pathSolutions

TotalView Administration Guide

earch Options (Ctrl+E)	TotalView			
/ TotalView	^	License Information		
Data Retention		Customer Number:		
➤ Email	pathSolutions:			
Alert Options	padroorations	Customer Location:		
Storage		Contact Name:		
Tech Support				
✓ Web Interface	TotalView	Contact Phone:		
API Keys	DathSolutions	Contact Email:		
Authentication	Factoriations			
Web Server	www.PathSolutions.com	MAC Address:		
Dashboard		Change (Malid	ato Liconco	
Weather Widget	Total Network Visibility®	Change / Valid	ate License	
Internet		Linear on Court		
Network	U.		404	
> Alerts		194 Licensed Interfaces x1	494	
Backup		20 <u>Servers</u> x 5	100	
		1 <u>Services</u> x 1	1	
		1 <u>Cloud</u> x 3	3	

NetOps | SecOps | Telecom Ops | Remotelnsight

PathSolutions, Inc.

www.PathSolutions.com

Support@PathSolutions.com

Sales@PathSolutions.com

Document and Software Copyrights

Copyright ©2024 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, RemoteInsight, Total Cloud Visibility, Total Network Visibility, and Total VoIP Visibility are Registered Trademarks of PathSolutions, Inc. in the United States and/or other countries. Network Weather Report and Network Prescription are Trademarks of PathSolutions, Inc. in the United States and/or other countries.

Version Information

TotalView Version: 14.2

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)



Contents

Conventions	Ę
Technical Support	5
Activation and Quick Config Wizard	6
Jsing the Configuration Tool	
Running the Configuration Tool	
Navigation	
Buttons	
Toolbars	
Restart Icon	
TotalView License Page	
Data Retention	1(
Email Configuration	1 [,]
Configuring the Weather Report	1 [,]
Configuring the Nightly Security Report	1 ⁻
Alert Options	
Storage	
Tech Support	
Web Interface	1!
Cloud Monitoring	2'
Dashboard Settings	22
Dashboard Authentication	2!
Internet Settings	27
NetAlly Settings	29
Network Monitoring	20
Δlerts	3(
Backup Configuration	23
BCP	
Custom OID	
Devices Configuration	
Ignored Error Counters	
Ignored Interfaces	
Ignored Type Nemee	
Interface Description	
Diagram (Interactive Diagrame)	
Favoriles	
IPAM	
Issues	
Maps	
Meraki	
NetFlow	
Network Thresholds	7
Polling Behavior	
Private IP	79
Syslog	80
TFTP Server	89
WAN Interfaces	90
NLT	
Remote Insight	9:
Reports	96
Risks Monitoring	96
Risks Alerts	98

	01
Dictionary	01
DNS (DNS Record Monitoring)10	02
Geographic	03
loT	04
Policies	06
Roque IT	09
Whitelist 1'	10
SD-WAN	11
Servers and Operating Systems	12
Linux Servers Monitoring	14
Windows Servers	21
Services	21
	21
	20
	30
	31
Phones	35
VoIP VLAN	36
SIP-Trunks	36
Using the Device Configuration Wizard	38
Re-Configuring TotalView When Your Network Changes14	42
Automatic Re-Configuration	43
Other Network Program Configuration Tools14	44
Interface Discovery Tool14	44
Config Editor14	47
Map Config Tool14	48
How to Add Maps14	49
How to Add Links1	51
How to Add Ping Points	52
How to Change Items on the Map	52
How to Delete Items on the Map	53
How to Save the Man	53
MIB Browser	54
	56
OID Monitoring	57
OID Granbing	60
SNIMD Tran Receiver Configuration	61
Poll Dovice Teel	67
	60
Sysiog viewei Tool	00
Remoternsignt Script Editor 1001	74
Appendix A. Email Report Templates and Variables	74
	78
Appendix B. SMTP Email Forwarding	79
Appendix C. Overriding Displayed Device Icons	80
Appendix D. Changing Interface Names and Speed	81
Appendix E. Contiguring Multiple Locations	82
Appendix F. Custom OID Monitoring	84
Appendix G. Configuring Additional OUIs for Phones	85
Appendix H. Changing the WAN Tab18	86
Appendix I. Adding a Static Route to the Call Path	87
Appendix J. Automatic Update Scheduling18	88
Appendix K. Changing the Map Fetch Variables to Improve Map Stability	89
Glossary	90

Conventions

The following conventions are used in this manual:

Italic

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

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

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

Bold

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

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

Technical Support

For technical support:

Support@PathSolutions.com

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

Activation and Quick Config Wizard

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

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

Using the Configuration Tool

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

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

Running the Configuration Tool

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

Navigation

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

2						_		×
Devices 📥 Cloud	<u>Serve</u>	rs 🔔 Services 📄 Reports						
Search Options (Ctrl+E)		TotalView						
 TotalView Data Retention Email Alert Options Storage Tech Support Web Interface API Keys* 	~	pathSolutions ⁻	License Information Customer Number: Customer Location: Contact Name: Contact Phone:	Steve Winter				^
Authentication Multi-Site Web Server Cloud V Dashboard Weather Widget		PathSolutions www.PathSolutions.com Total Network Visibility®	Contact Email: MAC Address:	swinter @pathsolutions 00-50-56-b2-42-65 Change / Valie	com date License			
Internet Network ✓ Alerts Device Alerts Parent/Child Route Alerts ✓ Backup Credentials Devices Schedule Variables ✓ Credentials		Service version: 14.2.14238 Config tool version: 14.2.110 Wizard version: 14.2.49 Call Simulator version: 8.0.8151 RemoteInsight version: 14.1.14120 Copyright 2025	License C 795 Lic 23 Ser 1 Servi 1 Clour 0 SD-V 0 SIP-T	ount ensed interfaces x 1 vers x 5 ces x 1 d x 3 (AN) x 3 Total used Licensed nsight License Count	795 115 1 3 0 0 914 250000			ļ
✓ BGP Alerts Peers Guttom OID	~	Copy version info to dipboard	Remotel	Insight Agents	100	Revert	Ap	≻ ply

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

Buttons

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

Add	Change	Delete	Shift Up	Shift Down

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

Revert Apply	Revert	Apply
--------------	--------	-------

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

Toolbars

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

Restart Icon

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



TotalView License Page

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

TotalView Configuration Tool					-		×
Cloud Servers	Services Reports						
Search Options (Ctrl+E)	TotalView						<u>ک</u>
✓ TotalView		License Information					
Data Retention		Customer Number:	_				
✓ Email	pathSolutions ⁻						
Alert Options		Customer Location:	: 1				
Tech Support		Contact Name:	Tim Titus				
✓ Web Interface	TotalView	Contact Phone:	408-748-1777				
API Keys	, otanion						
Authentication	PathSolutions	Contact Email:	demo@pathsolutior	ns.com			
Web Server	www.PathSolutions.com	MAC Address:					
Cloud X Dashboard			Change / Valig	late License			
Weather Widget	Total Network Visibility®		change / vail	duce Electrice			
Internet		License Cou	nt				
✓ Network		834 Licens	sed interfaces x 1	834			
✓ Alerts		0 Servers	x 5	0			
Device Alerts		1 Services	x 1	1			
✓ Backup		1 Cloud >	x 3	3			
Credentials	Service version: 14.1.14140	0 SD-WAN	<u>x</u> x 3	0			
Devices	Wizard version: 14.1.39	0 <u>SIP-Trur</u>	nks x3	0			
Schedule	Call Simulator version: 8.0.8151		Total used	838			
Variables	Remoteinsight version: 14.1.14115		Licensed	10000			
Custom OID	Copyright 2024	RemoteInsi	ght License Count				
✓ Devices	Copy version info to clipboard	RemoteInsi	ight Agents	5			
Ignored Error Counters							
Ignored Interfaces							
Ignored Type Names							
Laver-3 Excludes							
Layer-3 Ignores							
Layer-3 Static Links							
					Revert	Ap	ply
							4

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

License Information		\times	<
Enter your license information. All field	s are required for	validation.	
Customer Number:			
Customer Location:			
1			
Contact Name:			
Tim Titus			
Contact Phone:			
408-748-1777			
Contact Email:			
demo@pathsolutions.com			
MAC Address:			
	Check License	Cancel	

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

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

Data Retention

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

TotalView Configuration Tool					-		Х
Search Options (CityLE)	ces Reports						
Devices Cloud Servers Servit Search Options (Ctrl+E) TotalView Data Retention Email Storage Tech Support Web Interface Cloud Dashboard Internet Network NLT Remotelnsight Reports SD-WAN Servers Services VolP Services VolP Services VolP Services Servi	Reports Data Retention Associations Database: Cloud Information Database: Device Backups Database: Device/Interface Database: Linux Servers Database: NetFlow Database: NetFlow Database: Remote Insight Tests Database: SD-WAN Database: SIP-Trunks Database: Windows Servers Database:	32 • 5 • 96 • 96 • 30 • 30 • 90 • 5 • 5 • 30 •	days days days days days days days days	18 MB 4 MB 553 MB 10 MB 56 KB 7 MB 13 MB 256 KB 324 KB			
					Revert	Арр	ły

Email Configuration

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

arch Options (Ctrl+E)	Email						
TotalView Data Retention	Mail Server A	Address: 10.0.0.10		Port: 25			
> Email Storage	Encryption:	● None ○ TLS ○ SSL	Authenticate				
Tech Support	Send from:	LAB-Velma-Reports@PathSolutions.com	Username:				
> Web Interface Cloud Dashboard		Example: noc@company.com	Password:				
Internet Network	Send d	aily network "Weather Report"					
NLT Remotelnsight	The "Weat	ther Report" can help you keep track of your n	etwork health on a daily basis.	Send Wea	ther Report Now		
Reports	Send to:	swinter@pathsolutions.com			Test		
Risks		Example: jdoe@hotmail.com, flb@aol.com					
SD-WAN Servers Services VolP	This rep	This report can be customized to include specific information, or simply provide an overview of general health. Edit Report					
	Send N	lightly Security Report					
	A nightly s	security report showing footprint, exposures a	Send Sec	urity Report Now			
	Send to:	swinter@pathsolutions.com;ttitus@pathsolu	itions.com		Test		
		Example: jdoe@hotmail.com, flb@aol.com					

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

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

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

Configuring the Weather Report

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

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

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

Note: The report uses MIME encoding to allow email readers to respect the content as HTML formatted content. If you need assistance with modifying this report, and do not understand MIME encoding, refer to the IETF's RFC1521 (www.ietf.org) or contact PathSolutions Technical Support for assistance support@pathsolutions.com.
 Note: Do NOT put a period (".") on its own line anywhere in this file.

