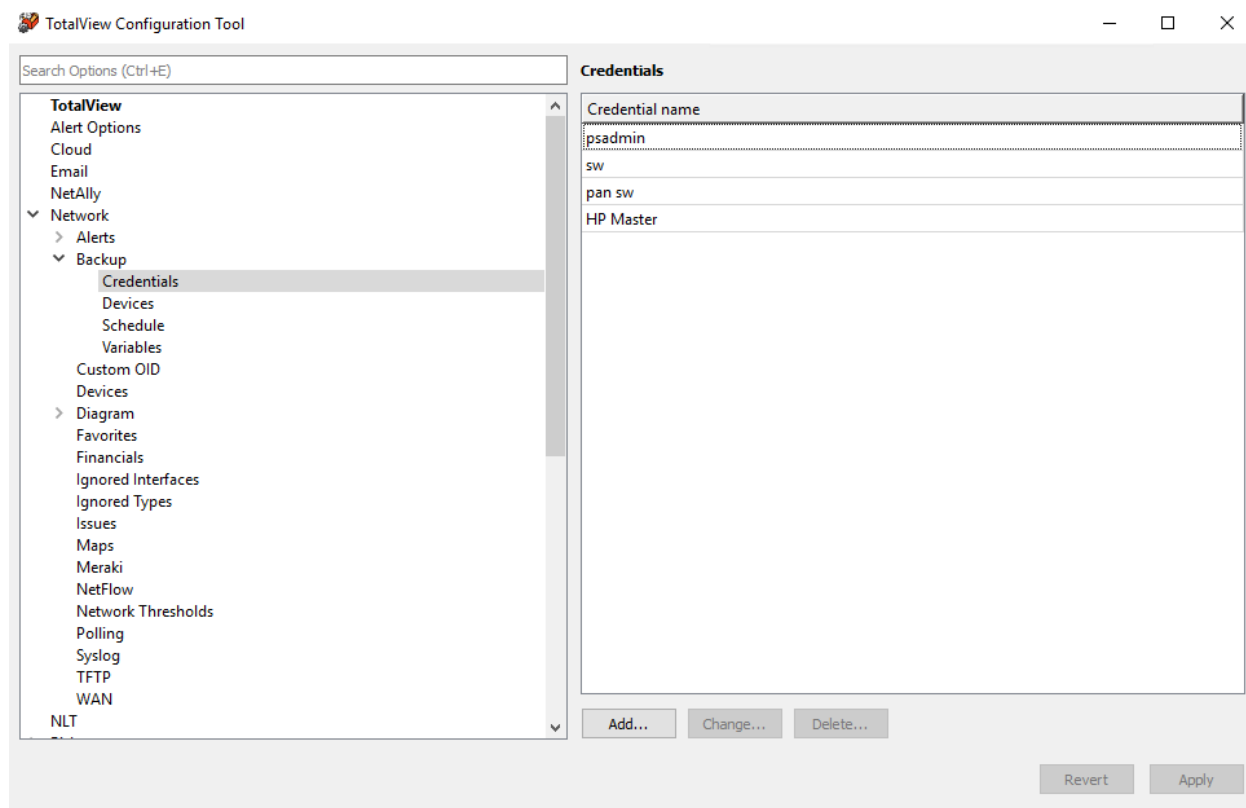
Once the master authorization password is set, click in the Credentials section.

Credentials

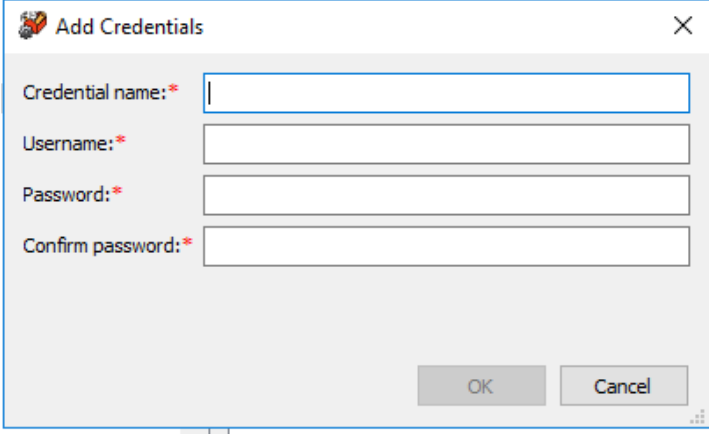
The first time you click on Backup > Credentials in the menu (or any other Backup subsection), you will get a message to enter the Device Authorization password:



Enter the password and select “Authenticate”. This calls up the list of configured credentials:



Select “Add” to add credentials to the system. The dialog box asks you to enter 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.



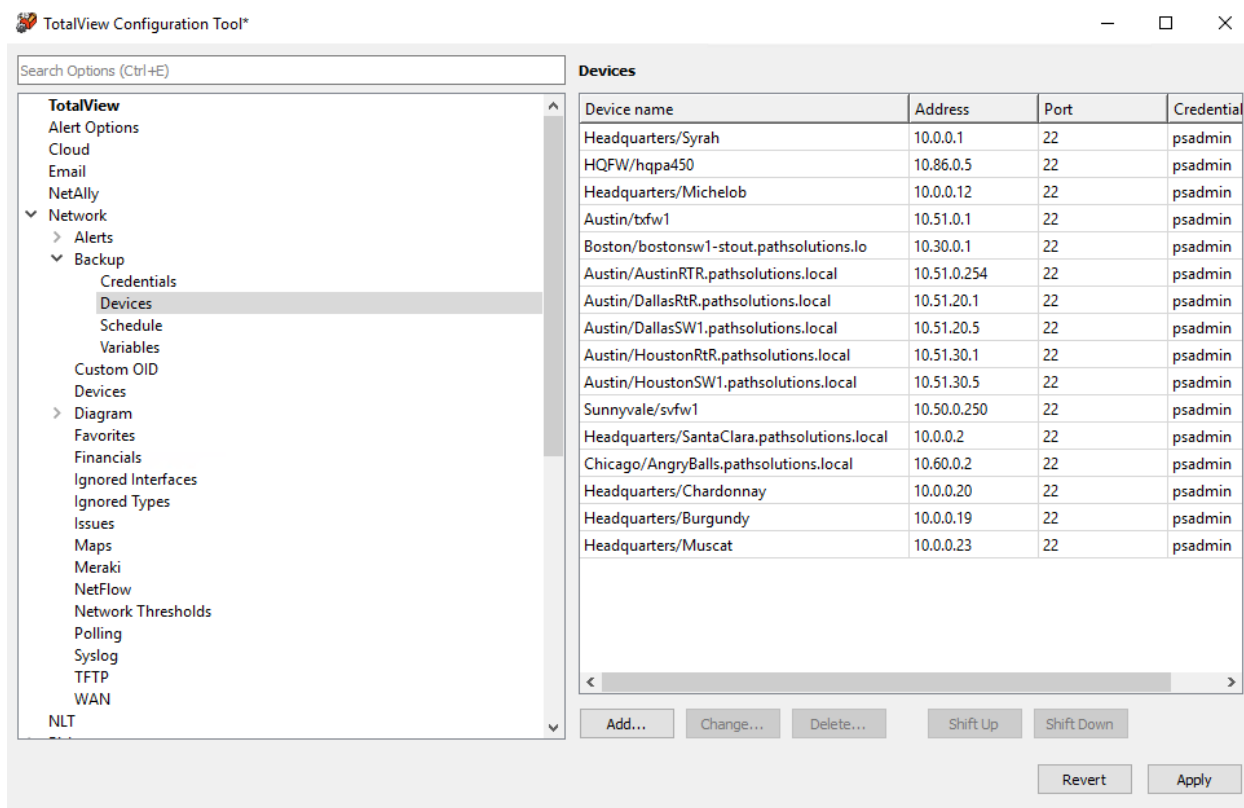
The image shows a Windows-style dialog box titled "Add Credentials" with a close button (X) in the top right corner. The dialog contains four text input fields, each preceded by a label and a red asterisk indicating it is required:

- Credential name:*
- Username:*
- Password:*
- Confirm password:*

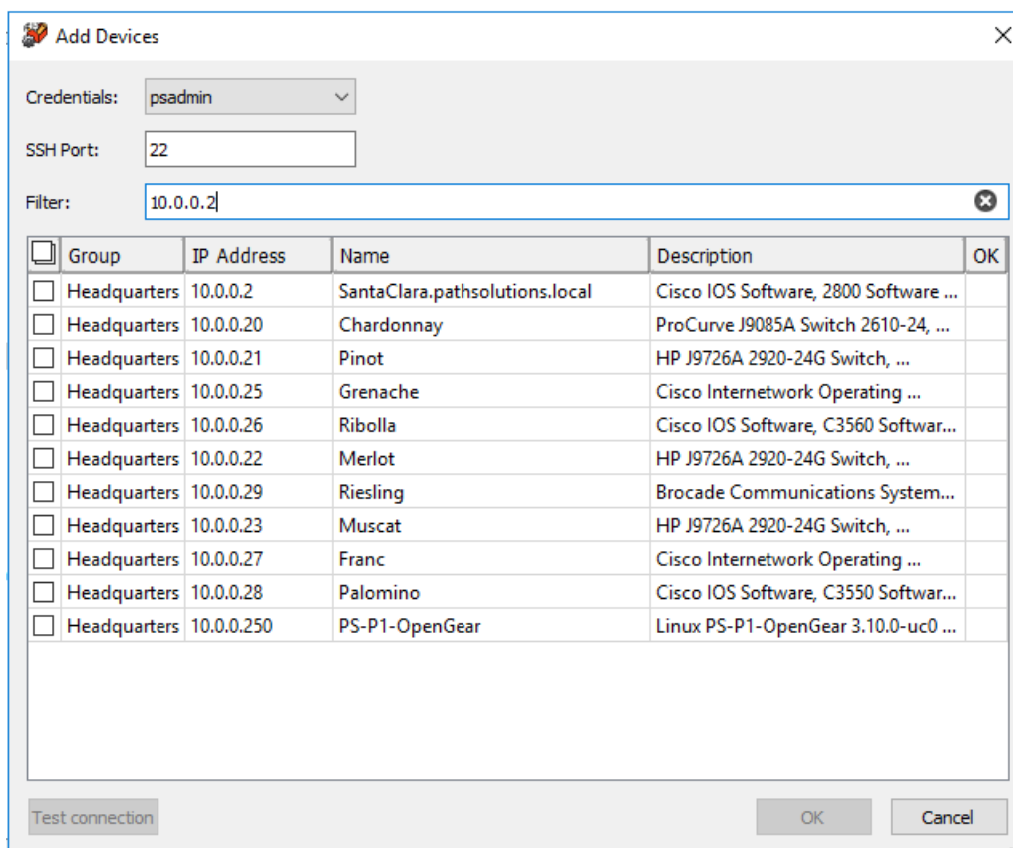
At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Devices

Go to the Backup > Devices section to assign device backups. This calls up the list of devices with backup configurations:



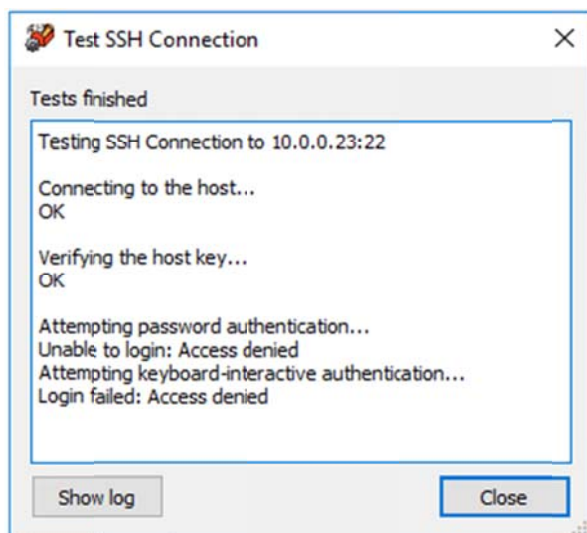
Click "Add" if you need to add a device to the configuration.



When you select the credentials from the drop-down menu, it will show you the internal system description a list of devices, so you can use the appropriate credentials for the device. You can use the filter field to filter the list.

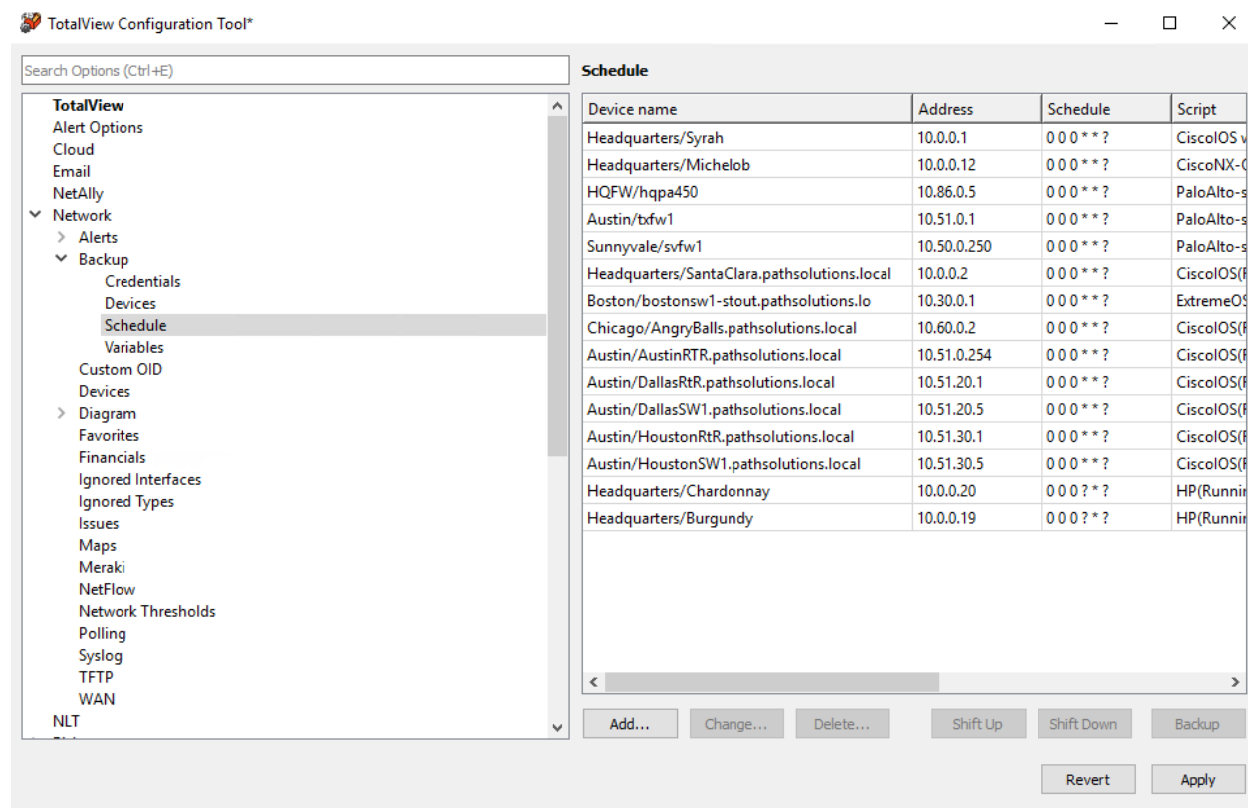
It is recommended to select the device then click on “Test connection” to verify communications with those credentials are working, and the security token is read and stored. If this is the first time communicating with the device, it will ask you to verify the hardware security token.

Here is an example of testing a connection:

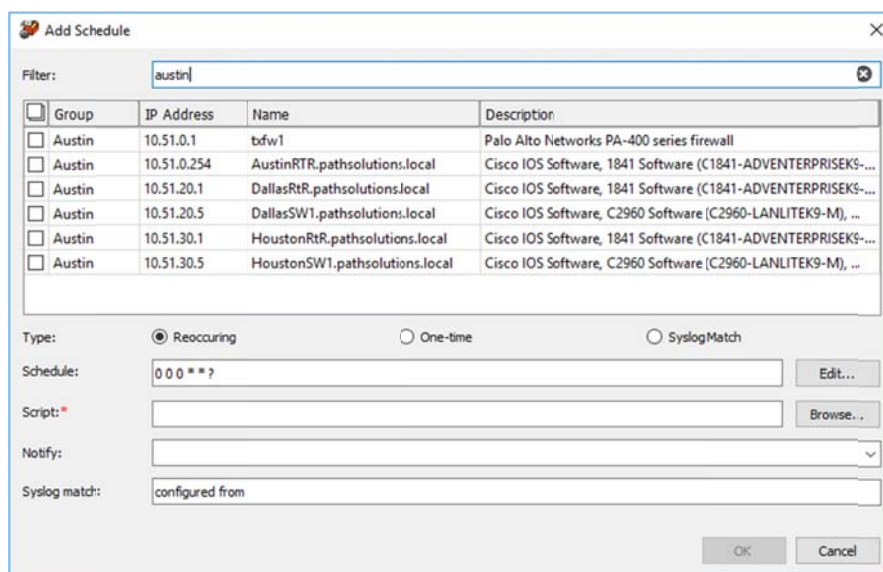


Schedule Backup

Go to the Backup > Schedule section to create a backup schedule of network devices. This calls up the list of devices with schedules:



Click on “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.



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 clicking on the “Edit” button 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 5 10 15 20 25 30 35 40 45 50 55

Minutes: ☐ Every 1 minute(s) ☒ Specific 0 5 10 15 20 25 30 35 40 45 50 55

Hours: ☐ Every 1 hour(s) ☒ Specific 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Days of month: ☐ Any ☒ Every 1 day(s) ☐ Specific 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Months: ☒ Every 1 month(s) ☐ Specific Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Days of week: ☒ Any ☐ Specific MO TU WE TH FR SA SU

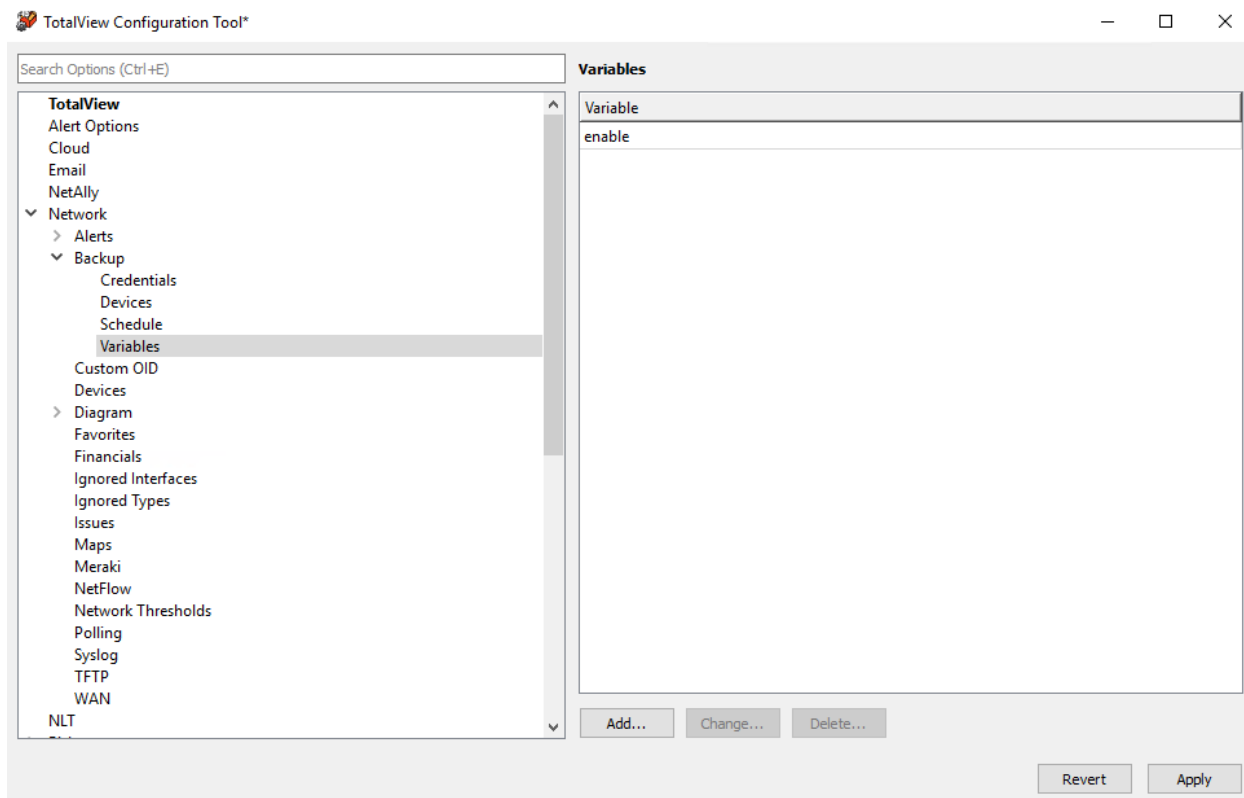
OK Cancel

Click on “Change” to edit any of the backup configurations.

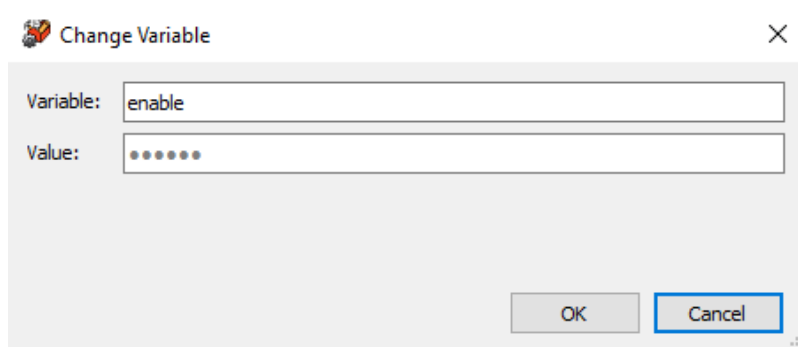
Variables

Go to the 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.

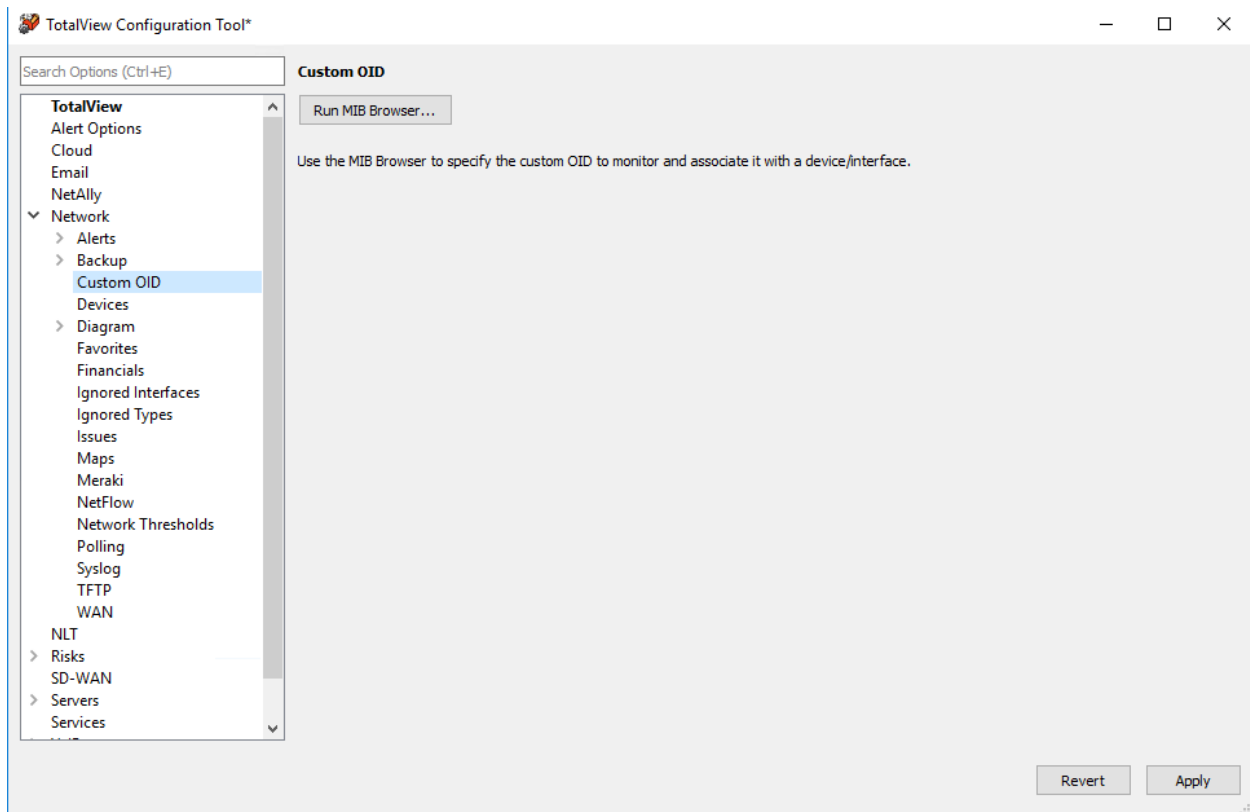


Add or change variables by clicking on the “Add” and “Change” buttons and filling out the variable name and its stored value:



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.



The MIB Browser will open in a separate window. See the section [MIB Browser](#) for OID lookups, OID monitoring and OID graphing.

Note: You can also customize OID monitoring reports by editing the cfg file. See Appendix F. Custom OID Monitoring.

Devices Configuration

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

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

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

TotalView Configuration Tool*

Search Options (Ctrl+E)

Devices

Find: Group, Device name, IP Address, Description

General Support

Group	Device name	IP Address	Int	SNMP	Description
Headquarters	Syrah	10.0.0.1	54	v3	Device
Headquarters	SantaClara.pathsolutions.local	10.0.0.2	4	v2c	Device
Headquarters	RuckusAP	10.0.0.6	18	v2c	Device
Headquarters	tempranillo.pathsolutions.local	10.0.0.7	9	v2c	Device
Headquarters	kmax-mm.pathsolutions.local	10.0.0.8	3	v2c	Device
Headquarters	Michelob	10.0.0.12	72	v2c	Device
Headquarters	Burgundy	10.0.0.19	32	v3	Device
Headquarters	Chardonnay	10.0.0.20	30	v3	Device
Headquarters	Pinot	10.0.0.21	35	v2c	
Headquarters	Grenache	10.0.0.25	25	v2c	
Headquarters	Ribolla	10.0.0.26	27	v2c	
Headquarters	Shiraz	10.0.0.35	34	v2c	
Headquarters	Merlot	10.0.0.22	35	v2c	
Headquarters	Riesling	10.0.0.29	29	v2c	
Headquarters	Muscat	10.0.0.23	35	v2c	
Headquarters	Franc	10.0.0.27	51	v2c	Device
Headquarters	Palomino	10.0.0.28	27	v2c	Device
Headquarters	PS-PTR1	10.0.0.30	1	v2c	Device
Headquarters	Dubonnet	10.0.0.32	61	v2c	

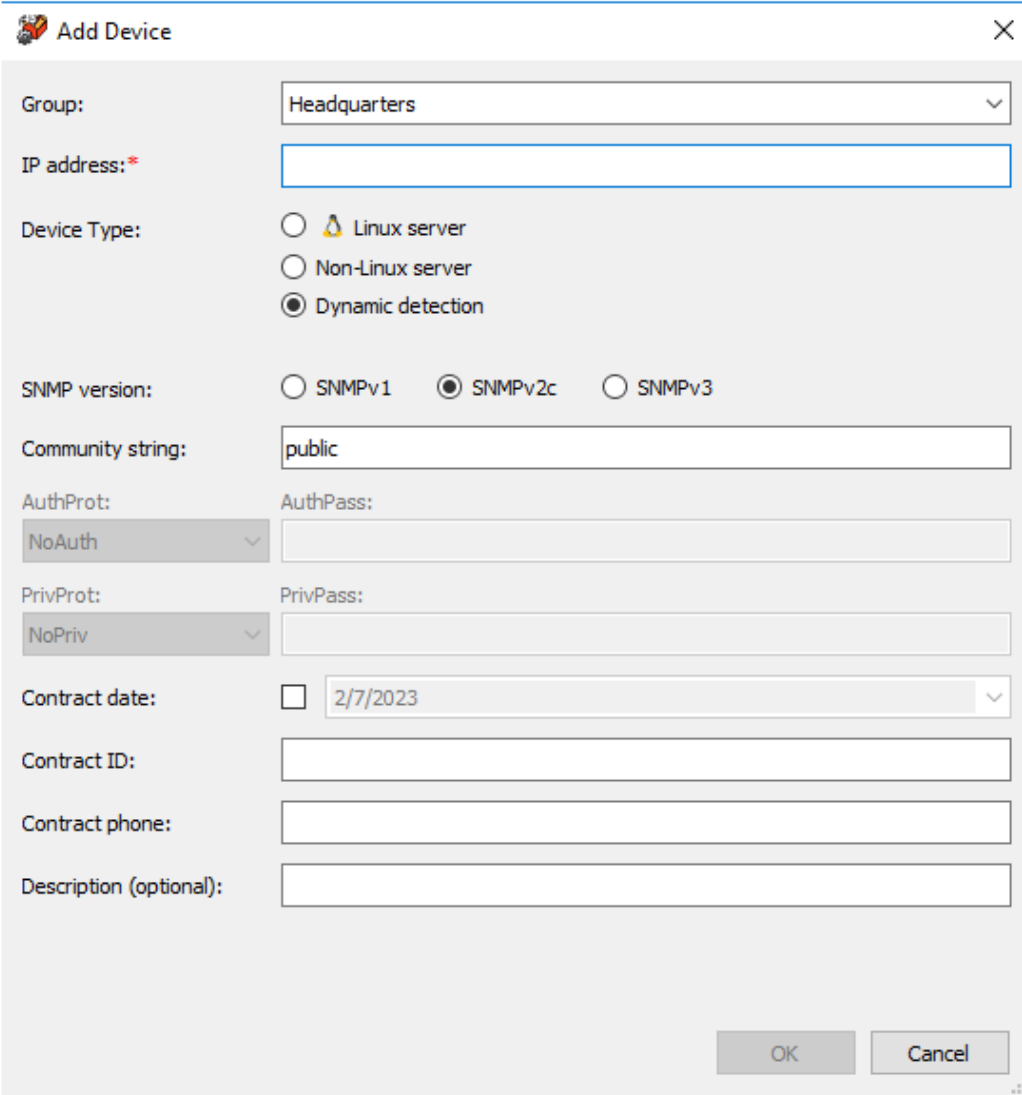
Add... Change... Delete... Shift Up Shift Down

Revert Apply

You can change the sort order for TotalView web display if desired. To move items on the list up or down, click on the item, and then click "Shift Up" or "Shift Down".

Adding Devices

To add a device, click "Add". You will see the "Add device" dialog:

The image shows a "Add Device" dialog box with a title bar containing a small icon and a close button. The dialog is organized into several sections. The first section has a "Group:" label and a dropdown menu showing "Headquarters". The second section has an "IP address:*" label and an empty text field. The third section has a "Device Type:" label and three radio buttons: "Linux server" (with a Linux logo), "Non-Linux server", and "Dynamic detection" (which is selected). The fourth section has an "SNMP version:" label and three radio buttons: "SNMPv1", "SNMPv2c" (which is selected), and "SNMPv3". The fifth section has a "Community string:" label and a text field containing "public". The sixth section has two labels, "AuthProt:" and "AuthPass:", with a dropdown menu showing "NoAuth" and an empty text field. The seventh section has two labels, "PrivProt:" and "PrivPass:", with a dropdown menu showing "NoPriv" and an empty text field. The eighth section has a "Contract date:" label, a checkbox, and a date field showing "2/7/2023". The ninth section has a "Contract ID:" label and an empty text field. The tenth section has a "Contract phone:" label and an empty text field. The eleventh section has a "Description (optional):" label and an empty text field. At the bottom right, there are "OK" and "Cancel" buttons.

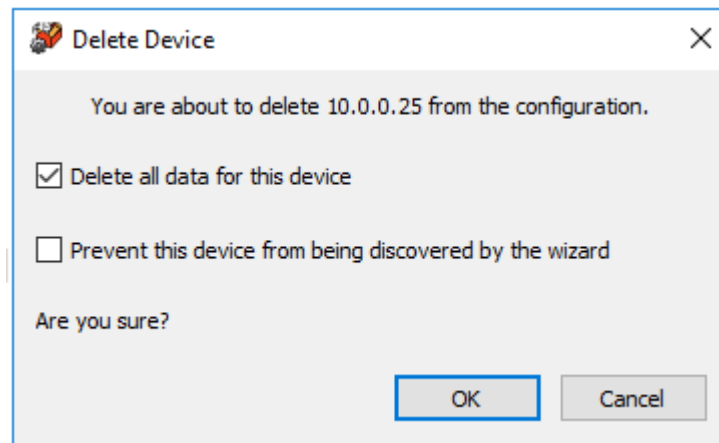
Enter the IP address and SNMP read-only community string for the device.

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.

Click "OK" to add the device, or click "Cancel".

Deleting Devices

To delete a device, click on the device and then click "Delete". You will see the "Delete Device" dialog:



If you click on the second checkbox the device will no longer be discovered when running the wizard.

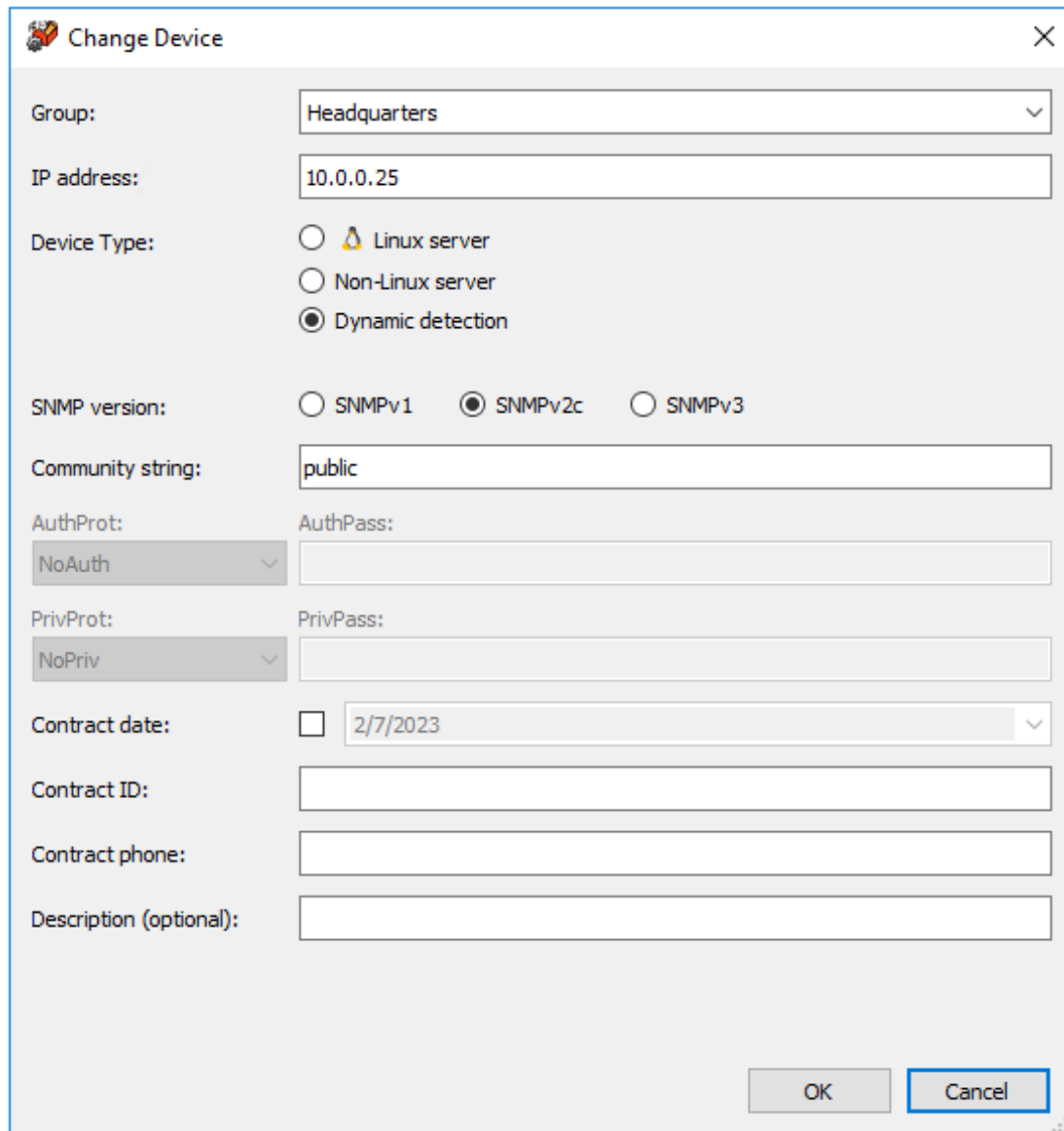
Note: Deleting a device from monitoring will not delete the previously collected graph data. You can add the device back to monitoring and it will continue to use the same data file for graph data storage.

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 C:\Program Files (x86)\PathSolutions\TotalView. Save the file after any modification.

Changing Device Information

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

You will be presented with the "Change device" dialog:



The "Change Device" dialog box is a window with a title bar containing a small icon and the text "Change Device" and a close button (X). The dialog contains several fields and options for configuring a device. The fields are arranged in a vertical list on the left, with their corresponding input areas on the right. The fields are: "Group:" with a dropdown menu showing "Headquarters"; "IP address:" with a text box containing "10.0.0.25"; "Device Type:" with three radio buttons: "Linux server" (unselected), "Non-Linux server" (unselected), and "Dynamic detection" (selected); "SNMP version:" with three radio buttons: "SNMPv1" (unselected), "SNMPv2c" (selected), and "SNMPv3" (unselected); "Community string:" with a text box containing "public"; "AuthProt:" with a dropdown menu showing "NoAuth"; "AuthPass:" with a text box; "PrivProt:" with a dropdown menu showing "NoPriv"; "PrivPass:" with a text box; "Contract date:" with a checkbox and a date picker showing "2/7/2023"; "Contract ID:" with a text box; "Contract phone:" with a text box; and "Description (optional):" with a text box. At the bottom right of the dialog are two buttons: "OK" and "Cancel".

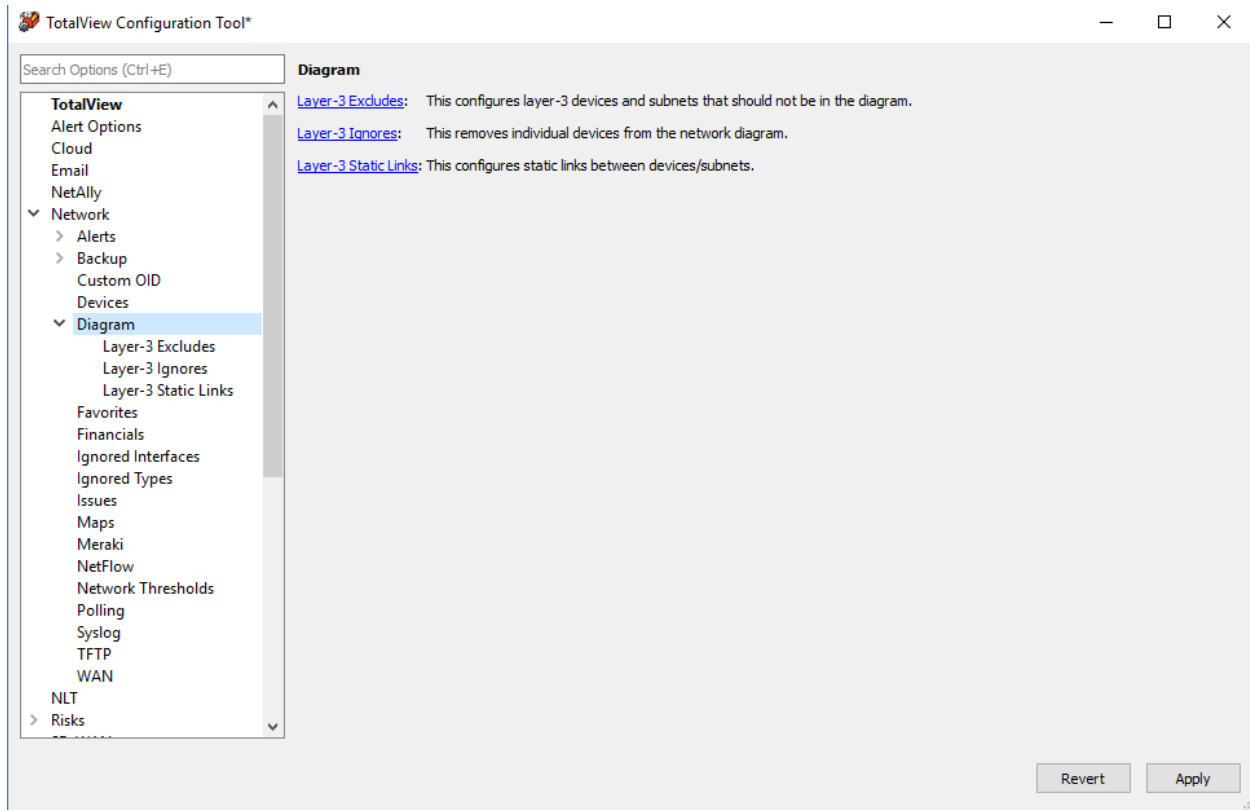
The only required fields for a device are the Group, IP address, and SNMP community string fields.

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.

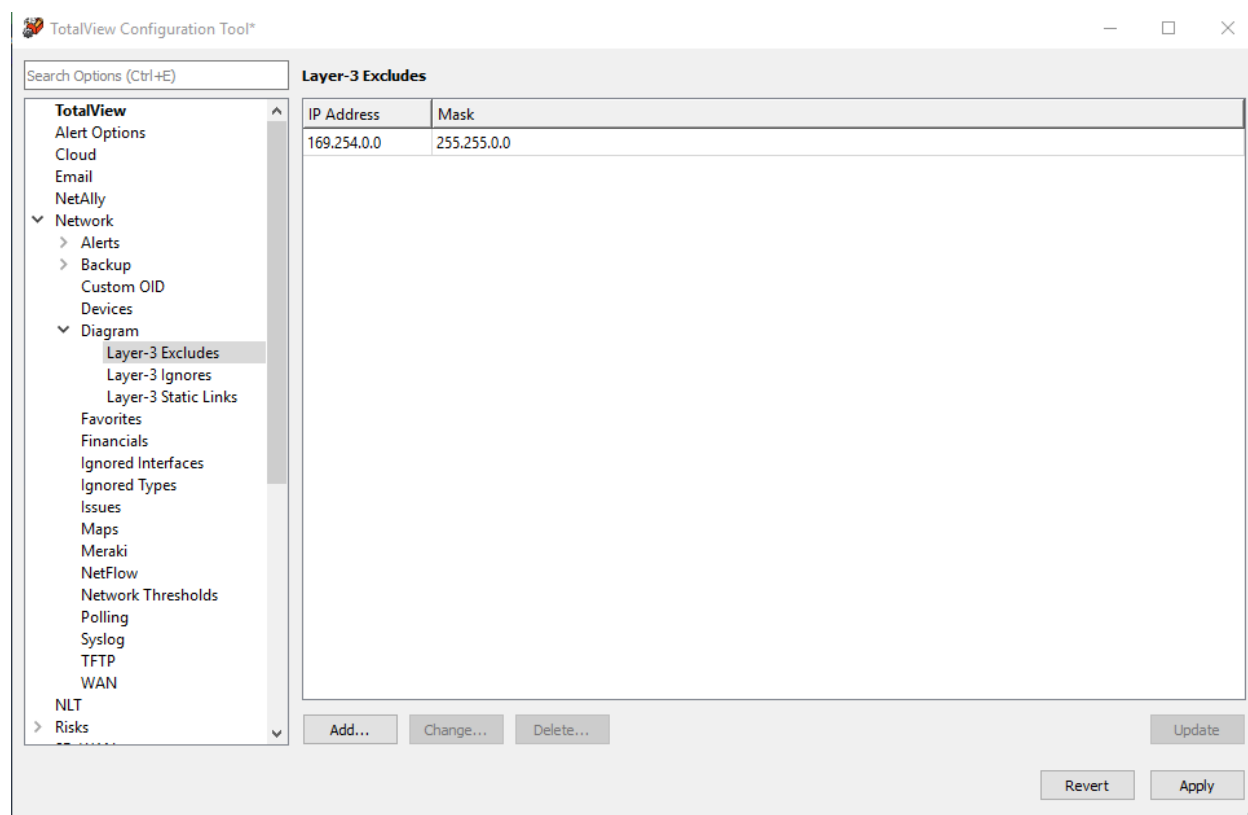
Diagram (Interactive Diagrams)

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.