Configuring the Nightly Security Report

If you have the Security Operations Manager module, you can get a nightly security report sent to your mailbox that has a summary of your security posture. If you want to receive the Nightly Security Report, select the **Send Nightly Security**

Report checkbox and enter one or more email addresses who should receive the report. Separate each email address with a space, comma, or semicolon

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

Alert Options

TotalView Configuration Tool				_		\times
🔀 Devices 📥 Cloud 🗐 Servers 🔔 Servi	ces <mark>Report</mark>	3				
Search Options (Ctrl+E)	Alert Options					
✓ TotalView	ID Prefix	Alert After	Email Priority			
Data Retention	default	1 poll	Not Set			
Storage Tech Support > Web Interface Cloud > Dashboard Internet > Network NLT > RemoteInsight Reports > Risks SD-WAN						
 > Servers Services > VoIP 	Add	Change Dr	elete Shift Up Shift Down Reset Sort			
			Rev	ert	App	y y

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

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

 Alert every poll Send alert every poll while the value exceeds the threshold, then once when the value normalizes. Alert after 1 polls Send alert once after the value exceeds the threshold for specified number of polls, then once when the value normalizes. Email priority: Not Set 	Prefix:	default
 Send alert every poll while the value exceeds the threshold, then once when the value normalizes. Alert after 1 polls Send alert once after the value exceeds the threshold for specified number of polls, then once when the value normalizes. Email priority: Not Set 	Alert	every poll
 Alert after 1 polls Send alert once after the value exceeds the threshold for specified number of polls, then once when the value normalizes. Email priority: Not Set 	Sen the	ad alert every poll while the value exceeds the threshold, then once when value normalizes.
Send alert once after the value exceeds the threshold for specified number of polls, then once when the value normalizes. Email priority: Not Set	Alert a	after 1 polls
Email priority: Not Set	Sen	ad alort once after the value exceeds the threshold for specified number of
Email priority: Not Set	noll	is then once when the value pormalizes
	poll	Is, then once when the value normalizes.
	poll Email pric	Is, then once when the value normalizes.
	poll Email pric	Is, then once when the value normalizes.
	poll	Is, then once when the value normalizes.
	poll	Is, then once when the value normalizes.

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

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

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

Storage

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

TotalView Configuration Tool		-		×
Search Ontions (Chrl +F)	storage			A
Search Options (Ctrl+E)	Storage Application folders: Data (including Netflow) 14.3 GB / 16.5 GB free on drive C:\ C: \Program Files (x86)\PathSolutions\TotalView\DATA Netflow 13.6 GB / 16.5 GB free on drive C:\ C: \Program Files (x86)\PathSolutions\TotalView\DATA Syslog 382 MB / 16.5 GB free on drive C:\ C: \Program Files (x86)\PathSolutions\TotalView\SYSLOG Device Backup Logs 334 MB / 16.5 GB free on drive C:\			٨
> VolP	C: \Program Files (x86) \PathSolutions\TotalView \DeviceBackup Clear TFTP 26 MB / 16.5 GB free on drive C:\ C: \Program Files (x86) \PathSolutions\TotalView \TFTP Clear			
		Revert	App	ly

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

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

Tech Support

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

Secretes Cloud Services Services Search Options (Ch1+E) Tech Support Service Account ✓ IotalView Data Retention ✓ Ensil A left Options Storage Tech Support > Web Interface Cloud > Dashboard Internet > Network Network Network Service Status Service is running Start Service account (PATHSOLUTIONS/swinter Change Account groups: Administrators, Users Service Status Service Status Service Status Service is running Start Service automatically upon system startup Resports Services VolP VolP VolP URL Check URL Check URL Check Deserver: sub01.insubscription.com OK Network Device COS Winerability checks: https://noi.nit.cov/ OK P Gountry Usit VRI: https://noi.nit.cov/ OK OUI Manufacturer list: https://lowindad.co.on/lise/P2.OCATION+ITE-DB1.CSV.ZP OK OUI Manufacturer list: https://lowindad.co.on/lowindad.co.on/lise/P2.OCATION+ITE-DB1.CSV.ZP OK OUI Manufacturer list: https://lowindad.co.on	TotalView Configuration Tool				-	×
Search Options (CtH+E) Tech Support ✓ Total/liew Data Retention ✓ Email Alert Options Alert Options Service account: Partial Alert Options Storage Change Account groups: Administrators, Users Octod Service Status > Dashboard Service Status Internet Service account: NUT Start Service With Reports > Network Start Service actomatically upon system startup Reports Sarvices Service: > Network NUT URL Check URL Check Usense server: Services ViolP > VoiP ViolP > VoiP Pladdet UR1: > Meakid UR1: https://wid.ist.dov OUTry List UR1: https://wid.ist.dov OUTry List UR1: https://wid.ist.dov > VoiP ViolP	Cloud Servers 🔊 Servi	ces Reports				
✓ TotalView Data Retention ✓ Email Alert Options Alert Options Service account: PATHSOLUTIONS/pwinter Change Account groups: Administrators, Users Tech Support Service Status > Web Interface Service Istatus Cloud Service Istatus > Dashboard Service is running Network NLT > Remotelnsight Resports Sprives Start Service automatically upon system startup URL Check Ucense server: Services Service OS Vulnerability checks: > VolP VolP VolP P Country List URL: Dedidst URL: https://dowlbad.pSocation.com OK OK P Gootory URL URL: https://dowlbad.pSocation.com/list.pop VolP OVIP VolP OK P Country List URL: https://dowlbad.pSocation.com/list.ps.cov.znp OUT Manufacturer Ist: https://dowlbad.pSocation.com/list.ps.com/list.ps Network Device OS Vulnerability checks: https://dowlbad.pSocation.jt.pdf P Edidst URL: https://dowlbad.	Search Options (Ctrl+E)	Tech Support				۵
Event Log Log Level nvF 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Search Options (CH1+E) V Total/View Data Retention V Email Alert Options Storage Tech Support > Web Interface Cloud Dashboard Internet > Network NLT > RemoteInsight Reports > Risks SD-WAN > Services > VoIP	Service Account Service Account Service account: PATHSOLUTIONS\s Account groups: Administrators, Use Service Status Service is running Start Service VIL Check License server: Network Device OS Vulnerability checks: IP Blackist URL: IP Country List URL: Geolocation information: OUI Manufacturer list: Merak API: Event Log Log Level D 0 0	winter rs Restart Service tem startup sub01.nlsubscription.com https://mvd.nist.gov https://download.jp2location.com/ite/IP2LOCATION-I https://download.jp2location.com/ite/IP2LOCATION-I https://download.jp2location.com/ite/IP2LOCATION-I https://download.jp2location.com/ite/IP2LOCATION-I https://download.jp2location.com/ite/IP2LOCATION-I https://opi.merais.com/api/r1/organizations 0 0 0 0 0 0 0 0	Stop Servic OK OK	Change re	×

Web Interface

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

Search Options (Ctrl+E) Web Interface	
Search Options (Ctrl+E) Web Interface	
TotalView API Keys: This configures API keys for the web server.	
Data Retention Authentication: This configures how users are permitted to login to the web server.	
Alert Options Web Server: This configures how the web server operates. Storage Tech Support > Web Interface Cloud > Dashboard Internet > Network NLT > RemoteInsight Reports > Risks SD-WAN > Services > VolP	

API Keys

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

TotalView Configuration Tool					-		×
Cloud Servers Service	es <mark>Reports</mark>						
Search Options (Ctrl+E)	API Keys						
TotalView	Name	API Key	Expires	Role			
 Versite All Art All Art Options Storage Tech Support Web Interface API Keys Authentication Web Server Cloud Dashboard Internet Network NLT Remotelnsight Reports Risks SD-WAN Servers Services VolP 	Test	Soff8e86b-e0b2-43d4-93c1-033014a3635f	Unlimited	TV-Users			
					Revert	App	ly

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

Kev Name:*				
API Key:	bb117721-d	799-4d9a-b377-46b8631abb17		Generate
Expires:	O Unlimite	d		
		5/23/2024 11:03 AM		
Role:*				
			OK	Cancol

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

You can also set an expiration date on the key.

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

Authentication

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

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

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

Cloud Servers Services Reports	
Search Options (Ctrl+E) Authentication*	
▼ TotalView Data Retention > Email Alert Options Storage Tech Support > Web Interface API Keys Authentication* Web Server Cloud Dashboard Internet Nearly > Network NLT > Reports Services > VolP VolP	pply

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

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

TotalView Configuration Tool*					-	- 🗆	×
🔀 Devices 📥 Cloud 🗐 Servers 🔔 Servi	ces Report	<u>s</u>					
Search Options (Ctrl+E)	Authenticatio	n*					δ
 ✓ TotalView Data Retention ✓ Email Alert Options 	O None) Internal (Active Director	ry () Radius			
Storage	Name			Role			
Tech Support	admin			TV-Users			
✓ Web Interface							
API Keys							
Web Server							
Cloud							
> Dashboard							
Internet							
NetAlly	Add	Change	Delete	Reset Sort			
> Network	Poles						
NLI Remotelosiaht	Roles			1			
Reports	Role			Access			
> Risks	TV-Users			*, @pscan, @pcontrol,	@vulnerability, @svccontrol,	@bckpcont	rol
SD-WAN							
> Servers							
Services							
> VoIP							
	Add	Change	Delete	Reset Sort			

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

TotalView Configuration Tool		-	\times
Cloud Servers Servin	ces Reports		
Search Options (Ctrl+E)	Authentication		۵
V TotalView Data Retention	○ None ○ Internal	tory O Radius	
✓ Email	AD Security Group	Access	
Alert Options Storage	TV-Users	*, @pscan, @pcontrol, @vulnerability, @svccontrol, @bckpcontrol, @scriptcontrol, .	
Tech Support			
Veb Interface			
Authentication			
Web Server			
Cloud			
Internet			
> Network			
NLT Nerrotelesieht			
Reports			
> Risks			
SD-WAN			
Services			
> VoIP			

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

TotalView Configuration Tool*		– 🗆 X
🔀 Devices 🔺 Cloud 🗐 Servers 🔔 Servic	<u>ces</u> <mark>Reports</mark>	
Search Options (Ctrl+E)	Authentication*	٨
 TotalView Data Retention Email Alert Options Storage Tech Support Web Interface API Keys Authentication* Web Server Cloud 	None Internal Active Directory Server address:*	y Radius
> Dashboard	Role	Access
Internet	TV-Users	*, @pscan, @pcontrol, @vulnerability, @svccontrol, @bckpcontrol
NetAlly NetWork NLT Reports Risks SD-WAN Servers Services VolP	Add Change Delete	Reset Sort
		Revert Apply

Web Server

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

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

TotalView Configuration Tool					-		×
Search Options (Ctrl+E)	Web Server						δ
 ✓ TotalView ▲ Email Alert Options Storage Tech Support ✓ Web Interface Authentication Web Server Cloud 	Web Server Options Web Page Reload: Unlock Web Configur Records to list on the Built-in Web server to Built-in Web server p	0	View Web Page				
✓ Dashboard Weather Widget	Certificate		Access Control List:				
Internet NetAlly VetWork Alerts BGP Alerts Device Alerts Route Alerts Backup Credentials Devices Schedule Variables Custom OID Devices Variables Custom OID Devices Variables Custom OID Devices	Server Certificate: Date is valid. Private key match Valid: Subject: Alternative names: Issuer: Generate CSR:	View Full Info hes the certificate. 8/22/2023 10:31 PM – 8/21/2024 4:55 PM C = US, ST = California, L = Santa Clara, O = PathSolutions, OU = IT Operations, CN = *.pathsolutions.local DNS:*.pathsolutions.local DC = local, DC = pathsolutions, CN = pathsolutions-DAPHNE-CA Generate Certificate Request	The list is empty. Any client can access the web server.				
Layer-3 Ignores Layer-3 Static Links Favorites Financials	Import Certificate:	Import KEY file Import Certificate file Validate Certificate					
ignored Interfaces Ignored Type Names Issues Maps	Restore Certificate:	View Backup Certificate	Edit list				
Meraki NetElow				R	evert	Ap	ply .:

The Web page reload allows for global setting to have web pages refresh after a set number of seconds. This will affect all pages viewed on the site. To change an individual page's refresh, AutoRefresh.cfg can be modified to specify the page and refresh interval for that page.

The web front-end can be unlocked with the checkbox to permit removing individual interfaces from being monitored as well as add interfaces to the WAN and global Favorites list.

The next field controls how many records to list on the "Top-10" list.

The built-in webserver can use either HTTPS (recommended) or HTTP for communications. The webserver port can be overridden to be any port desired as long as it is not used on the server.

There are certificate handling capabilities on this page allowing you to create a certificate request and then import the KEY file and certificate file after they are generated by your certificate authority.

You can add an access control list to only permit certain IP addresses or subnets to use the web pages.

Cloud Monitoring

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

Tatallian					
Cloud	Find: Group, Address, Nam	e			
Dashboard	Group	Address	Name	Latency, ms	Loss,
Internet	Internal	10.51.0.1	TX-FW1		
NET	Internal	10.51.30.5	TX_Lab_Switch		
Remotelnsight	Internal	10.50.0.1	SV-FW		
Reports	Reflectors-ICMP	chi01.pathsolutions.com	Chicago (chi01.pathsolutions.com)		80
Risks	Reflectors-ICMP	nj01.pathsolutions.com	New Jersey (nj01.pathsolutions.com)		80
SD-WAN	Reflectors-ICMP	sea01.pathsolutions.com	Seattle (sea01.pathsolutions.com)		80
Services	Remote_Site_RR-ICMP	10.51.0.1	Round Rock FW		80
VoIP	Remote_Site_RR-ICMP	10.51.0.5	Round Rock SW3		80
	Remote_Site_SV-ICMP	10.50.0.1	Sunnyvale FW		80
	Remote_Site_SV-ICMP	10.50.0.4	Sunnyvale Shed SW1		80
	Web	www.pathsolutions.com	PS Website		80
	Web	www.google.com	Google Search		
	Web	admin.office.com	Office 365 Admin Page		

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

🚀 Change	Cloud Se	rvice	×				
Group:	0-HQGe	ar	~				
Address:	8.8.4.4						
Name:	Google [oogle DNS Secondary					
Icon:	GoogleC	loud.png					
DSCP:	0						
Email A	lerts						
Email:			~				
Latency th	reshold:	0					
Loss thres	hold:	0					
Route	change						
		ОК	Cancel				

Dashboard Settings

The Dashboard page allows controlling dashboard widgets.



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

Weather Widget Page

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

2			-		×
Cloud Servers	vices Reports				
Search Options (Ctrl+E)	Weather Wid	t i i i i i i i i i i i i i i i i i i i			
Alert Options	∧ Site name	Coordinates			
Storage	once nume				
Tech Support	Santa Clara	37.3784579, -121.9678433			
✓ Web Interface	Washington	38.8976667, -77.0365371			
API Keys	The Alamo	29.4260629, -98.4861715			
Authentication					
Web Server					
Cloud					
✓ Dashboard					
Weather Widget					
Internet					
✓ Network					
✓ Alerts					
Device Alerts					
Route Alerts					
✓ Backup					
Credentials					
Devices					
Schedule					
Variables					
✓ BGP					
Alerts					
Peers					
Custom OID					
✓ Devices					
Ignored Error Counters					
Ignored Interfaces					
Ignored Type Names					
Interface Description					
✓ Diagram					
Layer-3 Excludes					
Layer-3 Ignores					
Layer-3 Static Links					
Favorites					
* IPAIVI					
Incurs					
Mang					
Maps					
NetFlow					
Network Thresholds					
Polling					
System					
TETP					
WAN					
NLT					
✓ Remotelnsight					
Script Editor					
Web Server	Add	Delete Beest Sert			
Poporte	✓ A00	Reset Sort			
			Revert	Ap	ply



The resulting weather dashboard widget will look like this

Dashboard Authentication

You can optionally create a Dashboard URL that doesn't require Authentication for NOC monitoring computers. Create a role (TotalView -> Web Interface -> Authentication) with Dashboard Only view

TotalView Configuration Tool*		- 🗆 X
Cloud Serve	rs Services Reports	
Search Options (Ctrl+E)	Authentication	▲
✓ TotalView Data Retention	None Internal Active D	irectory ORadius
✓ Email	AD Security Group	Access
Alert Options	Default	*, @pscan, @vulnerability, @pcontrol, @svccontrol, @bckpcontrol
Tech Support	TV-Users	*, @pscan, @pcontrol, @vulnerability, @svccontrol, @bckpcontrol
Veb Interface	Dashboard Only	Dashboard
API Keys*		
Authentication		
Multi-Site		
Goud		
✓ Dashboard		
Weather Widget		
Internet		
✓ Network		
✓ Alerts		
Device Alerts		
Parent/Child		
Route Alerts		
Credentials		
Devices		
Schedule		
Variables		
✓ BGP		
Alerts		
Peers V	Add Change Delete	Reset Sort
(ustom (III)		
		Revert Apply

Create an API with the view selected.

- 1) Go to TotalView -> Web Interface -> API Document section
- 2) Create and API Key with a Dashboard only Restricted View.

At this point, you can use the API in a HTTP call to display the Dashboard Information without Login required.

If you create an API key and then use it as part of the URL for the dashboard, a logged in user on a NOC monitoring machine should have continuous access to the dashboard information after the service is restarted:

Example:

https:/<TotalViewServer>/dashboard.html?api_key=<API Key with no brackets>



Internet Settings

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

濴 TotalView Configuration Tool		-		×
Cloud Servers	Services Reports			
Search Options (Ctrl+E)	Internet			δ
 TotalView Data Retention Email Alert Options Storage Tech Support Web Interface API Keys Authentication Web Server Cloud Dashboard Weather Widget Internet Network Alerts Device Alerts Route Alerts Backup Credentials Devices Schedule Variables BGP Custom OID Devices Ignored Error Counters Ignored Type Names Diagram Layer-3 Excludes Layer-3 Static Links 	Internet Lookup Name: www.google.com Remote DNS Server: 8.8.8.8	vevert	Δησίο	V
		Cyclt	App	7 .::/

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

NetAlly Settings

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

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

TotalView Configuration Tool*		_		×
Cloud Servers Services	es Reports			
Search Options (Ctrl+E)	NetAlly			6
> TotalView Cloud > Dashboard Internet NetAlly > Network NLT > RemoteInsight Reports > Risks SD-WAN > Servers Services > VoIP	brack NetAlly Link-Live Integration Login: Password:	Devert	Âm	
		kever(Арр	

Note: If the NetAlly tab does not show up on your deployment, contact <u>support@pathsolutions.com</u> for it to be enabled.