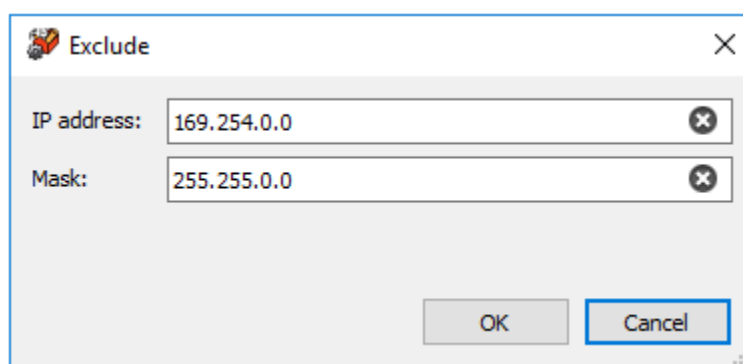


Layer-3 Excludes

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.



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 click “OK” to close this dialog, and the subnets and devices will be removed from the diagram:



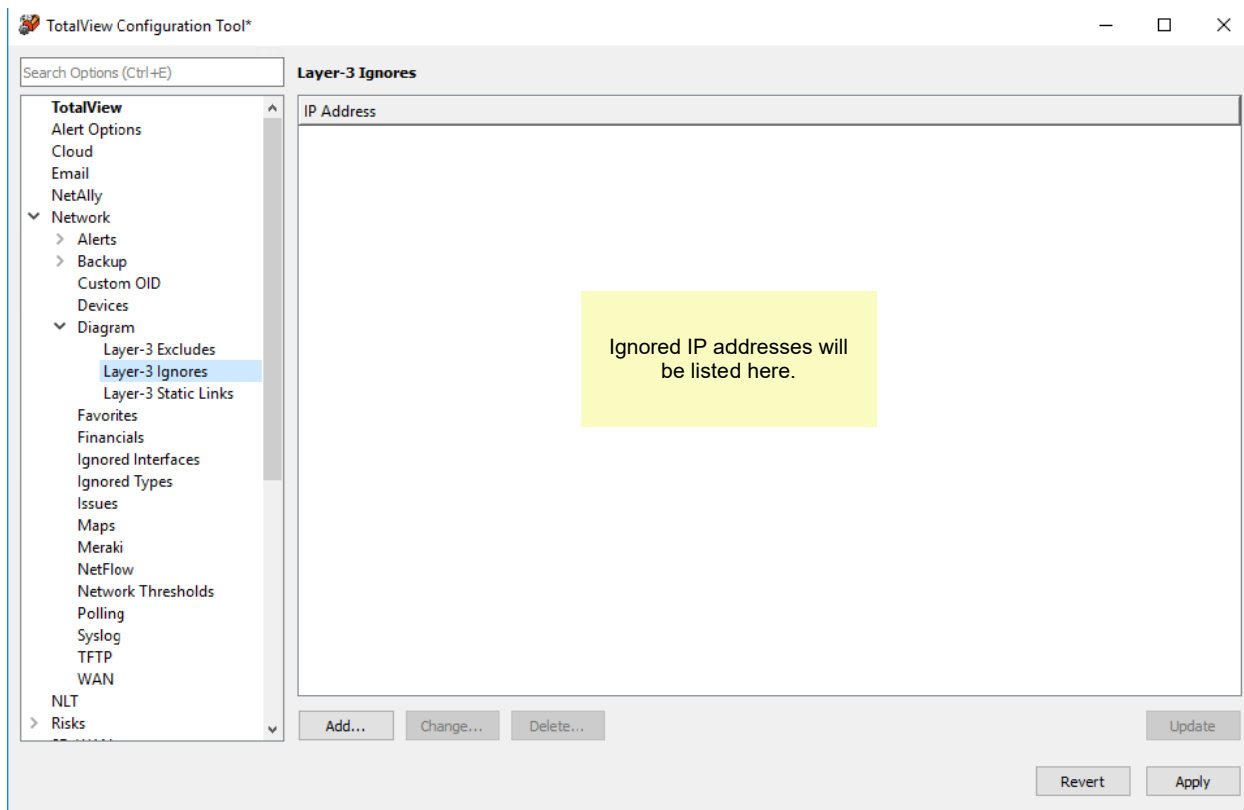
After finishing a batch of additions and changes, to preview the changes to the diagram, click “Update” and then refresh your browser window.

Note: The “Update” button will do an instant update (approximately 2 seconds) of any diagram changes that you have made.

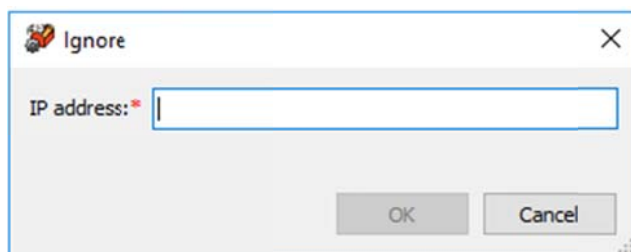
It is good practice to use the “Update” button rather than the “Apply” button for checking the diagrams. The “Apply” button would stop and start TotalView with the latest configured settings, which may take a lot longer.

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 click “OK” to close this dialog:



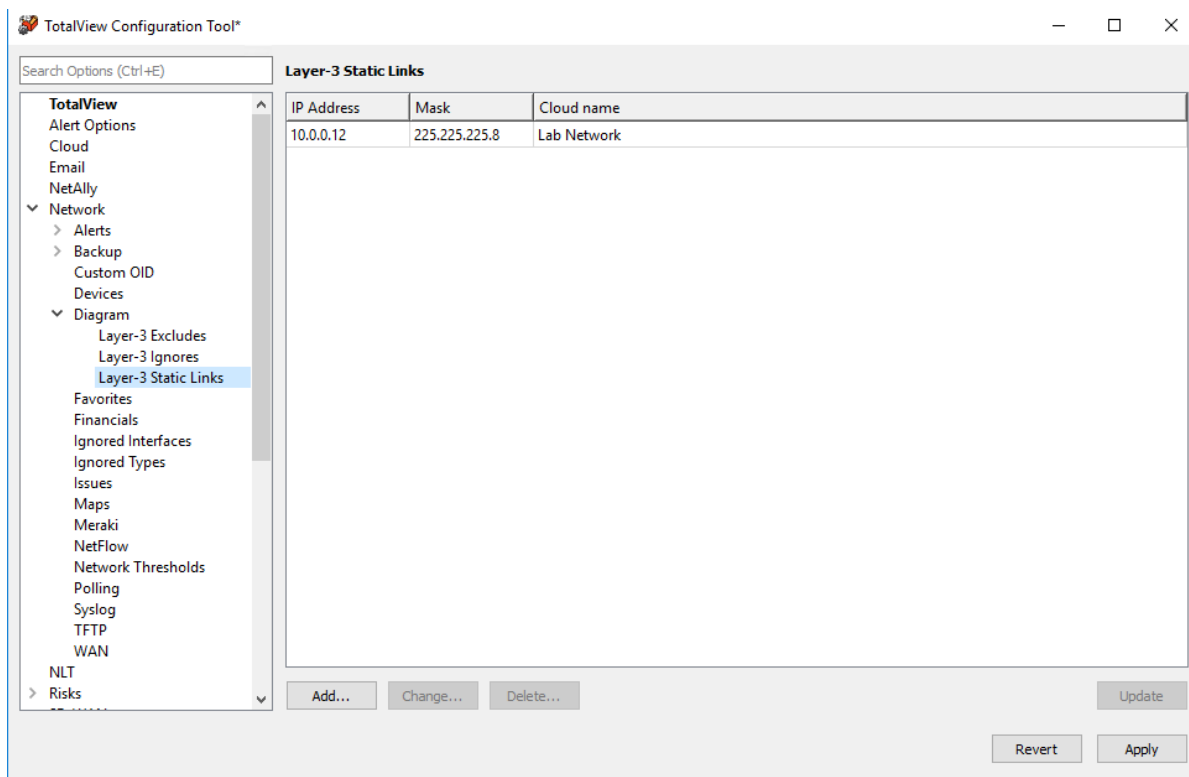
To review your work on the diagram, click “Update” and then refresh your browser window to verify that item was removed.

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.

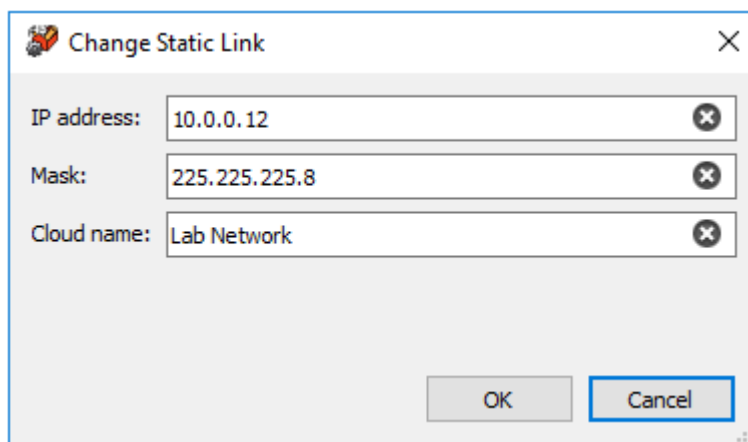
Layer-3 Static Links

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.

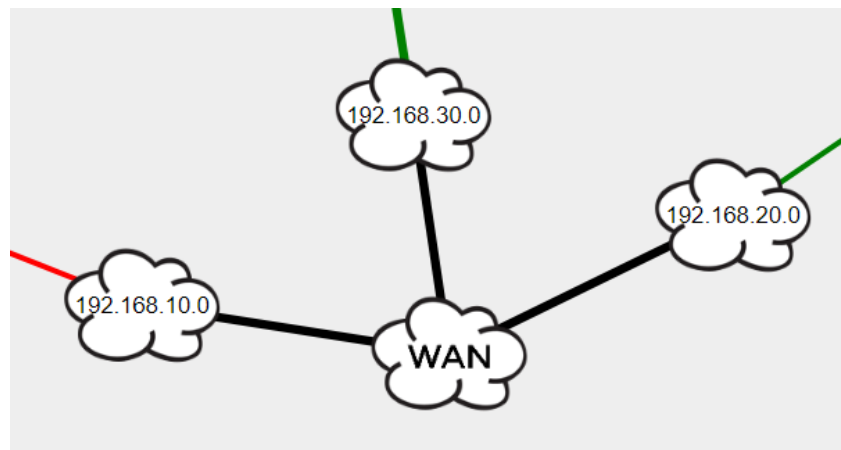


Enter the IP address and mask of an existing subnet and the Name of the cloud that you want to connect.



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.

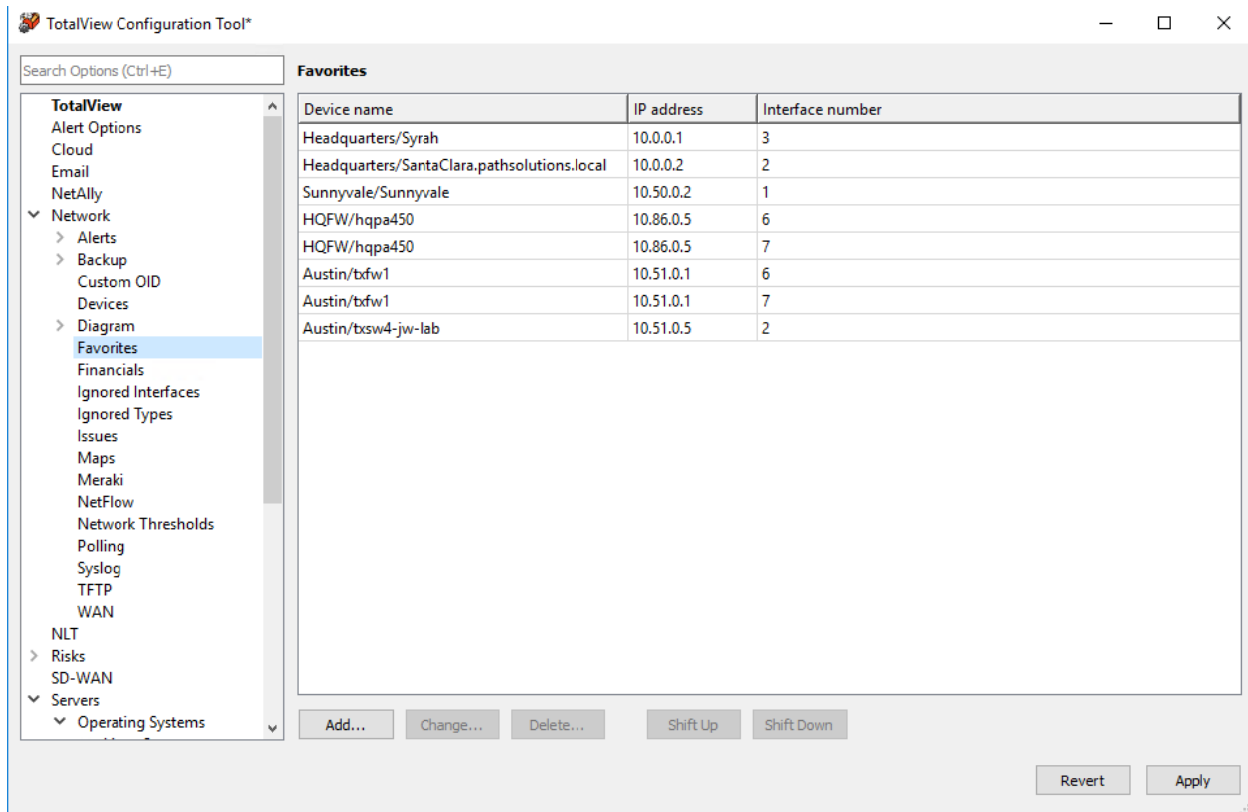
Here is an example of a WAN cloud that connects three subnets together:



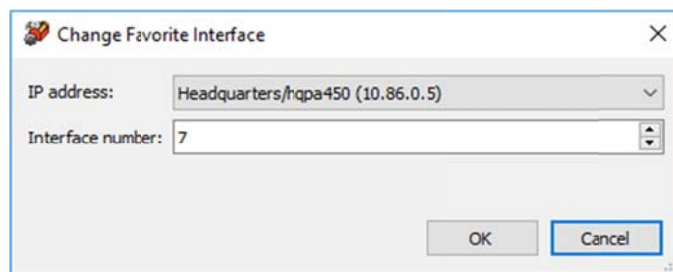
When you are finished adding your links, click the “Update” button and then refresh the web page to see how it takes effect. This allows you to quickly make changes and see the results.

Favorites

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



Click on the “Add” and “Change” buttons to add or change the items on the list of Favorites:

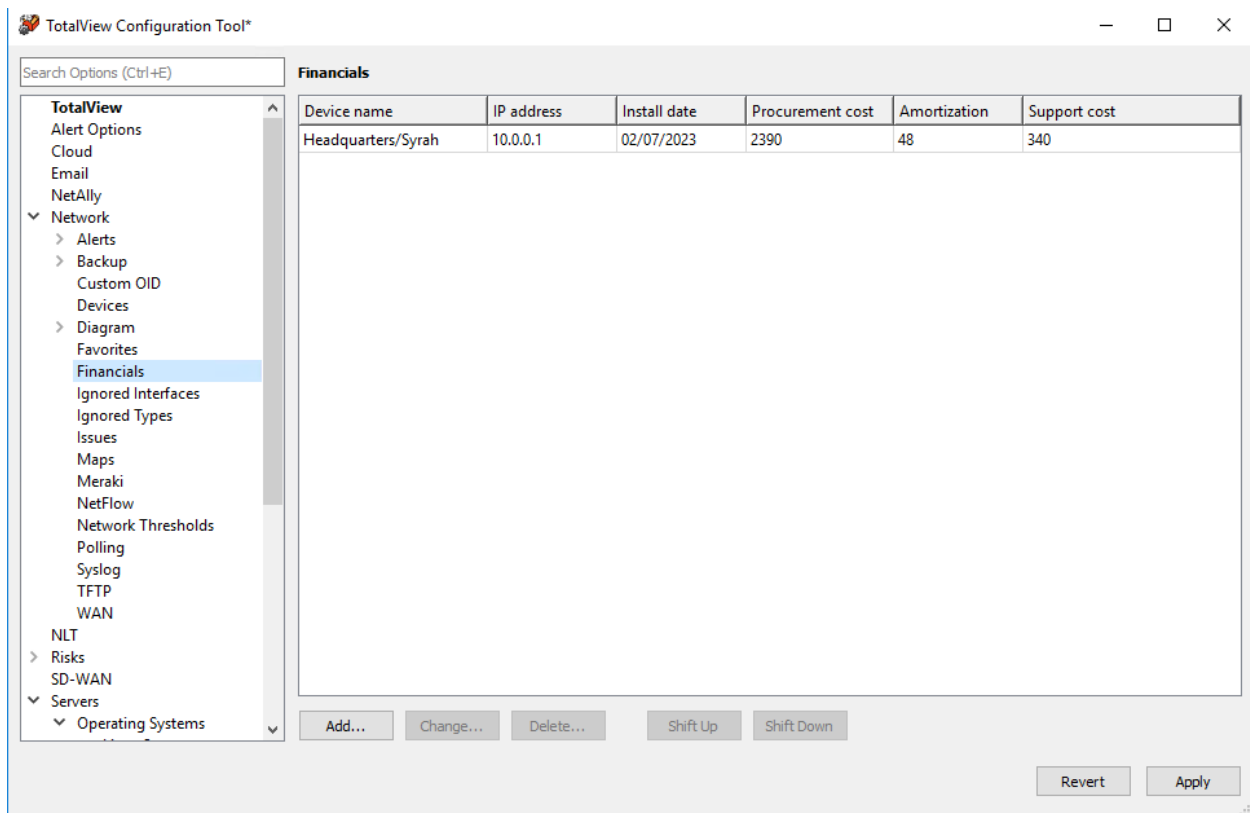


You can also configure it so that users can chose Favorites while in the TotalView web interface.

Note: The web server must be unlocked in order for the Favorites column to show up in TotalView. See the Section [Web Server \(Options\)](#) for how to lock and unlock the web server.

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:



You can add and change financial records, by clicking on the “Add” and “Change” buttons and entering new information:

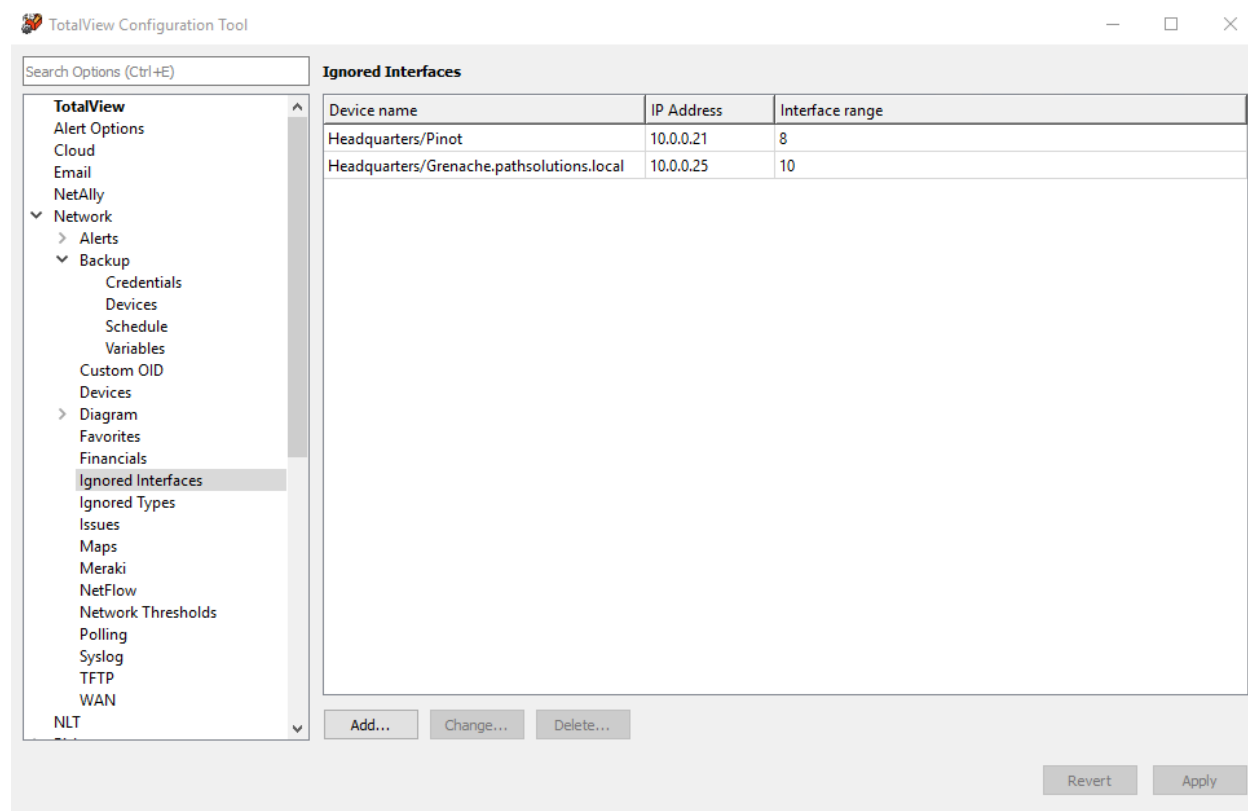
The 'Add Financials Record' dialog box contains the following fields and values:

- IP address: Headquarters/Syrah (10.0.0.1)
- ☒ Install date: 2/7/2023
- Procurement cost: 2390
- Amortization: 48
- Annual support cost: 340

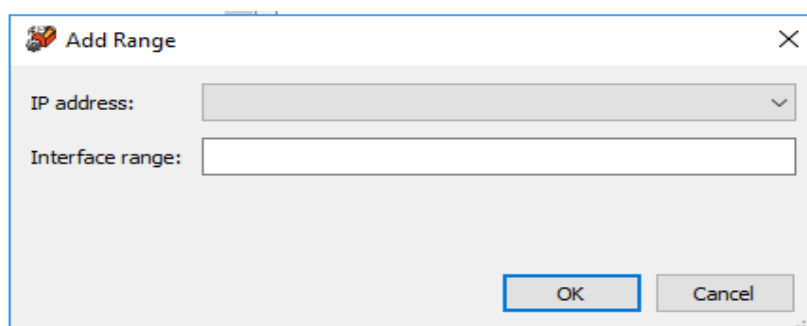
At the bottom right are 'OK' and 'Cancel' buttons.

Ignored Interfaces

Go to Network > Ignored Interfaces, and add, delete and change the list of interfaces to ignore here:



Select “Add” or “Change” buttons to add devices by IP address and interface ranges to the ignored list:



Alternate Methods to Ignore Interfaces

There are also 2 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 up in Notepad for editing. After you save the file, stop and restart the service to have this change take effect.

These file is located in one of the following directories:

For 64 bit – C:/Program Files (x86)/PathSolutions/TotalView/IgnoreList.cfg
 For 32 bit – C:/Program Files/PathSolutions/TotalView/IgnoreList.cfg

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

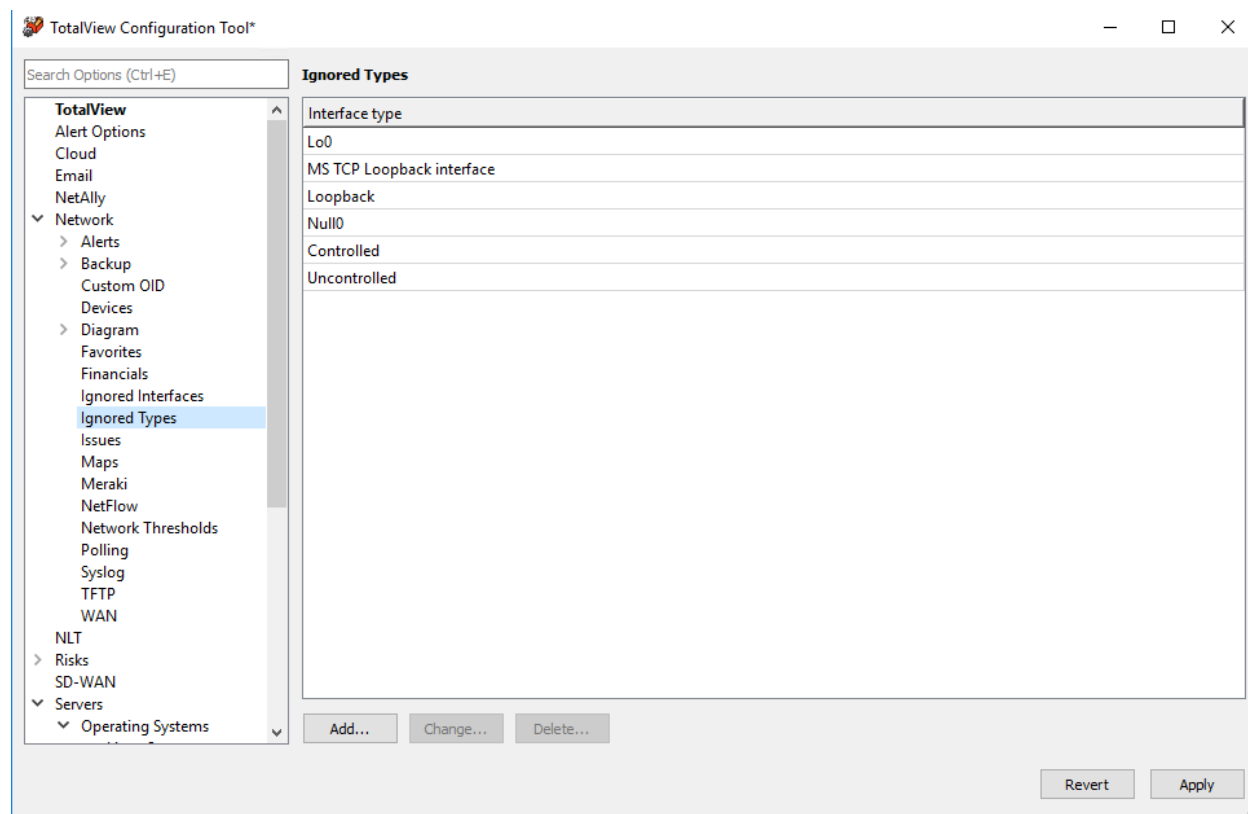
Note: The web server must be unlocked in order for the Ignore column to show up in TotalView. See the section [Web Server \(Options\)](#) for how to lock and unlock the web server.

The screenshot shows the TotalView Web Interface. The top navigation bar includes tabs like Path, Map, Diagram, Gremlins, Devices, Favorites, Issues, Netflow, IPAM, Top-10, Wan, Interfaces, SD-WAN, and Tools. The 'Devices' tab is selected, showing a table with columns: Device Name, Device IP Address, SNMP Version, Manage, CPU, Oper Down, Admin Down, Location, Contact, and Uptime. Below this, the 'Interfaces' tab is selected, showing a table with columns: Interface, Favorite, WAN, IP Address, Description, Ignore, Queue Type, MAC Address, MTU, Type, and State. A red arrow points to the 'Ignore' column in the 'Interfaces' table.

Interface	Favorite	WAN	IP Address	Description	Ignore	Queue Type	MAC Address	MTU	Type	State
INT#1	Favorite	WAN	1: 1		Ignore		40a8f00dfff3f	1520	ethernetCsmacd	116 days 00:06:00.05
INT#2	Favorite	WAN	2: 2		Ignore		40a8f00dfff3e	1520	ethernetCsmacd	116 days 00:06:10.89
INT#3	Favorite	WAN	3: 3		Ignore		40a8f00dfff3d	1520	ethernetCsmacd	116 days 00:06:10.89
INT#4	Favorite	WAN	4: 4		Ignore		40a8f00dfff3c	1520	ethernetCsmacd	116 days 00:06:10.89
INT#5	Favorite	WAN	5: 5		Ignore		40a8f00dfff3b	1520	ethernetCsmacd	116 days 00:06:10.89
INT#6	Favorite	WAN	6: 6		Ignore		40a8f00dfff3a	1520	ethernetCsmacd	116 days 00:06:10.89
INT#7	Favorite	WAN	7: 7		Ignore		40a8f00dfff39	1520	ethernetCsmacd	114 days 03:03:31.59
INT#8	Favorite	WAN	8: 8		Ignore		40a8f00dfff38	1520	ethernetCsmacd	116 days 00:06:10.89
INT#9	Favorite	WAN	9: 9		Ignore		40a8f00dfff37	1520	ethernetCsmacd	116 days 00:06:10.89
INT#10	Favorite	WAN	10: 10		Ignore		40a8f00dfff36	1520	ethernetCsmacd	116 days 00:06:10.89
INT#11	Favorite	WAN	11: 11		Ignore		40a8f00dfff35	1520	ethernetCsmacd	116 days 00:06:08.81
INT#12	Favorite	WAN	12: 12		Ignore		40a8f00dfff34	1520	ethernetCsmacd	116 days 00:06:10.89
INT#13	Favorite	WAN	13: 13		Ignore		40a8f00dfff33	1520	ethernetCsmacd	17 days 18:44:06.82
INT#14	Favorite	WAN	14: 14		Ignore		40a8f00dfff32	1520	ethernetCsmacd	116 days 00:06:10.89
INT#15	Favorite	WAN	15: 15		Ignore		40a8f00dfff31	1520	ethernetCsmacd	103 days 14:10:53.99
INT#16	Favorite	WAN	16: 16		Ignore		40a8f00dfff30	1520	ethernetCsmacd	116 days 00:06:10.89
INT#17	Favorite	WAN	17: 17		Ignore		40a8f00dfff2f	1520	ethernetCsmacd	116 days 00:06:10.89

Ignored Types

Select Network > Ignored Types then add, change or delete the interface types you want to ignore;



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 up in Notepad for editing. After you save the file, stop and restart the service to have this change take effect.

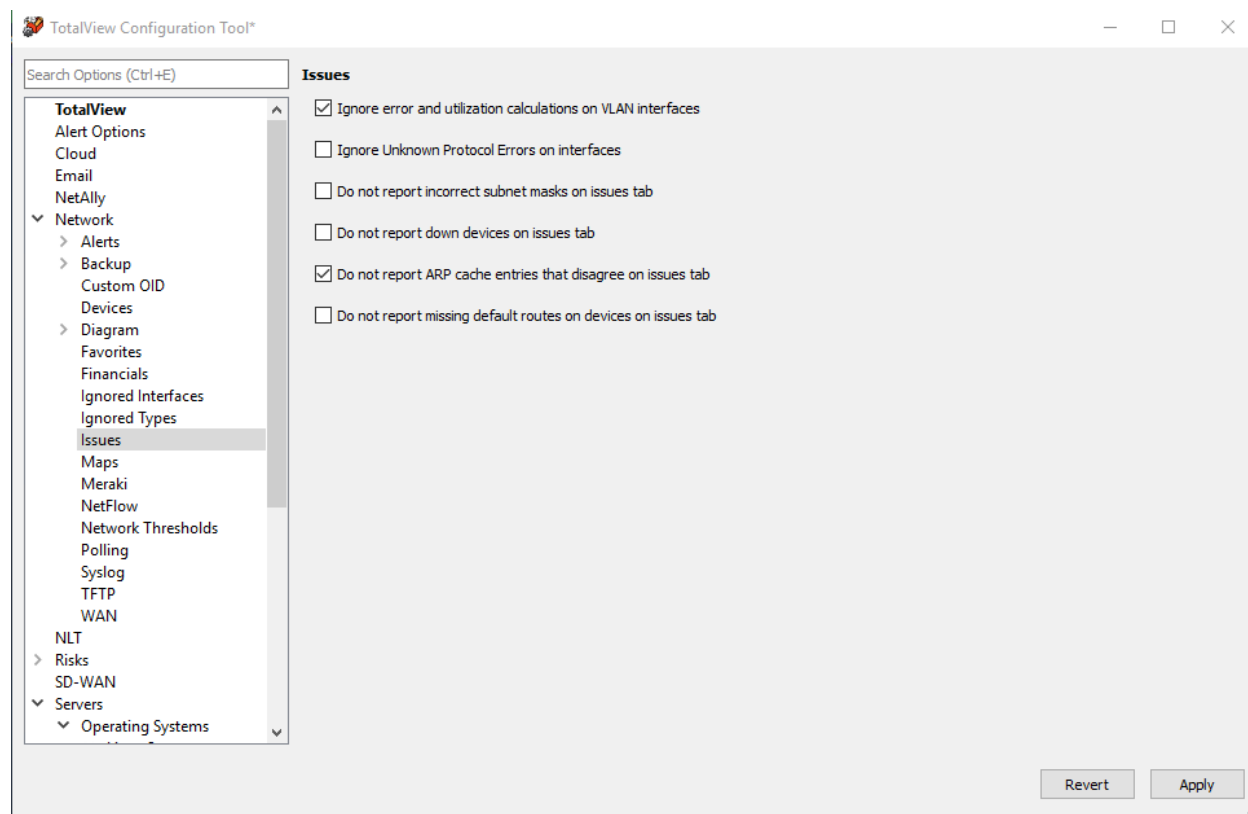
This files is located in one of the following directories:

For 64 bit – C:/Program Files (x86)/PathSolutions/TotalView/IgnoreType.cfg

For 32 bit – C:/Program Files/PathSolutions/TotalView/IgnoreType.cfg

Issues

You can specify what issues you want to see, or ignore, on the issues list:



How to Ignore Unknown Protocol Errors

You can check the box besides “Ignore Unknown Protocol Errors”, 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.

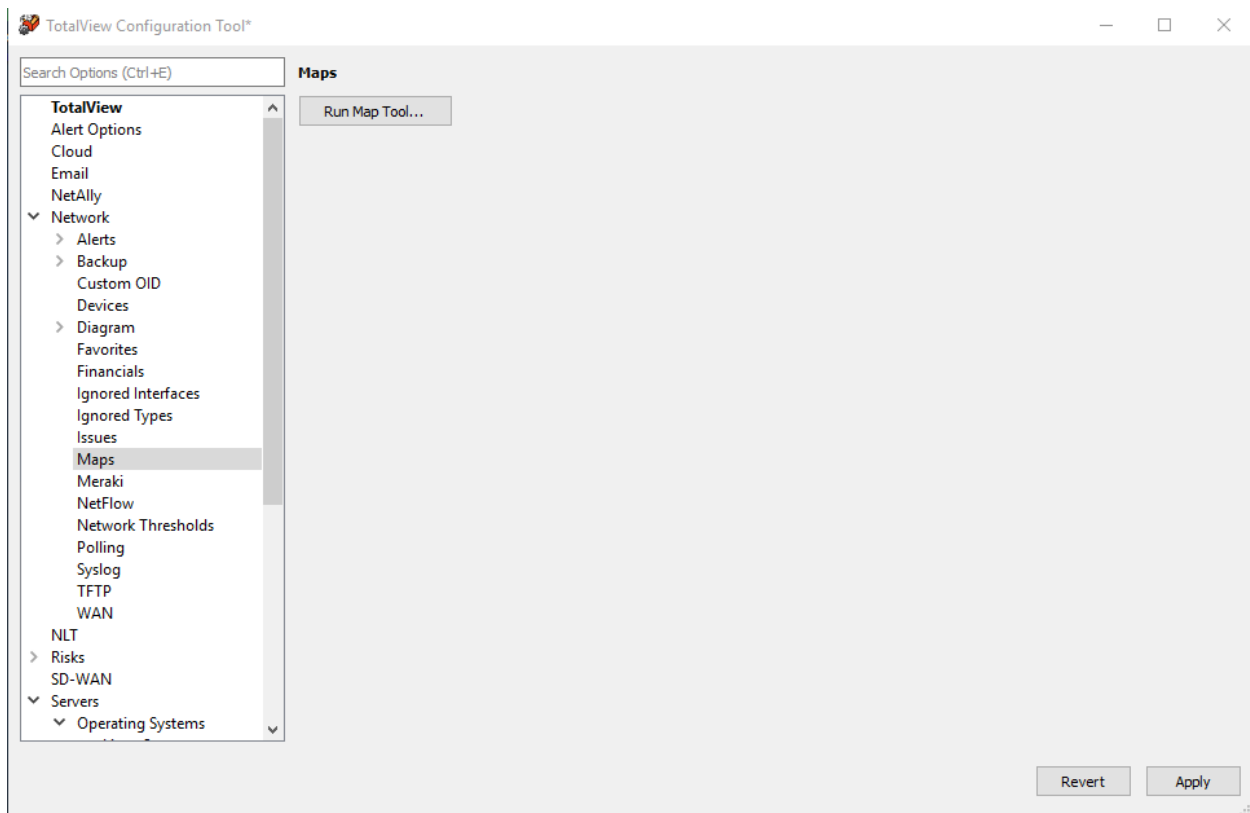
How to Ignore VLAN Interface Errors

You can check the box besides “Ignore errors and utilization calculations on VLAN interfaces” 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, check the “Ignore error calculations on VLAN interfaces” box. The VLAN interface will still be listed, but it will not be listed on the TotalView “Issues” tab.

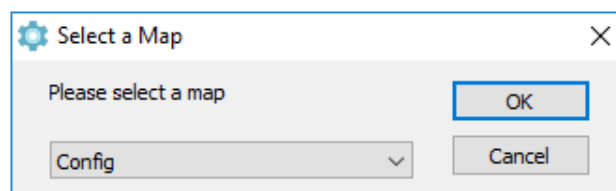
Maps

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



Note: You can ignore the “Apply” and “Revert” buttons on screen in this section. They do not save the map or revert the map.

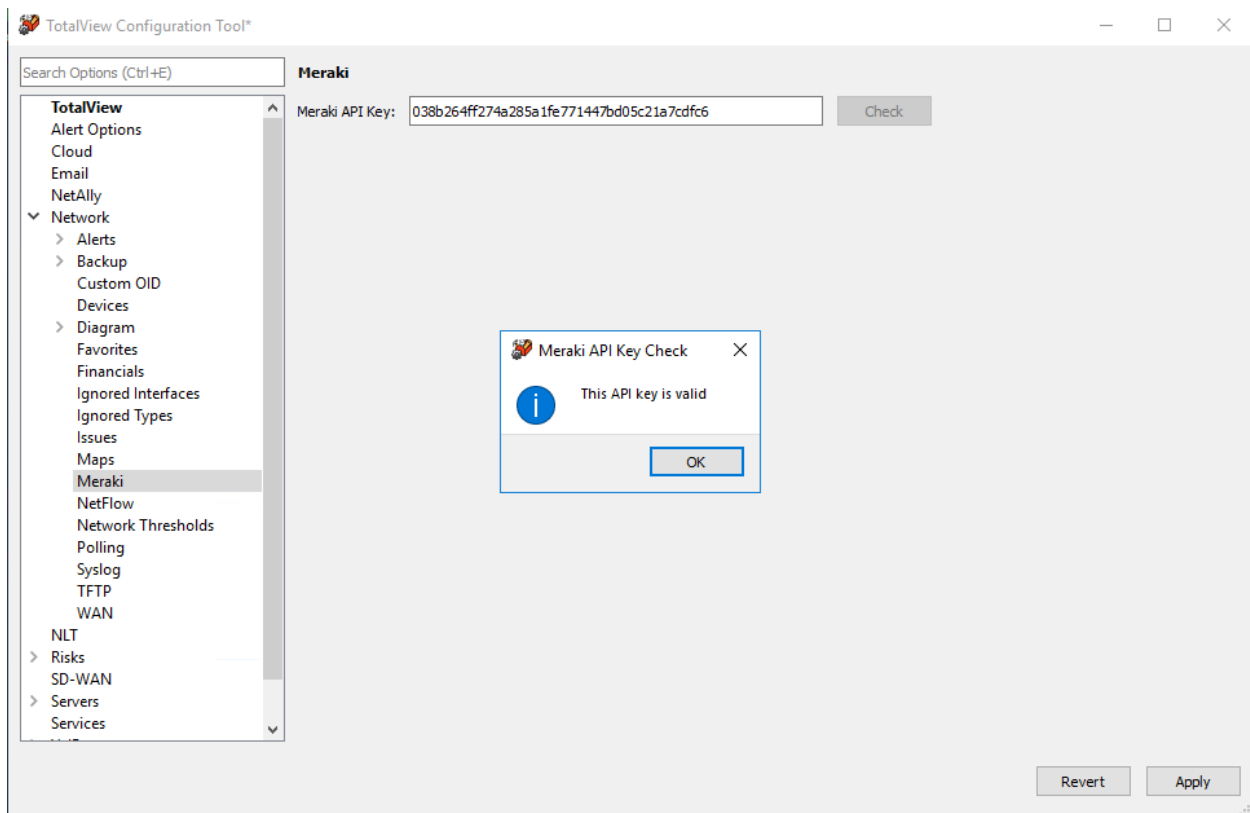
Select the button “Run Map Tool” button. The Map Config Tool will open in a new window, and will ask you to select a map. Select a map from the drop-down menu.



See the section on the [Map Config Tool](#) for instructions how to use this tool.

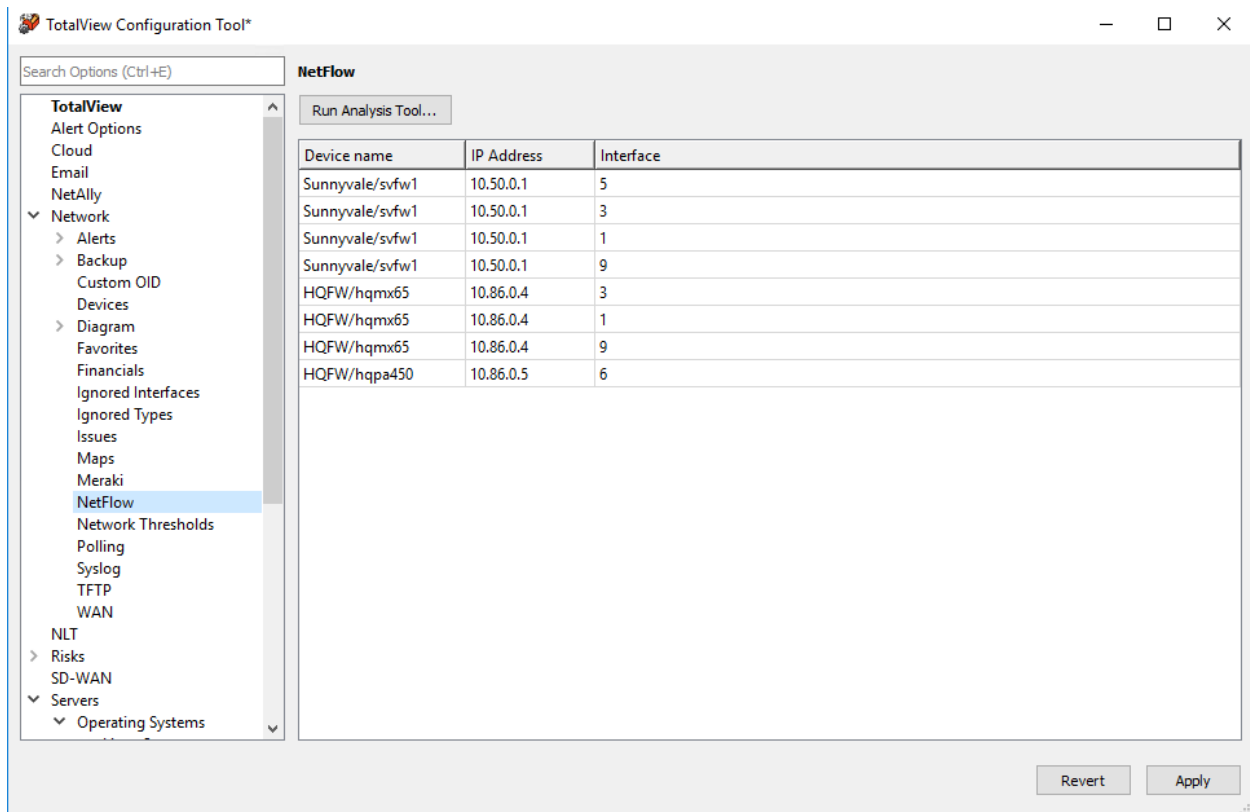
Meraki

Select Network > Meraki from the left-hand list. Enter the Meraki API key. Select the “Check” to check the key is valid. A notice will tell you if the API key is valid:

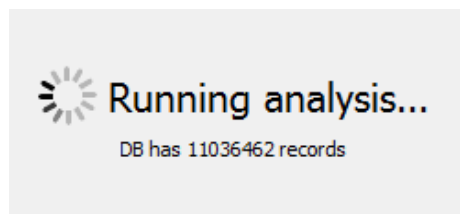


NetFlow

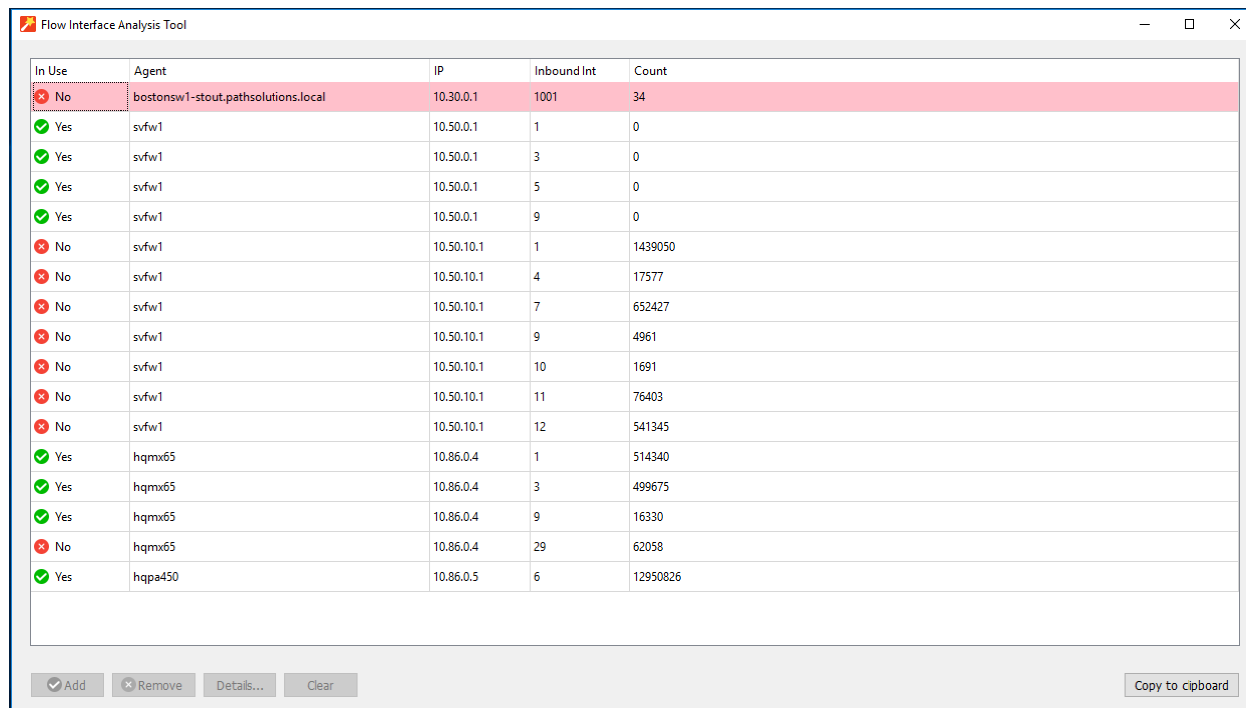
To configure NetFlow, select Network > NetFlow from the left-hand menu. Here you can run a NetFlow Analysis by pressing “Run Analysis Tool” at top, and also adjust the interfaces displayed on the NetFlow section:



The “Run Analysis Tool” button performs a NetFlow analysis (allow 3-5 minutes for it to run).



The NetFlow analysis report then gets called up in a new window, and looks like this:

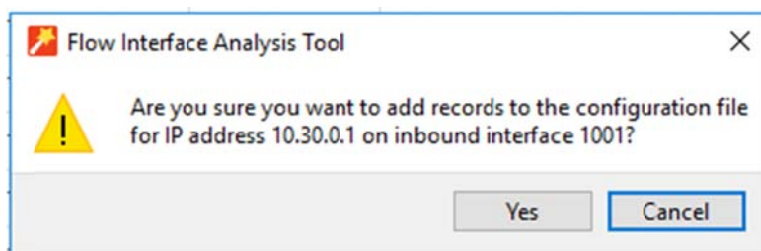


In Use	Agent	IP	Inbound Int	Count
No	bostonsw1-stout.pathsolutions.local	10.30.0.1	1001	34
Yes	svfw1	10.50.0.1	1	0
Yes	svfw1	10.50.0.1	3	0
Yes	svfw1	10.50.0.1	5	0
Yes	svfw1	10.50.0.1	9	0
No	svfw1	10.50.10.1	1	1439050
No	svfw1	10.50.10.1	4	17577
No	svfw1	10.50.10.1	7	652427
No	svfw1	10.50.10.1	9	4961
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

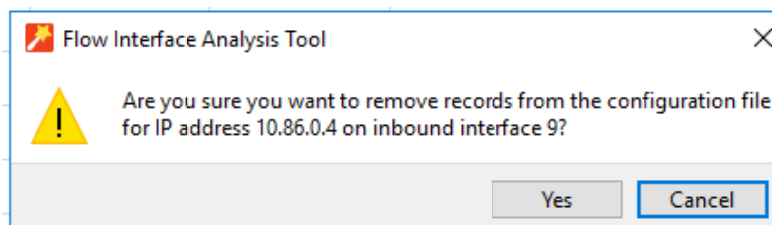
Buttons: Add, Remove, Details..., Clear, Copy to clipboard

Here you can change the sort order, by selecting items on the list, then clicking the “Shift Up” or “Shift Down” buttons. You can also assign the sort order by entering an Interface number.

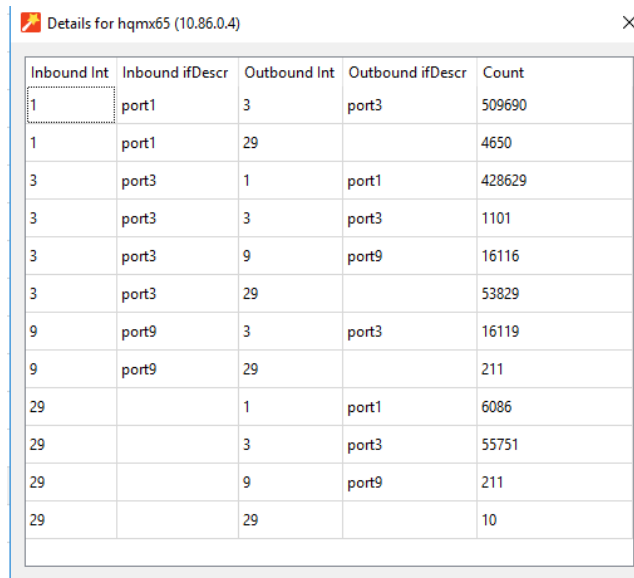
To add an interface, select something marked “No” from the list. Then select the “Add” button at the bottom. It will ask if you are sure you want to add records to the configuration file? Select “Yes” or “Cancel”:



To remove an interface, select something from the list marked “Yes”. Then click the “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”:



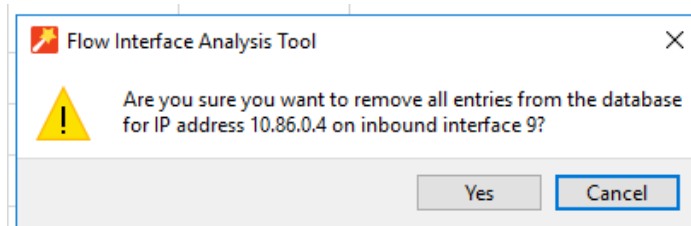
To view the NetFlow details of any agent, select something from the list, then click the “Details” button:



A screenshot of a window titled "Details for hqmx65 (10.86.0.4)". It contains a table with 5 columns: Inbound Int, Inbound ifDescr, Outbound Int, Outbound ifDescr, and Count. The table lists 13 rows of network flow data.

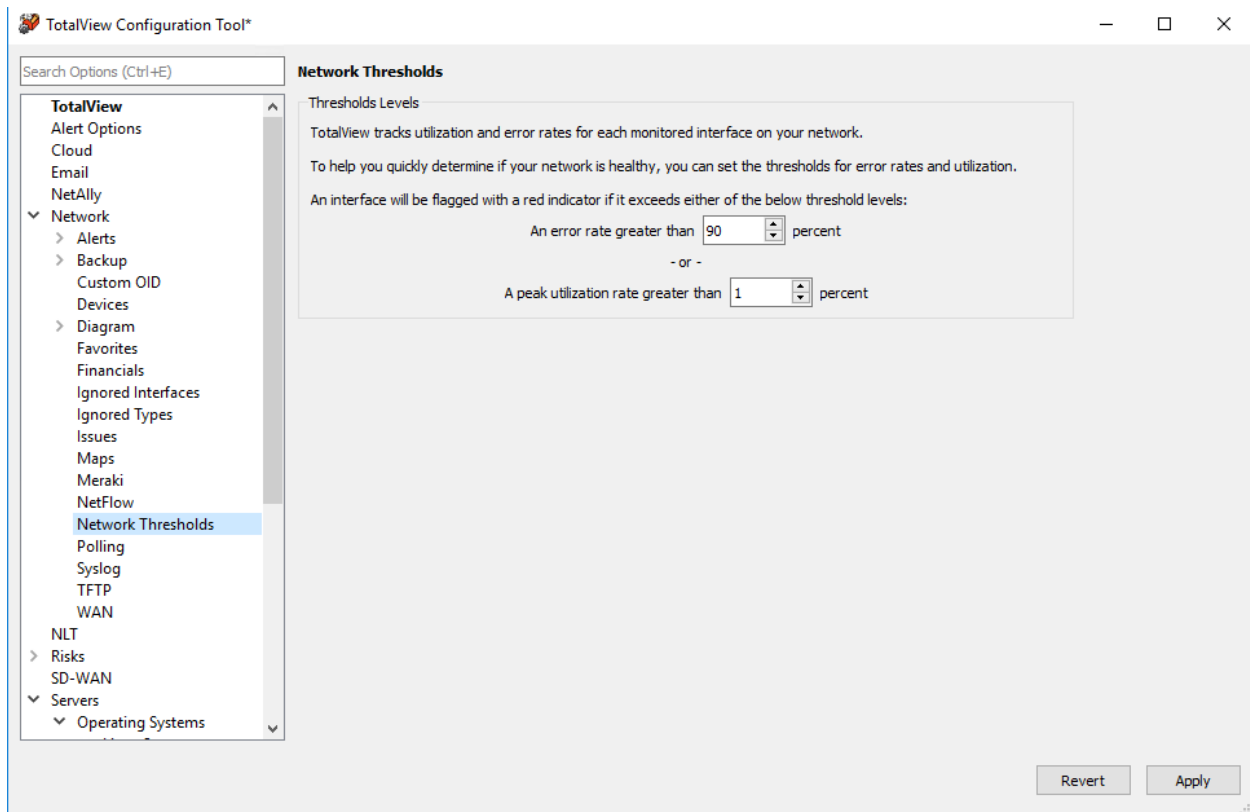
Inbound Int	Inbound ifDescr	Outbound Int	Outbound ifDescr	Count
1	port1	3	port3	509690
1	port1	29		4650
3	port3	1	port1	428629
3	port3	3	port3	1101
3	port3	9	port9	16116
3	port3	29		53829
9	port9	3	port3	16119
9	port9	29		211
29		1	port1	6086
29		3	port3	55751
29		9	port9	211
29		29		10

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".



Network Thresholds

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



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

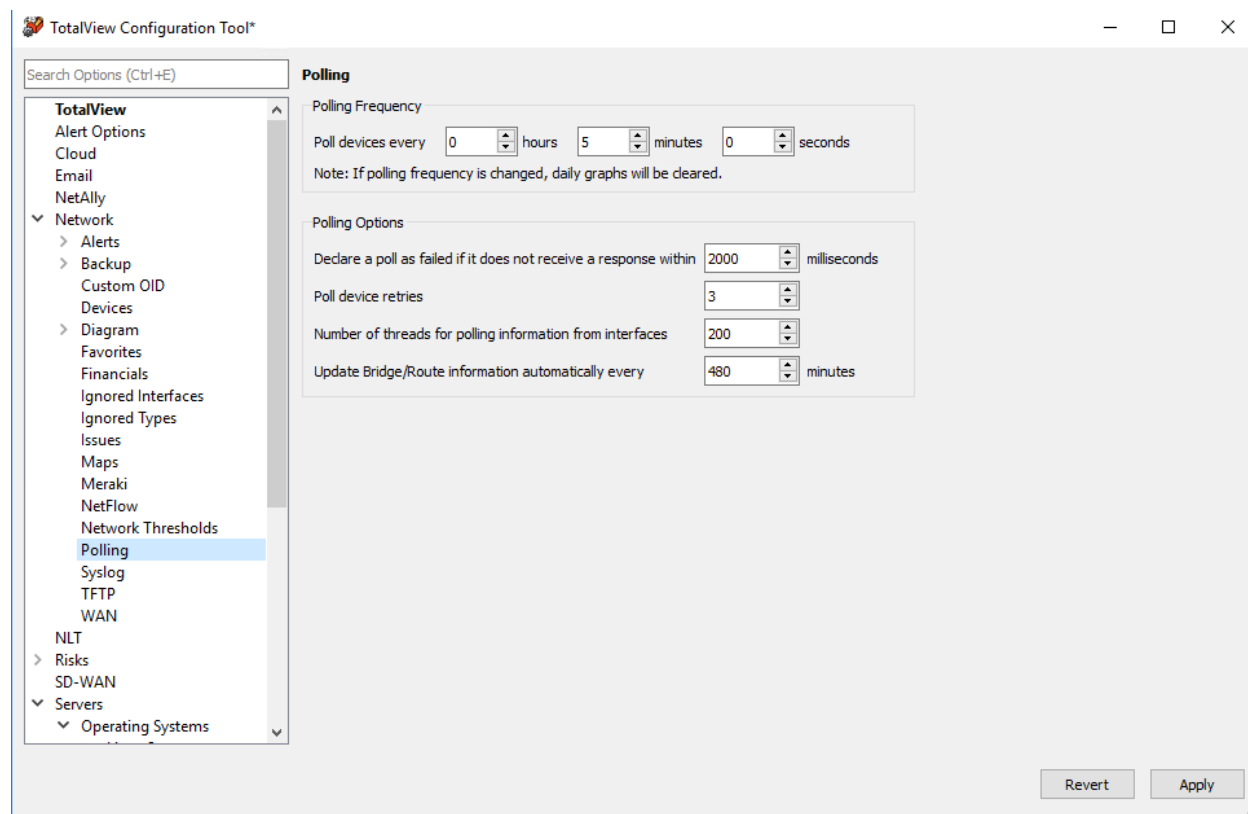
If an interface has a peak utilization rate (transmitted or received) over 90%, network status will be changed to 'Degraded'.

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

When you are finished making changes, click "Apply" to commit the changes to memory.

Polling Behavior

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



TotalView is very 'network friendly', and makes every attempt to prevent flooding the network 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 you can 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 this number. 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.

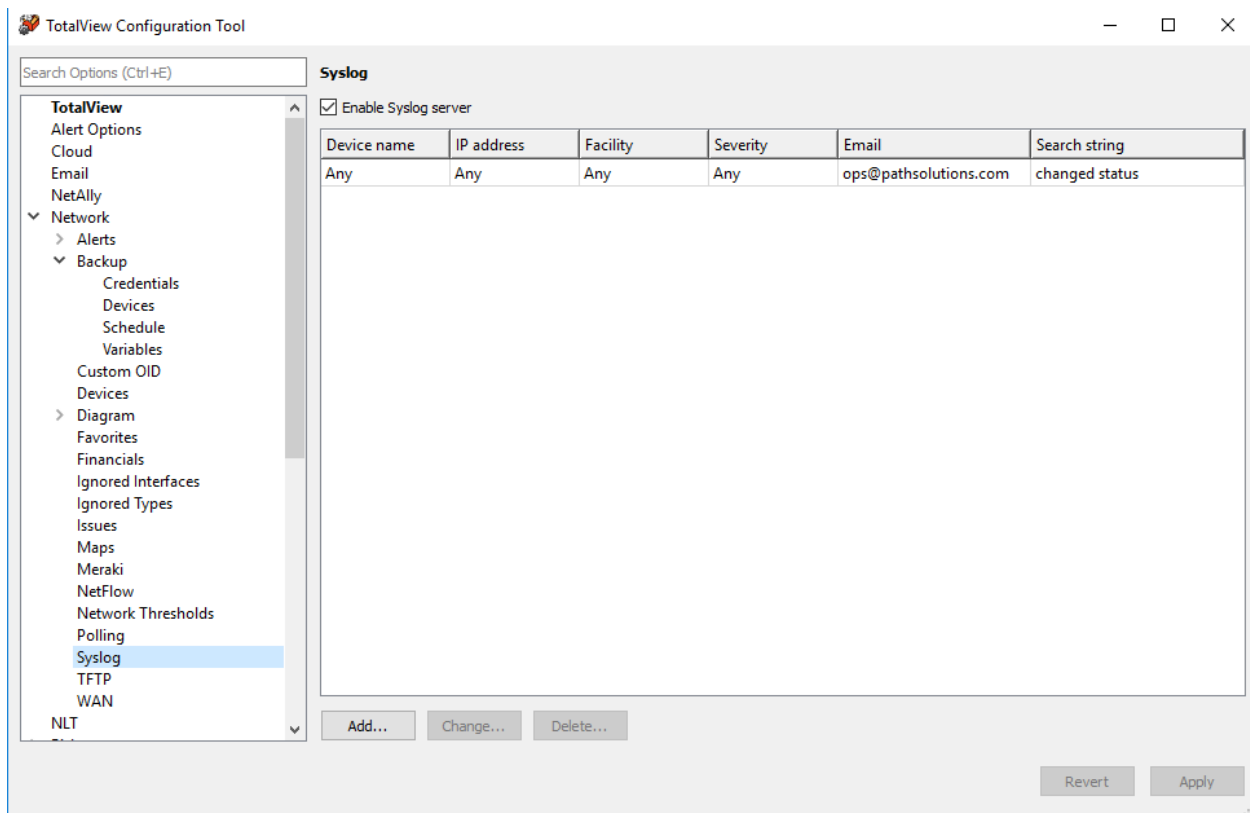
The default is 5 minutes. Less frequent polls will decrease the traffic on your network; however, it will not provide you with as granular information on utilization and error rates.

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

Note: It is very important to make sure you do not 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:

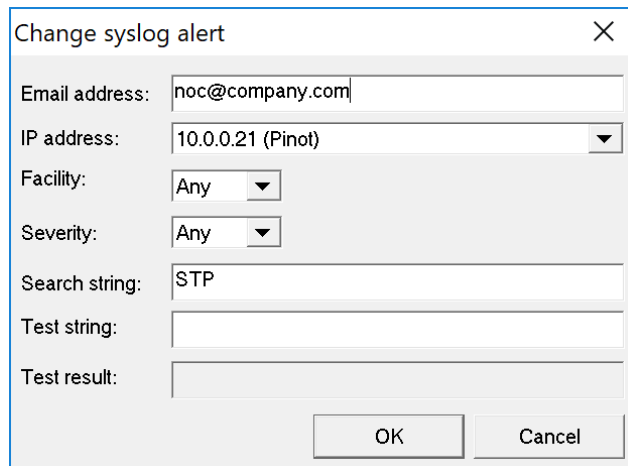


To enable the syslog server, check the box “Enable Syslog Server”.

Syslog messages will be captured and be visible from the web pages. Click on 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.

You can add or change alerting for syslog messages by clicking on the “Add” and “Change” buttons. You should see the following dialog:



The image shows a dialog box titled "Change syslog alert" with a close button (X) in the top right corner. The dialog contains several input fields and dropdown menus. The "Email address:" field contains "noc@company.com". The "IP address:" field contains "10.0.0.21 (Pinot)". The "Facility:" dropdown menu is set to "Any". The "Severity:" dropdown menu is set to "Any". The "Search string:" field contains "STP". The "Test string:" field is empty. The "Test result:" field is empty. At the bottom right, there are "OK" and "Cancel" buttons.

Email address:	noc@company.com
IP address:	10.0.0.21 (Pinot)
Facility:	Any
Severity:	Any
Search string:	STP
Test string:	
Test result:	

If you enter the search string with a regular expression, you can then 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 differently.[4] The list of facilities available: (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 or 15 or both may be used. The confusion is even greater regarding auth/authpriv. 4 and 10 are most common but 13 and 14 may also 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.	Info 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. But the regex syntax allows for special characters and expressions in the pattern.

Special Pattern Characters

Special pattern characters are characters (or sequences of characters) that 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 <i>line terminators</i> (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 <code>letter</code>	control code	a control code character whose <i>code unit value</i> is the same as the remainder of dividing the <i>code unit value</i> of <i>letter</i> by 32. For example: \ca is the same as \u0001, \cb the same as \u0002, and so on...
\x <code>hh</code>	ASCII character	a character whose <i>code unit value</i> has a hex value equivalent to the two hex digits <i>hh</i> . For example: \x4c is the same as L, or \x23 the same as #.
\u <code>hhhh</code>	Unicode character	a character whose <i>code unit value</i> has a hex value equivalent to the four hex digits <i>hhhh</i> .
\0	null	a null character (same as \u0000).
\int	backreference	the result of the submatch whose opening parenthesis is the <i>int</i> -th (<i>int</i> shall begin by a digit other than 0). See groups below for more info.
\d	digit	a decimal digit character (same as <code>[[:digit:]]</code>).
\D	not digit	any character that is not a decimal digit character (same as <code>[^[:digit:]]</code>).
\s	whitespace	a whitespace character (same as <code>[[:space:]]</code>).
\S	not whitespace	any character that is not a whitespace character (same as <code>[^[:space:]]</code>).
\w	word	an alphanumeric or underscore character (same as <code>[_[:alnum:]]</code>).
\W	not word	any character that is not an alphanumeric or underscore character (same as <code>[^_[:alnum:]]</code>).

<code>\character</code>	character	the character <i>character</i> as it is, without interpreting its special meaning within a regex expression. Any <i>character</i> can be escaped except those which form any of the special character sequences above. Needed for: <code>^ \$ \ . * + ? () [] { } </code>
<code>[class]</code>	character class	the target character is part of the class (see character classes below)
<code>[^class]</code>	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:

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

Quantifiers

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

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

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
<code>(subpattern)</code>	Group	Creates a backreference.
<code>(?:subpattern)</code>	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 <i>line terminator</i> .
\$	End of line	Either it is the end of the target sequence, or precedes a <i>line terminator</i> .
\b	Word boundary	The previous character is a <i>word character</i> and the next is a <i>non-word character</i> (or vice-versa). Note: The beginning and the end of the target sequence are considered here as <i>non-word characters</i> .
\B	Not a word boundary	The previous and next characters are both <i>word characters</i> or both are <i>non-word characters</i> . Note: The beginning and the end of the target sequence are considered here as <i>non-word characters</i> .
(?=subpattern)	Positive lookahead	The characters following the assertion must match <i>subpattern</i> , but no characters are consumed.
(?!subpattern)	Negative lookahead	The characters following the assertion must not match <i>subpattern</i> , 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
[: <i>classname</i> :]	character class	Uses the <i>regex traits</i> ' isctype member with the appropriate type gotten from applying lookup classname member on <i>classname</i> for the match.
[. <i>classname</i> .]	collating sequence	Uses the <i>regex traits</i> ' lookup collatename to interpret <i>classname</i> .
[= <i>classname</i> =]	character equivalents	Uses the <i>regex traits</i> ' transform primary of the result of regex_traits::lookup collatename for <i>classname</i> 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.

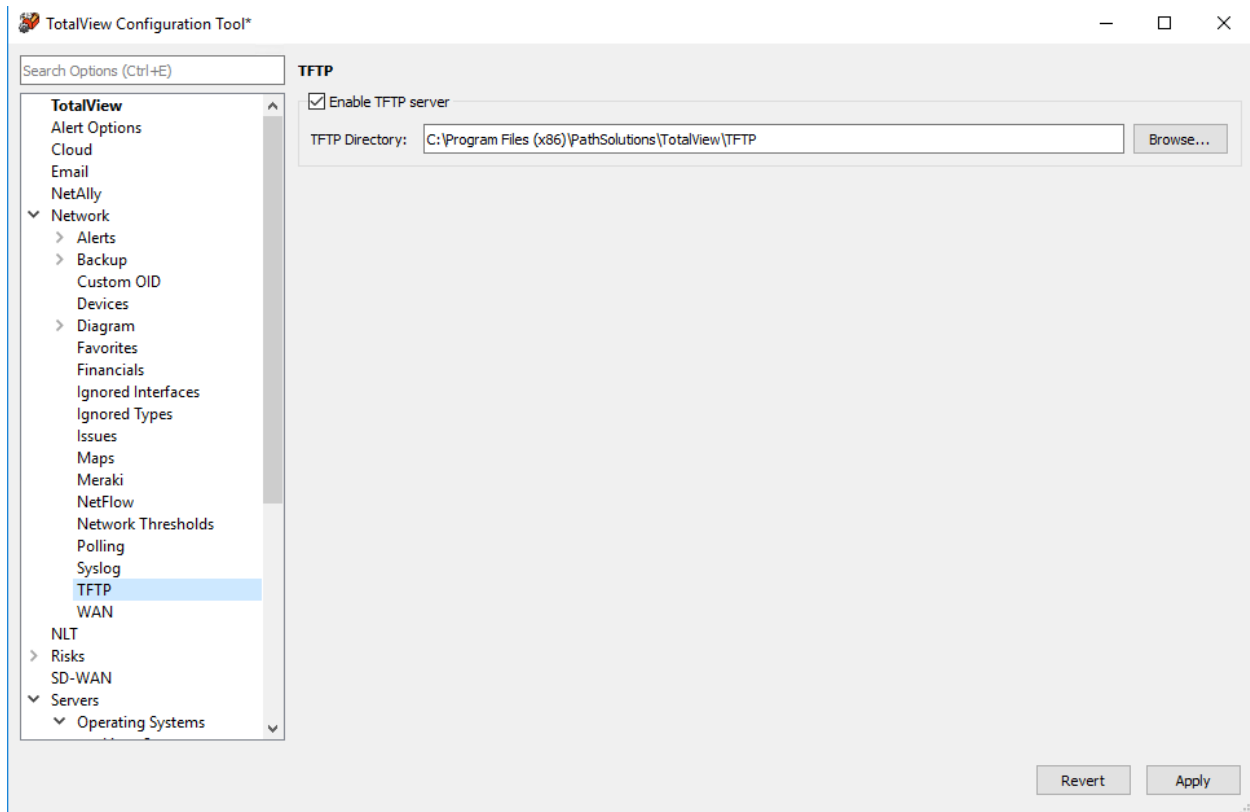
[^[:space:]] is a character class that matches any character except a whitespace.

- **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 heavily 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 [ctype](#) for a classification of characters.

TFTP Server

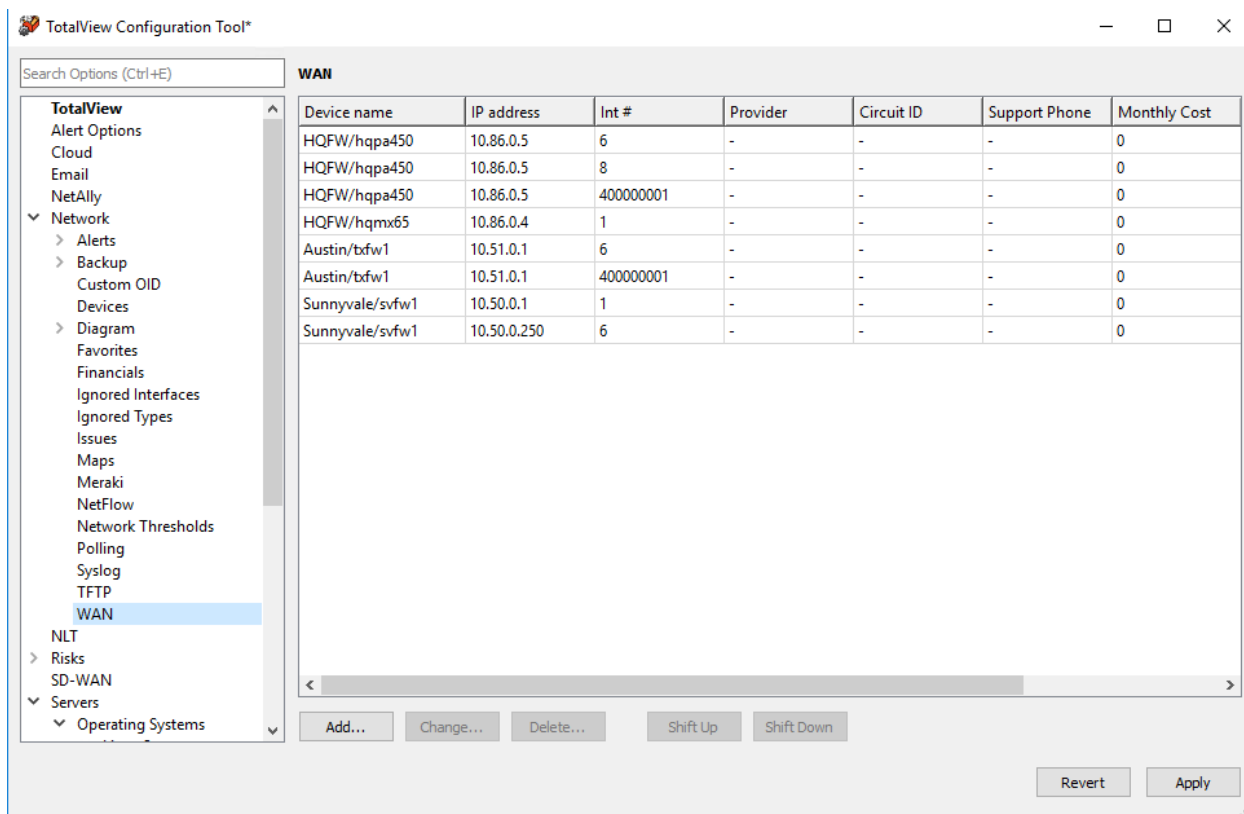
The system can receive TFTP files from network devices via the built-in TFTP server:



You can click on “Enable TFTP server”. If desired, “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 any Notes about a device to display on the “WAN” tab.



To add an interface, click on the “Add” button and add the details. Then select OK:

Add WAN interface ✕

IP address:

Interface number:

Provider:

Circuit ID:

Support phone:

Monthly cost:

Expiration date: ☒

Notes:

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.

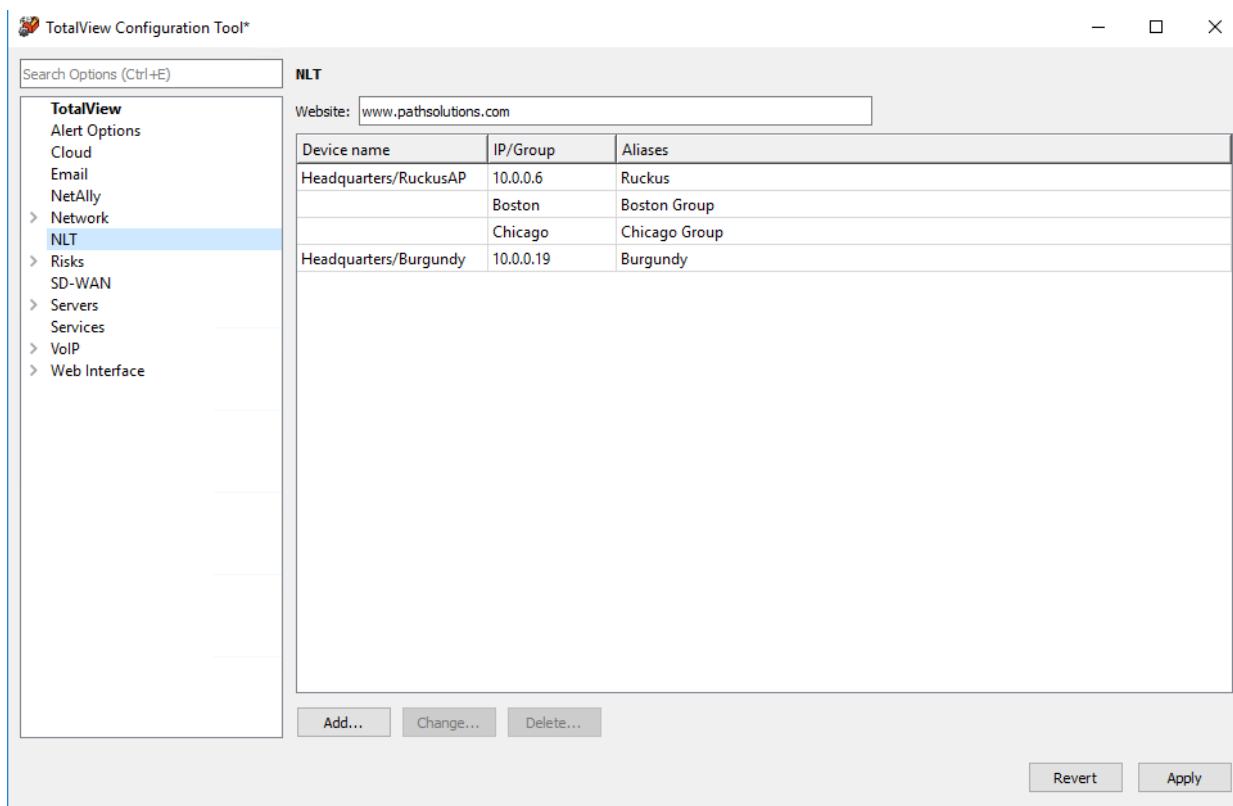
You can also configure it so that users can add WAN interfaces while in the TotalView web interface.

Note: The web server must be unlocked in order for the Favorites column to show up in TotalView. See the Section [Web Server \(Options\)](#) for how to lock and unlock the web server.

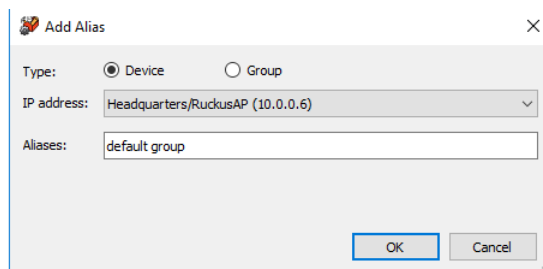
Note: You can also add WAN by editing the CFG text file. See [Appendix H. Changing the WAN Tab](#).

NLT

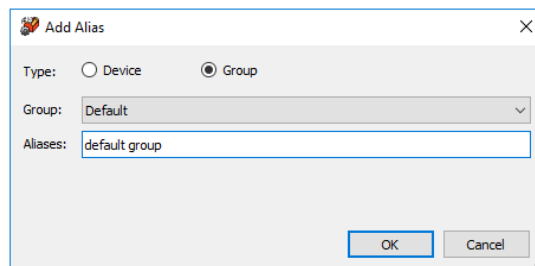
Go to the NLT section to add a website, and to setup alias names. Aliases allow you to refer to devices and groups by aliases when asking questions on the TotalView “NLT” tab.



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

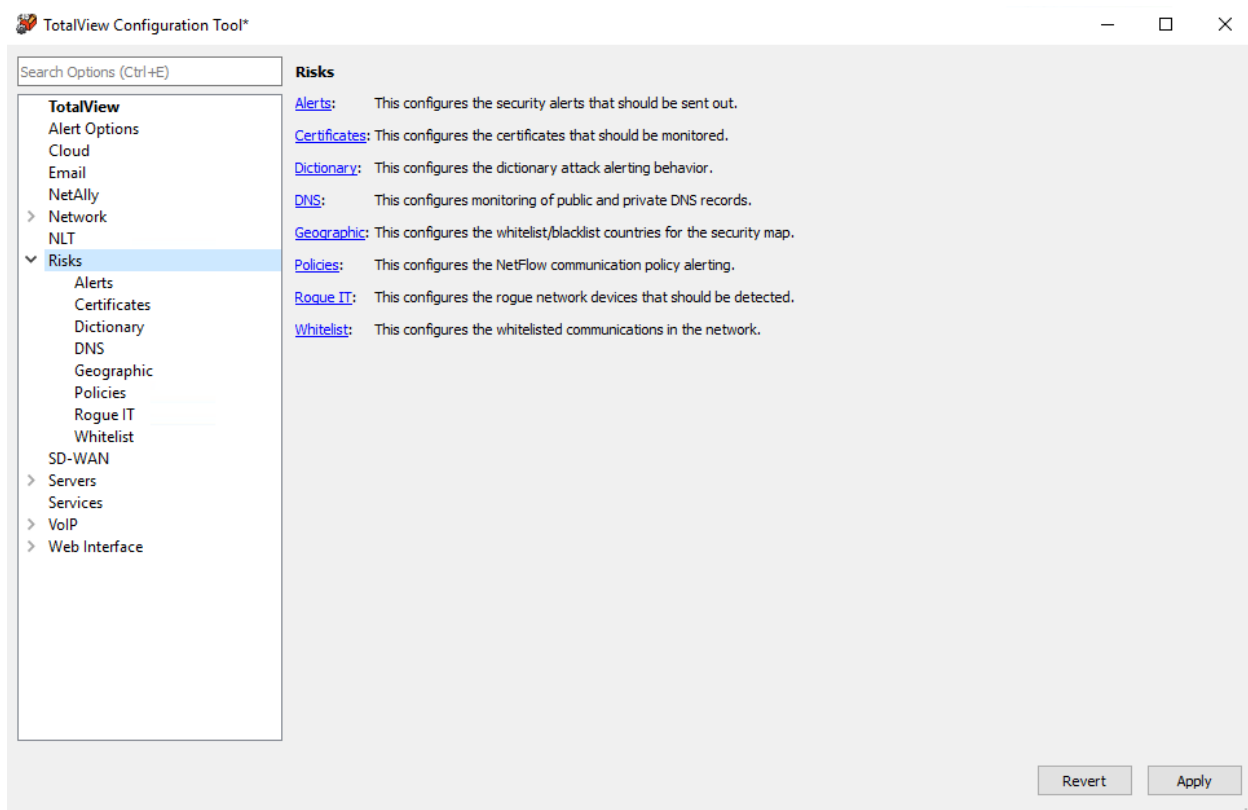


For groups, select the type “Group” then pick a group from the drop-down menu and give it an alias:



Risk Monitoring

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



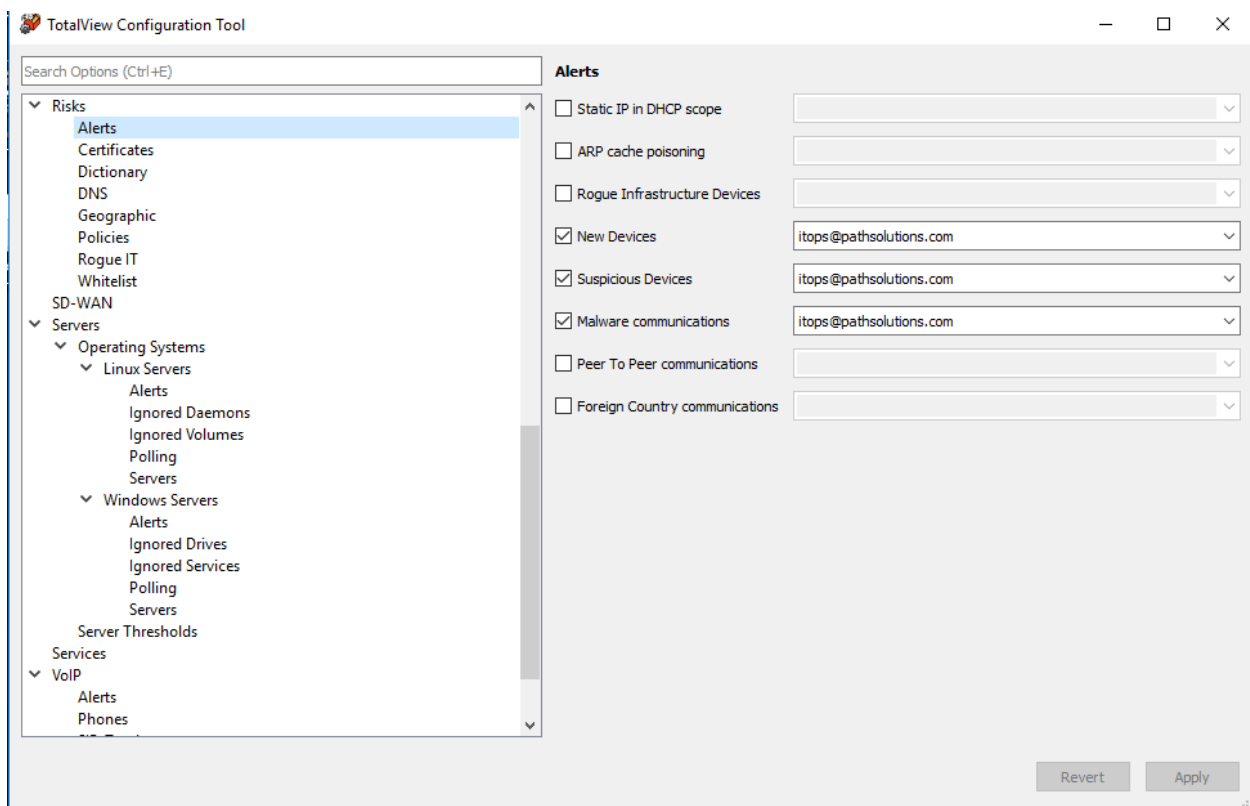
Alerts

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 you can checkmark the type of alerts to receive here*:

- 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.