Network Monitoring

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

TotalView Configuration Tool			_		Х
Cloud Servers Servi	ces Reports				
Search Options (Ctrl+E)	Network Config	juration Group			
> TotalView	This section configu	res network related communications and alerts.			^
Cloud	Alerts:	This allows communications alerts relating to network devices and interfaces.			
Dashboard Internet Network	Backup:	This section configures SSH communications with network devices to perform device backups a management.	and config	guration	
NLT	BGP:	This configures BGP alerting for peers.			
> Remotelnsight Reports	Custom OID:	Configures custom OIDs to be monitored and associated with a device/interface.			
> Risks	Devices:	This configures SNMP communications with network devices.			
SD-WAN	Diagram:	This configures the dynamic network diagram to include or exclude subnets and devices.			
Services	Favorites:	This configures interfaces to show on the Favorites tab.			
> VoIP	Financials:	This configures information to show on the Financials tab.			
	Issues:	This shows what types of issues will show up on the Issues tab.			
	Maps:	This configures network maps on the Maps tab.			
	Meraki:	Configures Meraki API key.			
	NetFlow:	This configures interfaces that are NetFlow enabled.			
	Network Thresholds	: This changes the network visual alert threshold levels.			
	Polling:	This configures the polling timeframe and behavior.			
	Syslog:	This enables and configures syslog alerts.			
	TETP:	This enables and configures the TFTP server.			
	WAN:	This configures the interfaces to show on the WAN tab.			
					~
		Ret	vert	Арр	ly .:i

Alerts

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



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

Device Alerts

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

TotalView Configuration Tool						-		×
Search Options (Ctrl+E)	Device Alerts							
> TotalView ^	Device name	IP address	Alert type	Email	TX	RX	Err	St
Cloud		Any	Communication Failure	swinter@pathsolutions.com				
Internet								
✓ Network								
✓ Alerts								
Device Alerts								
Route Alerts								
BGP								
Custom OID								
> Devices								
> Diagram								
Financials								
Issues								
Maps								
Meraki								
NetFlow Network Thresholds								
Polling								
Syslog								
TFTP								
WAN								
> Remotelnsight	<							>
Reports								
> Risks 🗸	Add Ch	hange De	elete Rese	tSort				
					_	_		_
					Rev	ert	App	ly
								:

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

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

😻 Add Alert	×
Email address:	itops@pathsolutions.com ~
Description:	utilization
IP address:	Any ~
Alert type:	O Device Communications Failure
	O Cisco CPU Utilization 80
	O Cisco free RAM 4096 bytes
	O MOS score 3.4 🜩
	○ Spanning-Tree topology change
	O Any Interface
	O Interface Number(s) (i.e. 1,5,7-10)
	O 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
	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 select Any from the IP address field to match any device or device group.

Choose a device-related alert like the following:

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

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

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

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

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

Group Alerting

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

🛿 🌮 Add Alert	×
: Email address:	itops@pathsolutions.com ~
Description:	рое
IP address:	Any from group "Chicago"
Alert type:	O Device Communications Failure
	O Cisco CPU Utilization 80 💂 %
	O Cisco free RAM 4096 bytes
	O MOS score 3,4 (♣)
	○ Spanning-Tree topology change
	Any Interface
	O Interface Number(s) (i.e. 1,5,7-10)
	O Interface Description
	O Interface Type other V 1
	O Infrastructure Interface
Tx Utilization:	80 💂 percent utilized
Rx Utilization:	80 🖕 percent utilized
Error percentage:	10 🔶 percent packet lost
Status change:	PoE change \checkmark
	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 select **Add**.

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

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

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

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

Email address: itops@pathsolutions.com Description: poe IP address: Any from group "Chicago" Alert type: O Device Communications Failure O Cisco CPU Utilization 80 + % O Cisco free RAM 4096 MOS score 3.4 + O Spanning-Tree topology change Interface O Interface Number(s) (i.e. 1,5,7-10)	
Interpretation Interpretation Description: poe IP address: Any from group "Chicago" Alert type: O Device Communications Failure O Cisco CPU Utilization 80 ÷ % O Cisco free RAM 4096 MOS score 3.4 ÷ O Spanning-Tree topology change Interface O Interface Number(s) (i.e. 1,5,7-10)	Л
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)	
Alert type: Device Communications Failure O Cisco CPU Utilization 80 + % O Cisco free RAM 4096 bytes MOS score 3.4 + Spanning-Tree topology change Image: Any Interface Interface Number(s)	
 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) 	
 Cisco free RAM 4096 bytes MOS score 3.4 + Spanning-Tree topology change Any Interface Interface Number(s) (i.e. 1,5,7-10) 	
 MOS score 3.4 + Spanning-Tree topology change Any Interface Interface Number(s) (i.e. 1,5,7-10) 	
 Spanning-Tree topology change Any Interface Interface Number(s) (i.e. 1,5,7-10) 	
Any Interface Interface Number(s) (i.e. 1,5,7-10)	
 Interface Number(s) (i.e. 1,5,7-10) 	
O Interface Description	
○ Interface Type other ∨ 1	
O Infrastructure Interface	
Tx Utilization: 80 💂 percent utilized	
Rx Utilization: 80 🖕 percent utilized	
Error percentage: 10 🖕 percent packet lost	
Status change: PoE change	~
OK Cancel	

Parent/Child

This feature is used to establish relationships between devices for alerting notifications. If the parent is unresponsive the children will not alert.

2		– 🗆 ×	(
Cloud Servers Devices	s Reports		
Search Options (Ctrl+E) Pare	ent/Child	A	5
✓ Email	ice name	IP address	٦.
Alert Options	Santa Clara/Surah	10001	4
Storage	Santa Clara/Syran	10.001	
Tech Support	Santa Clara/SantaClara.pathsolutions.iocal	10.0.0.2	
✓ Web Interface	Santa Clara/tempranilio.pathsolutions.iocal	1000.7	
API Keys	Santa Clara/Michelob	1000.12	
Authentication	Santa Clara/Burgundy	10.0.19	
Multi-Site	Santa Clara/Chardonnay	10.0.20	
Web Septer	Santa Clara/Pinot	10.0.21	
Claud	Santa Clara/Merlot	10.0.22	
Cloud .	Santa Clara/Muscat	10.0.23	
* Dashboard	Santa Clara/Palomino	10.0.0.28	
Weather Widget	Santa Clara/Riesling	10.0.0.29	
Internet	Santa Clara/Dubonnet	10.0.032	
 Network 	Santa Clara/barleywine	10.0.033	
✓ Alerts	Santa Clara/Alsace	10.0.039	
Device Alerts	Santa Clara/hof140d-poe	10.0.46	
Parent/Child	Santa Clara/houns1	10.0.120	
Route Alerts	Santa Clara/PS OpenGear	10.0.250	
✓ Backup	Sunna clara/FS_Opendeal	10.50.1	
Credentials	Supported Street and a state of the set	10.50.0	
Devices	Sunnyvale/Sunnyvale.pathsolutions.local	10.00.2	
Schedule	Sunnyvale/Tim's sysw2-sned	10.00.04	
Variables	Sunnyvale/svap1-office	10:00.5	
× BGP	Sunnyvale/svap2-shed	10.30.06	
Alerts	Sunnyvale/HardCider	10.50.07	
Deer	Sunnyvale/Chianti	10.50.0.10	
Custom OID	Sunnyvale/Tim's svsw1-office	10.50.0.142	
Custom of D	Sunnyvale/UBNT	10.50.0.174	
* Devices	Sunnyvale/svfw1	10.50.0.250	
Ignored Error Counters			
Ignored Interfaces			
Ignored Type Names			
Interface Description*			
✓ Diagram			
Layer-3 Excludes			
Layer-3 Ignores			
Layer-3 Static Links			
Favorites			
Einancials			
Y IPAM			
IPAM Subpets			
Institutes			
Mana			
Maghi			
Net Flere			
NetFlow			
Network Thresholds			
Polling			
Private IP			
Syslog			
TFTP			
WAN			
✓ Remotelnsight			
Script Editor			
Web Server			
Reports			
✓ Risks			
Alerts			
Contificator			
Dictionant			
Dictionary			_
bha Li cruu	top-level device Add child device Delete		
Geographic	Delete		
			-
		Revert Apply	

Select the top level(parent) and then choose the children devices.

Select top-level devices

Group	Device name	IP Address	^
Santa Clara	Syrah	10.0.0.1	
Santa Clara	SantaClara.pathsolutions.local	10.0.0.2	
Santa Clara		10.0.0.6	
Santa Clara	tempranillo.pathsolutions.local	10.0.0.7	
Santa Clara	Michelob	10.0.0.12	
Santa Clara	Burgundy	10.0.0.19	
Santa Clara	Chardonnay	10.0.0.20	
Santa Clara	Pinot	10.0.0.21	
Santa Clara	Merlot	10.0.0.22	
Santa Clara	Muscat	10.0.0.23	
Santa Clara	Palomino	10.0.0.28	
Santa Clara	Riesling	10.0.0.29	
Santa Clara		10.0.0.30	
Santa Clara	Dubonnet	10.0.0.32	
Santa Clara	barleywine	10.0.0.33	
Santa Clara	Alsace	10.0.0.39	
Santa Clara	hqf140d-poe	10.0.0.46	
Santa Clara	hqups1	10.0.0.120	
Santa Clara		10.0.0.137	
Santa Clara	PS_OpenGear	10.0.0.250	
Sunnyvale	svfw1	10.50.0.1	
Sunnyvale	Sunnyvale.pathsolutions.local	10.50.0.2	
Sunnyvale	Tim's svsw2-shed	10.50.0.4	
Sunnyvale	svap1-office	10.50.0.5	
Sunnyvale	svap2-shed	10.50.0.6	
Sunnyvale	HardCider	10.50.0.7	
Sunnyvale	Chianti	10.50.0.10	
Sunnyvale	Tim's svsw1-office	10.50.0.142	
Sunnyvale	UBNT	10.50.0.174	
Sunnyvale	svfw1	10.50.0.250	
Santa Clara	titos	10.0.0.13	¥

OK

Cancel

 \times
Route Alerts

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

arch Options (Ctrl+E)		Route Alerts						
TotalView	^	Device name	IP Address	Route	Mask	Туре	Alert	
Cloud		HQ FW/hqpa450	10.86.0.5	0.0.00	0.0.00	ACD	swinter@pathso	lutions.cr
Dashboard								
Network								
Device Alerts								
Route Alerts								
> Backup								
BGP								
Custom OID								
> Devices								
> Diagram								
Favorites								
Financials								
Issues								
Maps								
Meraki								
NetFlow								
Network Thresholds								
Polling								
тетр								
WAN								
NLT								
Remotelnsight		<						
Reports								
Risks	~	Add Ci	hange De	ete	Reset Sort			

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

🐉 Change	Route Alert ×
IP Address:	Any ~
Route:	10.51.30.0
Mask:	255.255.255.0
Type:	Add I Change I Delete
Alert email:	$\fbox{itops@pathsolutions.com} \lor$
Note:	Change to Houston Routes
	OK Cancel
	······································