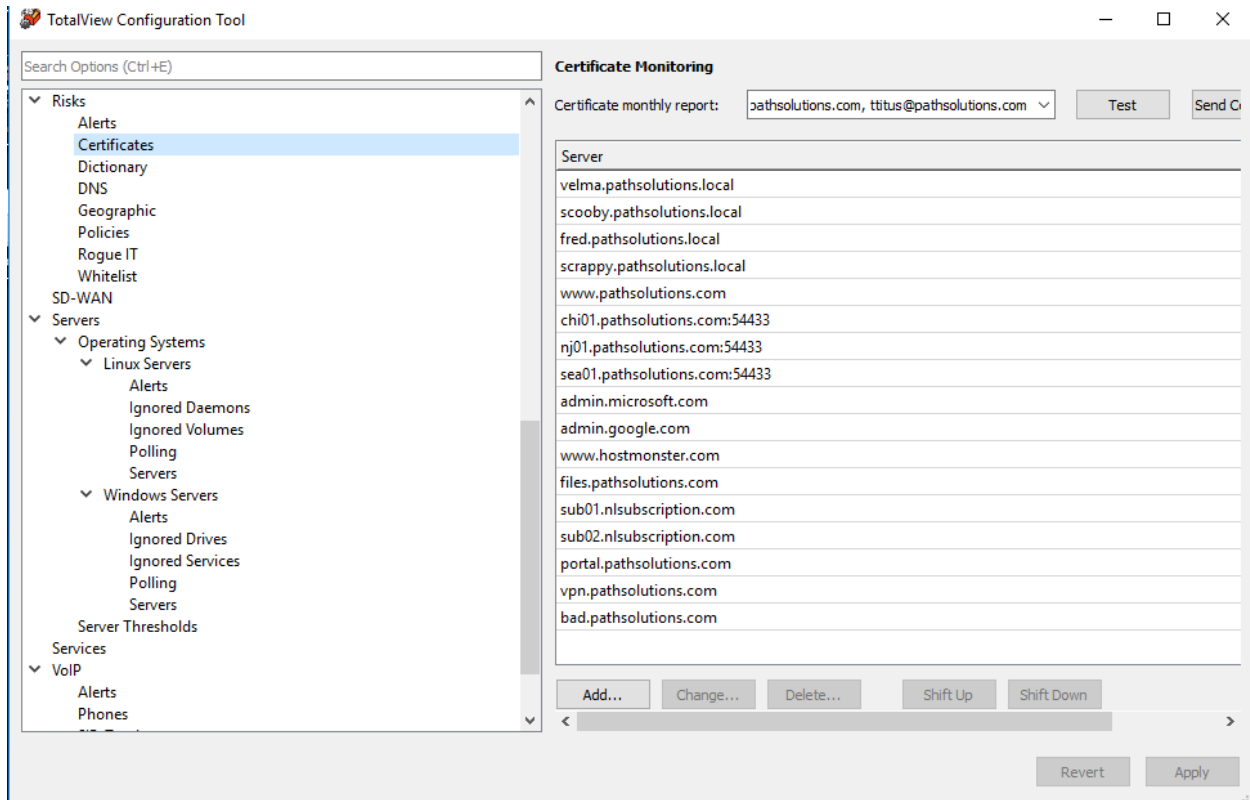
Checkmark the security alerts you want to get, and specify the email to send security alerts to in this menu:



Certificates/SSL **NEW**

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

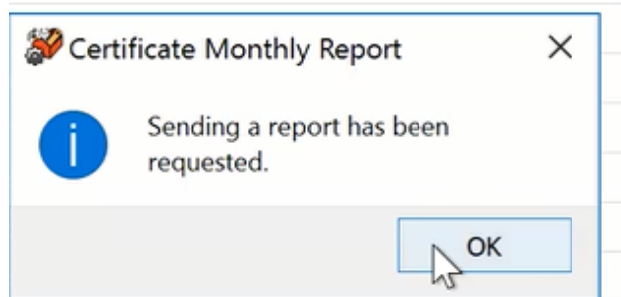
At the top of the left-hand, enter the name of the person to get the email reports on certificate status. To make that easy, you can see commonly used email addresses in the drop-down menus.




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

If you want to check certificates now, use the “Check Certificates” button.

If you want to get an emailed report now, select the button to “send report now”. A small menu will confirm that you are going to send monthly reports. Select OK:



Here is an example of the emailed report:

lab-fred-reports@pathsolutions.comIT Operations; Tim TitusTue 2:59 PM

TotalView Expired Certificates Report

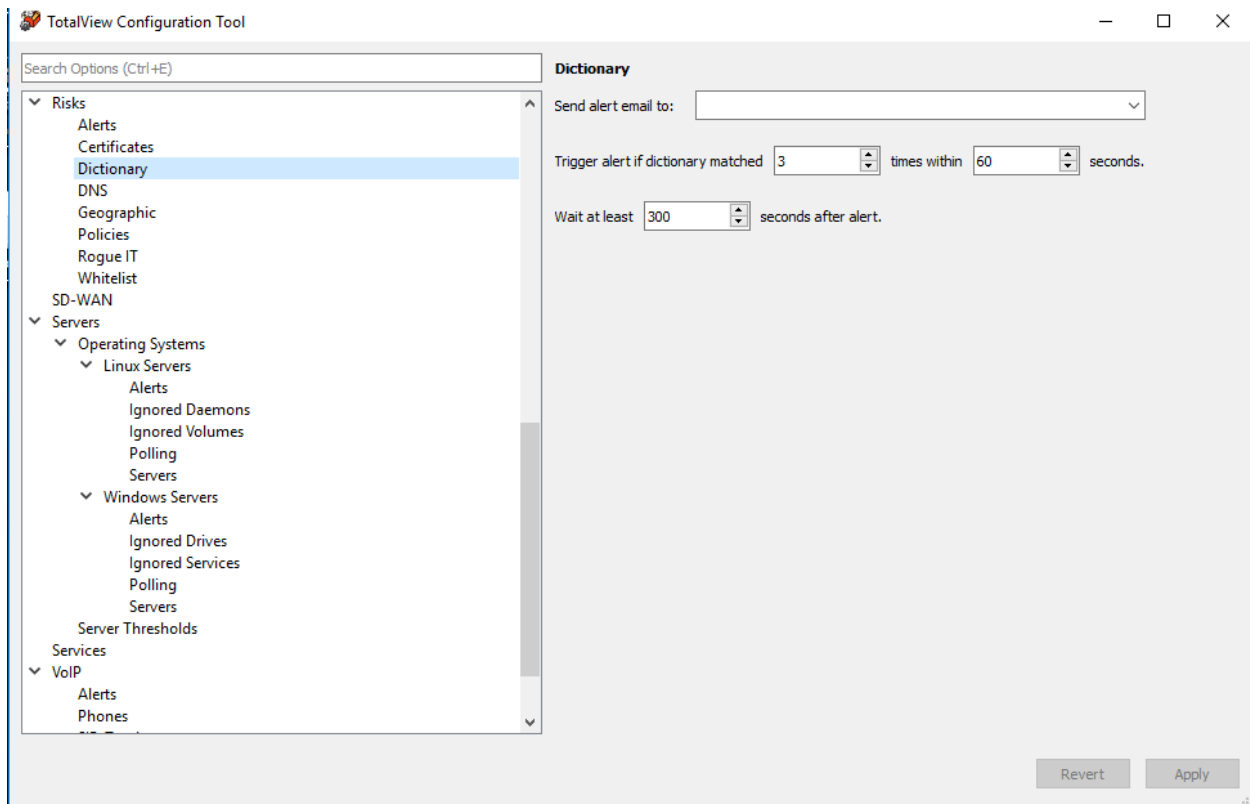
TotalViewExpired Certificates as of 1/31/2023 2:59:19 PM

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.

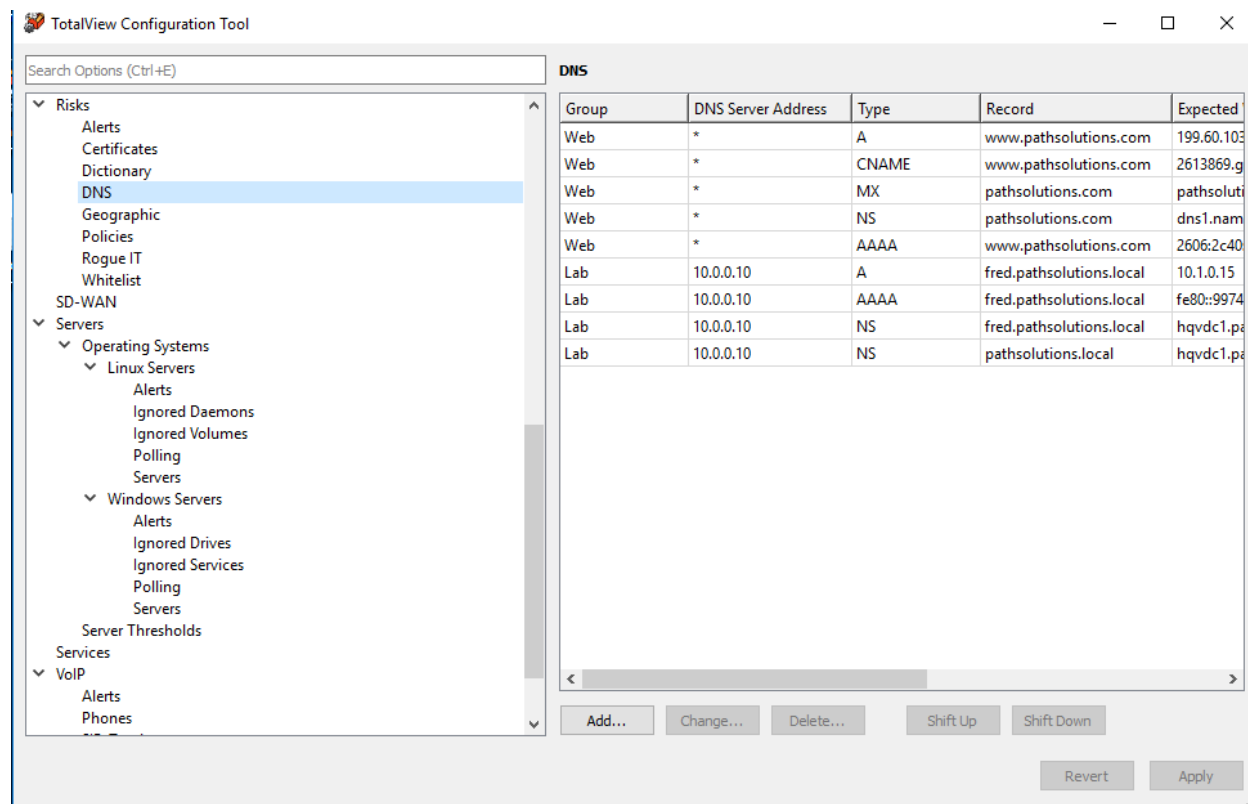
Dictionary

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



DNS Record Monitoring **NEW**

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



Add, change, and delete URL's on the DNS Monitoring list by using the buttons below the list. Here is an example of the "Change" dialog box:

Change

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 Resolve

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

Note:

OK Cancel

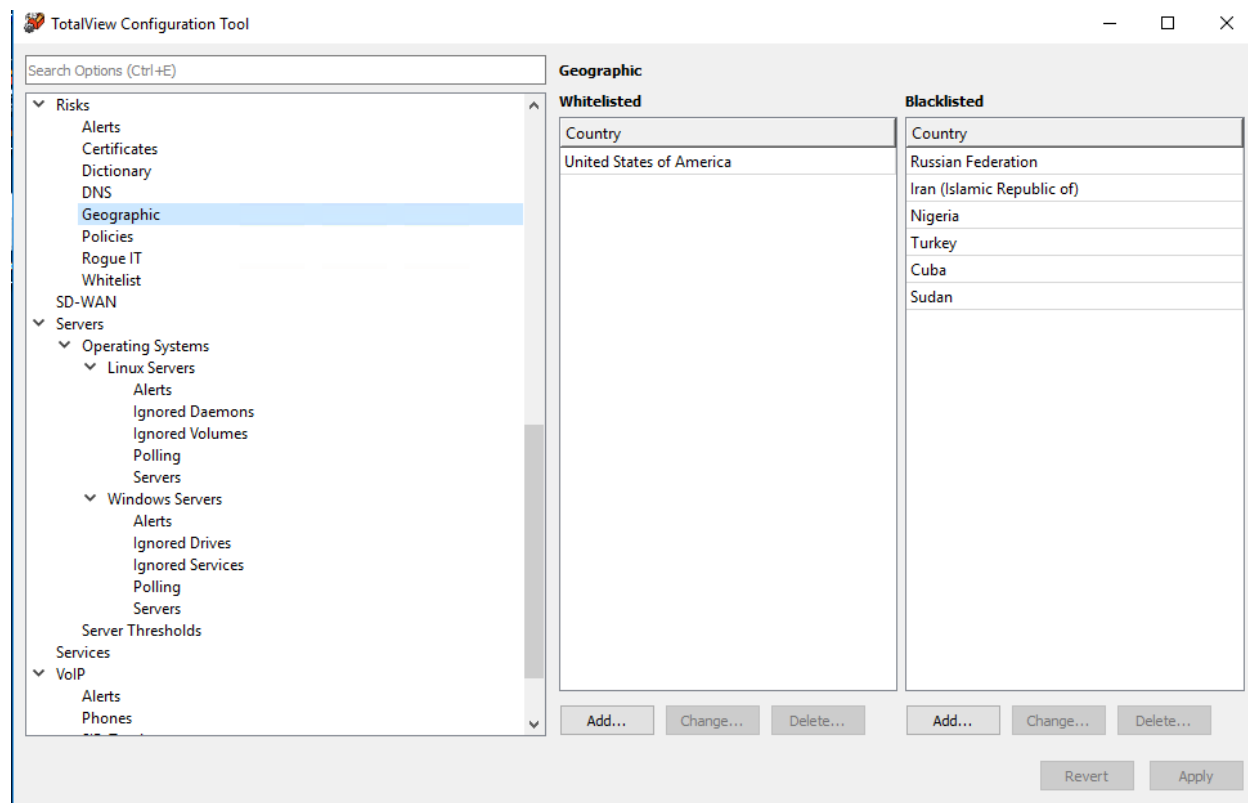
For the "Add" and "Change" dialog boxes, use the drop-down menus to select the group, DNS server address, and record type you want to monitor. Enter the hostname for the record, "Expected Value", and the emails to send the alerts to.

If you do not know the “Expected Value” for the record, select “Resolve” and it will fill in this field for you. You can also select “Resolve” to check and correct this field.

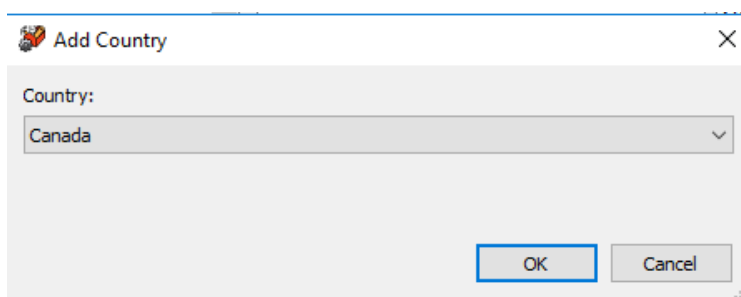
Geographic

In the Risks > Geographic section, configure the Whitelist and blacklists for monitoring communications by geographic location. These lists will allow you to filter the communications in the web interface and sort between Whitelist (safer) communications and Blacklist (riskier) communications.

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

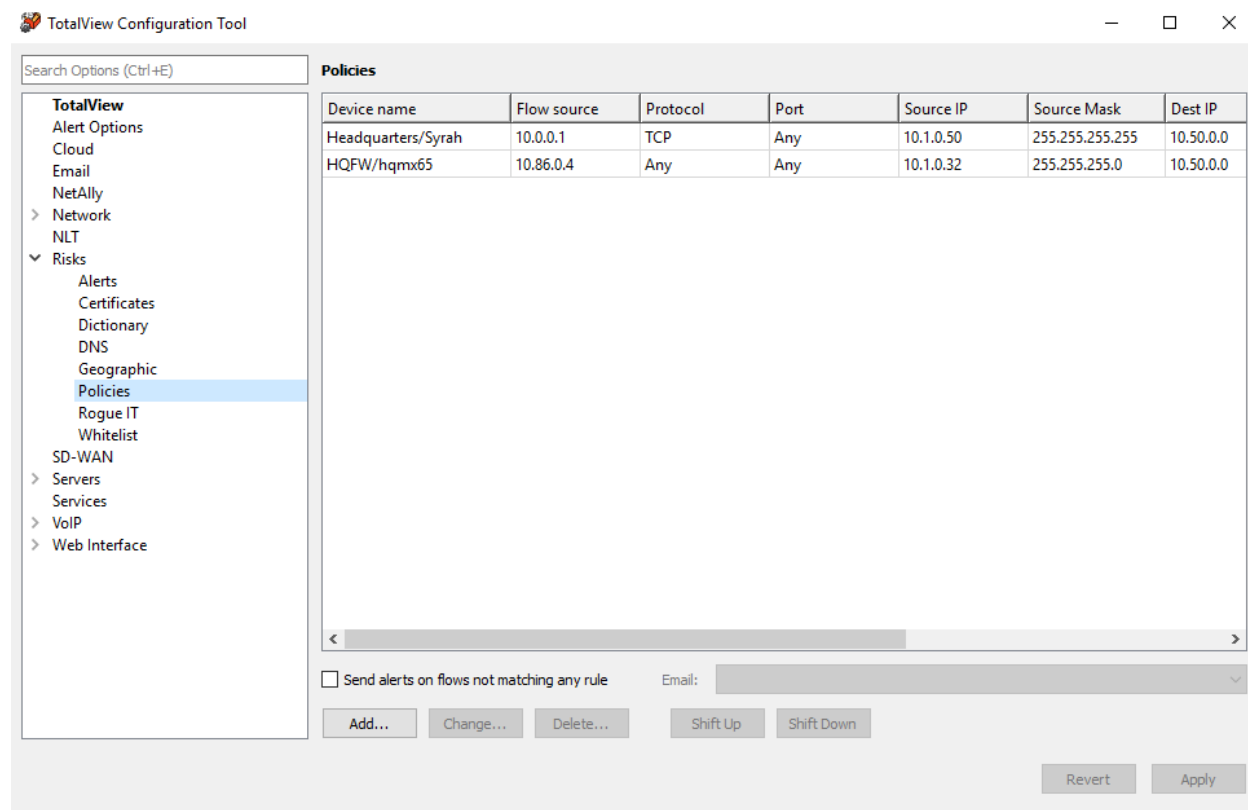


Use the “Add”, “Change” and “Delete” buttons to edit the Whitelist and Blacklist of countries. Here is the “Add Country” dialog box:



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.



To create a security policy, click “Add”. You will be presented with the Add Policy dialog:

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

OK Cancel

A single policy match can be defined on this dialog.

The Source Device 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 are used to define a subnet or host of the source of the flow.

The Destination IP and Destination Mask are used to 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.

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

If this communications occurs, you can 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.

You should define all of the policy matches that are appropriate for your network, and change the policy match order to generate alerts for policies that you deem unacceptable.

Here is an example of a policy list:

<i>Flow Source</i>	<i>Protocol</i>	<i>Port</i>	<i>Source IP</i>	<i>Source Mask</i>	<i>Destination IP</i>	<i>Destination Mask</i>	<i>Email</i>
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	

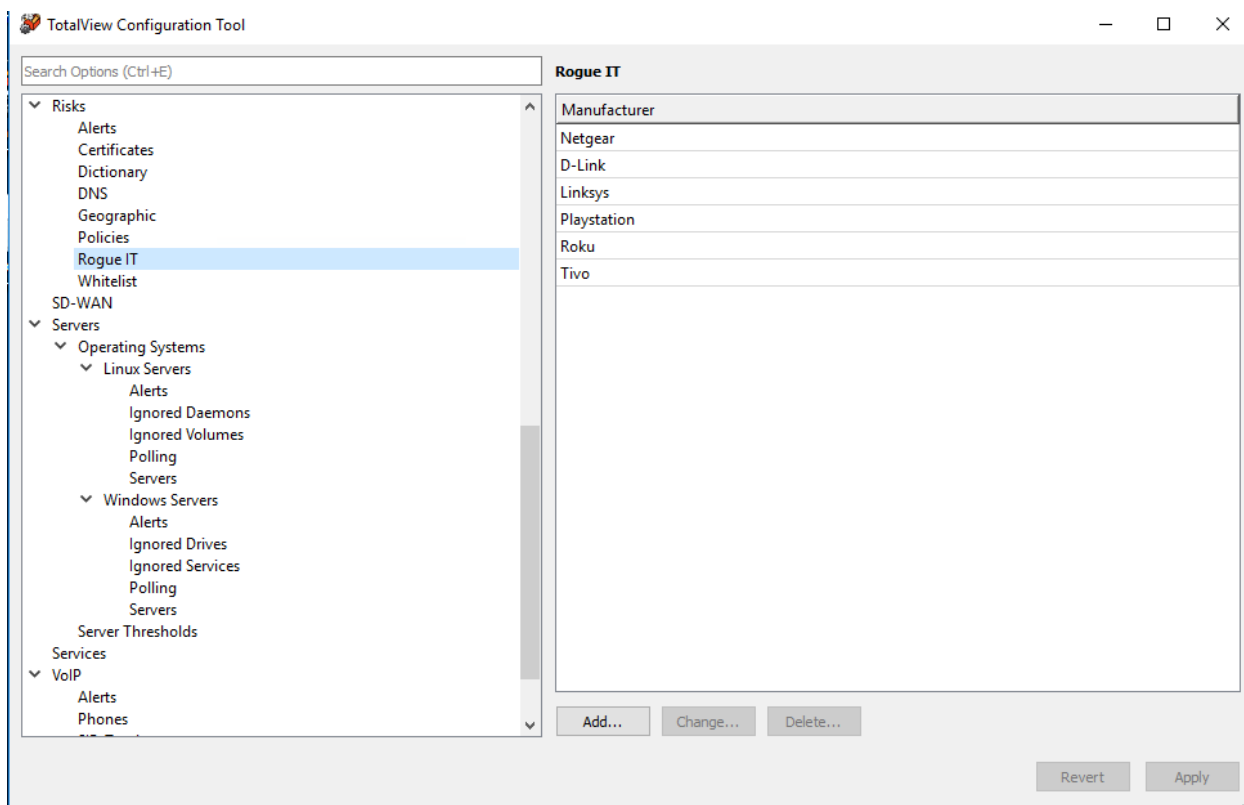
In the above example, the first policy will match any traffic from any internal source to any other internal source and stop checking after it finds match. Thus, if Flow Source for “Any” going to Destination 255.0.0.0 is Yes, the second and third policy will never be checked. If the first policy does 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.

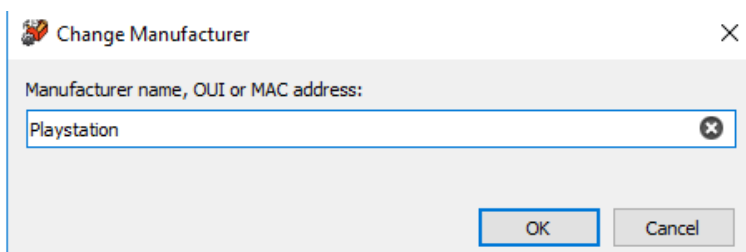
Once you setup a security policy, you will receive e-mail alerts when communications occurs outside of the policy.

Rogue IT

In the Risks > Rogue IT section, to 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 of your network equipment is manufactured by Cisco, if a D-Link device shows up on the network, it is rogue and unapproved.

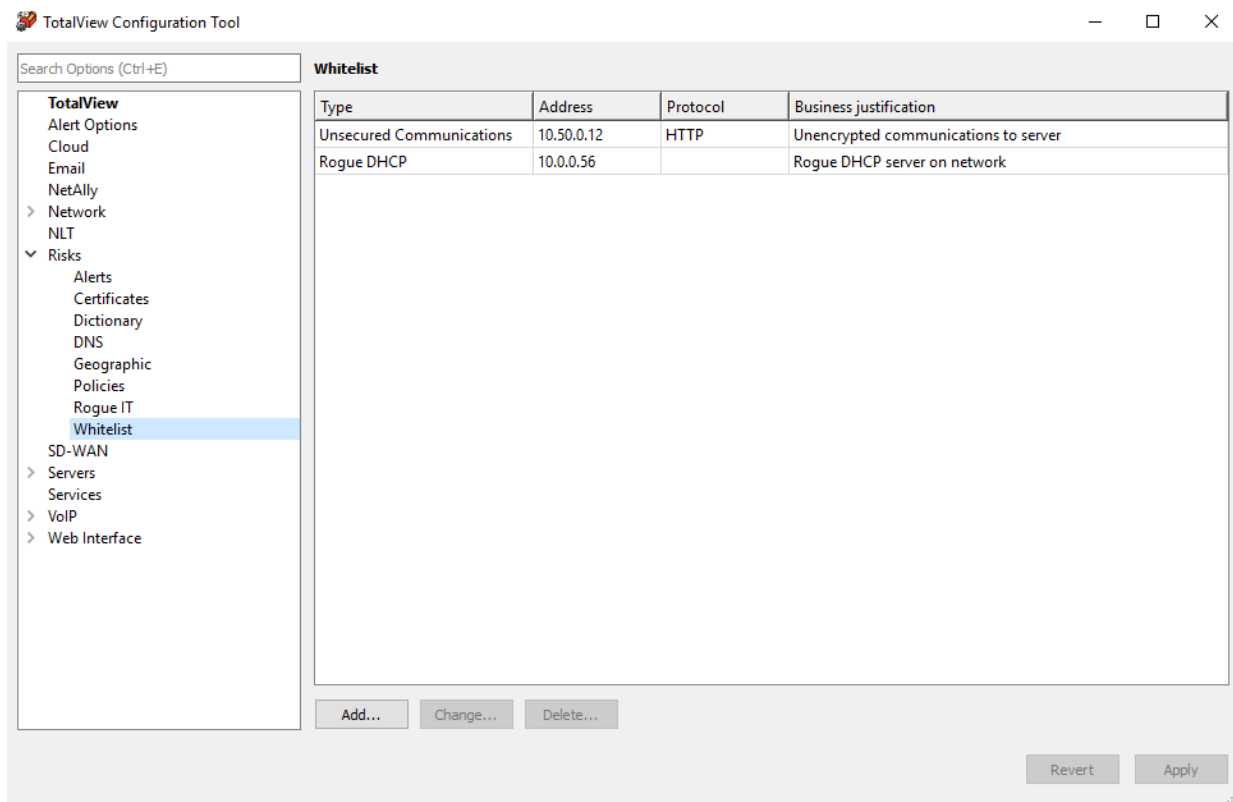


Use the “Add” or “Change” buttons to add or change manufacturer names, OUI and Mac Addresses on the Rogue IT list:

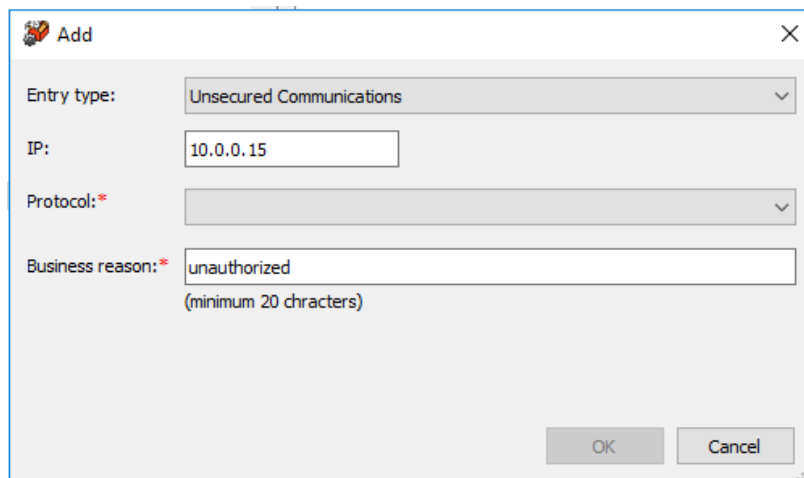


Whitelist

You can Whitelist devices that you do not need to monitor as a security risk:

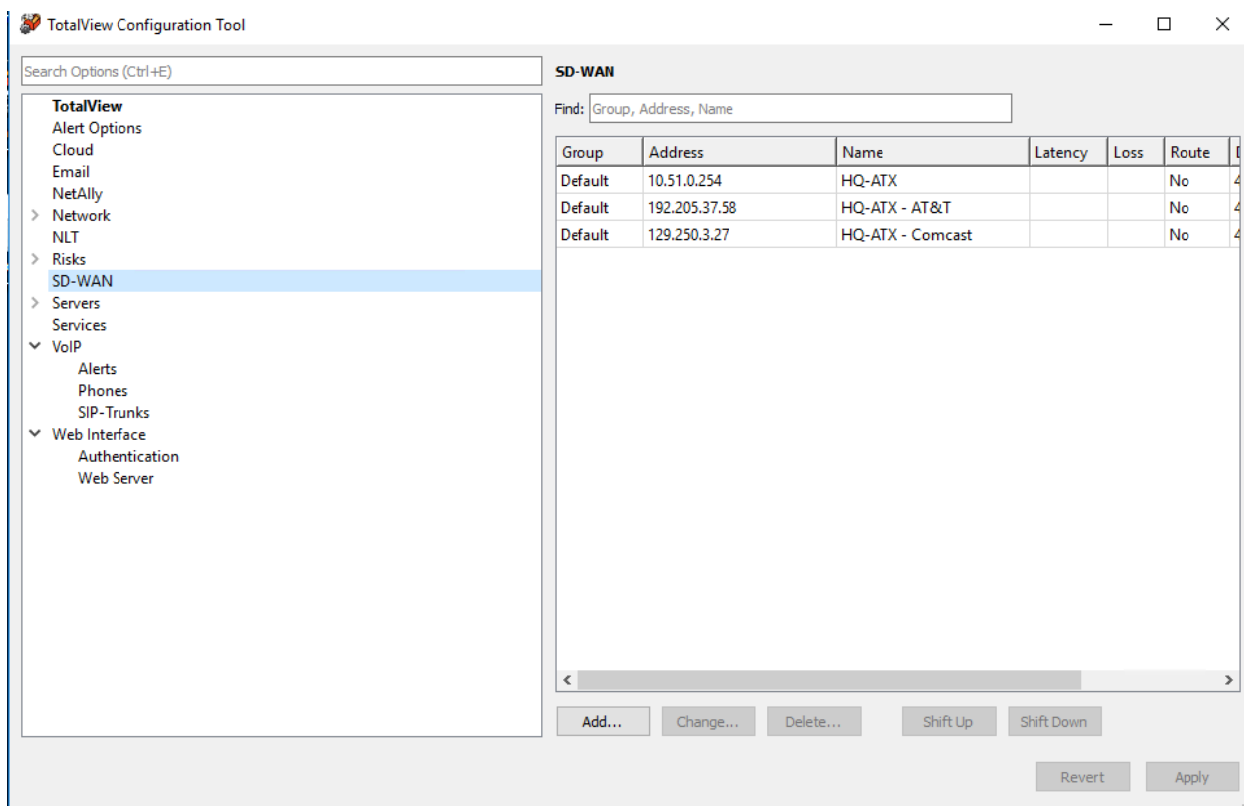


To add or change items to the Whitelist, use the “Add” or “Change” buttons. The popup menu shows a list of entry types to Whitelist in the drop-down menu such as: Unsecured Communications, Unauthorized Static IP, New Devices and Rogues. It will ask you to specify the IP address or Mac Address, the protocol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

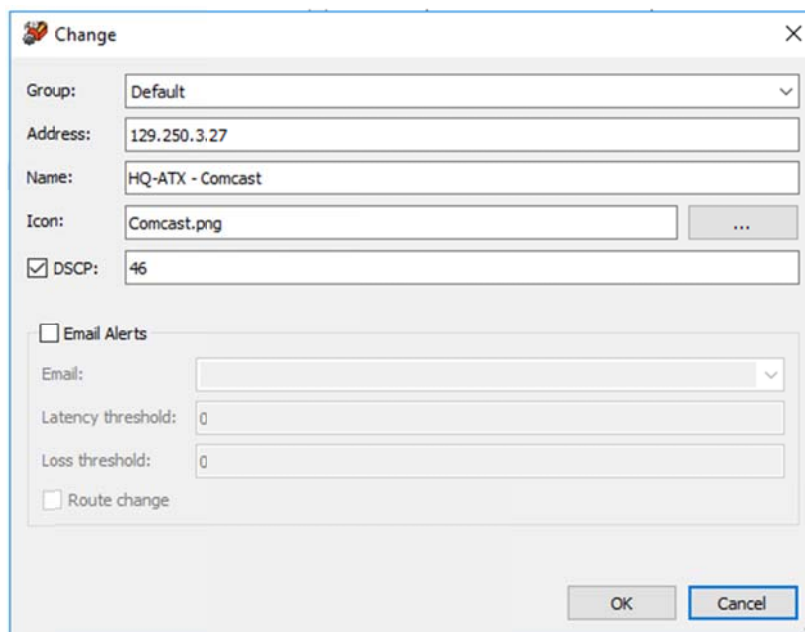


SD-WAN

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

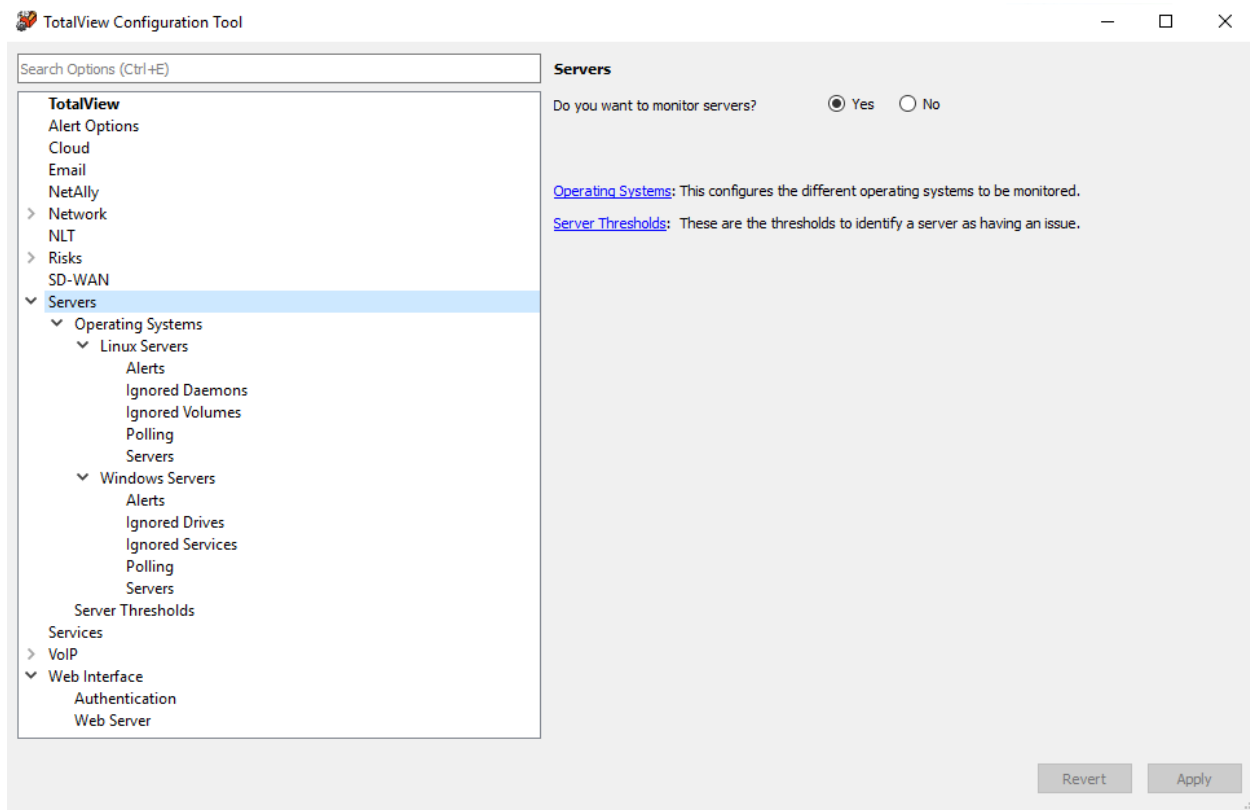


You can also setup email alerts for latency and loss thresholds on the submenu. You can also assign a sort order, by using the “Shift Up” or “Shift Down” keys.



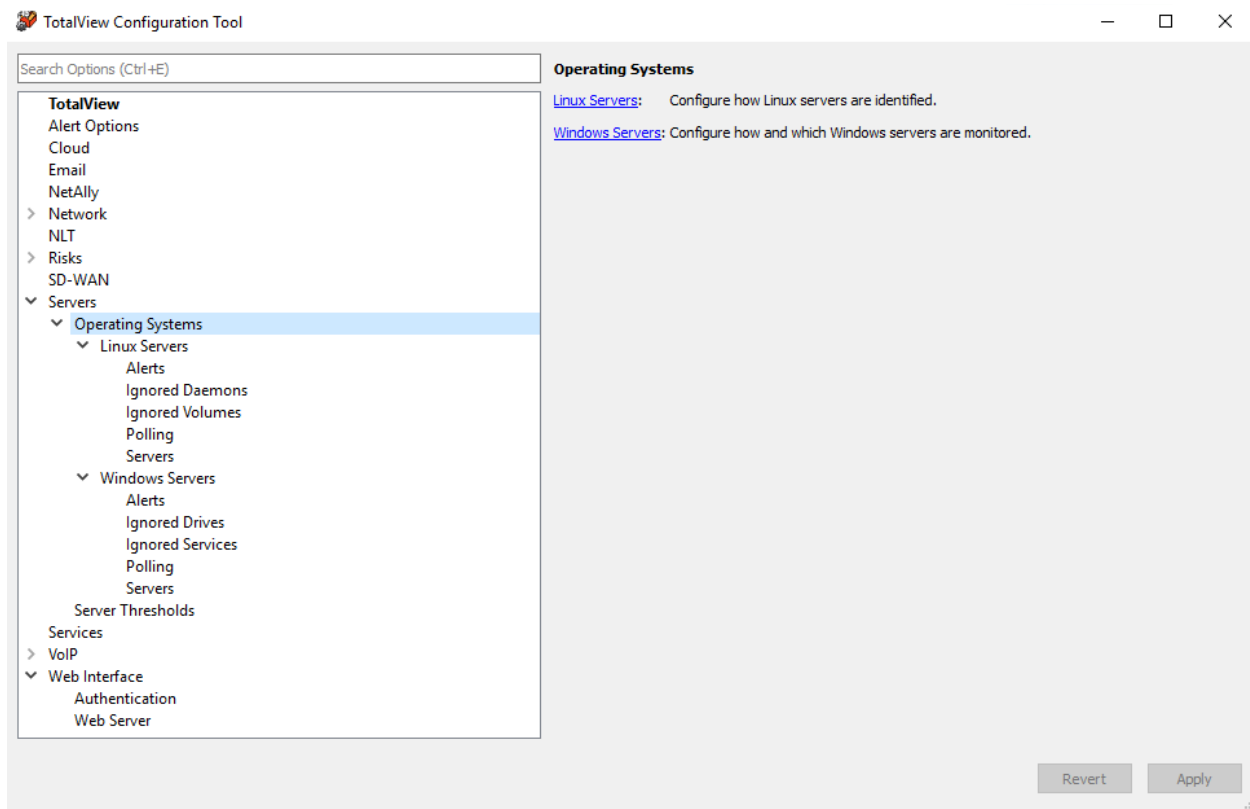
Servers and Operating Systems

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



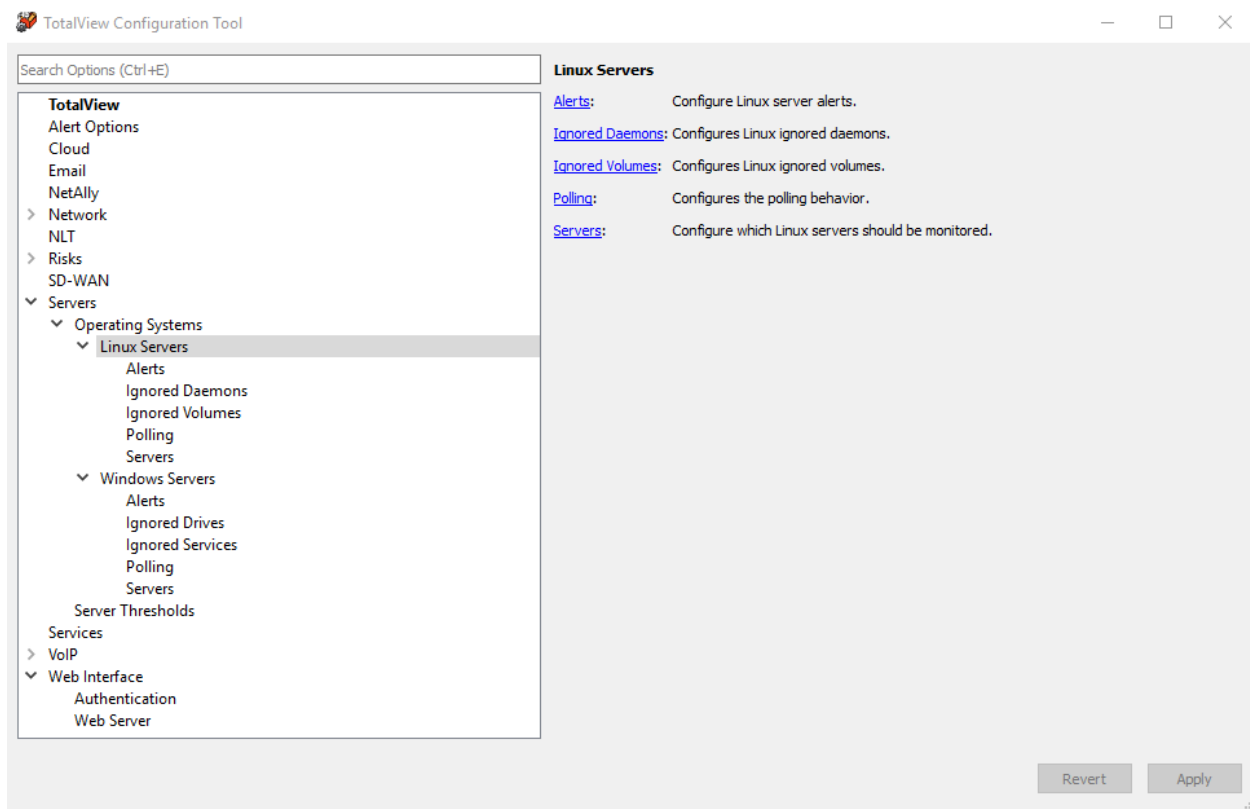
Do you want to monitor servers? Select “Yes” or “No” here.

The operating systems section links to Linux and Windows:



Linux Servers Monitoring **NEW**

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



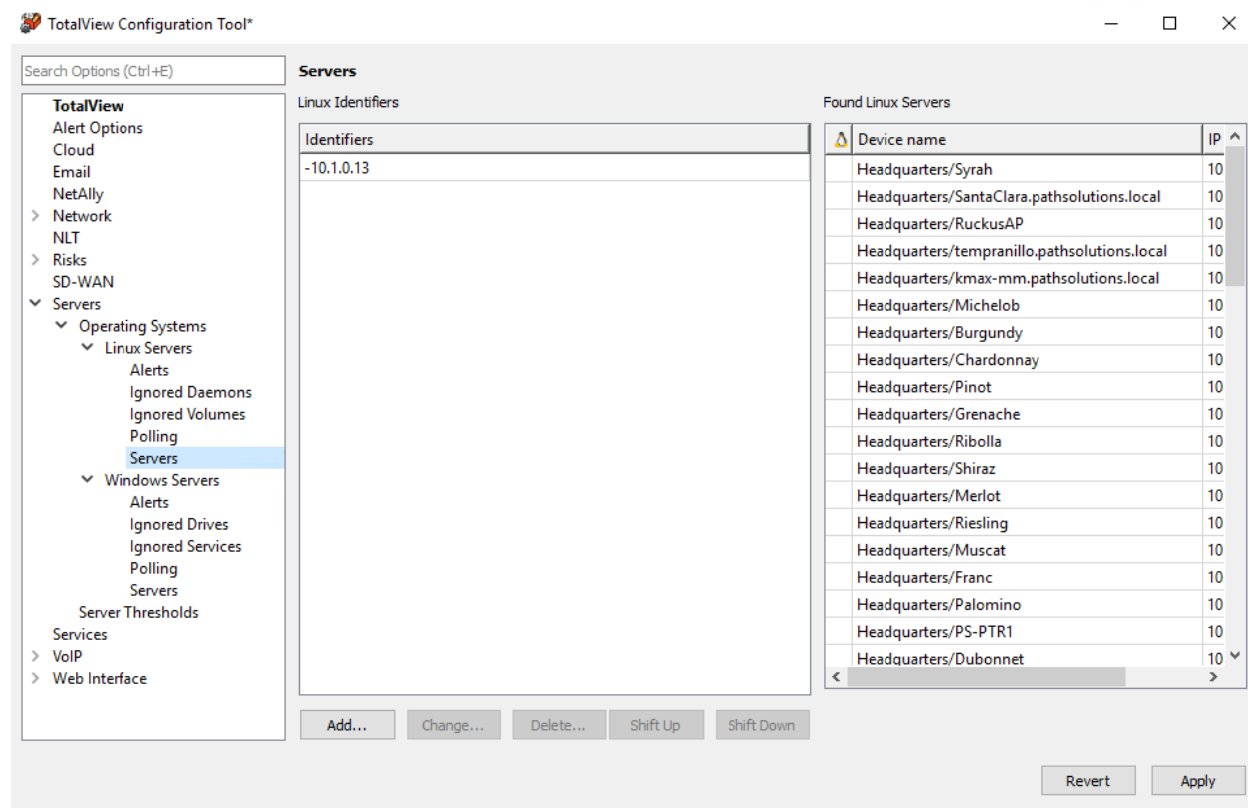
How to Identify Linux Servers

TotalView will recognize anything with a system description for Linux, as well as any IP's 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:

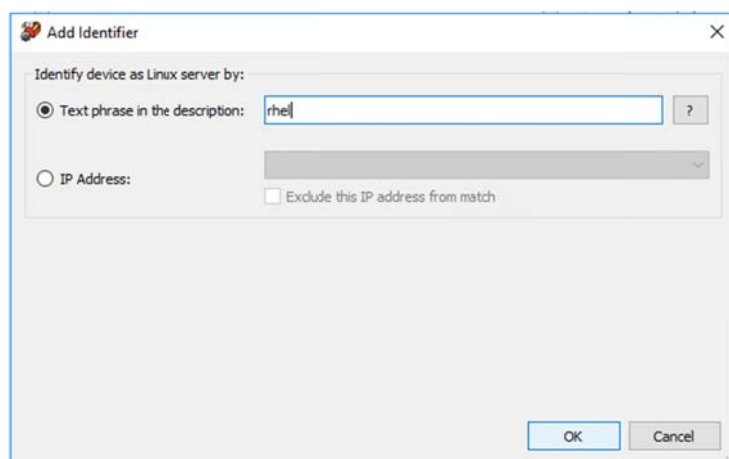
Note: You can also customize OID monitoring reports by editing the cfg file. See Appendix F. Custom OID Monitoring.

Devices Configuration).

Then navigate to this section, Servers > Operating Systems > Linux Servers > Servers, to designate the Linux Servers (identifiers). You will be building a list of Linux identifiers.

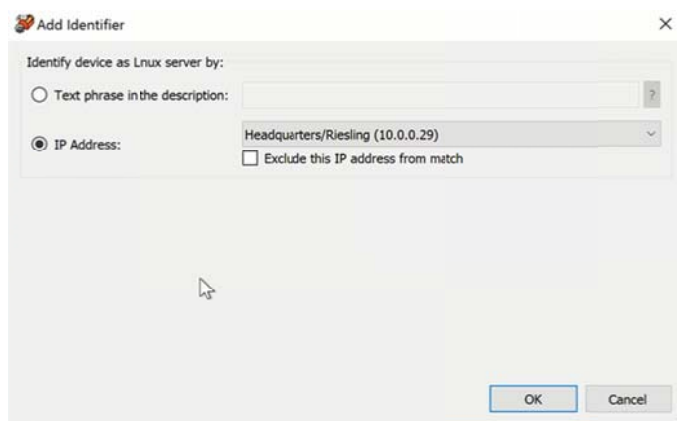


Under the middle column, click "Add". The "Add Identifier" window will appear. In the field for "text phrase in the description", add the phrase of *rhel*, which stands for *Red Hat Enterprise License* (as a common identifier for a Linux server):



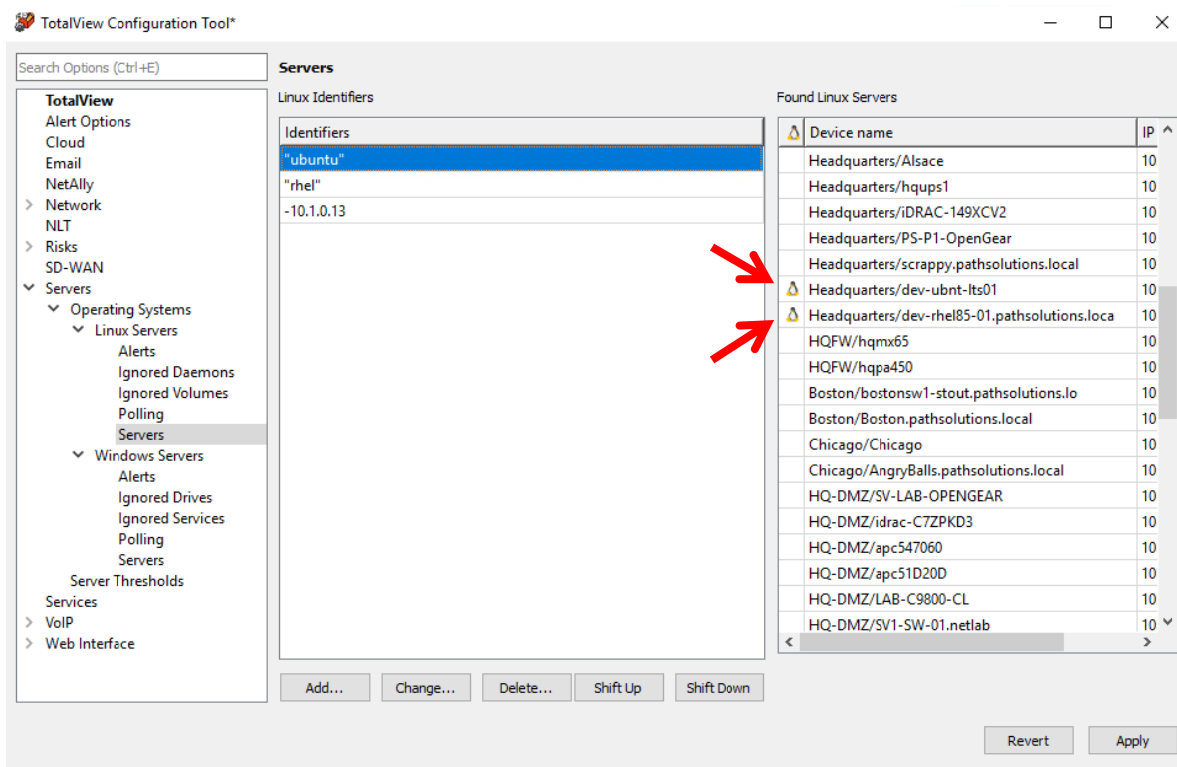
Repeat this step and add the phrase of *Ubuntu* (another common identifier for a Linux server).

You can also enter specific Linux devices here, by selecting the button next to "IP address" and selecting from the devices in the drop-down menu. Then select "ok".



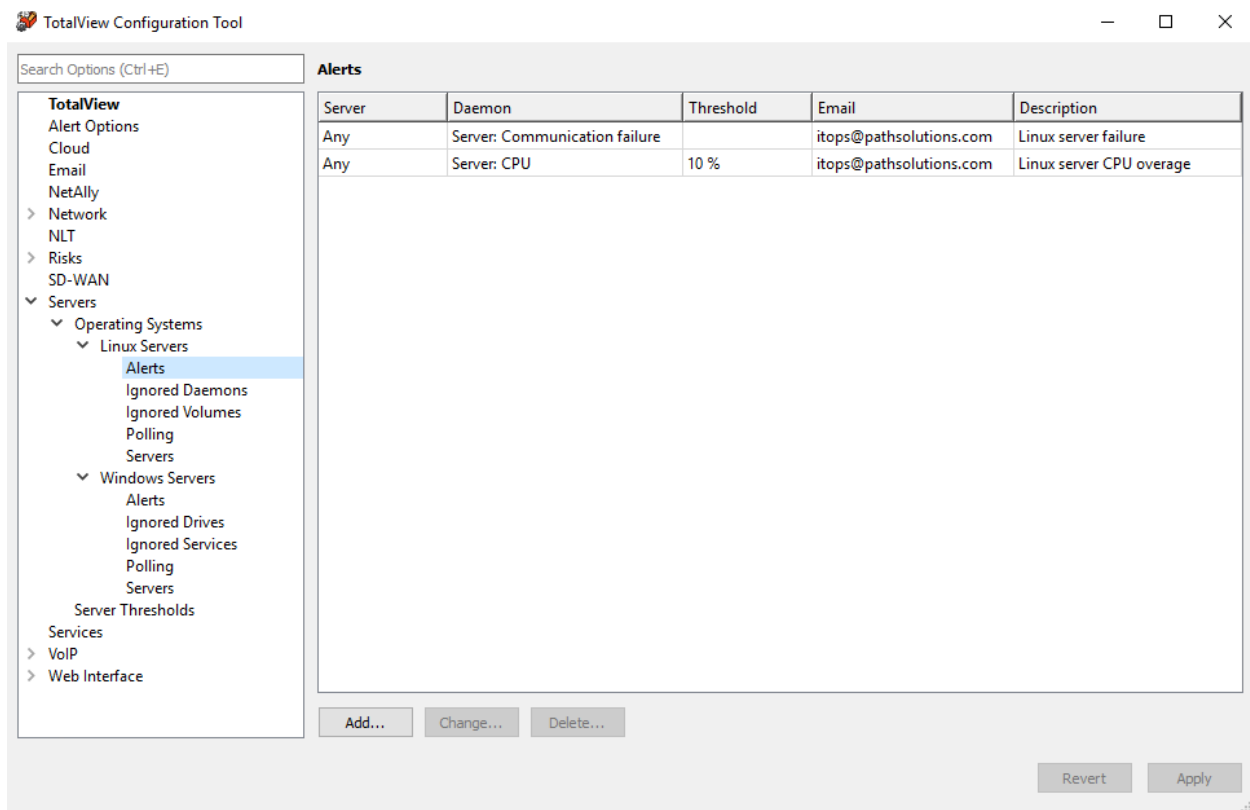
You can also exclude devices here, by adding their IP addresses. Find the IP address, then select the “exclude” button. Then select “ok”.

Now the Linux servers are identified in the list at the far right, with a small penguin. You can edit the Linux identifiers, as needed using the “Add”, “Change” and “Delete” buttons:

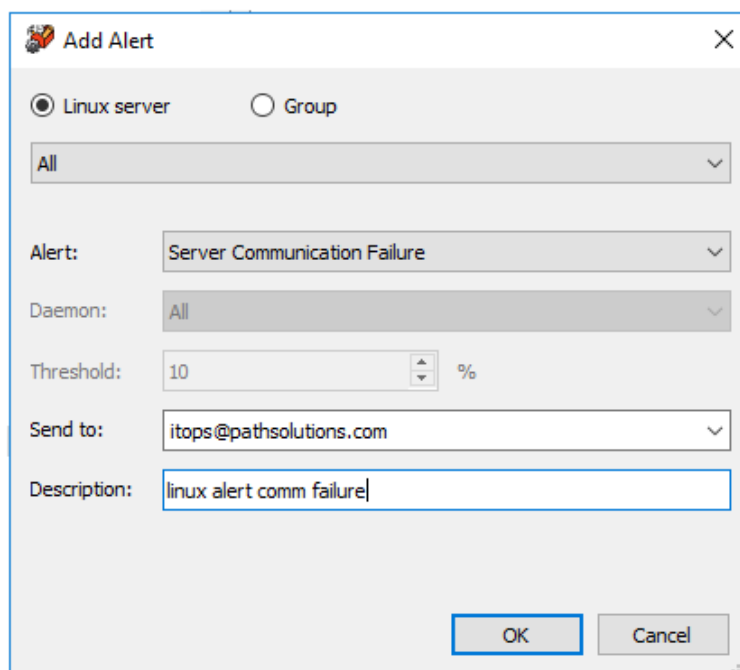


Linux - Alerts

Go to the Linux Alerts section to set Linux alerts, the thresholds that trigger alerts, and the emails to send alerts here.

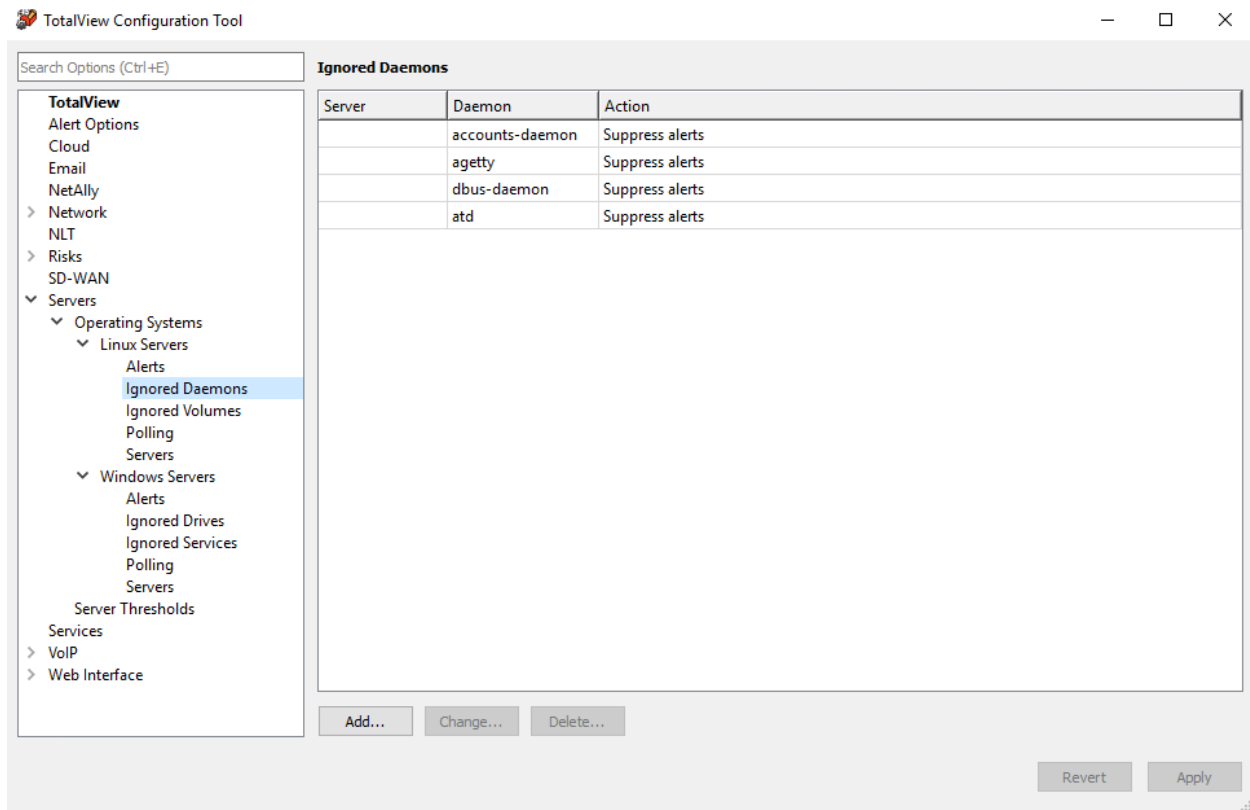


Use the "Add" and "Change" buttons to modify the alerts.

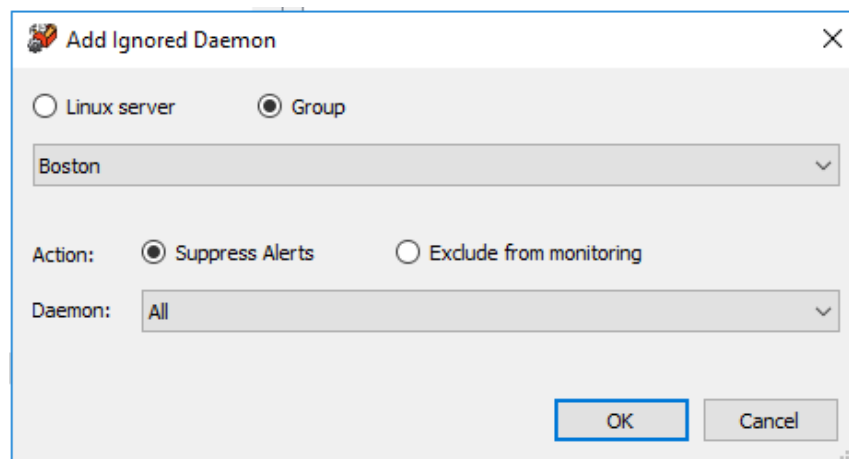


Linux - Ignored Daemons

Go to the Linux “Ignored Daemons” section to identify the Daemons to ignore.

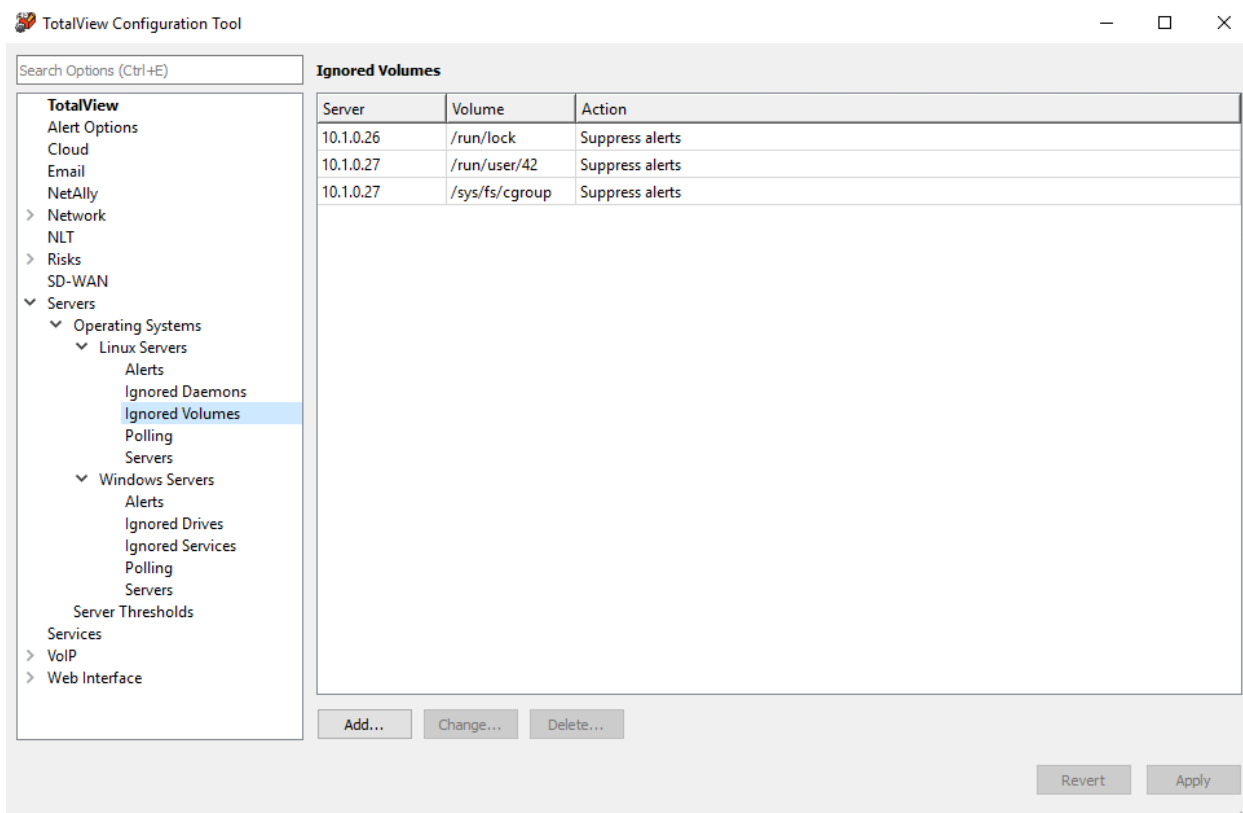


Use the “Add” and “Change” buttons to edit the list of ignored Daemons, and whether to suppress alerts or exclude each one from monitoring altogether:

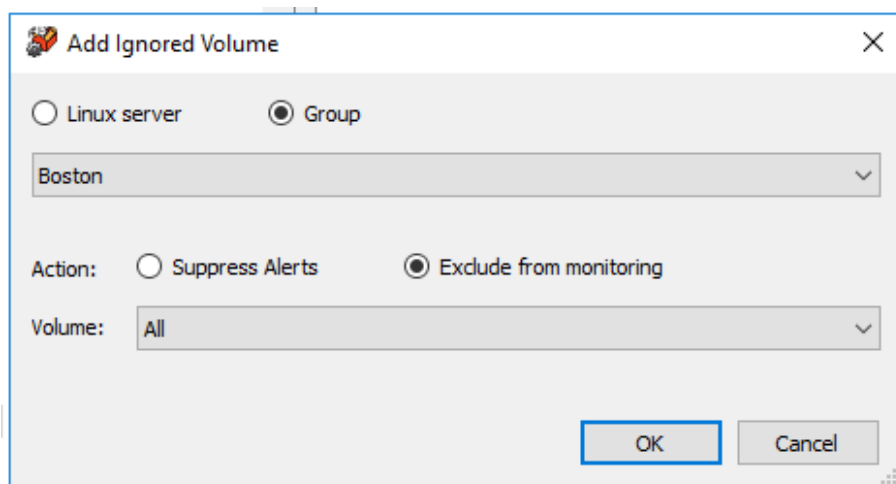


Linux - Ignored Volumes

Go to the Linux “Ignored Volumes” section to identify the Linux Volumes to ignore.

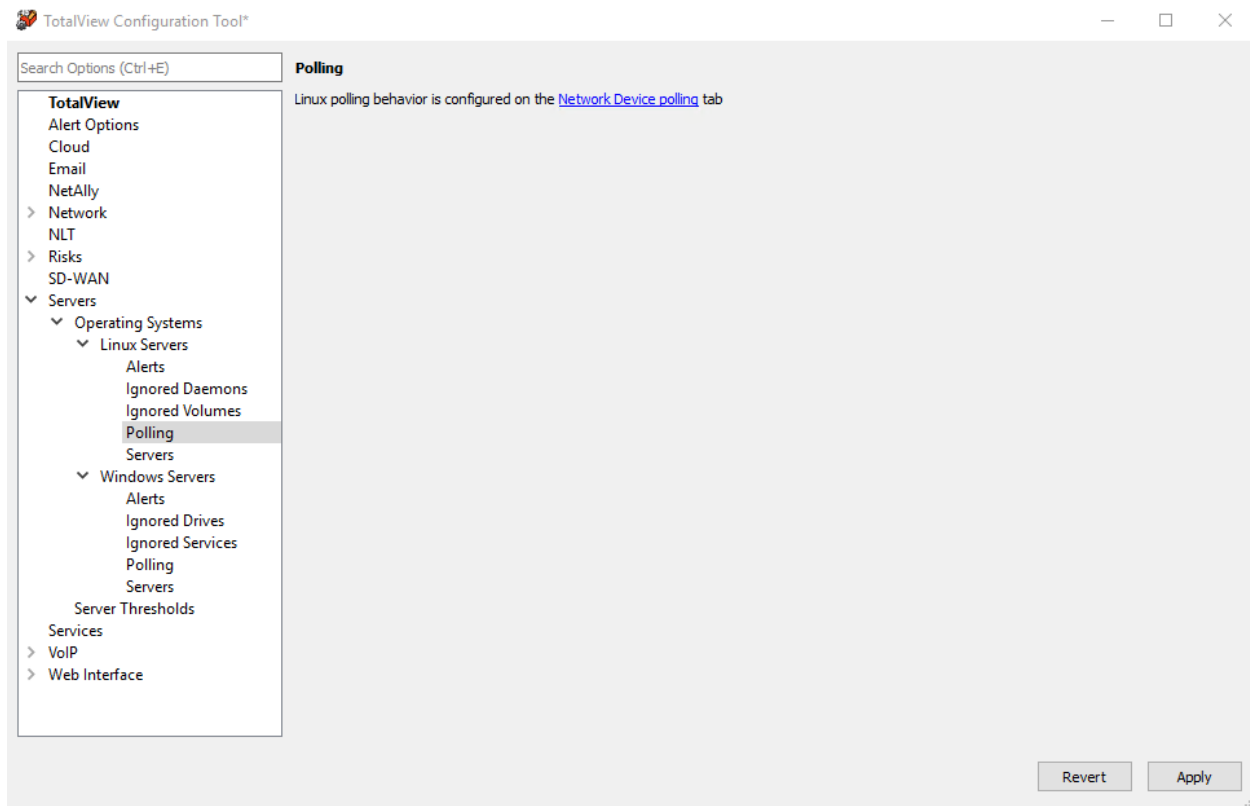


Use the “Add” and “Change” buttons to edit the list of ignored Volumes, and whether to suppress alerts or exclude each one monitoring them altogether:



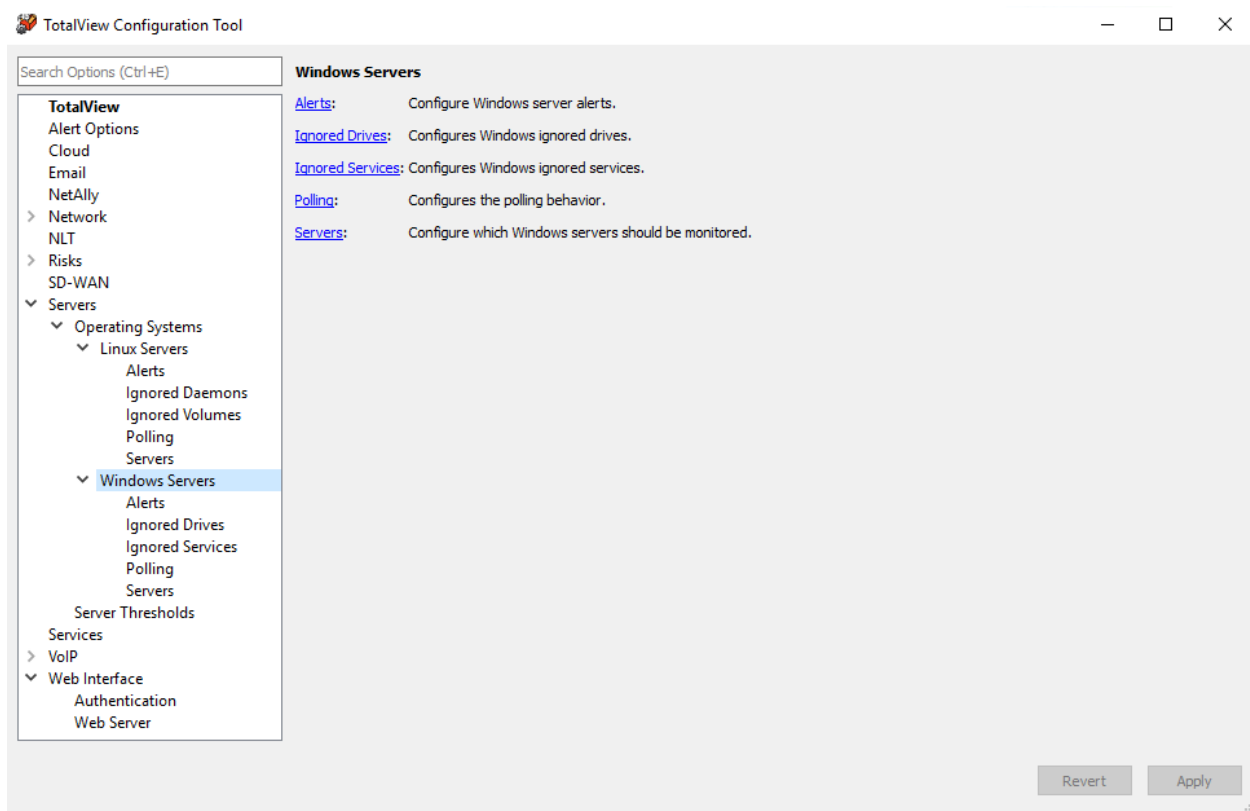
Linux - Polling

The Linux “Polling” section, tells you that polling is configured on the Network Device Polling section, and takes you there. Set up polling there.



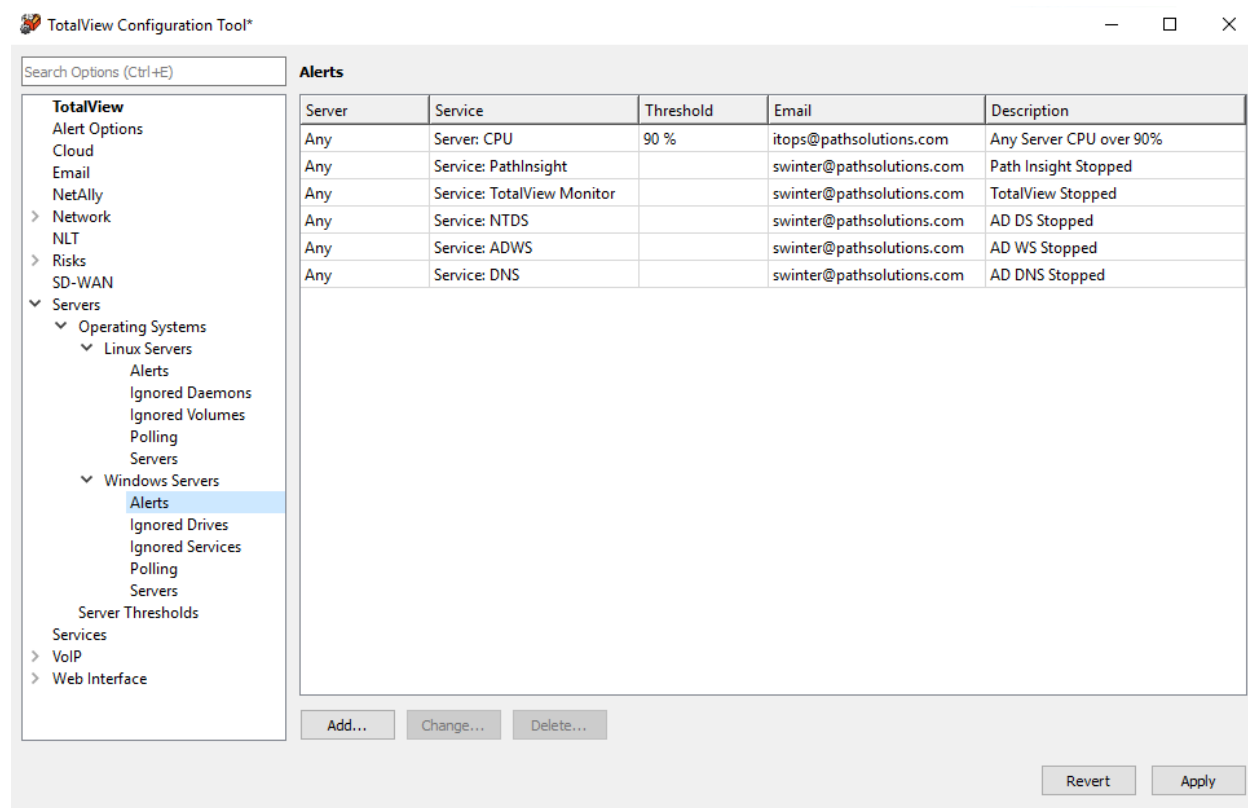
Windows Servers

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:

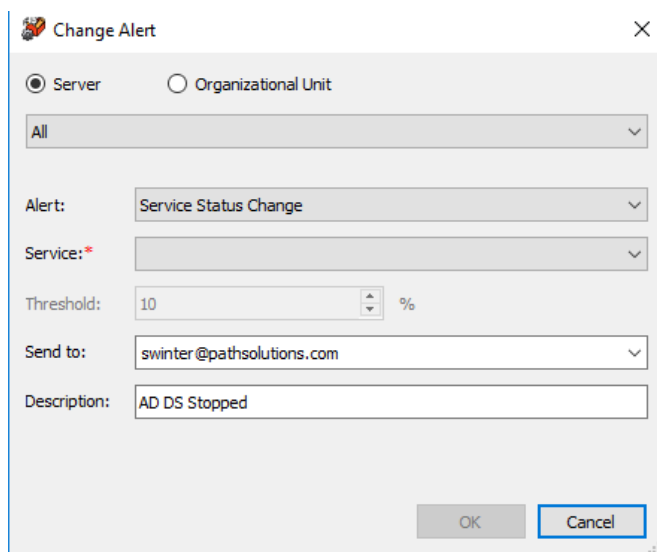


Windows - Alerts

Go to Windows Servers > Alerts section to set Windows alerts, the thresholds that trigger alerts, and the emails to send alerts to.

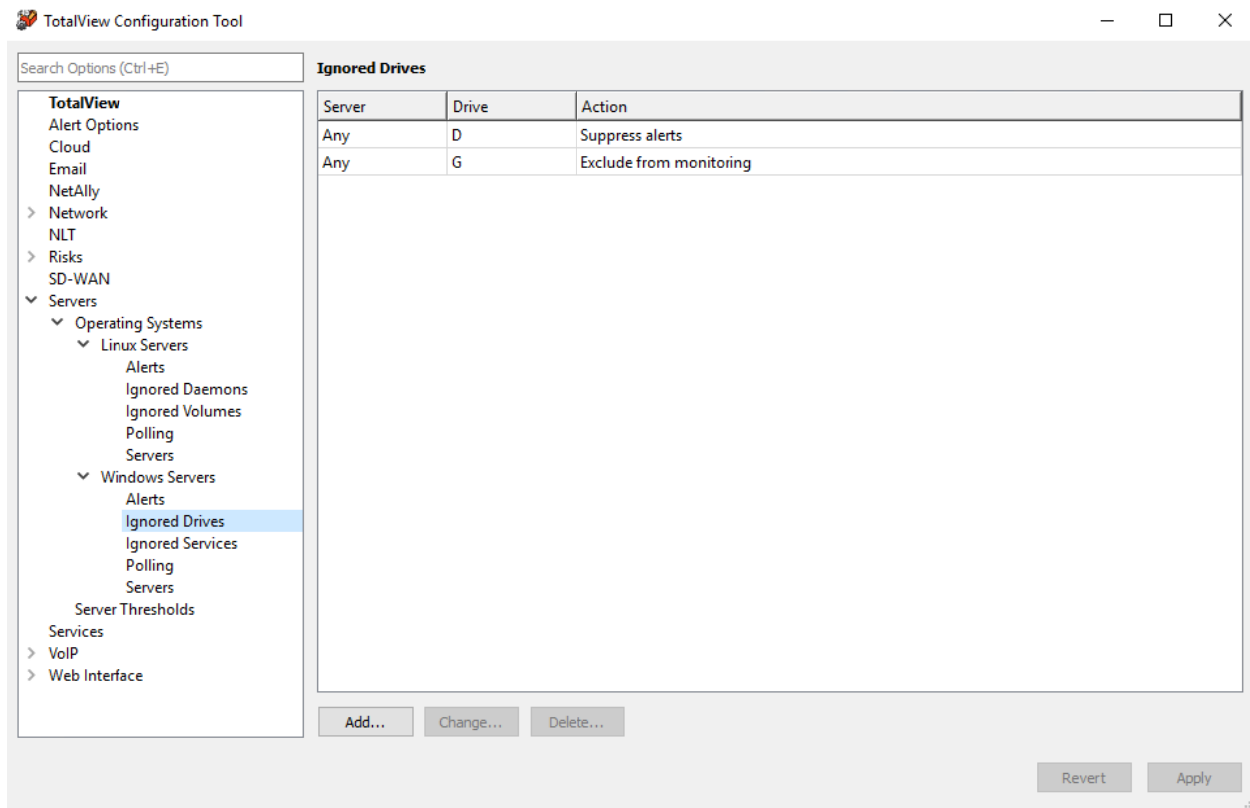


Use the "Add" and "Change" and "Delete" buttons to set up Window Server alerts. Also, designate the email where the alerts will go to:

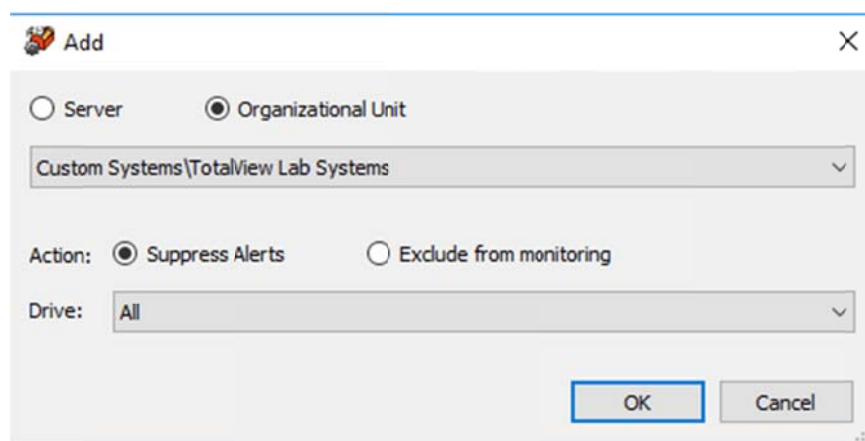


Windows - Ignored Drives

Go to the Windows “Ignored Drives” section to identify the Windows Volumes to ignore.

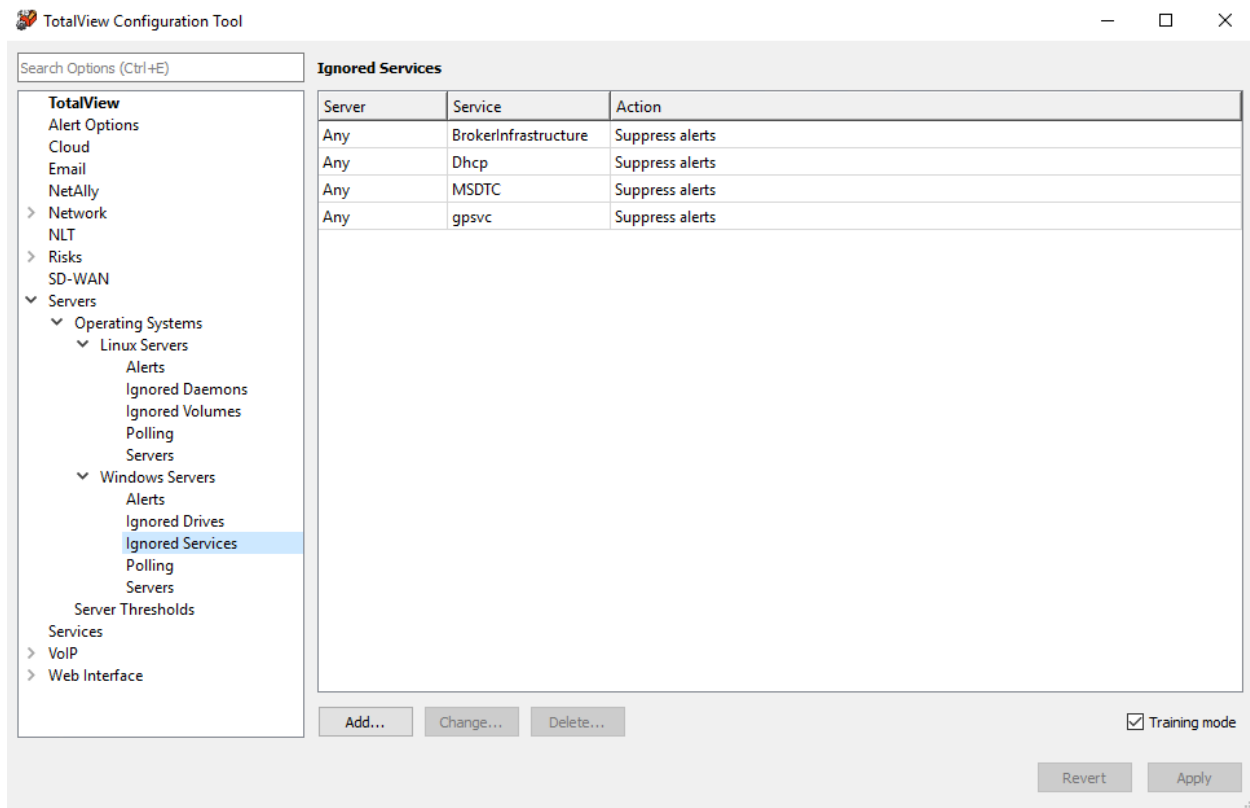


Use the “Add” and “Change” buttons to modify the Windows Drives on the Ignore List, and whether to suppress alerts or exclude each one from monitoring altogether:

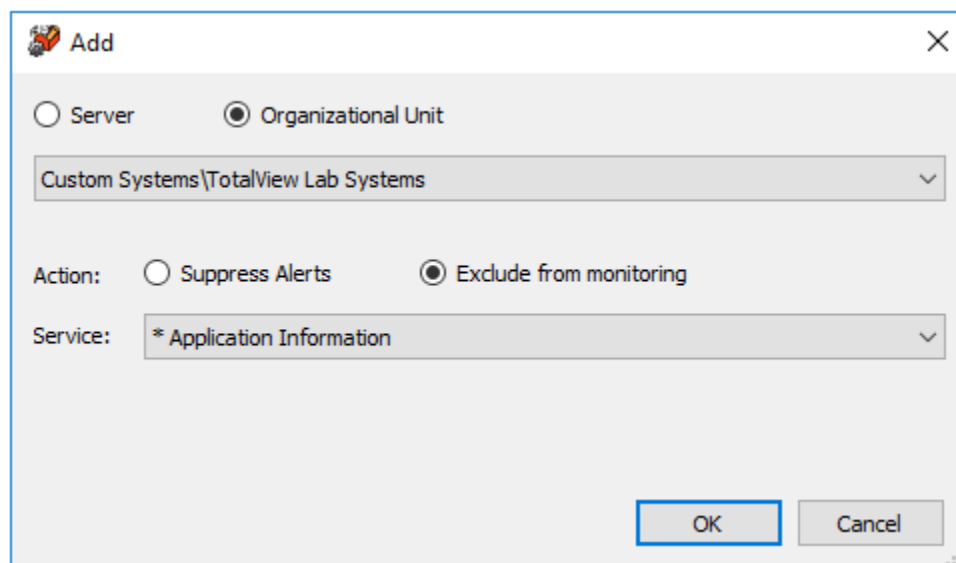


Windows - Ignored Services

Go to the Windows “Ignored Services” section to identify the Windows Services to ignore.