Backup Configuration

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

TotalView Configuration Tool		-		×
Cloud Servers	rvices Reports			
Search Options (Ctrl+E)	SSH Authorization			
Devices Cloud Servers Set Search Options (Ctrl+E) TotalView Cloud Dashboard Internet Network Alerts Backup BGP Custom OID Devices Diagram Favorites Financials Issues Maps Meraki Nettrow Thresholds Polling Syslog TFTP WAN NLT	vices Reports SSH Authorization The authorization password has been configured. This password is required to be used anytime changes are made to device configurations with the Config Change Wizard. Change password Change password Reset password Credentials: This configures the SSH credentials used to login to network devices. Devices: This configures the devices to use the SSH credentials. Schedule: This configures the schedule and script to perform backups. Variables: This configures custom variables to be used in scripts.			
 Remotelnsight Reports Risks SD-WAN SD-WAN 				
> Servers	R	evert	Арр	ly .:

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

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

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

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

Credentials

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

Ceck Codd Internet Network Alets Backup Ordeentials Divices Backup Obvices Backup Ovirables BGP Custem OlD Disgramn Favorites Polling VAN NLT VAN	TotalView Configuration Tool		-		×
Vectorities Vectorities V TotalView Could Dashboard Internet Network Sackup Credentials Devices Schedule Variables BGP Custom OID Devices Financials Issues Maps Meraki NetFlow Network Thresholds Polining Systog TFTP WAN NLT Remotelnsiaht 	Court Outine (Colum)	es Reports			
TotaWiew ^ Coud	Search Options (Ctri+E)	Credentials			<u>_</u>
Revert Apply	 TotalView Cloud Dashboard Internet Network Alerts Backup Credentials Devices Schedule Variables BGP Custom OID Devices Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight 	Enter the Device Authorization password:			
		Rev	ert	Appl	y

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

TotalView Configuration Tool*		_	×
Cloud Servers 🔔 Services	es Reports		
Search Options (Ctrl+E)	Credentials		
> TotalView	Credential name		
Cioud	swinter		
Internet	SW PAN		
NetAlly	HP Manager		
✓ Network	psbadmin		
> Alerts			
✓ Backup			
Credentials			
Devices			
Schedule			
Variables			
BGP			
Custom OID			
Discours			
> Diagram			
Favorites			
Mans			
Meraki			
NetFlow			
Network Thresholds			
Polling			
Syslog			
TFTP			
WAN	Add Change Delete Deset Sort		

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

TotalView Configuration Tool*		_		\times
Devices Loud Server	Services Reports			
Search Options (Ctrl+E)	Credentials			۵
TotalView Cloud Dashboard	Credential name swinter			
Internet NetAlly	SW PAN SW PAN X			
 Alerts Backup Credentials 	Credential name:*			
Devices Schedule Variables BGP	Password:* Confirm password:*			
Custom OID Devices Diagram Envoriter				
Financials Issues Maps	OK Cancel			
Meraki NetFlow Network Thresholds Polling				
Syslog TFTP WAN	Add Change Delete Reset Sort			
		Revert	Арр	ly

Devices

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

earch Options (Ctrl+E)		Devices			
TotalView	^	Device name	Address	Port	Credentia
Alert Options Cloud Email		Headquarters/Syrah	10.0.0.1	22	psadmin
		HQFW/hqpa450	10.86.0.5	22	psadmin
NetAlly		Headquarters/Michelob	10.0.0.12	22	psadmin
Network		Austin/txfw1	10.51.0.1	22	psadmin
> Alerts		Boston/bostonsw1-stout.pathsolutions.lo	10.30.0.1	22	psadmin
✓ Backup		Austin/AustinRTR.pathsolutions.local	10.51.0.254	22	psadmin
Devices		Austin/DallasRtR.pathsolutions.local	10.51.20.1	22	, psadmin
Schedule		Austin/DallasSW1.pathsolutions.local	10.51.20.5	22	, psadmin
Variables		Austin/HoustonRtR.pathsolutions.local	10.51.30.1	22	psadmin
Custom OID		Austin/HoustonSW1.pathsolutions.local	10.51.30.5	22	psadmin
Diagram		Sunnvvale/svfw1	10.50.0.250	22	psadmin
Favorites		Headquarters/SantaClara.pathsolutions.local	10.0.0.2	22	psadmin
Financials		Chicago/AngryBalls.pathsolutions.local		22	psadmin
Ignored Interfaces		Headquarters/Chardonnay	10.0.0.20	22	psadmin
Ignored Types		Headquarters/Burgundy	10.0.0.19	22	nsadmin
ISSUES Mans		Headquarters/Muscat	10.0.0.23	22	nsadmin
Meraki		The adduaters muscat	10.0.0.25	22	paduluu
Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT	v	< Add Change Delete	Shift Up	Shift Down	

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

🌮 Add Devie	ces				×
Credentials:	psac	lmin	~		
SSH Port:	22				
Filter:	10.0	.0.2			Θ
Group		IP Address	Name	Description	ОК
Headqua	arters	10.0.0.2	SantaClara.pathsolutions.local	Cisco IOS Software, 2800 Software	
🗌 Headqua	arters	10.0.0.20	Chardonnay	ProCurve J9085A Switch 2610-24,	
🗌 Headqua	arters	10.0.0.21	Pinot	HP J9726A 2920-24G Switch,	
🗌 Headqua	arters	10.0.0.25	Grenache	Cisco Internetwork Operating	
🗌 Headqua	arters	10.0.0.26	Ribolla	Cisco IOS Software, C3560 Softwar	
🗌 Headqua	arters	10.0.0.22	Merlot	HP J9726A 2920-24G Switch,	
🗌 Headqua	arters	10.0.0.29	Riesling	Brocade Communications System	
🗌 Headqua	arters	10.0.0.23	Muscat	HP J9726A 2920-24G Switch,	
🗌 Headqua	arters	10.0.0.27	Franc	Cisco Internetwork Operating	
🗌 Headqua	arters	10.0.0.28	Palomino	Cisco IOS Software, C3550 Softwar	
🗌 Headqua	arters	10.0.0.250	PS-P1-OpenGear	Linux PS-P1-OpenGear 3.10.0-uc0	
Test connection	on			OK Cance	el

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

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

The screenshot below displays an example of testing a connection.

Test SSH Connection	×
Tests finished	
Testing SSH Connection to 10.0.0.23:22	
Connecting to the host OK	
Verifying the host key OK	
Attempting password authentication Unable to login: Access denied Attempting keyboard-interactive authentication Login failed: Access denied	
Show log Close	

Schedule Backup

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

TotalView Configuration Tool*				- 🗆 X
Search Options (Ctrl+E)	es Reports Schedule			٨
> TotalView	Device name	Address So	chedule	Script
Cloud	HQ FW/hqpa450	10.86.0.5 0	00**?	PaloAlto-set(RunningConfig).tx
> Dashboard	HQ LAN/Syrah	10.0.0.1 0	00**?	CiscolOS with enable(RunningC
NetAlly	HQ LAN/Dubonnet	10.0.0.32 0	00**?	HP2920(RunningConfig).txt
✓ Network	HQ LAN/Pinot	10.0.0.21 0	00**?	HP2920(RunningConfig).txt
> Alerts	HQ LAN/Muscat	10.0.0.23 0	00**?	HP2920(RunningConfig).txt
✓ Backup Credentials	HQ LAN/SantaClara.pathsolutions.local	10.0.0.2 0	00**?	CiscolOS(RunningConfig).txt
Devices	HQ LAN/MPLSCore.pathsolutions.local	10.0.0.3 0	00**?	CiscolOS(RunningConfig).txt
Schedule	HQ LAN/tempranillo.pathsolutions.local	10.0.0.7 0	00**?	CiscolOS(RunningConfig).txt
Variables	SV LAN/Sunnyvale.pathsolutions.local	10.50.0.2 0	00**?	CiscolOS(RunningConfig).txt
Custom OID	Boston/bostonsw1-stout.pathsolutions.lo	10.30.0.1 0	00**?	ExtremeOS(RunningConfig).txt
 > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetWork Thresholds Polling Syslog TFTP 	<			>
WAN V	Add Change Delete	Shift Up	Shift Down	Reset Sort Backup
				Revert Apply

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

Add Schedule				×				
Filter:	IP address, Gr	oup, Name or Description						
Group	IP Address	Name	Description					
HQ LAN	10.0.0.32	Dubonnet	HP J9729A 2920-48G-POE+ Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swl	buildm/rel_ajanta_arenal_qaoff/code/				
HQ LAN	10.0.0.23	Muscat Dubonnet	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm	/rel_ajanta_arenal_qaoff/code/build/				
HQ LAN	10.0.0.21	Pinot	HP J9726A 2920-24G Switch, revision WB.16.10.0022, ROM WB.16.03 (/ws/swbuildm	/rel_ajanta_arenal_qaoff/code/build/				
HQ FW	10.86.0.5	hqpa450	Palo Alto Networks PA-400 series firewall					
Chicago	10.60.0.2	AngryBalls.pathsolutions.local	Cisco IOS Software, C3550 Software (C3550-IPSERVICESK9-M), Version 12.2(50)SE1, F	RELEASE SOFTWARE (fc2)				
HQ LAN	10.0.0.3	MPLSCore.pathsolutions.local	Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-M), Version 15.1(1)T, RELE	ASE SOFTWARE (fc1)				
HQ LAN	10.0.0.12	Michelob	Cisco NX-OS(tm) n9000, Software (n9000-dk9), Version 7.0(3)I1(1b), RELEASE SOFTV	VARE Copyright (c) 2002-2013 by Cisc				
HQ LAN	10.0.0.2	SantaClara.pathsolutions.local	Cisco IOS Software, 2800 Software (C2800NM-IPVOICEK9-M), Version 15.1(1)T, RELE	ASE SOFTWARE (fc1)				
HQ LAN	10.0.0.7	tempranillo.pathsolutions.local	Cisco IOS Software, ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Vers	ion 15.5(3)S1a, RELEASE SOFTWARE				
SV LAN	10.50.0.2	Sunnyvale.pathsolutions.local	Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 15.0(1)M	10, RELEASE SOFTWARE (fc1)				
Boston	10.30.0.1	bostonsw1-stout.pathsolutions.local	ExtremeXOS (X440-8p) version 16.2.3.5 16.2.3.5 by release-manager on Tue Apr 4 16	:13:34 EDT 2017				
HQ LAN	10.0.0.1	Syrah	Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.5b, RELEASE					
Type:	Reoccuring	l i i i i i i i i i i i i i i i i i i i	O One-time O Syslog Match					
Schedule:	000**?			Edit				
Script:*				Browse				
Notify:	🗹 On Failure	On Success Email:		~				
Syslog match:	configured fro	m						
				OK Cancel				