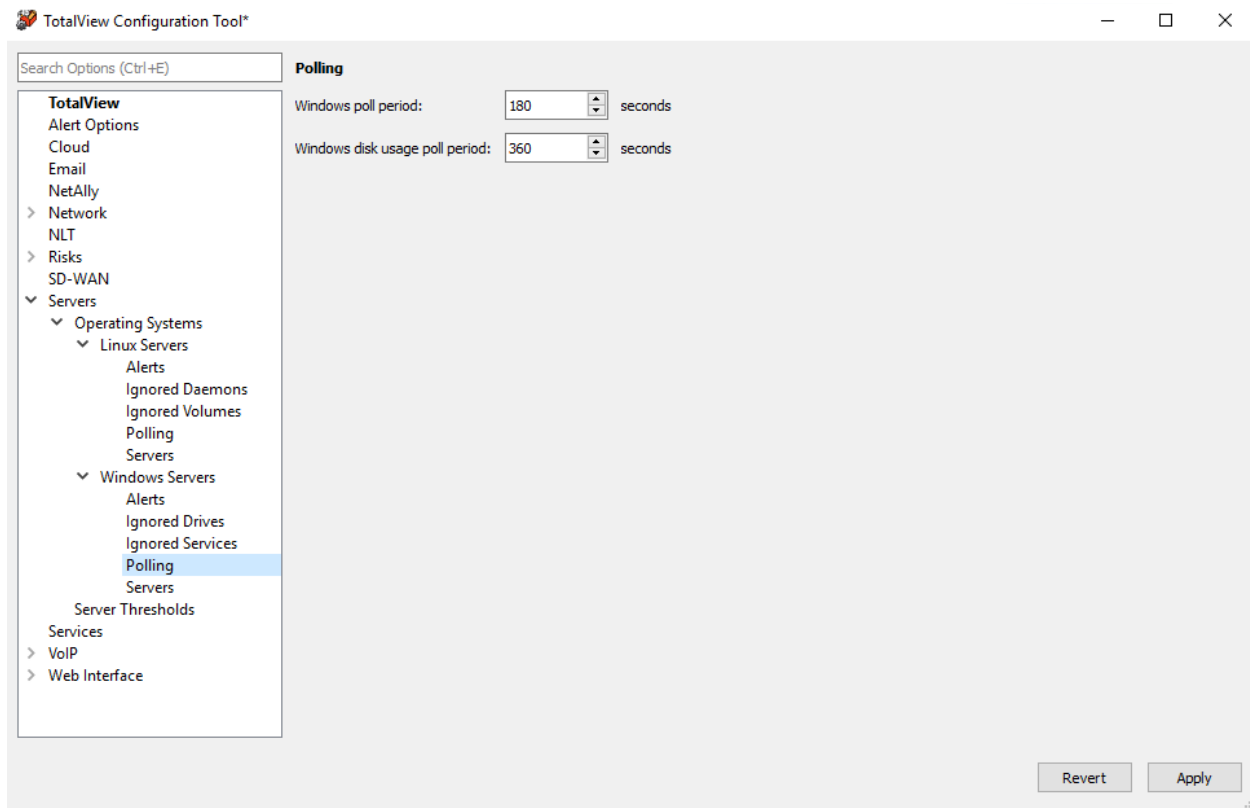


Use the “Add” and “Change” buttons to modify the Windows Services on the Ignore List, and whether to suppress alerts or exclude each one from monitoring altogether:



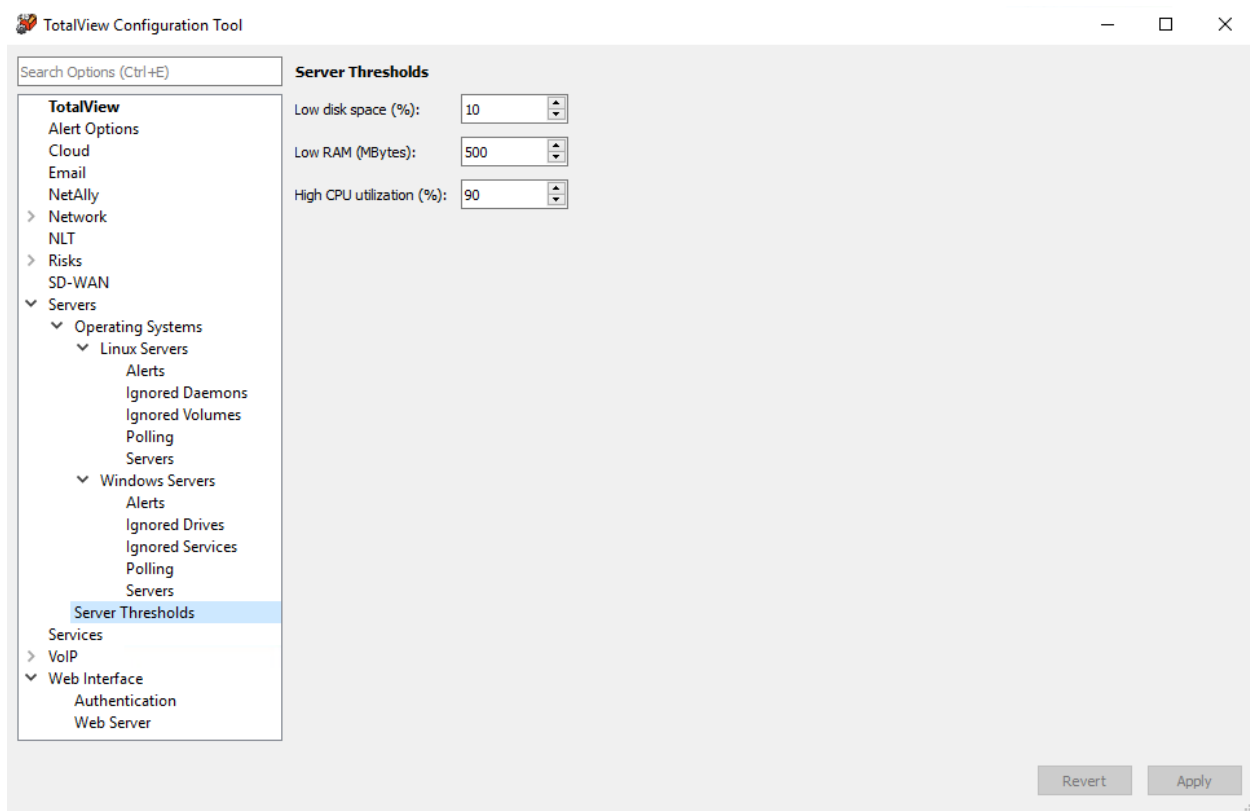
Windows - Polling

The Windows “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” save, or “Revert” to cancel your changes.



Server Thresholds

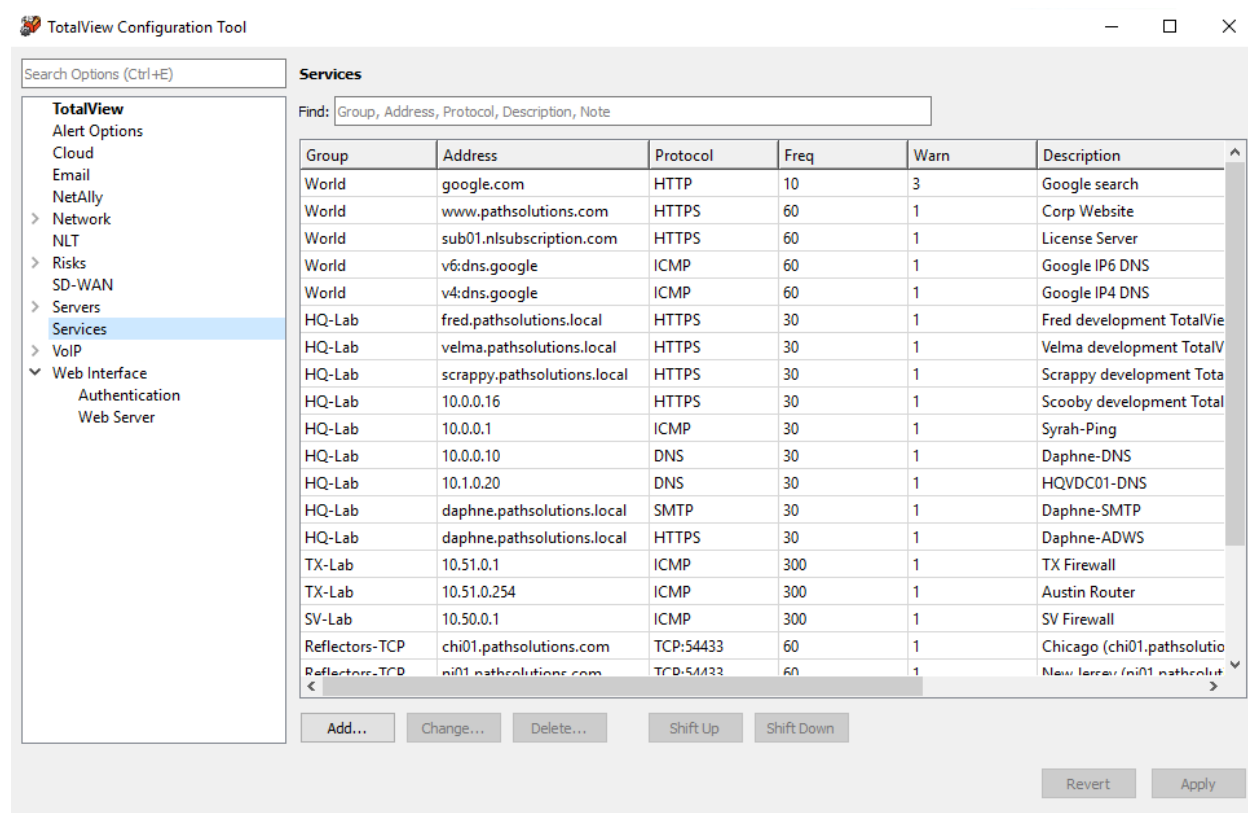
Go to the Server Thresholds section to set server thresholds for Low Disk Space, Low RAM (Mbytes), and High CPU utilization.



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 field to “find” and filter the list. You can find and filter services this way by group, address, protocol, description and by notes:



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 here:

Change Service

Group:

Address:

IP version: ☒ Auto ☐ IPv4 ☐ IPv6

Protocol:

Port:

Poll period: seconds

Alert after: failures

Description:

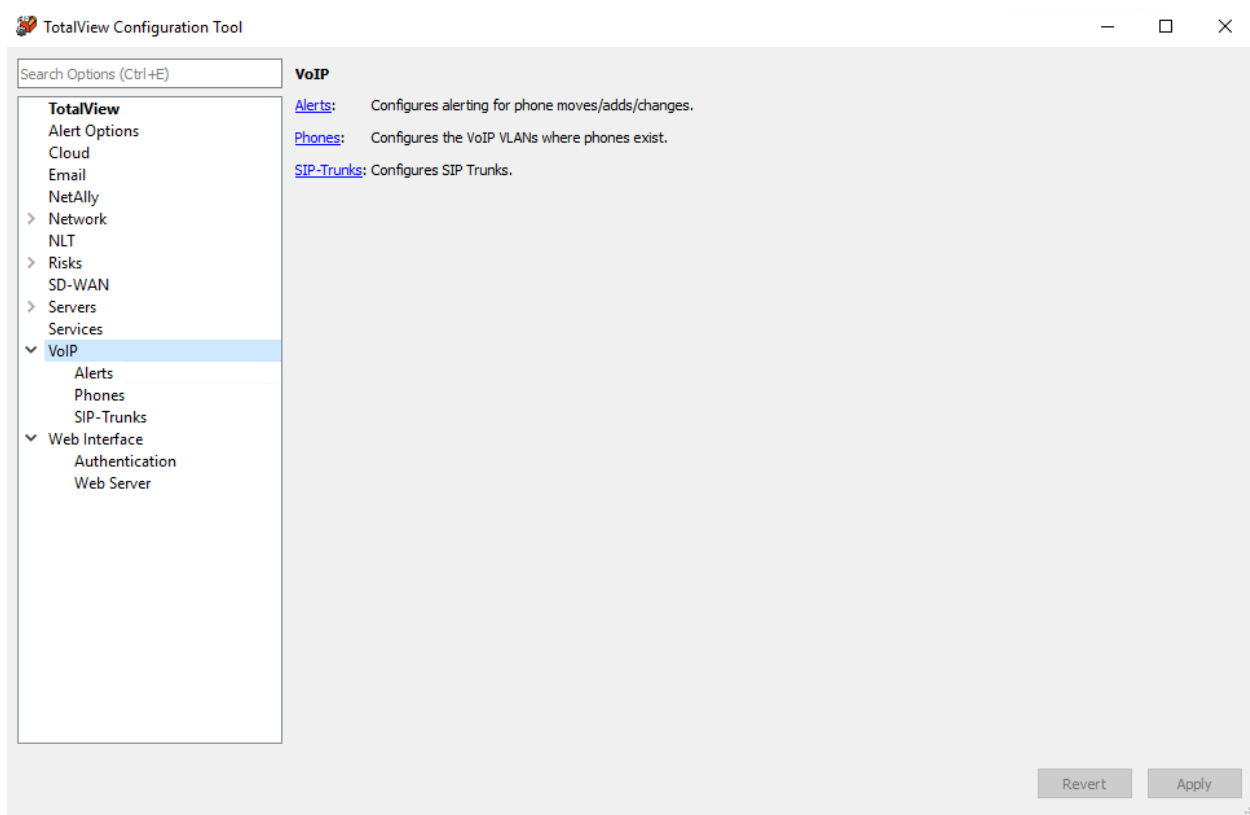
Note:

Send Alert to:

OK Cancel

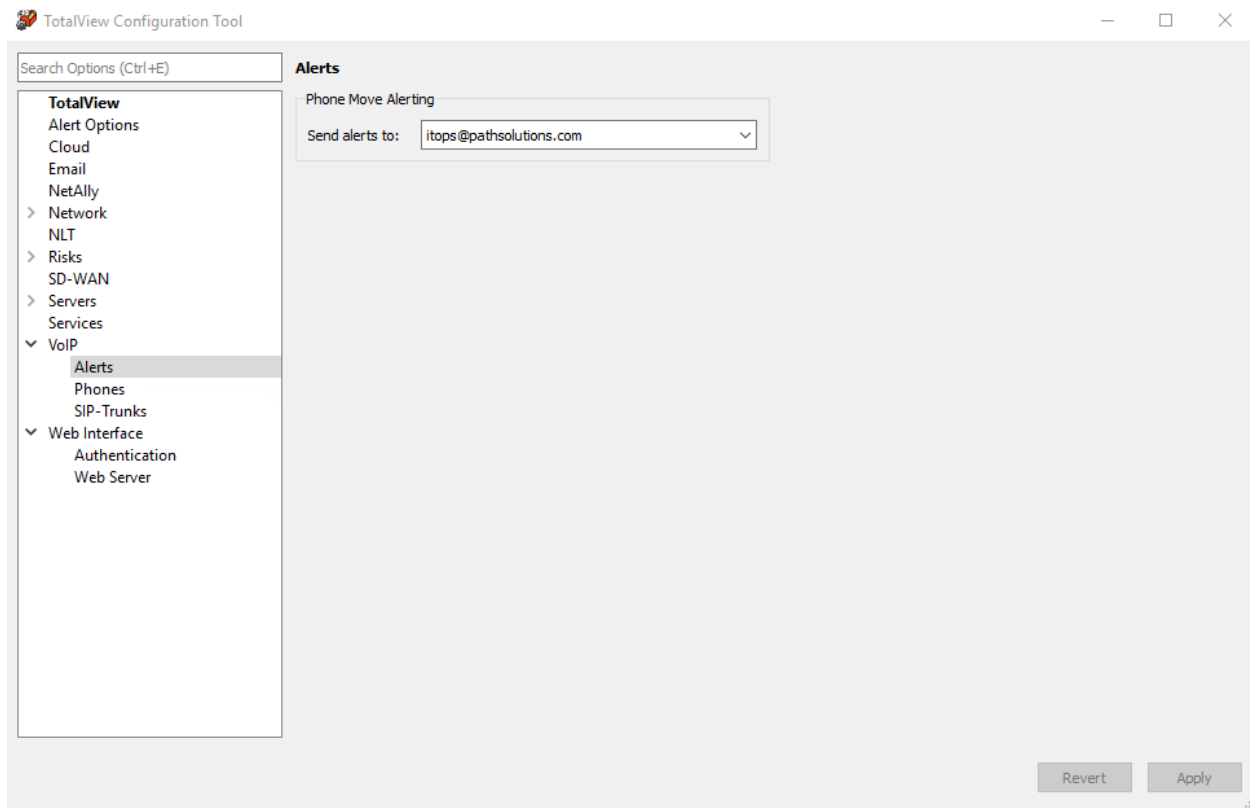
VoIP

This section will appear if you have the VoIP module license. To configure VoIP/Telecom settings, go the VoIP in the left-hand menu. You will see options to configure alerts, phones and SIP-Trunks:



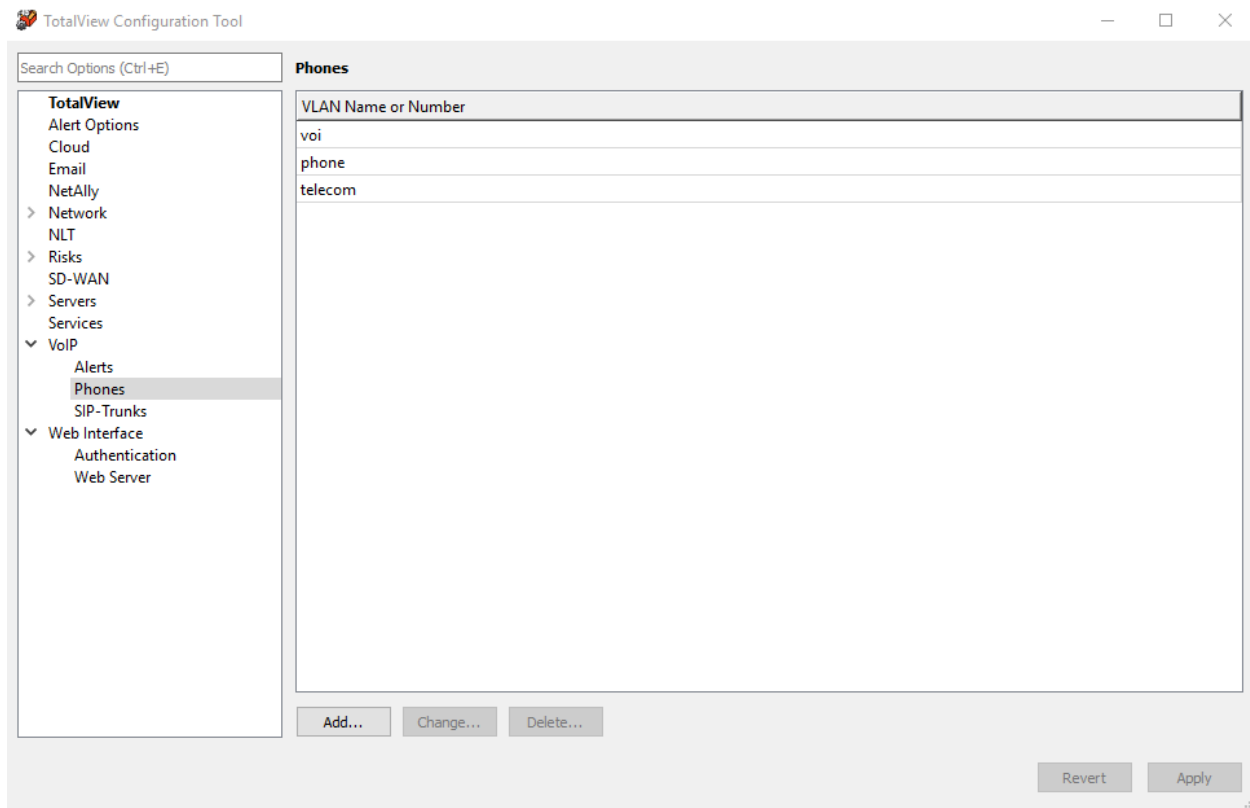
VoIP Alerts

On the VoIP Alerts section, you can chose where to send email alerts for Phone Move Alerting:

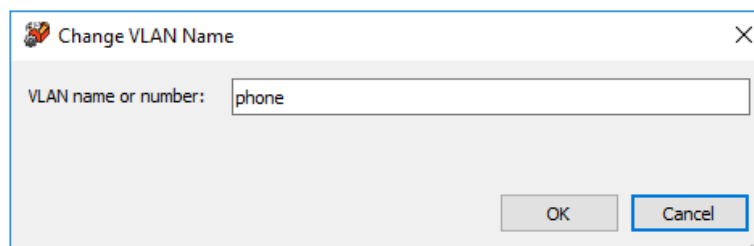


Phones

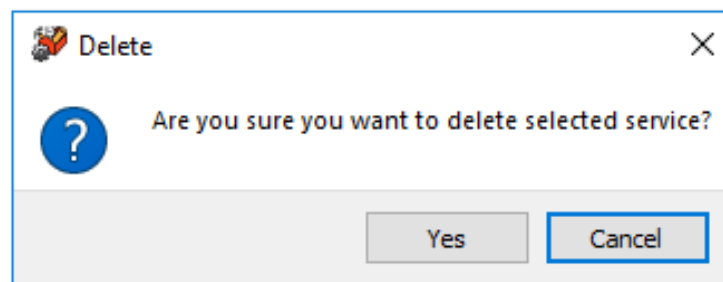
In the VoIP > Phones section, you enter the VLAN name and/or number:



Use the “Add” and “Change” buttons to add and edit VLAN names or numbers:

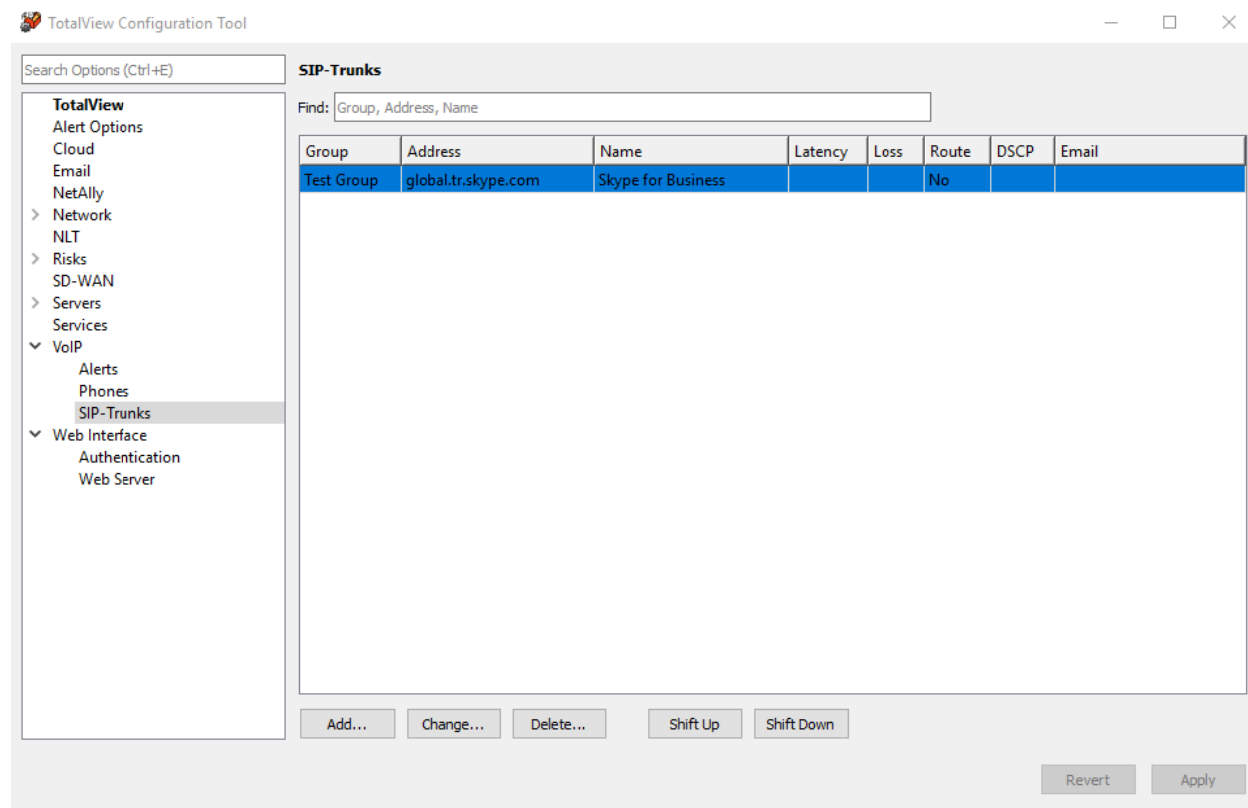


Use the delete button to delete one:



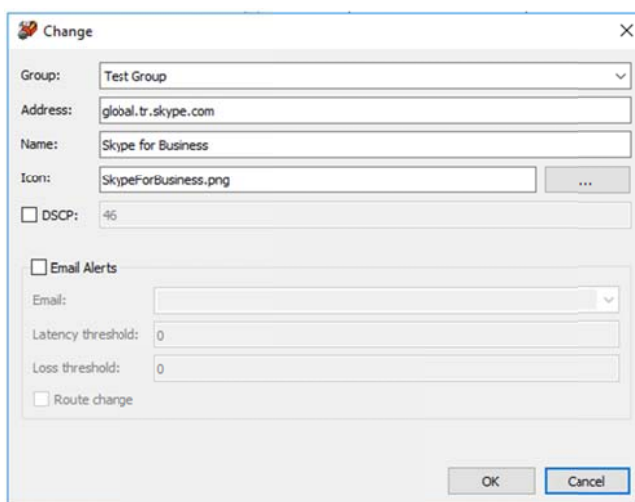
SIP-Trunks

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



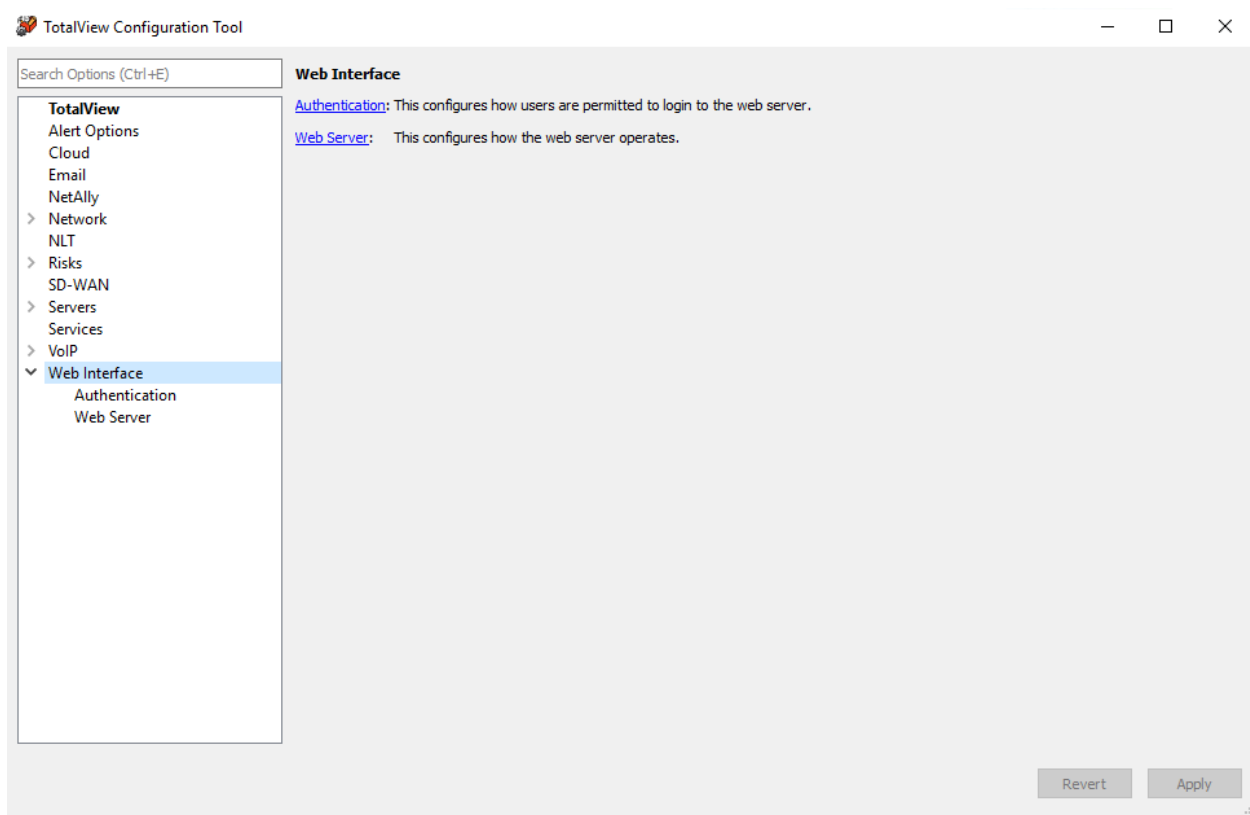
You can add, change, or delete any service by using the “Add”, “Change” and “Delete” buttons, and entering the group, address and name. Adding an “Icon” (a service picture) is optional.

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:



Website Interface

Select the Website Interface section from the left-hand menu. You will see the dialog box for configuring user authentication to login to the web server, and web server operators:

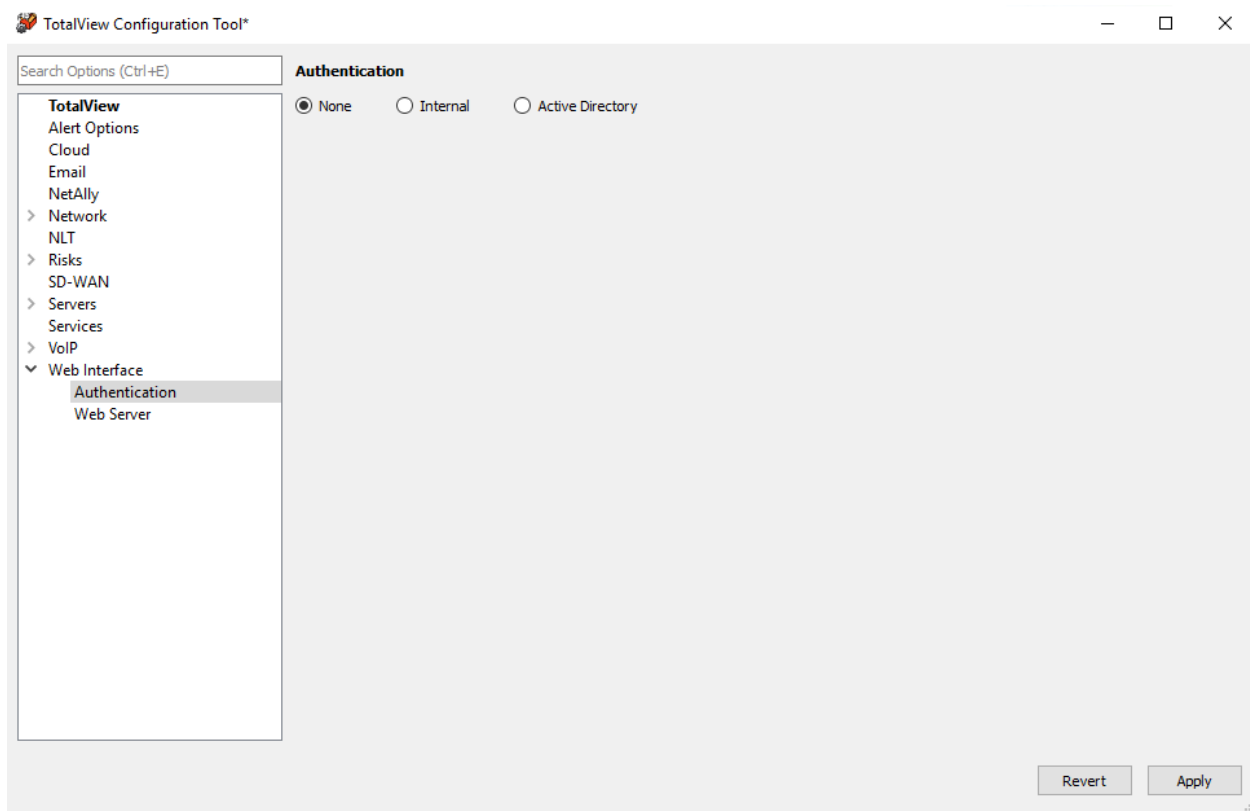


Web Authentication

In the Web Authentication section, you setup groups and assign user permissions for access to view and modify TotalView web pages. First select “None”, “Internal” or “Active Directory” from the selection at the top.

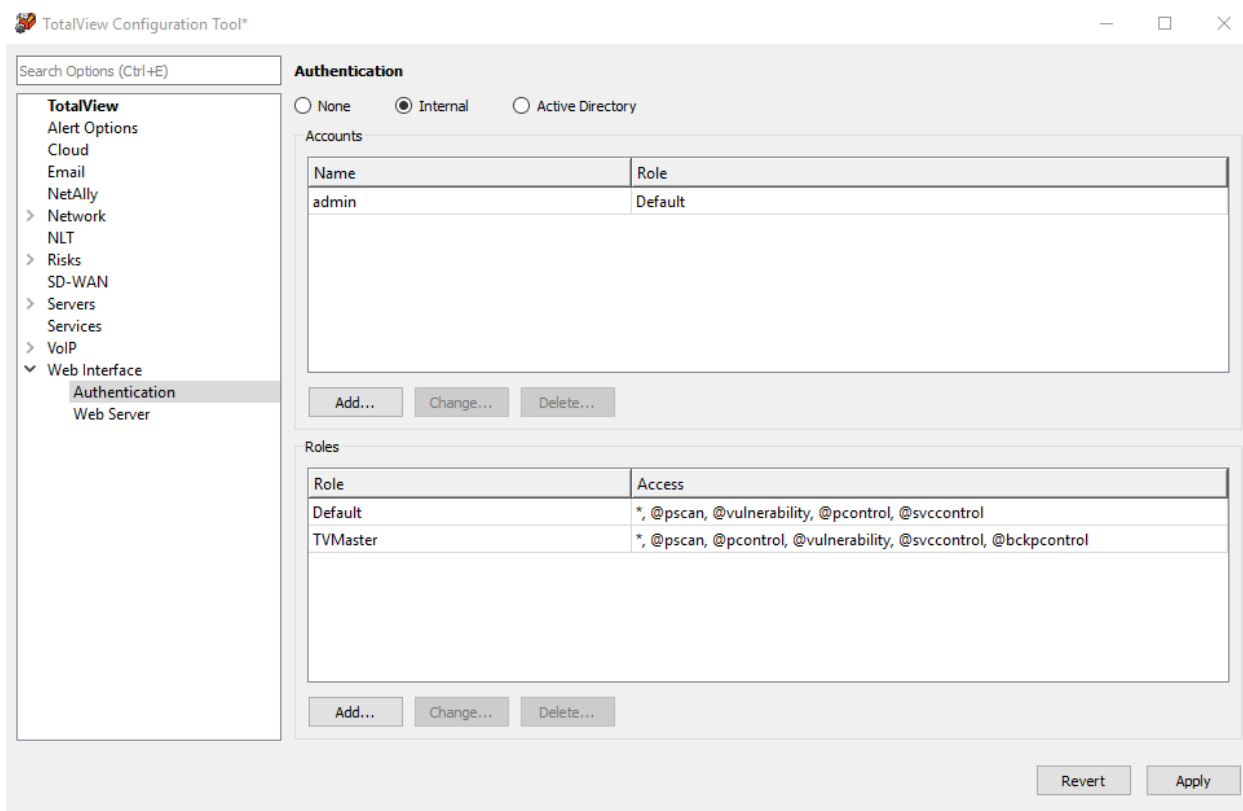
No Authentication

If you select “None”, no user permissions apply to TotalView users. TotalView works the same for any user.

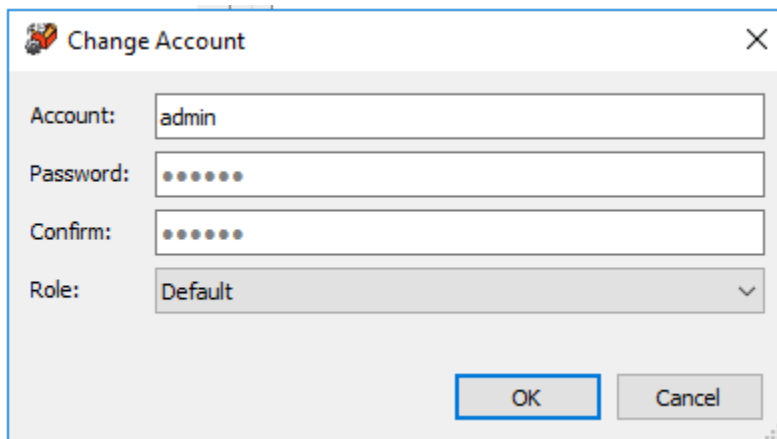


Internal Authentication

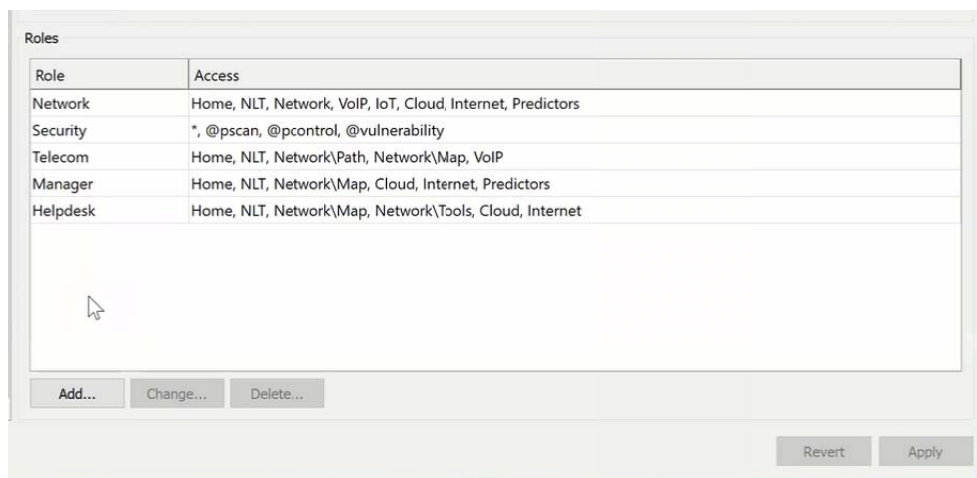
In the Web Authentication section, if you select “Internal” at top, access to TotalView is protected with internal security measures. Internal security means that TotalView will control all logins. You would create logins and assign them to groups that you create.



Under the top right box “Accounts”, you can add, change, and delete the login accounts by using the “Add”, “Change” and “Delete” buttons. The popup dialog will have you set user accounts, passwords and roles:

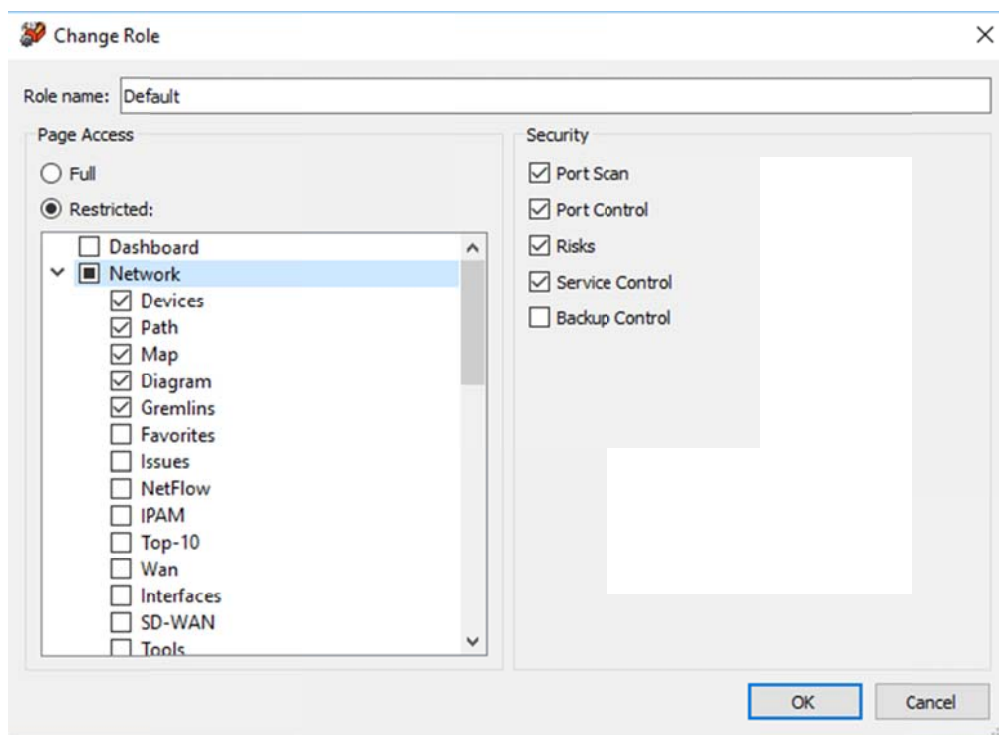


On the lower half of authentication interface, under “Roles”, you setup and configure the access for different types of roles.



Use the "Add", "Change" and "Delete" buttons on that section to create and edit the page access for each of the roles named, giving full or restricted web access to sections of TotalView. This sets the user access privileges.

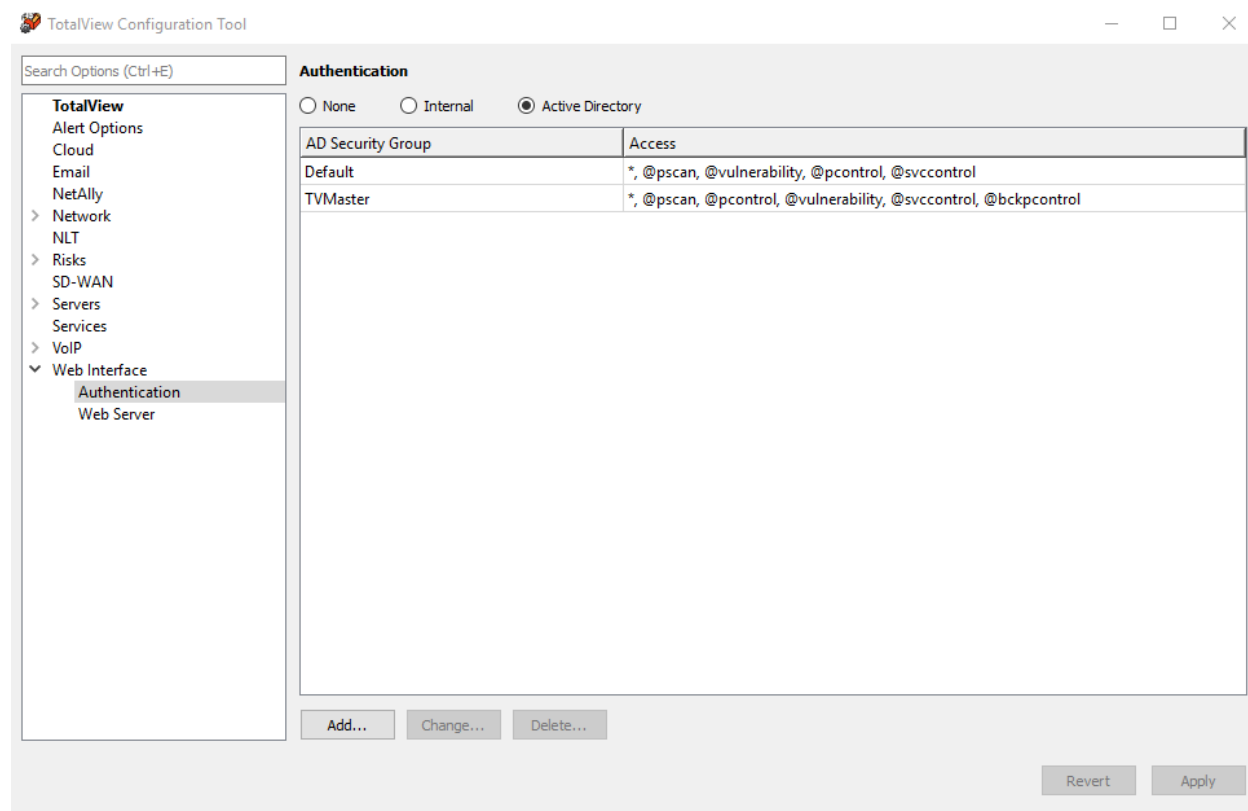
Here's an example of the dialog box setting restricted access:



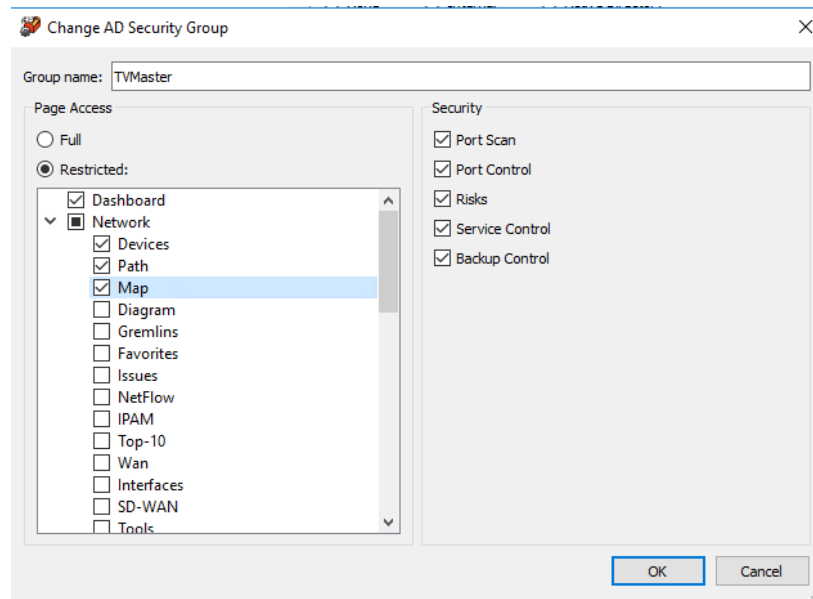
Active Directory Authentication

If you select “Active Directory” at the top of the Authentication section, user permissions are assigned in conjunction with the Microsoft account management system.

You would configure accounts in one location and it would control rights to different servers and services in the domain. In this section, enter the active directory group names, aka “Security Groups”, that would have TotalView rights. Users would be assigned into these Active Directory groups via the Microsoft Active Directory management console.

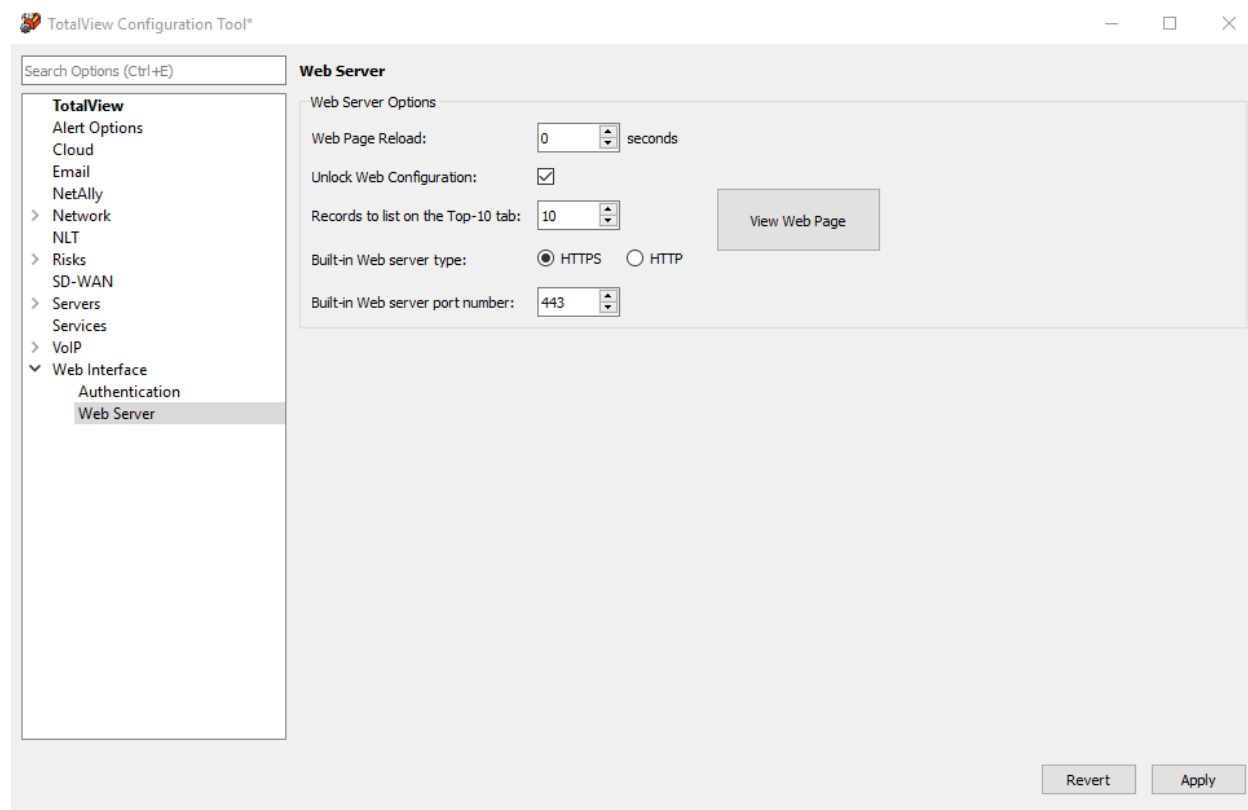


In this section you add and edit the Active Directory “Security Groups” by using the “Add”, “Change” and “Delete” buttons. The dialog will let you give the Security Group full or restricted access to the different sections of TotalView:



Web Server (Options)

The Web Interface > Web Server section lets you set some basic web server options for TotalView: page reload, unlocking web configuration, records to list on the top 10 section, the built-in web server type (HTTPS or HTTP), and server port number.



You can also quickly view the web page in a separate window, by clicking on “View Web Page”.

Page Reload Settings

The web browser should automatically refresh the web page and reload. It is advised to use the default of 0 (zero) in the Web Page Reload field. If you do not want the web pages to reload automatically, use a number like 300 seconds (5 minutes) or adjust as needed.

Unlocking Web Configuration

If the web configuration is locked, and you want to unlock it, check the box by “Unlock Web Configuration”.

Unlocking will allow users to do the following things in the TotalView web interface: add favorites to the “Favorites” tab, ignore devices, and add interfaces to the “WAN” tab.

If you keep it locked, the options to add favorites and ignore devices do not appear in the web interface.

Listing Records on the Top-10 tab

The number of interfaces displayed on TotalView’s Top-10 tab can be adjusted by increasing or decreasing this value.

Built-in web server type (HTTPS or HTTP)

Select the server type.

Built-in Web Server Port Number

If you are using the integrated Web server to serve pages, you can specify the port that the program should use. You should choose a port that is unused on your system or the service may not be able to use that port.

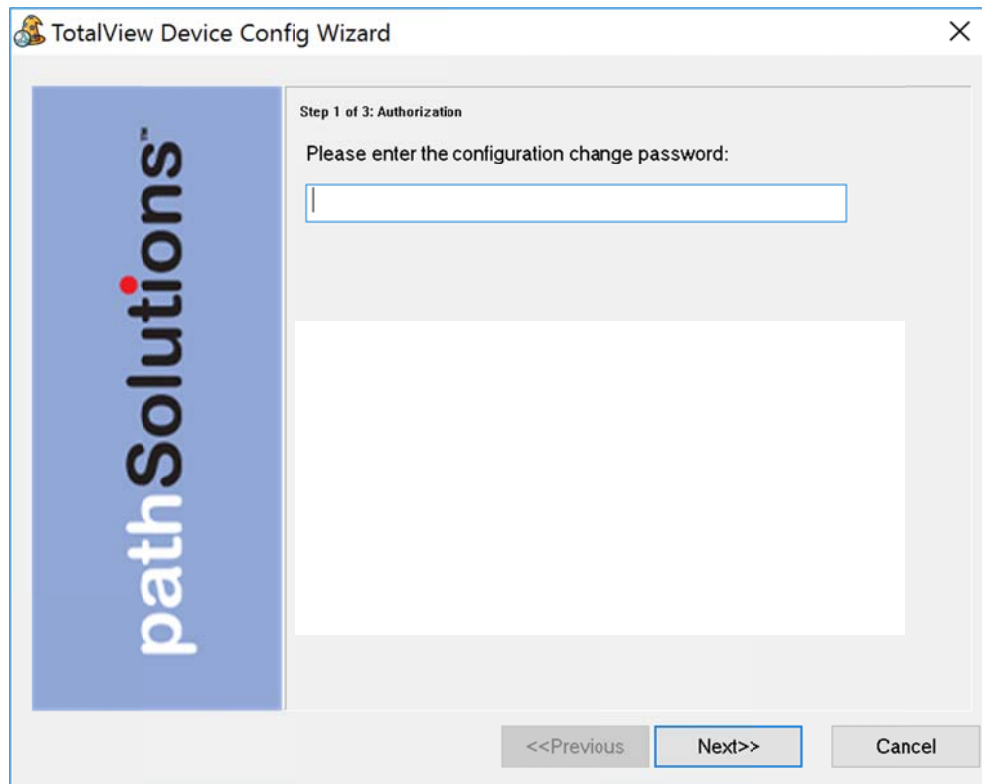
Note: If you select a port and then apply the changes by clicking on "Apply" or "OK", and the server does not respond on that port, check the application event log to determine if there may be a port conflict.

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.

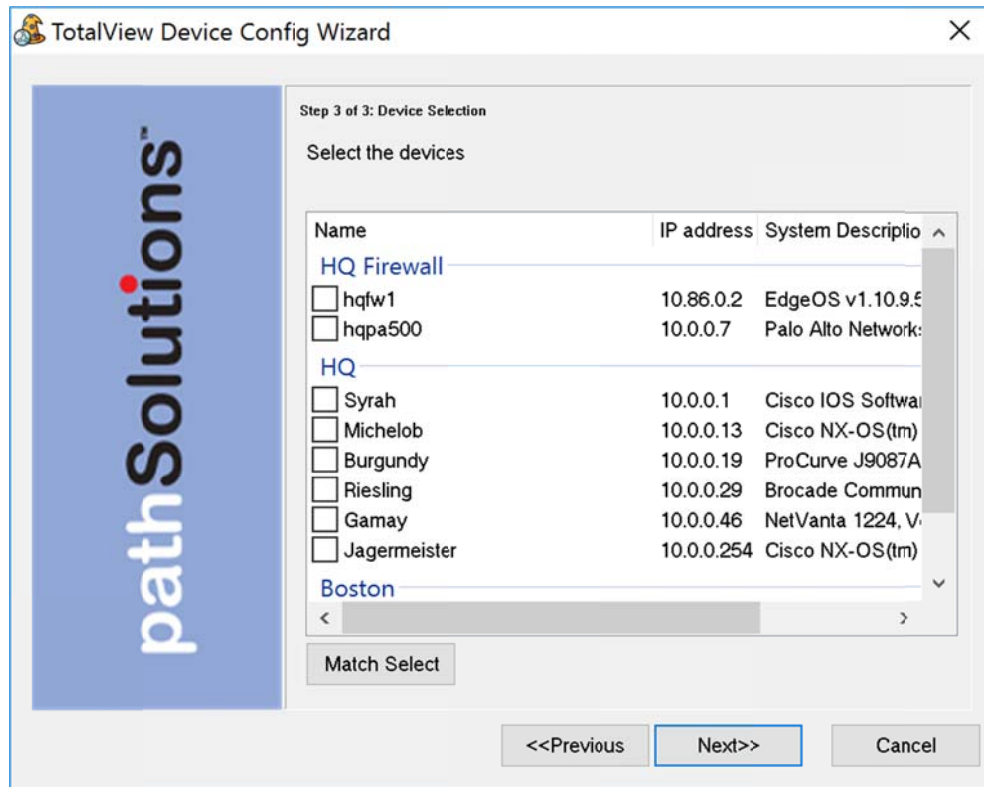
The program can be launched on the server's console by clicking "Start", choosing "PathSolutions", then choose "TotalView". Then select "TotalView Device Config Wizard".

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.

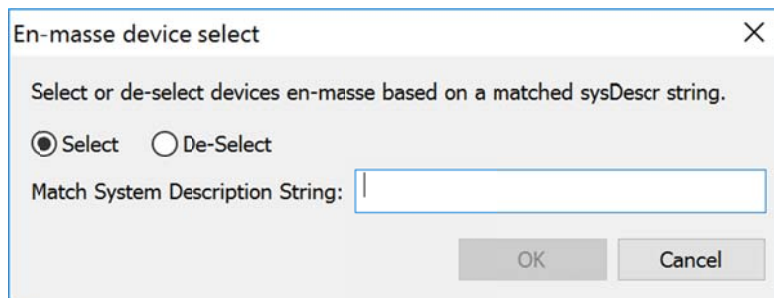


Click "Next" to continue.

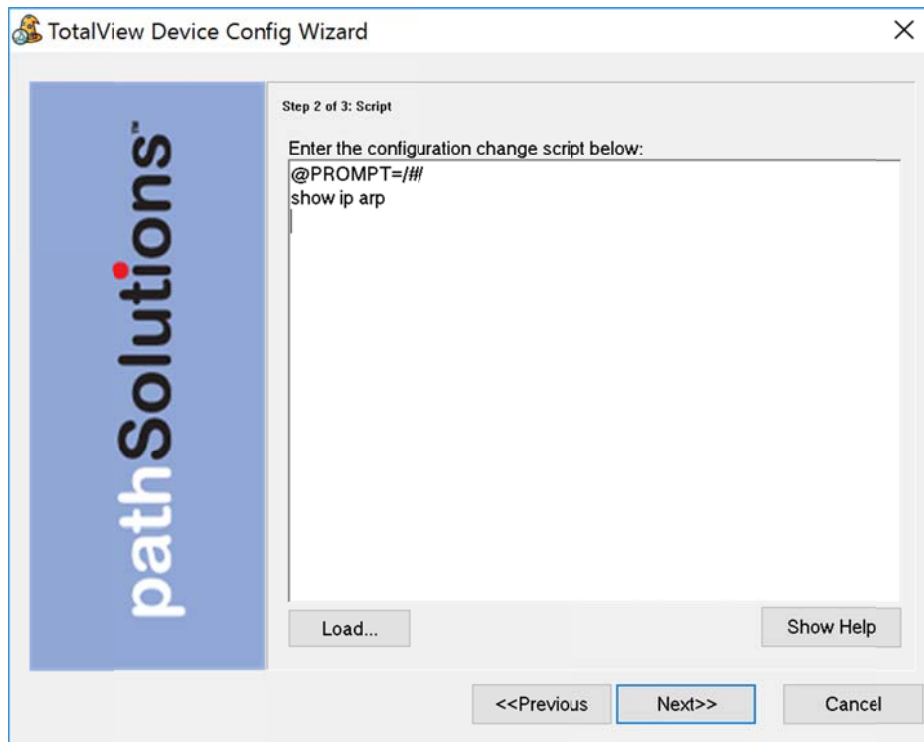
Step 2 will permit you to select devices. Check the appropriate device or devices that you want the configuration to apply to:



If you want to do global selects, this can be done with the “Match Select” option. For example, you can click “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.

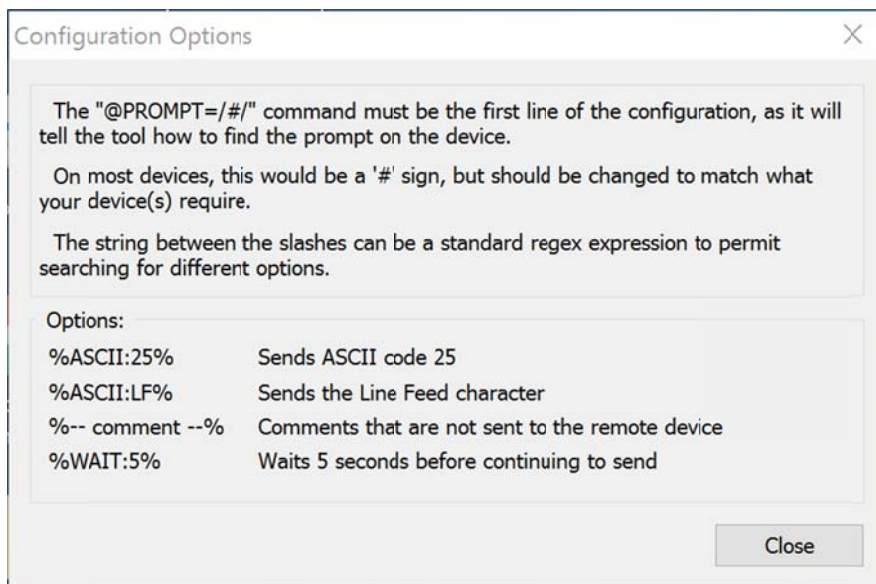


Then in step 3, enter the configuration change script. If needed select “Load” or “Show Help.” When finished, click “Next”:



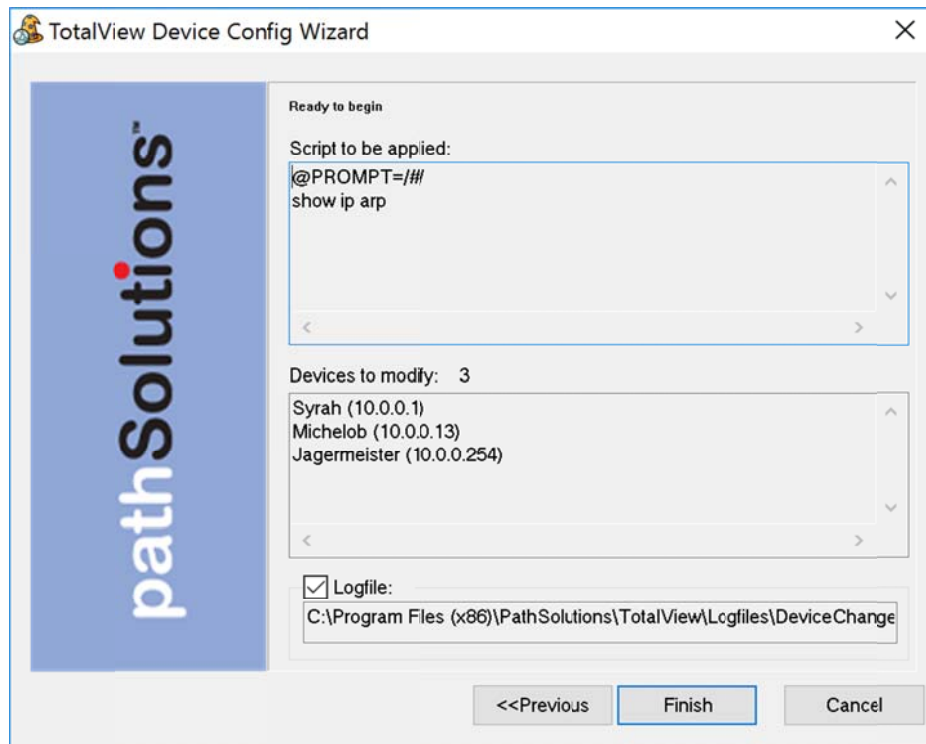
Note: The “@PROMPT=/#/” must be the first or second line, as this tells the program how to identify that the console is ready to accept input. This may be different depending on the device being connected to.

Additional options can be entered in the configuration. Click “Show Help” to open a non-modal dialog box that can help with the configuration input:



Click “Next” to continue.

A final confirmation will appear. Select “Finish” if everything looks correct:



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 communications.

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, click on "Start". Then choose "Programs", "PathSolutions", "TotalView", and "QuickConfig Wizard".

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

The screenshot shows the 'TotalView QuickConfig Wizard' window, specifically 'Step 1 of 4: Network Address Ranges'. On the left is a blue vertical bar with the 'pathSolutions' logo. The main area contains instructions: 'The QuickConfig Wizard 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.' Below this is a 'New Address Range' section with input fields for 'Starting:', 'Ending:', and 'Group:' (set to 'Default'), followed by an 'Add' button. Underneath is an 'Address Ranges to be Checked' list box containing two entries: '10.0.0.1 - 10.0.0.254 [Santa Clara]' and '10.86.0.1 - 10.86.0.10 [Santa Clara]', with a 'Delete' button to the right. At the bottom are navigation buttons: '<<Previous', 'Next>>', and 'Cancel'.

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 also fine-tune which interfaces are monitored. This can help reduce the number of monitored interfaces to fix license limitation problems.

The Interface Discovery Tool can be launched on the server's console by clicking "Start", choosing "PathSolutions", then choose "TotalView", then select "IntDiscoveryTool."

It will launch and show the first step:

The screenshot shows a window titled "TotalView Interface Discovery Tool" with a close button (X) in the top right corner. On the left side of the window is a large blue vertical banner with the "pathSolutions" logo. The main content area is titled "Step 1 of 3: Network Address Ranges". Below the title, it says: "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." There is a section labeled "New Address Range" containing three input fields: "Starting:" (with a dropdown arrow), "Ending:" (with a dropdown arrow), and "Group:" (with a dropdown arrow showing "Sunnyvale"). To the right of these fields is an "Add" button. Below this is a section titled "Address Ranges to be Checked" containing a list box with two entries: "10.50.0.1 - 10.50.0.254 [Sunnyvale]" and "10.50.4.1 - 10.50.4.254 [Sunnyvale]". To the right of the list box is a "Delete" button. At the bottom of the window are three buttons: "<<Previous", "Next>>", and "Cancel".

This step will allow you to enter subnets that should be scanned to find new devices.

The second step allows you to enter SNMP credentials to communicate with network devices:

TotalView Interface Discovery Tool

Step 2 of 3: SNMP Security

Specify the SNMP read only security credentials that are used on devices in your network. These will be used to access interface information on your devices.

New credentials

SNMP version: ☐ v1 ☒ v2c ☐ v3

Community string:

AuthProt: AuthPass:

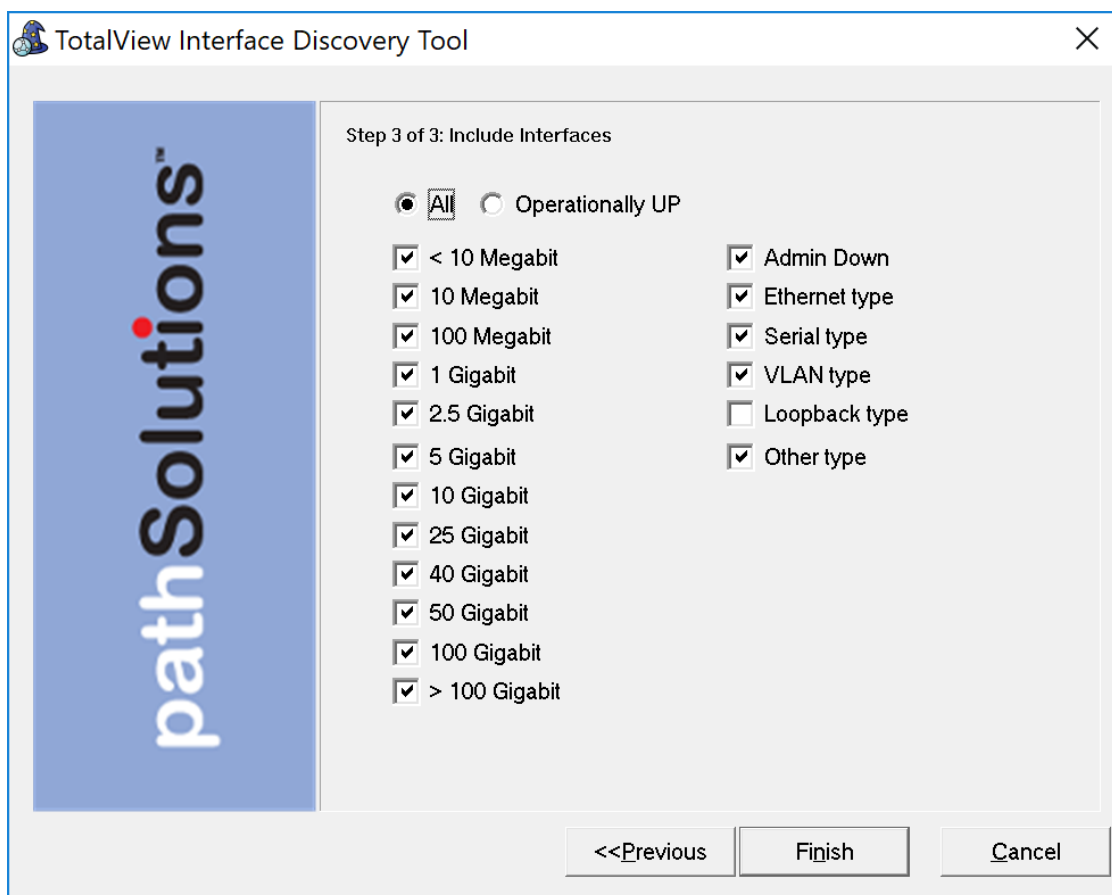
PrivProt: PrivPass:

Credentials to be checked

Enter your credentials and click "Next" to continue.

Note: The credentials should be listed in the same order as is used in the QuickConfig Wizard to prevent community strings from changing on existing devices.

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

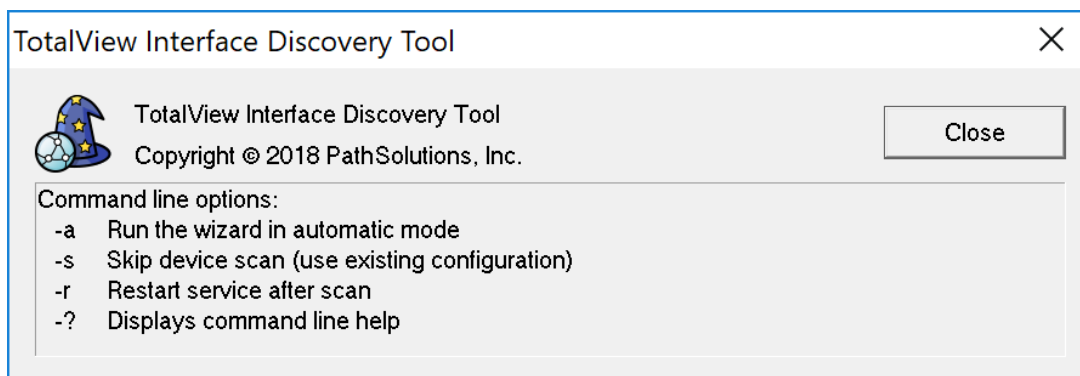


If an interface type is not checked, it will not be included in TotalView's configuration.

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

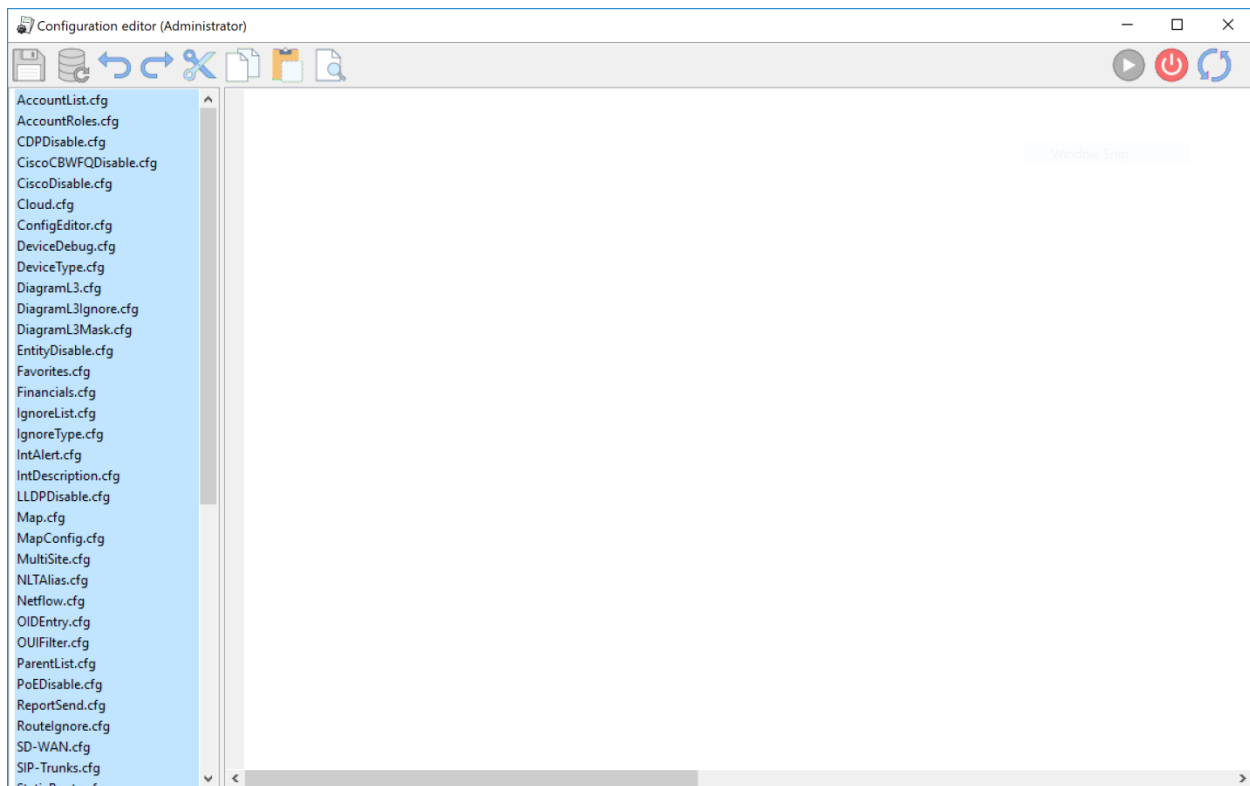
The service will then be restarted.

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



Config Editor

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



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 clicking on the disk icon in the toolbar.

The service can be restarted by clicking on the far right toolbar icon.

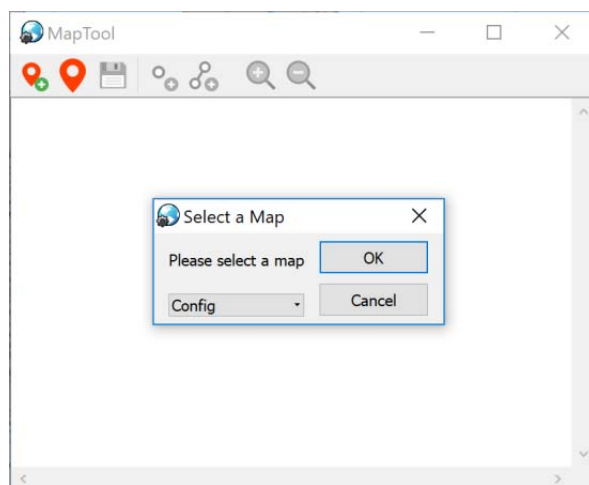
Note: Some configuration files will take immediate effect and do not require a service restart.

Map Config Tool

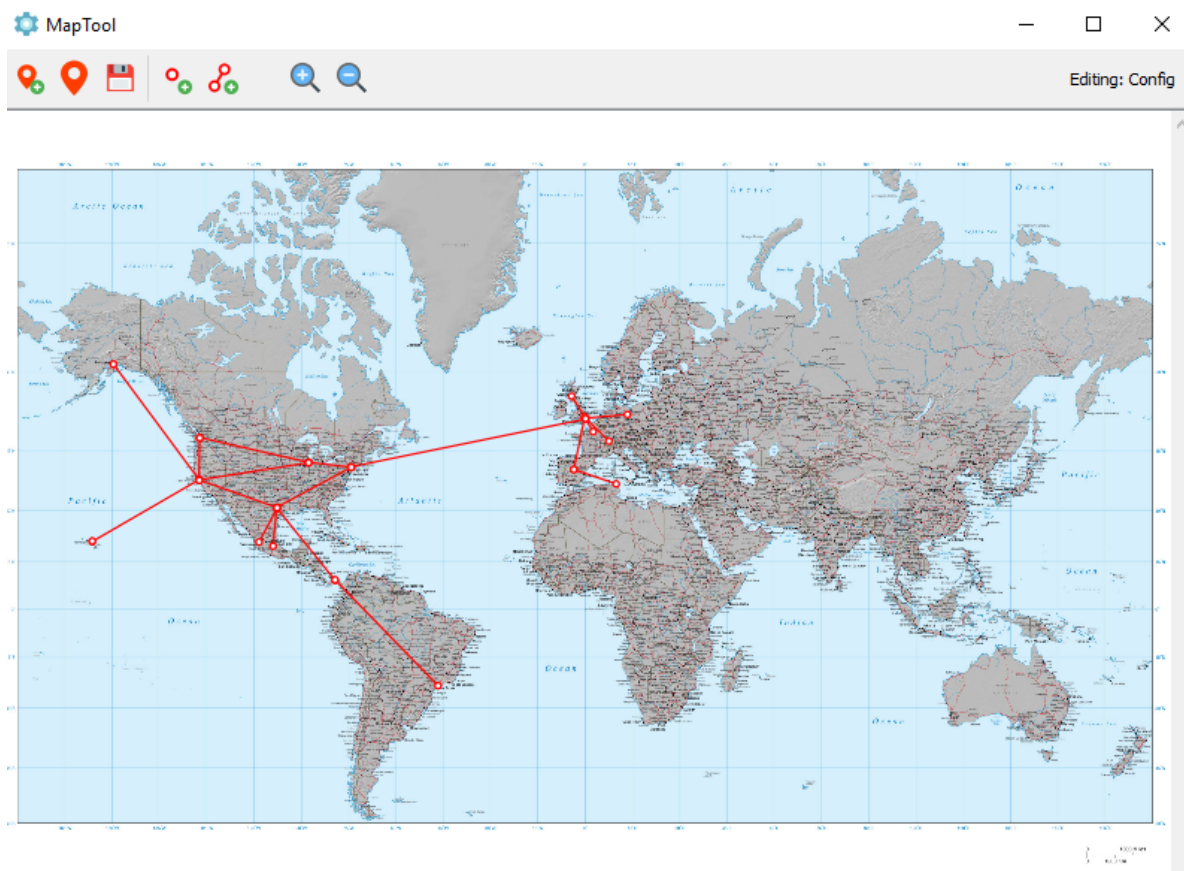
The Map Config Tool can be used to create and update the “Map” tab on the web user interface. It can be launched from the Configuration Tool. It can also be run from the console where TotalView is installed.

To run from the console, go to Start/Programs/PathSolutions/TotalView and choose the Map Config 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, previously.



Once 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:



Click on this pointer symbol top select and open a map:



Click on 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:



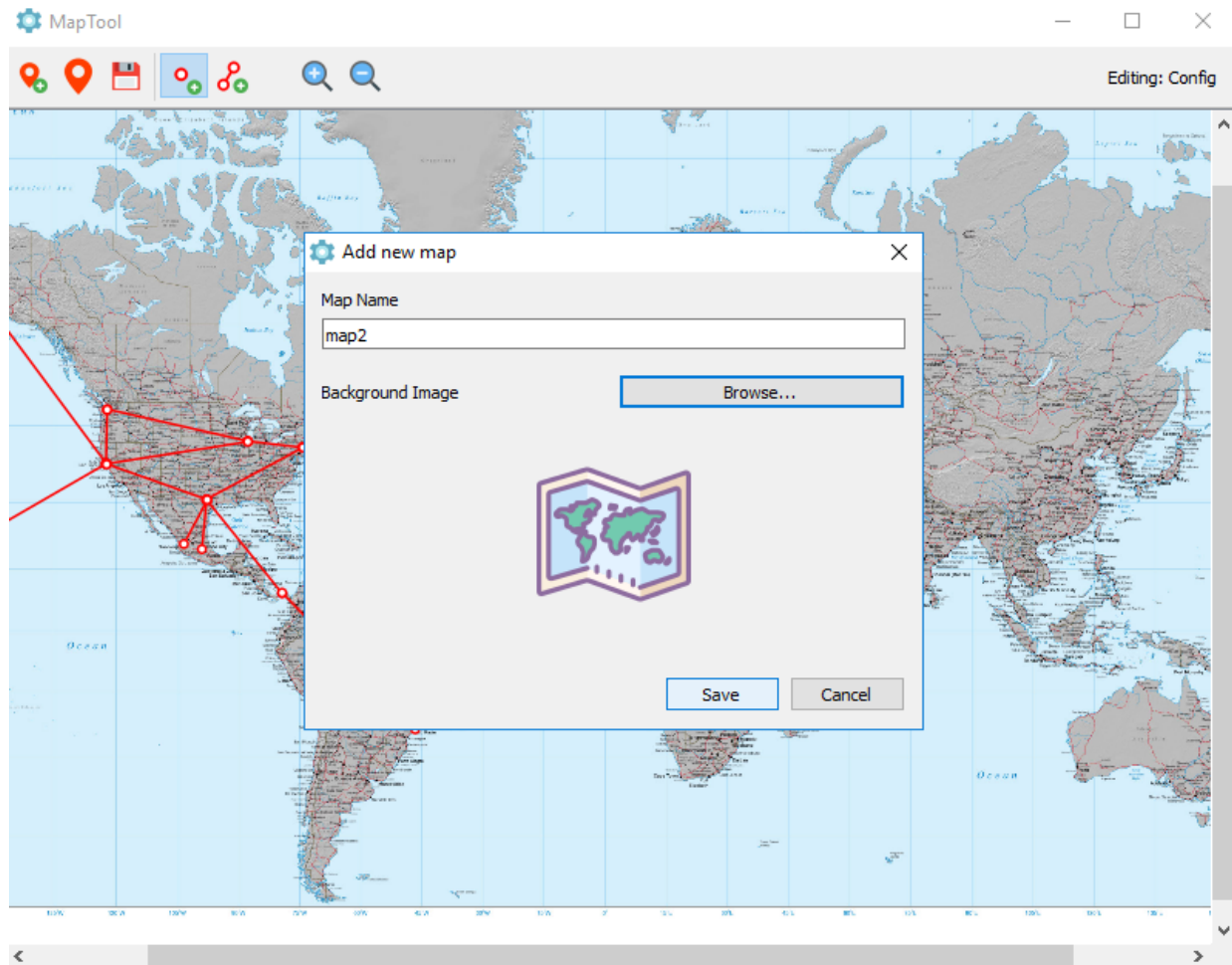
To change magnification up or down, click on the magnifying icons:



How to Add Maps



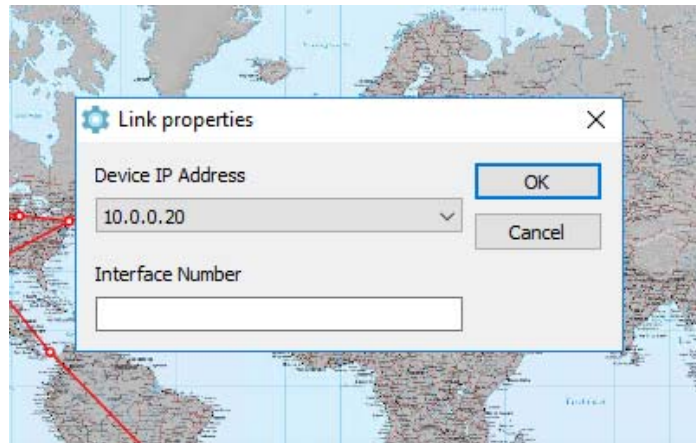
Select the “Add Map” icon and this popup menu will ask you to name the map and select a map background image from computer files. Select a map from your TotalView Graphics folder. Multiple Maps can be created this way.



How to Add Links

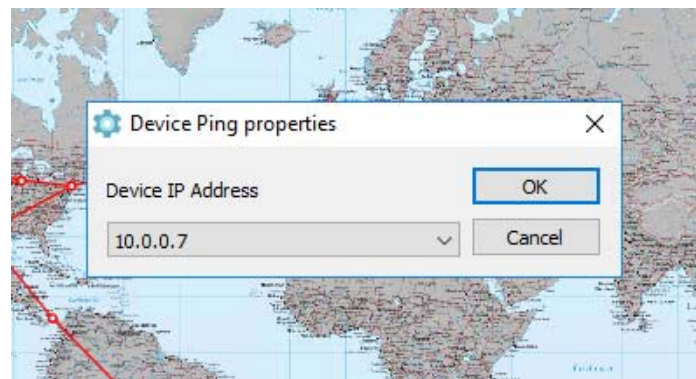


To add a link connection between coordinates, choose the “Add Link” icon. It will ask you to select the device IP address and interface that should be associated with the link:



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 click.

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

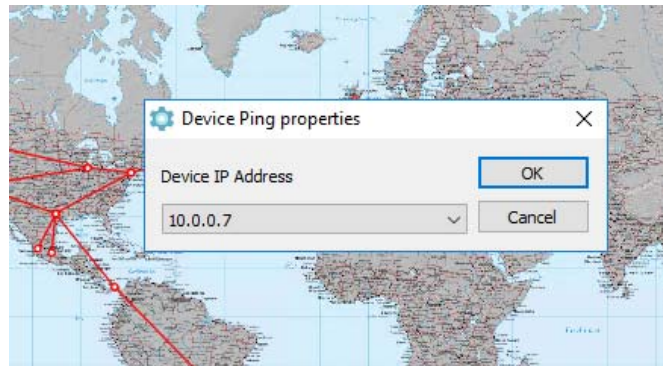


If you save the map, you can immediately check the web page’s map to see the change automatically updated. (There’s no need to restart the service or refresh the browser window).