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

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

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

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

🌮 Backup Scł	nedule												
Cron string:	000**?												
Next launches:	2/8/2023 12	:00 AM, 2/	/9/2023	12:00 AM	1, 2/10/2	023 12:0	0 AM, 2/	11/2023	12:00 AM	1, 2/12/	2023 12:0	0 AM,	
Seconds:	O Every	1	* *	second	(s)								
	Specific	0	5	10	15	20	25	30	35	40	45	50	55
Minutes:	O Every	1	*	minute((s)								
	Specific	0	5	10	15	20	25	30	35	40	45	50	55
Hours:	O Every	1	A T	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)								
		Jan		Feb		Mar	A	pr	May		Jun		
		Jul		Aug		Sep	0	ct	Nov		Dec		
Days of week:	Any												
	O Specific	MO		TU		WE	Т	н	FR		SA		SU
										_		_	
											OK	0	Cancel

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

Select \mathbf{OK} to completed the schedule changes.

Variables

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

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

Services Cloud Services Variables Variables Variables BGP Custom CID > Devices > Schedule Variables BGP Custom CID > Devices > Diagram Financials Issues Maps Metakis Nettrok Nettrok Poling Sysig TTP Wark Nettrok Network Nettrok Network Nettrok Network Not Not Not Not Not Not Not Not Not	TotalView Configuration Tool*			-		×
Search Options (Ctrl+E) Search Options (Ctrl+E) South Options (Ctrl+E) South Options Dashboard Internet NetAlly Network Netroork Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Devices Schedule Variable BGP Custom OID Add Change Delete Reset Sort Revert Apply	Servers Loud Servers	vic	es Reports			
S TotalView Coud Double Could Internet NetAlly Veries Schedule Variables B6P Custom OlD Devices Schedule Variables B6P Custom OlD Devices Schedule Variables B6P Custom OlD Devices Schedule Variables B6P Custom OlD Devices Schedule Variables B6P Custom OlD Devices Signarm Favorites Financials Issues Maps Merski NetFlow NetWork Thresholds Polling Syslog TTP TTP WAN Veritor NetWork Thresholds Solution NetWork Thresholds Solution NetWork Thresholds NetWork Thresholds NetWork Thresholds Polling Syslog TTP WAN Veritor NetWork Thresholds Solution NetWork Thresholds Solution Subscription NetWork Thresholds NetWork Thresholds NetWork Thresholds Solution NetWork Thresholds Polling Syslog TTP WAN Veritor NetWork Thresholds Solution NetWork Thresholds Solution NetWork Thresholds Solution NetWork Thresholds Solution NetWork Thresholds Solution Syslog TTP TTP WAN Veritor NetWork Thresholds Solution NetWork Thresholds Solution Solution NetWork Thresholds Solution NetWork Thresholds Solution Solution NetWork Thresholds Solution NetWork Thresholds Solution NetWork Thresholds Solution Solution NetWork Thresholds Solution Solution NetWork Thresholds Solution Sol	Search Options (Ctrl+E)		Variables			
Variable Variable Cloud > Dashboard Internet NetAlly * Retro > Alerts * Backup Credentials Devices Schedule Variables BGP Custom OID > Devices Schedule Variables BGP Custom OID > Devices Signam Favorites Financials Issues Maps Metridion NetFlow NetFlow NetFlow NetFlow NetWork Thresholds Polling Syslog TFTP WAN MAT Add	TetaWienu					_
 Dashboard Internet NetAlly NetAlly Netvork Alerts Backup Credentials Devices Schedule Wriables BGP Custom OID Devices Diagram Favorites Financials Issues Maps Metaki NetFlow NetFlow<	Cloud		Variable			
Internet NetAlly V Network > Alerts V Devices Schedule Viriables BGP Custom OID > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetWork Thresholds Polling Syslog TFTP WAN V MT Mag. Delete Reset Sort Revert Apply	> Dashboard		enable			
NetAlly ✓ Network > Alerts Backup Credentials Devices Schedule Variables BGP Custom OID > Devices - Schedule Variables BGP Custom OID > Devices - Schedule Variables BGP Custom OID > Devices - Sortes - Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN WAN WAN WAN WAN WAN Change Delete Reset Sort Revert Apply	Internet					
 Network Alerts Backup Credentials Devices Schedule Variables BGP Custom OID Devices Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow NetWork Thresholds Polling Syslog TFTP WAN Add Change Delete Reset Sort 	NetAlly					
 > Alerts > Backup Credentials Devices Schedule Variables BGP Custom OlD > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow Meraki NetFlow NetFlow NetFlow Add Change Reset Sort 	✓ Network					
 Backup Credentials Devices Schedule Variables BGP Custom OID Devices Diagram Favorites Financials Issues Maps Meraki Nettflow Nettflow Nettflow Nettflow Nettflow Nettflow Nettflow Nettflow Nettors Thresholds Polling Syslog TFTP WAN Add Change Delete Reset Sort 	> Alerts					
Credentials Devices Schedule Variables BGP Custom OID > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetForw NetF	✓ Backup					
Verifies Schedule Variables BGP Custom OID > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN MIT Revert Apply	Credentials					
Wariables BGP Custom OID > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetWork Thresholds Polling Syslog TFTP WAN MT M T Add Change Delete Reset Sort Revert Apply	Schedule					
BGP Custom OID > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetWork Thresholds Polling Syslog TFTP WAN Nt T Add Change Delete Reset Sort	Variables					
Custom OID > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow NetWork Thresholds Polling Syslog TFTP WAN MIT Add Change Delete Reset Sort Revert Apply	BGP					
 > Devices > Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow NetFlow NetFlow Add Change Reset Sort 	Custom OID					
 Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow Network Thresholds Polling Syslog TFTP WAN Add Change Reset Sort 	> Devices					
Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN MIT Add Change Delete Reset Sort Revert Apply	> Diagram					
Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NIT NIT Reset Sort Revert Apply	Favorites					
Issues Maps Meraki NetRiow Network Thresholds Polling Syslog TFTP WAN WAN Add Change Delete Reset Sort Revert Apply	Financials					
Maps Meraki NetFlow NetWork Thresholds Polling Syslog TFTP WAN NIT Add Change Delete Reset Sort	Issues					
NetFlow NetWork Thresholds Polling Syslog TFTP WAN V Add Change Delete Reset Sort	Maps					
Network Thresholds Polling Syslog TFTP WAN V Add Change Delete Reset Sort NIT Revert Apply	NetElow					
Polling Syslog TFTP WAN V Add Change Delete Reset Sort NIT Revert Apply	Network Thresholds					
Syslog TFTP WAN MIT Add Change Delete Reset Sort Revert Apply	Polling					
TFTP WAN MIT Add Change Delete Reset Sort Revert Apply	Syslog					
WAN Add Change Delete Reset Sort	TFTP					
Revert Apply	WAN	~	Add Change Delete Reset Sort			
Revert Apply						
			Rev	/ert	App	ly

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

ge Variable				×
enable				
•••••				
			OK	Cancel
	ge Variable enable	ge Variable	ge Variable	ge Variable enable enable OK

BGP

Go to Network > Alerts > BGP Alerts, choose Alerts or Peers

Seven Options (Chi +E) BGP V TotaNew Action This configures BGP alerts. Part options Chi mil Alert Options Chi mil Authentication Parts Authentication Parts Westher Widget Internet Internet Parts Perices Alerts Perice Alerts Parts Perice Alerts Strabule Perice Alerts Perice Alerts Perice Ignored Error Counters Ignored Error Counters Ignored InterCounters Ignored InterCounters Ignored InterCounters Ign	Cloud Serve	s 🔔 Services 📥 Reports			
 VotaView VotaView Data Retention Tata Retention Familie Familie Alet Options Storage Tech Support We binefrace API Keys Authentication We binefrace API Keys Authent Widget Internet Vachorad Vachorad	Search Options (Ctrl+E)	BGP			
Data Retention Personal Kensil Alert Options Storage Tech Support Tech Support Personal Web Interface Personal ADI Keys Personal Webshewitization Personal Weshewitization Personal Valents Personal Decice Allerts Personal Cordentals Personal Decices Personal Variables Personal Versing Personal Personal Upgored from Counterse Ignored from Counterse	✓ TotalView	Alerts: This configures BGP alerts.			
Version of the form of the	Data Retention	Peers: Configures BGP peers that will be available for monitoring.			
Alet Options Storage Tech Support Web Interface ADI Kays ADI Kays ADI Kays ADI Kays ADI Kays ADI Kays ADI Kays ADI Kays ADI Kays Westher Widget Internet Usether Widget Internet Device Alets Route Alets Route Alets Route Alets Route Alets Route Alets Bolices Schedule Vanible Schedule Vanible Vanible Schedule Vanible Vanible Schedule Vanib	✓ Email				
Storage Tech Support Web Interface Authenfaction Web Server Oood Oood Valves Webstere Widget Internet V Network V Alets Dovice Alets Route Alets Devices Schedule Vinibles V Beres Custom OlD V Devices Ignored Interfaces Ignored Times V Diagaam Layer-3 Steckdes Layer-3 Steckdes Layer-3 Steckdes Layer-3 Steckdes	Alert Options				
<pre>Tech Support Web interface API Keys API Keys API Keys API Keys API Keys Authorication Web Server Coud Web Server Coud Web Server Coud Westher Widget Internet Authorication Vesther Widget Internet Authorication Vesther Widget Internet Secure Pers Credentials Devices Schedule Vinables Vesther Serve Ignored Error Counters Ignored Interfaces Ignored Inter</pre>	Storage				
 Veb Interface Authentication Web Server Cood Ood Dashboard Westher Widget Internet Network Vebuork Valets Dorice Alets Bobice Alets Credentials Dorices Schedule Variables Variables Pees Cuttom OID Verkers Ignored Interfaces Ignored Interfaces Ignored Trefaces I	Tech Support				
Arit Rejs Authentication Web Server Owd > Dashboard Weather Widget Internet Internet > Network > Network > Network > Network > Device Alerts Route Alerts Device Alerts Credentials Devices Schedule Wriables - Credentials Devices Schedule Wriables - Schedule Wriables - Schedule - Sche	 Web Interface 				
Authentication Web Sever Wether Wether Wether Widget Wether Widget Wether Widget Wether Widget Network Vetwork	API Keys				
Web Server Coud Coud Vesthe Widget Internet Westher Widget Internet Vetwork Vetwork Vetwork Vetres Device Alerts Route Alerts Credentials Devices Schedule Variables Verices Schedule Variables Variables Variables Verice Jonore Counters Ignored Interfaces Ignored Interfaces Ignored Type Names Interface Description Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favortes Verices	Authentication				
Uoid Vexther Widget V Dashboard Vexther Widget Internet Vexther V Network Vexther V Alerts Device Alerts Route Alerts Route Alerts V Backup Devices Credentials Devices Devices Schedule Vraibles Vertices Custom OID Vectors Ignored Tror Counters Ignored Tror Counters Ignored Tror Counters Ignored Tror Counters Ignored Tror Sciption Vertifies V Diagram Layer-3 Stacit Links Favorites Vectors	Web Server				
> Dashboard Wether Widget Internet > Network > Alerts Backup Credentials Devices Schedule Vainables Peers Custom OID > Devices Ignored fror Counters Ignored fror Counters Ignored fror Counters Ignored fror Schudes > Diagram Layer-3 Static Links Layer-3 Static Links	Cloud				
Wetther Widget Internet Internet Internet V Ekwork Person Device Alerts Person Route Alerts Person Credentials Person Devices Person Variables Person Variables Person Upored For Counters Ignored Interfaces Ignored Interfaces Ignored Specingtion Variables Person Variables Ignored Specingtion Variables Ignored Interfaces Ignored Specingtion Person Interface Description Person Layer-3 Strict Links Person	✓ Dashboard				
Network: Vetwork: Oevice Alerts Backup Credentials Credentials Devices Schedule Variables Variables Peers Alerts Peers Jogner Interfaces Ignored Tror Counters Ignored Tr	Weather Widget				
Verwork Verwork Verwork Verwork Pervice Alerts Route Alerts Route Alerts Credentials Devices Schedule Variables Variables Variables Variables Vervices Custom OID Vervices Ignored Interface Bescription Variage Interf	Internet M. Naturali				
 Areas Device Alerts Route Alerts Route Alerts Route Alerts Backup Credentials Devices Schedule Variables BBP Alerts Peers Custom OID Devices Ignored Interfaces Ignored Interfaces Interface Description Diagram Layer-3 Excludes Layer-3 Excludes<td> Network Materia </td><td></td><td></td><td></td><td></td>	 Network Materia 				
Bound Allerts Route Allerts Credentials Devices Schedule Variables Variables Alerts Peers Custom OlD Verices Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description Variables Variables	Alerts Device Alerts				
 Note Relations Beckup Credentials Devices Schedule Variables BGP Alerts Peers Custom OID Devices Ignored Interfaces Ignored Interfaces Ignored Interfaces Interface Description Diagram Layer-3 Excludes Layer-3 Excludes<td>Boute Alerts</td><td>0</td><td></td><td></td><td></td>	Boute Alerts	0			
Credentials Devices Schedule Variables V	× Backup				
Customologie Devices Schedule Variables BCP Alerts Peers Custom OID Devices Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description Dayer-3 Excludes Layer-3 Excludes Layer-3 Stxtic Links Favorites	Credentials				
Schedule Variables Variables Alerts Peers Custom OID Vevices Ignored Interfaces Ignored Interfaces Ignored Interfaces Ignored Interfaces Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favorites v	Devices				
Variables Variables Variables BGP Alerts Peers Custom OID Verces Ignored Interface Ignored Interface Ignored Interfaces Ignored Interfaces Ignored Spre Names Interface Description Vager-3 Excludes Layer-3 Excludes Layer-3 Static Links Favorites v	Schedule				
BGP Alerts Peers Custom OID Devices Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description V Diagram Layer-3 Excludes Layer-3 Static Links Favorites	Variables				
Alerts Peers Custrom OID V Devices Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description V Diagram Layer-3 Excludes Layer-3 Straic Links Favorites	✓ BGP				
Peers Custom OID V Devices Ignored Toro Counters Ignored Interfaces Ignored Type Names Interface Description V Diagram Layer-3 Excludes Layer-3 Straic Links Favorites	Alerts				
Custom OID V Devices Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description V Diagram Layer-3 Stockledes Layer-3 Stock Links Favorites	Peers				
V Devices Ignored Tror Counters Ignored Interfaces Ignored Interfaces Ignored Type Names Interface Description V Diagram Ignores Layer-3 Excludes Interface Description Layer-3 Strict Links V	Custom OID				
Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description V Diagram Layer-3 Excludes Layer-3 Straic Links Favorites V	V Devices				
Ignored Interfaces Ignored Type Names Interface Description Diagram Layer-3 Excludes Layer-3 Static Links Favorites	Ignored Error Counters				
Ignored Type Names Interface Description Diagram Layer-3 Excludes Layer-3 Static Links Favorites V	Ignored Interfaces				
Interface Description Viagram Layer-3 Excludes Layer-3 Static Links Favorites V	Ignored Type Names				
 Diagram Layer-3 Excludes Layer-3 Ignores Layer-3 Static Links Favorites 	Interface Description				
Layer-3 Excludes Layer-3 Ignores Layer-3 Static Links Favorites V	 Diagram 				
Layer-3 Ignores Layer-3 Static Links Favorites V	Layer-3 Excludes				
Layer-3 Static Links Favorites v	Layer-3 Ignores				
Favorites v	Layer-3 Static Links				
	Favorites	×			
			Revert	A	pply

BGP Alerts

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



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

💝 Add BGP Alert			×
Agent IP address:	Headquarters/Syrah (10.0.0.1)		~
Peer IP address:	10.0.0.2		
Alert email:	itops@pathsolutions.com		~
			_
		OK	Cancel

BGP Peers

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

TotalView Configuration Tool							-		×
Cloud Servers	Service	s Report	5						
Search Options (Ctrl+E)		BGP Peers							
✓ TotalView	^	BGP List	Show only in E	stablished state					Update
Data Retention		Device norma	D address	Decello	Connection State	A1-+			-
✓ Email		Device name	IP address	Peerip	Connection state	Alen			
Alert Options		HQ/Syrah	10.0.0.1	169.254.0.2	Established				
Storage		HQ/Michelob	10.0.0.12	169.254.0.1	Established				
lech Support									
 Web Interface ADI Kara 									
Arthestisation									
Web Server									
Cloud									
Y Dashboard									
Weather Widget									
Internet									
✓ Network									
✓ Alerts									
Device Alerts									
Route Alerts		Add Alert	Delete Alert	Allow Peer	Ignore Peer				
✓ Backup									
Credentials		Ignore Rules							
Devices		Device	Peer IP						
Schedule									
Variables									
✓ BGP									
Alerts									
Peers									
Custom OID									
Devices									
Ignored Interfaces									
Ignored Type Names									
Interface Description									
✓ Diagram									
Laver-3 Excludes									
Laver-3 Ignores									
Laver-3 Static Links									
Favorites	~	Add	Change	Delete	Shift Up Shift Do	wn Reset Sort			
							Revert	An	vla

Use the Add or Change buttons to add or modify devices and peers on the list.

🐉 Add	Ignore Rule	×
Device:	O All devices	
	• Specific:	HQ/Syrah (10.0.0.1)
Peer:	O All peers	
	Specific:	169.254.0.2 : Established ~
		✓ Only in Established state
		OK Cancel

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 <u>MIB Browser</u> for OID lookups, OID monitoring and OID graphing.



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

Devices Configuration

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

- **Note:** All interfaces for each switch are monitored by default, ignore individual interfaces from being monitored on the web interface.
- Note: If SNMPv3 is not enabled and is desired, contact support@pathsolutions.com.

earch Options (Ctrl+E)	De	evices					
TotalView	^ Fin	d: Group, Devic	e name, IP Address, Description				General Sup
Dashboard		Group	Device name	IP Address	Int	SNMP	Description
Internet		HQ FW	hqmx65	10.86.0.4	2	v2c	HQ Firewalls
Network		HQ FW	hqpa450	10.86.0.5	7	v3	HQ Firewalls
> Backup		HQ FW	hqf140d-poe	10.0.0.46	9	v2c	
BGP		HQ LAN	Syrah	10.0.0.1	11	v2c	HQ Lab Gear
Custom OID		HQ LAN	SantaClara.pathsolutions.local	10.0.0.2	3	v2c	HQ Lab Gear
> Devices		HQ LAN	MPLSCore.pathsolutions.local	10.0.0.3	4	v2c	HQ Lab Gear
Favorites		HQ LAN	RuckusAP	10.0.0.6	18	v2c	HQ Lab Gear
Financials		HQ LAN	tempranillo.pathsolutions.local	10.0.0.7	5	v2c	HQ Lab Gear
Issues		HQ LAN	Michelob	10.0.0.12	15	v2c	HQ Lab Gear
Maps		HQ LAN	Burgundy	10.0.0.19	29	v3	HQ Lab Gear
NetFlow		HQ LAN	Chardonnay	10.0.0.20	28	v2c	HQ Lab Gear
Network Thresholds		HQ LAN	Pinot	10.0.0.21	25	v2c	HQ Lab Gear
Polling		HQ LAN	Merlot	10.0.0.22	25	v2c	Device
Syslog		HQ LAN	Muscat	10.0.0.23	25	v2c	HQ Lab Gear
WAN		HQ LAN	Franc	10.0.0.27	51	v2c	HQ Lab Gear
NLT		HQ LAN	Palomino	10.0.0.28	26	v2c	HQ Lab Gear
Remotelnsight		HQ LAN	Riesling	10.0.0.29	29	v2c	Device
Reports		HQ LAN	PS-PTR1	10.0.0.30	1	v2c	HQ Lab Gear
KISKS SD-WAN							
Servers	~	Add	Change Delete Shift	Up Shift Down		Reset So	rt

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

Adding Devices

To add a device, select Add. The Add device dialog will display.