How to Add Ping Points

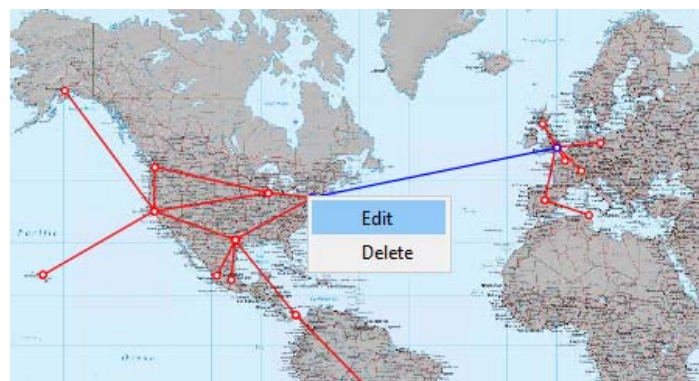


For a Ping point, choose the “Ping Point” icon, and then enter the Device’s IP address. This represents that the Device can be pinged. In TotalView, the point will display as a green dot (can ping), a red dot (cannot ping), or a black dot (device is down).



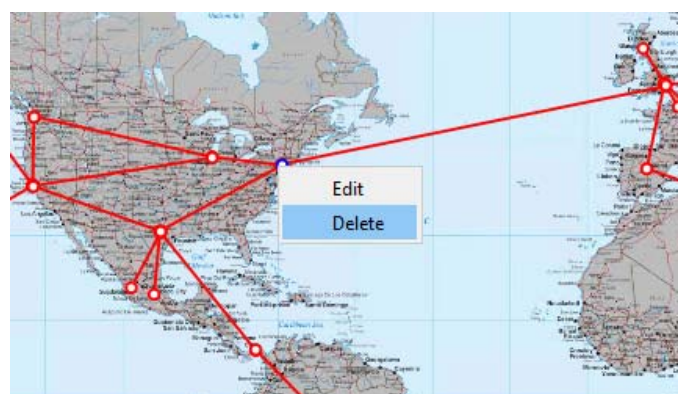
How to Change Items on the Map

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.



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, click on the “Save” icon to save the changes in the map. If you save the map, you can immediately check the web page’s map to see the change automatically update (no need to restart the service or refresh the browser window).

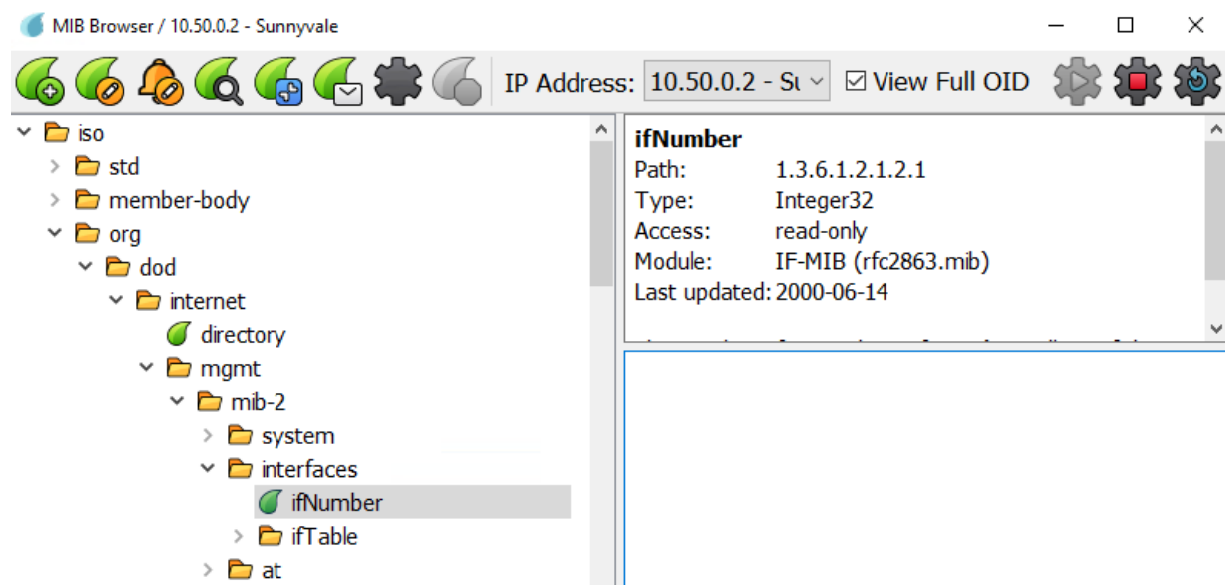
After saving, you can close the Map Tool.

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, click Start/Programs/PathSolutions/TotalView and choose the MIB Browser. (MIBBrowser.exe),

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



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.

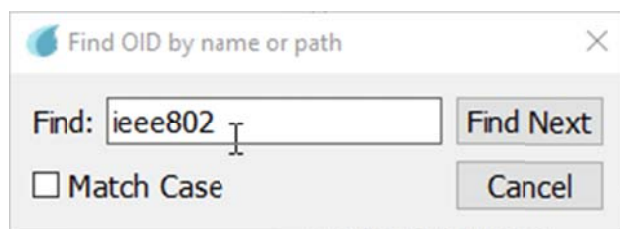
If you right-click on a variable, it shows information about the variables in the top right panel, and also offers the following options from a drop-down menu:

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, you can click on this search symbol in the top menu:



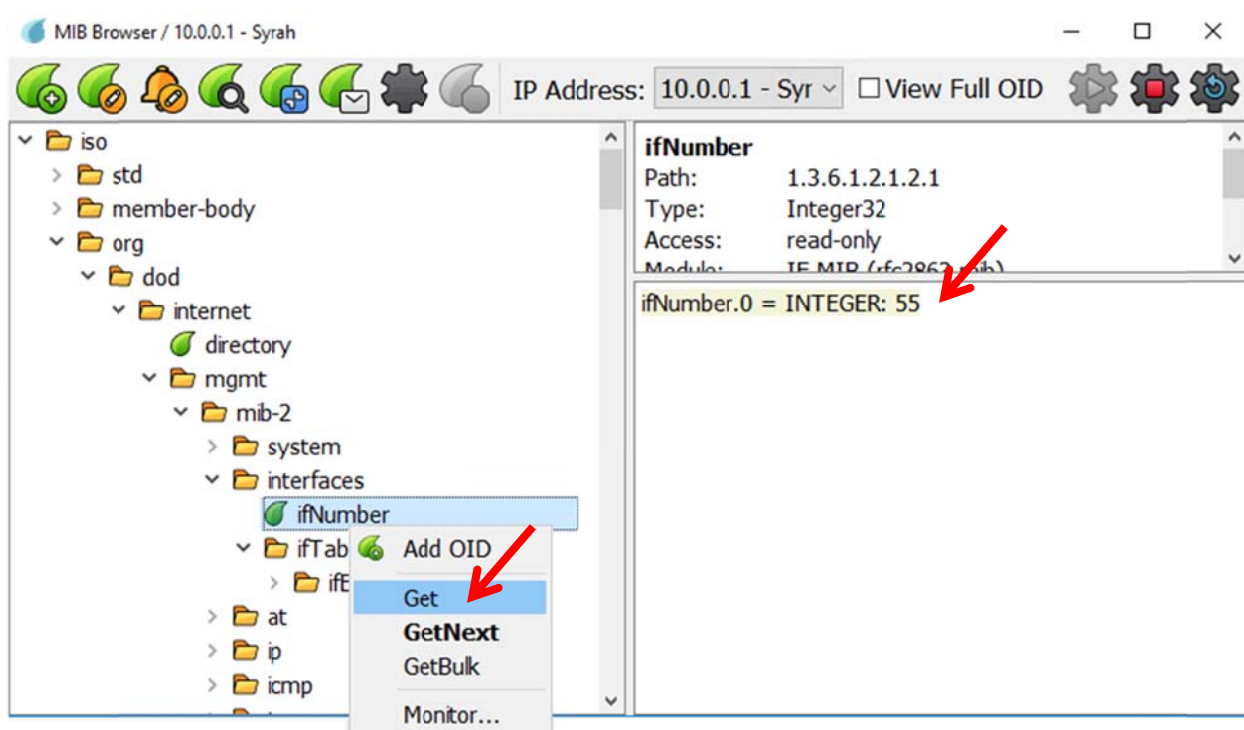
If you click it, the search menu will popup, Enter a search string, then select "Find Next" here:



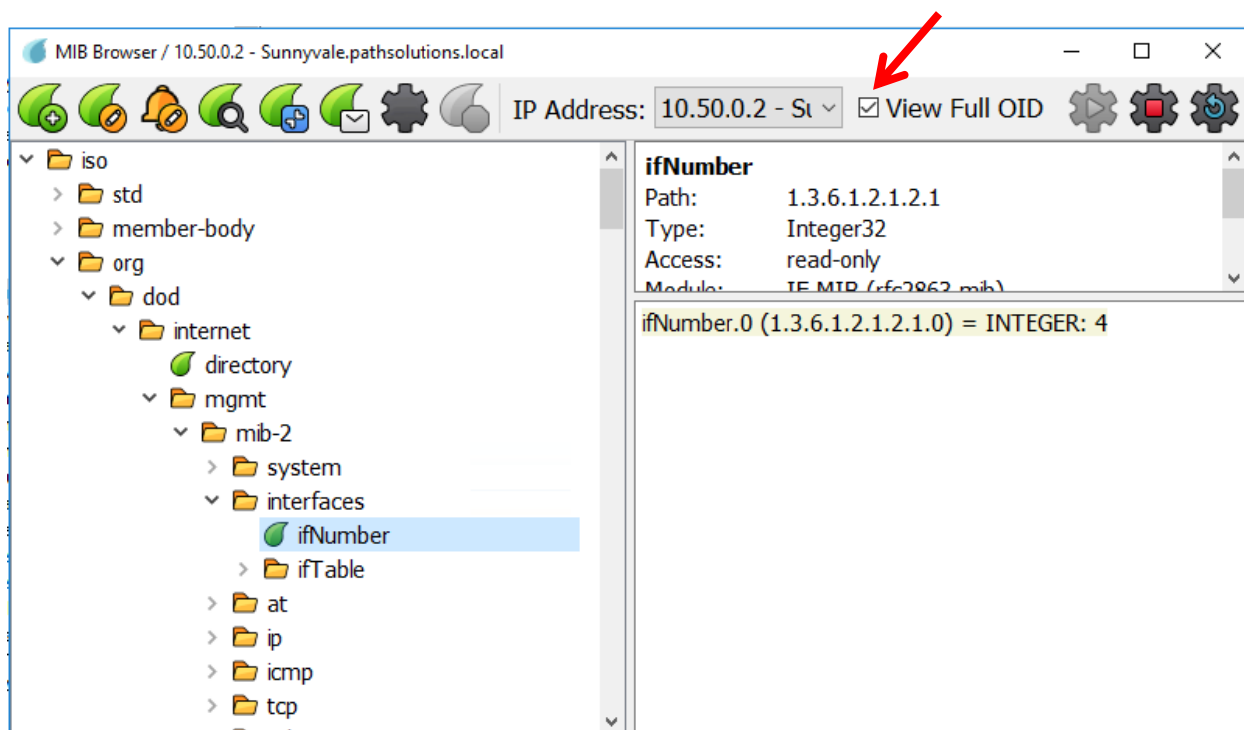
OID Lookups **NEW**

The left navigation panel allows you to navigate and choose an OID variable. Once you select a variable by clicking on one, 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 chose “Get” it will fetch that variable and display the name of it in the lower right panel:

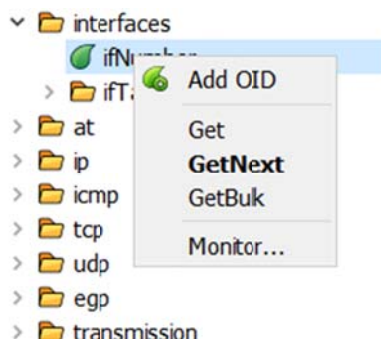


You can view the full OUI value in the lower right panel, by pressing the “View Full OID” button:



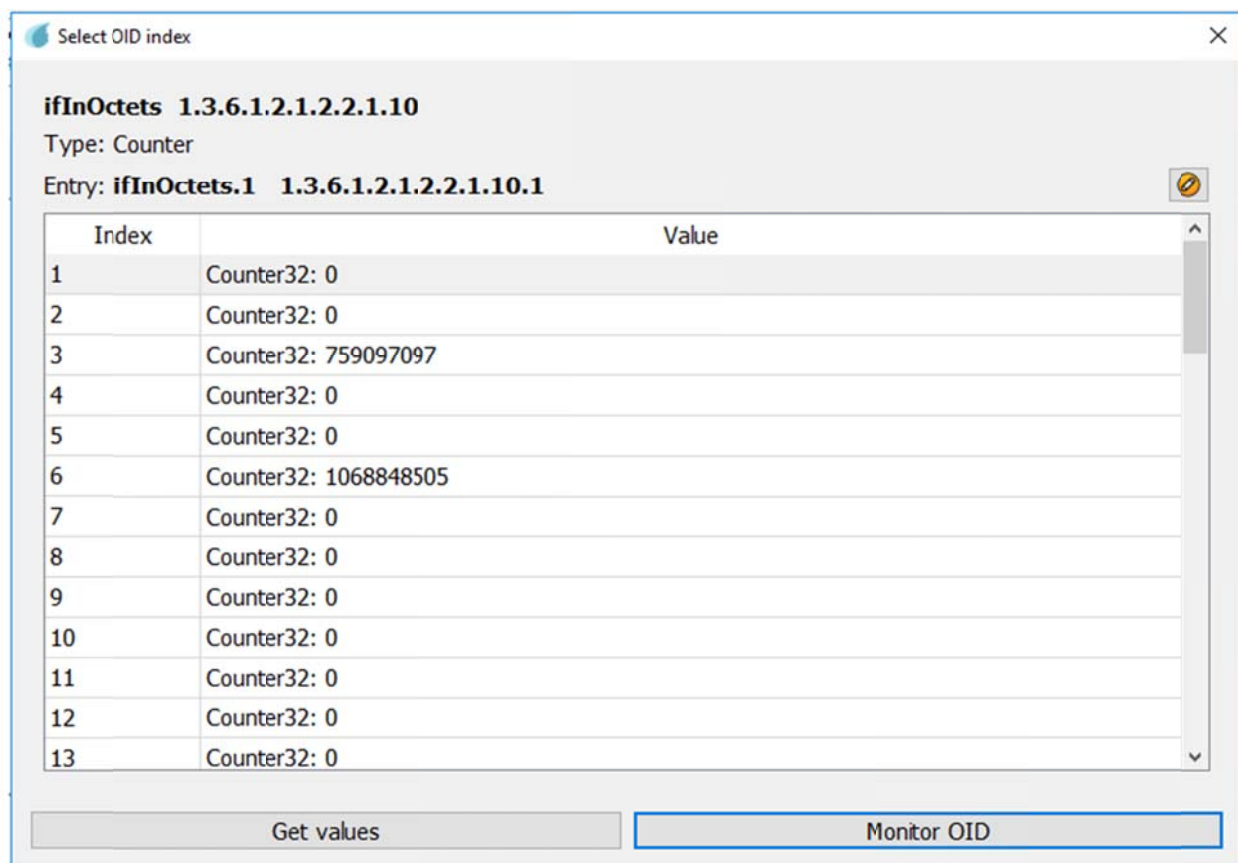
OID Monitoring **NEW**

When you right-click on an OID, it has a drop-down menu that allows you to choose “Monitor...”:



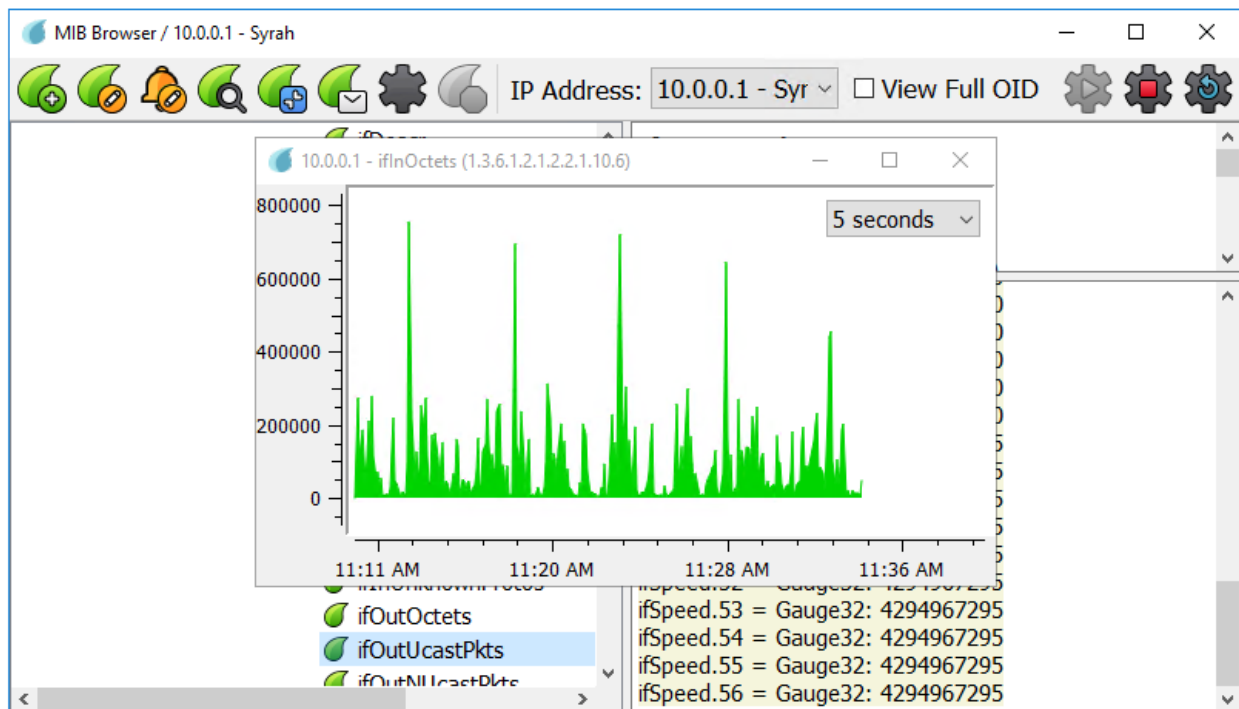
Select “Monitor...” and the dialog box for the selected Interface’s OID Index will popup.

If you select the button “Get values” button, it will refresh the values on screen, to show any updated information since the last query:



If you select the button “Monitor OID” button, 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.

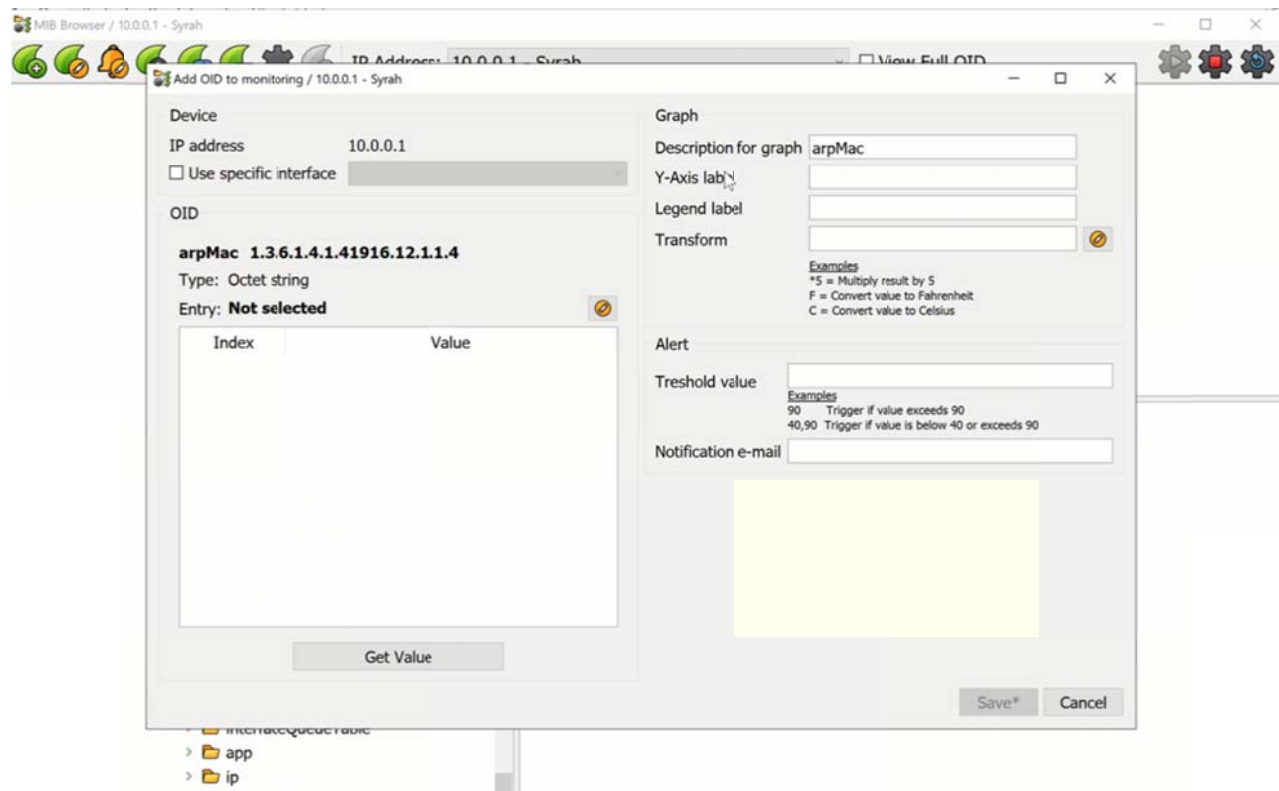
Tip: We recommend to set intervals to monitor less frequently, if your device does not update its SNMP counters as often.



OID Graphing

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

The “Add OID” dialog box will appear. In this dialog box, you can now add iterative calculations in the “transform” field for the graph labels. You can do things like add and multiply, convert from Celsius etc. Fill out the description and label fields, and transform fields, and select “Save”.



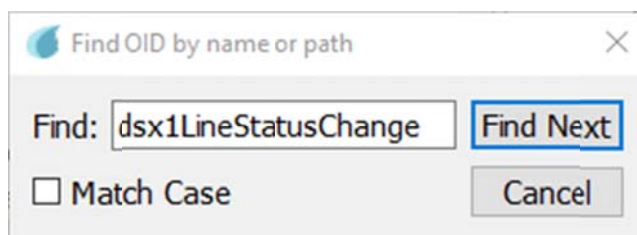
SNMP Trap Receiver Configuration

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

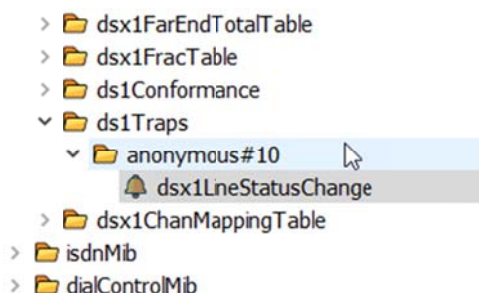
Note: The SNMP Trap Receiver service must be installed before it can be used. To install the SNMP Trap Receiver service, refer to the following KB entry:
<https://support.pathsolutions.com/support/solutions/articles/14000128376-totalview-12-installing-totalview-snmp-trap-service>

Alerting on a Specific Trap

Find the SNMP trap that you want to monitor in the MIB Browser. For example, here is the search for “dsx1LineStatusChange” then selecting “Find Next” several times to see all the instances of that string:



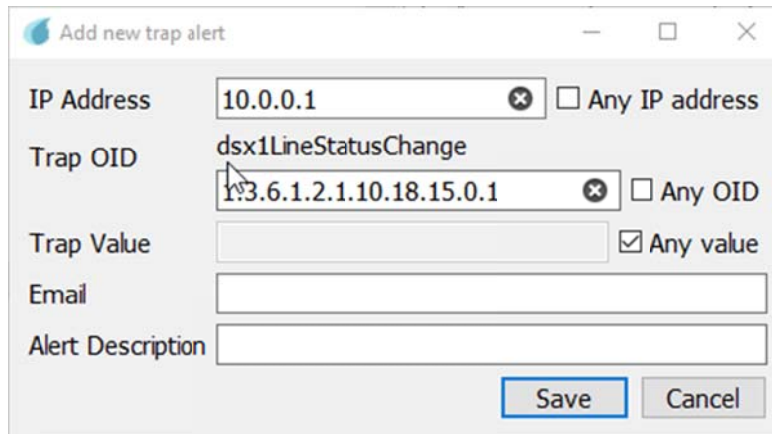
On the second instance, in this example, a bell icon next to the line item indicated it has a trap:



Right-click on the trap (the line item with the bell icon) and choose “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.



The 'Add new trap alert' dialog box contains the following fields and options:

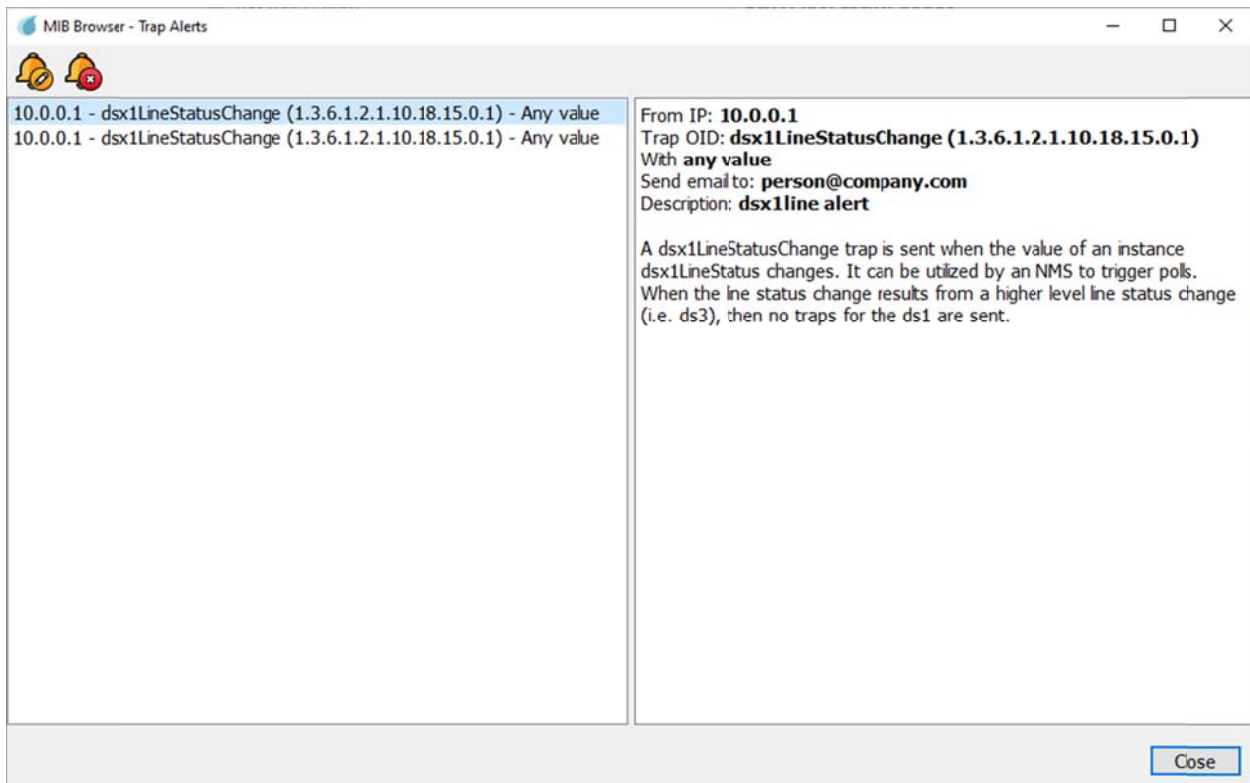
- IP Address:** A text box with '10.0.0.1' and a clear button (X). An unchecked checkbox labeled 'Any IP address' is to its right.
- Trap OID:** A text box with 'dsx1LineStatusChange' and a clear button (X). An unchecked checkbox labeled 'Any OID' is to its right.
- Trap Value:** A text box with an unchecked checkbox labeled 'Any value' to its right.
- Email:** A text box.
- Alert Description:** A text box.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

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 popup:



The 'MIB Browser - Trap Alerts' submenu displays a list of trap alerts on the left and a detailed view on the right.

Left Panel (List):

- 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

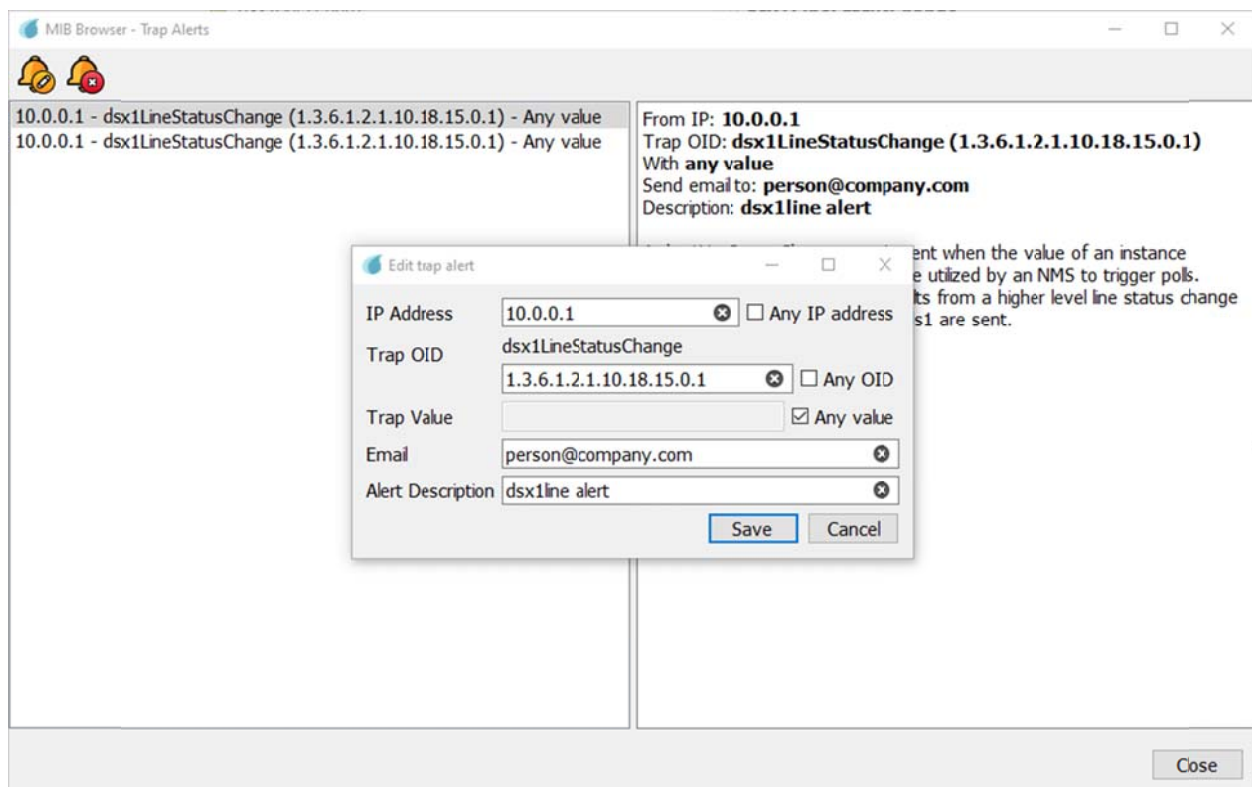
Right Panel (Details):

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.

Buttons: A 'Close' button is located at the bottom right.

Select the line item you wish to edit and click the bell-and-pencil symbol to modify it:

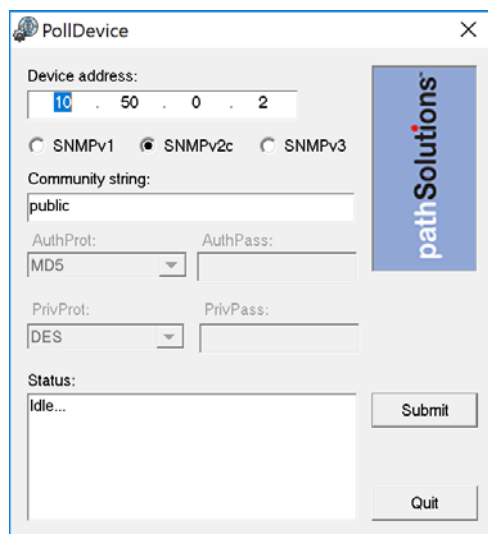


You may also delete any trap alert previously set up, in this submenu.

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

Poll Device Tool

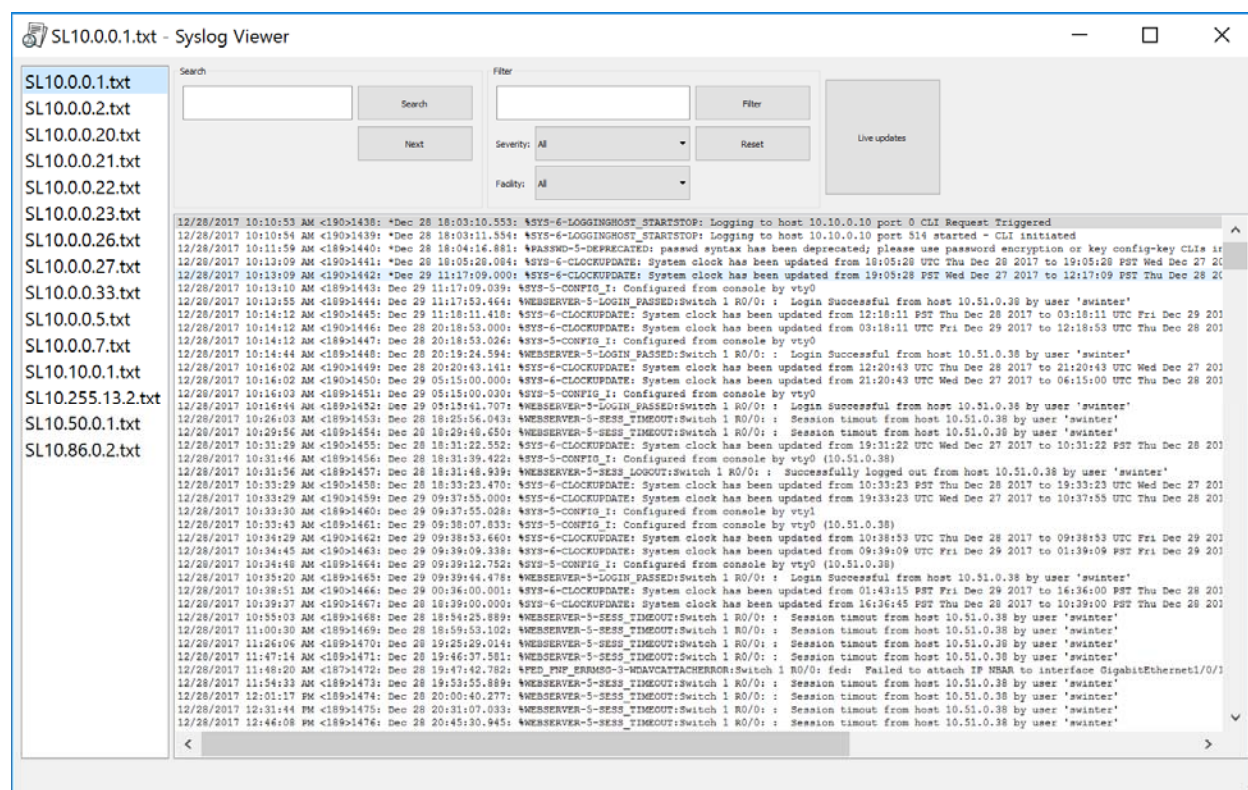
This is a simple test tool to verify that SNMP is communicating correctly. It is a stand-alone program and is run from the Start/Programs/PathSolutions/TotalView/Poll Device menu.

The screenshot shows the PollDevice application window. It has a title bar with a close button. The main area contains several input fields and radio buttons. The 'Device address' field is a dotted IP address field with '10', '50', '0', and '2' in the segments. Below it are three radio buttons: 'SNMPv1', 'SNMPv2c' (which is selected), and 'SNMPv3'. The 'Community string' field contains the text 'public'. There are two rows of authentication fields: 'AuthProt' with a dropdown menu showing 'MD5' and an empty 'AuthPass' field; and 'PrivProt' with a dropdown menu showing 'DES' and an empty 'PrivPass' field. At the bottom left is a 'Status' label above a text area that currently shows 'Idle...'. On the right side of the window is a vertical blue bar with the 'pathSolutions' logo. At the bottom right are two buttons: 'Submit' and 'Quit'.

Enter a device IP address and SNMP credentials and click “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.



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 choosing “Filter”.

Searching for text can be performed by entering text in the search field and clicking “Search” or “Next”.

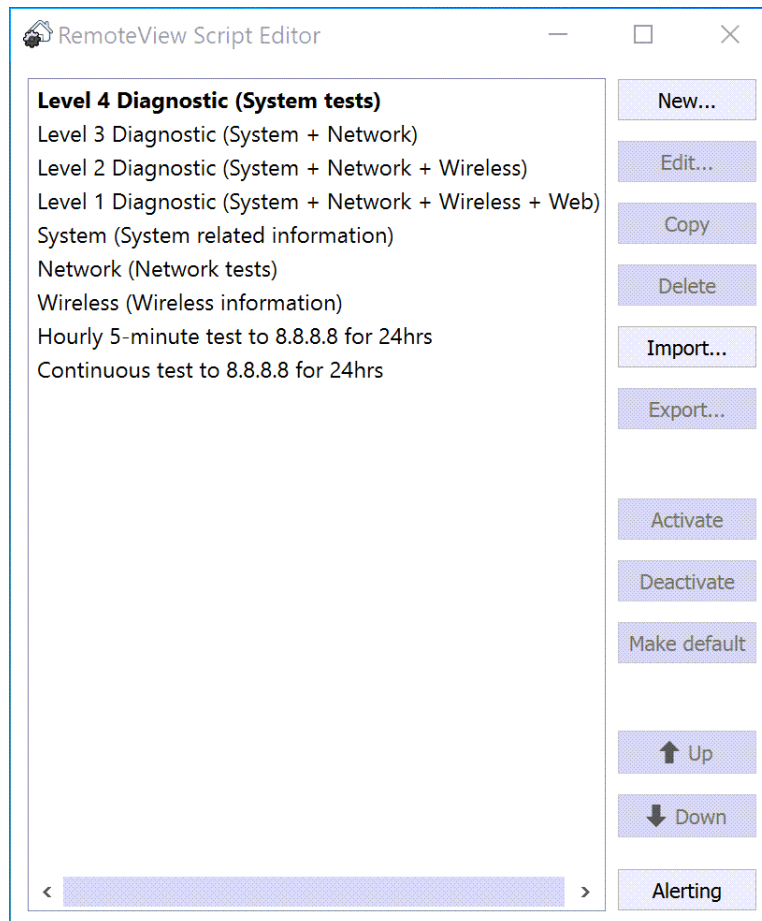
If you want to view newly received syslog messages from a device, click the “Live update” button to turn this feature on or off.

RemoteView Script Editor Tool

You have the ability to configure and create your own RemoteView batch scripts using this tool. To open the tool, click on "Start". Then choose "Programs", "PathSolutions", "TotalView", and "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.

Notice also you have buttons to select scripts and activate or deactivate them, and to make one a default:



To edit a script, select the script (the Level 4 Diagnostic is shown below), and select “Edit”. A dialog box will appear that gives you the ability 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:

Edit script

Name:

Description:

Logging: ☒ Server ☐ Local ☐ Both

Active: ☒

Tests:

-
-
-
-

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

Parameters:

note:

save_remote: ☒

notify:

You can add new commands to a script using the “Add” button. Then select a new command from the drop-down menu that will appear, then click “OK”.

Here is adding an end-to-end test:

The screenshot shows a 'Create new script' dialog box with the following fields and options:

- Name:** Call quality test script
- Description:** Script that tests for various call quality performance metrics
- Logging:** ☒ Server ☐ Local ☐ Both
- Active:** ☒

On the left side of the dialog, there are buttons: Add, Copy, Delete, Up, and Down. The 'Add' button is highlighted, and an 'Add new command' sub-dialog is open over the main dialog's content area.

The 'Add new command' sub-dialog has a 'Command:' label and a drop-down menu showing 'Test: End To End'. It has 'OK' and 'Cancel' buttons at the bottom.

At the bottom right of the 'Create new script' dialog, there are 'Save' and 'Cancel' buttons.

Here is 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: ☒

Add

Copy

Delete

↑ Up

↓ Down

Test: End To End

Parameters

duration60

address*

codecG.711(64)

calls10

dscp46

failed_if*...

note

save_remote☒

save_local...

notify☐

Save

Cancel

Here is setting the fail parameters on an end-to-end test:

The screenshot shows the 'Create new script' dialog box with the following fields and options:

- Name:** Call quality test script
- Description:** Script that tests for various call quality performance metrics
- Logging:** ☒ Server ☐ Local ☐ Both
- Active:** ☒

On the left side of the dialog, there are buttons: Add, Copy, Delete, Up, and Down.

An 'Edit parameter' sub-dialog box is open, showing the 'failed_if' section with the following parameters:

Parameter	Operator	Value
<input checked="" type="checkbox"/> QOS	<	4.0
<input type="checkbox"/> LOSS	>	0.5
<input type="checkbox"/> LATENCY	>	50
<input type="checkbox"/> JITTER	>	110

At the bottom of the 'Edit parameter' dialog are 'OK' and 'Cancel' buttons.

At the bottom of the main 'Create new script' dialog are 'Save' and 'Cancel' buttons.

Appendix A. Email Report Templates and Variables

Existing email report templates are located 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 rates
%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

If you desire to override the reported interface speed, you can enter the speed in bits per second here. For example: You may want 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 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:

```
;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 in order 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 ("jd@company.com")

Note: When entering the OID value, put 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, you will have to stop and restart the TotalView service for the changes to take effect.

Appendix G. Configuring Additional OUIs for Phones

A number of OUIs (Organizationally Unique Identifiers) for various VoIP equipment manufacturers have already been added to the OUIFilter.cfg file. This file can be edited with a text editor (like Notepad) to add additional OUIs.

```
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, you will have to 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):

```
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 that will 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):

```
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: You can 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. No need to stop and restart the service or collect re-collect information from switches & routers. This will help speed up troubleshooting and debugging of static routes in the environment.

Note: More likely, two static routes will 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 do this:

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 means we did not get any SNMP response from the device. The red dots mean that we did not get a 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 have to wait to see if we get a response. If we wait 2 seconds for the response and don't get one, we can send a second ping and then wait 2 seconds to get a response again. If we don't get a response from the second ping, then we should assume it is down.

TotalView's default does 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 now does 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, you can 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, you can 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 on a daily basis. 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.