🌮 Change Device	>	<
Group:	Santa Clara ~]
IP address:	10.0.0.1]
Device Type:	 O ▲ Linux server O Non-Linux server]
	Oynamic detection	
SNMP version:	○ SNMPv1	
Community string:*]
AuthProt:	AuthPass:	
NoAuth ~		
PrivProt:	PrivPass:	
NoPriv ~		
Contract date:	12/10/2024	
Contract ID:]
Contract phone:		1
Description (optional):	Device	1
		1
	OV Const	1
	UK Cancel	1

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

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

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

Deleting Devices

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



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

- **Note:** Deleting a device from monitoring will not delete the previously collected graph data. Add the device back to monitoring and it will continue to use the same data file for graph data storage.
- **Note:** Any device prevented from being re-discovered when the QuickConfig Wizard runs can be added back again by removing the device from being ignored in the **SwMonIgnore.cfg** file or by adding the device to be monitored again in the **SwitchMonitor.cfg** file. These files can be found in the following directory:

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

Save the file after any modification.

Changing Device Information

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

The **Change Device** dialog will display.

💞 Change Device	×
Group:	Headquarters ~
IP address:	10.0.25
Device Type:	🔿 🛕 Linux server
	O Non-Linux server
	Opprovide the second
SNMP version:	○ SNMPv1
Community string:	public
AuthProt:	AuthPass:
NoAuth	
PrivProt:	PrivPass:
NoPriv	
Contract date:	2/7/2023
Contract ID:	
Contract phone:	
Dessisting (astrono)	
Description (optional):	
	OK 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.

Ignored Error Counters

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

TotalView Configuration Tool					.—		×
Cloud Servers Services	es 📕 Reports						
Search Options (Ctrl+E)	Ignored Error Counters 💡						
> TotalView ^	Device/Group	Interface	Counter name	Suppress			
Cloud	SV LAN/UBNT (10.50.0.174)	8	Inbound Discards	Yes			
> Dashboard	SV LAN/UBNIT (10 50 0 174)	8	Inhound Errors	Vec			
Internet	SV LAN/URNIT (10 50 0 174)	0	Outhound Errors	Vec			
Network Alertr	SV LAN/0 BINT (10.30.0.174)	0		Tes V			
Backup	HQ LAN/Franc (10.0.0.27)	4	Frame Too Longs	Yes			
BGP	10.51.0.1	5	Inbound Discards	Yes			_
Custom OID	Any	Any	Inbound Unknown Protocols	Yes			_
✓ Devices	Any	Any	Outbound Queue Length	Yes			
Ignored Error Counters Ignored Interfaces Ignored Type Names Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT RemoteInsight P RemoteInsight P Source P Source P Source P P P P P P P P P P P P P P P P P P P							
Reports	Add Change	Delete	Shift Up Shift Down	Reset Sort			
					Revert	Арр	yk

Ignored Interfaces

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

TotalView Configuration Tool				-		×
Cloud Servers Service	es Reports					
Search Options (Ctrl+E)	Ignored Interfa	ices				
			lated are			_
✓ Network	Device name	IP Address	Interraces			_
> Alerts	HQ LAN/Syrah	10.0.0.1	1,4,5,7-12,14,22,23,25-30,32,33,45,48-50			_
> Backup	HQ LAN/	10.0.0.12	83886080, 151060590, 151060666, 151061190, 436207616, 436208128, 436	209664,	43621017	6,4
BGP	HQ FW/hqmx65	10.86.0.4	2,4-12			
Custom OID	HO FW/hgpa450	10.86.0.5	1-4.9-13			
✓ Devices						
Ignored Error Counters						
Ignored Interfaces						
Ignored Type Names						
> Diagram						
Favorites						
Financials						
Issues						
Marahi						
NetElow						
Network Thresholds						
Polling						
Syslog						
TFTP						
WAN						
NLT						
> Remotelnsight						
Reports						
> Risks						_
SD-WAN	Add	Thances	Delata Decat Sort			
> Servers Y	Audin	ananyeaa	Neser Sur L			
					_	
			Reve	ert	Appl	У

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

🐲 Add Range	×	
IP address:	~	
Interface range:		
	OK Cancel	
	8.9	

Alternate Methods to Ignore Interfaces

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

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

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

This file is located in the following directory:

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

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

Note: The web server must unlocked in order for the Ignore column to show up in TotalView. See the section <u>Error! R</u> <u>eference source not found.</u> for how to lock and unlock the web server.

	ram Grei	mlins De	vices Fa	ivorites Issues Netflo	w IPA	M	Top-10	Wan	erfaces SD-WAN Tools						Тс	tal Network Visibilit
Lock Web									General Traffic Pol	E STP	Inver	ntory De	scription Bac	kup	Support Financ	als Vulnerabilities
		Device	SNMP				Oper	Admin								
Device Name	1	IP Address	Version	n Manage	CPU	Int	Down	Down	Location				Conta	ot		Uptim
Sinot	10.	.0.0.21	v2c	Telnet SSH Web HTTPS Syslo		26	21	0		itops	@pat	thsolutions.	com			116d 00h 06
Interfaces									•							
∢ ►												General	Traffic Po	E ST	P Details CDF	/LLDP Connecte
									A							State
		ID								Innore		Queue	MAC			
Interface	Favorite	WAN Add	lress Desc	cription						Int	x	L Type	Address	мти	Type	Last Changed
• INT#1	Favorite	WAN	1:1							Ignore	• •	•	40a8f00dff3f	1526	ethernetCsmaod	116 days 00:06:09.0
INT#2	Favorite	WAN	2:2							Ignore	•	•	40a8f00dff3e	1526	ethernetCsmacd	116 days 00:06:10.
INT#3	Favorite	WAN	3: 3							Ignore	• •	•	40a8f00dff3d	1526	ethernetCsmacd	116 days 00:06:10.
INT#4	Favorite	WAN	4:4							Ignore	• •	•	40a8f00dff3c	1526	ethernetCsmacd	116 days 00:06:10.
INT#5	Favorite	WAN	5: 5							Ignore	• •	•	40a8f00dff3b	1526	ethernetCsmacd	116 days 00:06:10.
INT#6	Favorite	WAN	6: 6							lanore	• •	•	40a8f00dff3a	1526	ethernetCsmacd	116 days 00:06:10.
															attraction of Company	114 days 03-03-31
INT#7	Favorite	WAN	7:7							Ignore	• •	•	40a8f00dff39	1526	ememetCsmacu	111100330000001011
INT#7 INT#8	Favorite Favorite	WAN	7: 7							Ignore Ignore	•	•	40a8f00dff39 40a8f00dff38	1526 1526	ethernetCsmacd	116 days 00:06:10.8
INT#7 INT#8 INT#9	Favorite Favorite	WAN WAN WAN	7:7 8:8 9:9							Ignore Ignore Ignore	•	•	40a8f00dff39 40a8f00dff38 40a8f00dff37	1526 1526 1526	ethernetCsmacd ethernetCsmacd	116 days 00:06:10. 116 days 00:06:10.
INT#7 INT#8 INT#9 INT#10	Favorite Favorite Favorite	WAN WAN WAN	7:7 8:8 9:9 10:1	10						Ignore Ignore Ignore Ignore	• •	•	40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36	1526 1526 1526 1526	ethemetCsmacd ethemetCsmacd ethemetCsmacd	116 days 00:06:10.0 116 days 00:06:10.0 116 days 00:06:10.0
INT#7 INT#8 INT#9 INT#10 • INT#11	Favorite Favorite Favorite Favorite	WAN WAN WAN WAN	7:7 8:8 9:9 10:1 11:1	10						Ignore Ignore Ignore Ignore Ignore	• • •	•	40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36 40a8f00dff36	1526 1526 1528 1528 1528	ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd	116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10.
INT#7 INT#8 INT#9 INT#10 INT#11 INT#12	Favorite Favorite Favorite Favorite Favorite	WAN WAN WAN WAN WAN	7:7 8:8 9:9 10:1 11:1 12:1	10 11 12						Ignore Ignore Ignore Ignore Ignore Ignore	•	 	40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36 40a8f00dff35 40a8f00dff35	1526 1526 1528 1528 1528 1528	ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd	116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:06. 116 days 00:06:06. 116 days 00:06:10.
INT#7 INT#8 INT#9 INT#10 INT#11 INT#12 INT#13	Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN	7: 7 8: 8 9: 9 10: 1 11: 1 12: 1 13: 1	10 11 12 13						Ignore Ignore Ignore Ignore Ignore Ignore Ignore	• • •	•	40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36 40a8f00dff36 40a8f00dff34 40a8f00dff34	1526 1526 1526 1526 1526 1526 1526	ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd	116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:08. 116 days 00:06:10. 17 days 18:44:06.
INT#7 INT#8 INT#9 INT#10 INT#11 INT#12 INT#13 INT#14	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN VAN VAN VAN VAN VAN VAN VAN VAN VAN V	7: 7 8: 8 9: 9 10: 1 11: 1 12: 1 13: 1 14: 1	10 11 12 13 14						Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore			40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36 40a8f00dff36 40a8f00dff34 40a8f00dff34 40a8f00dff33	1526 1526 1528 1528 1528 1526 1526 1526	ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd	116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:06. 116 days 00:06:06. 116 days 00:06:10. 17 days 18:44:06. 116 days 00:06:10.
INT#7 INT#8 INT#9 INT#10 INT#11 INT#12 INT#12 INT#14 INT#14	Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite Favorite	WAN	7: 7 8: 8 9: 9 10: 1 11: 1 12: 1 13: 1 14: 1 15: 1	10 12 13 14 15						Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore		• •	40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36 40a8f00dff36 40a8f00dff34 40a8f00dff33 40a8f00dff32 40a8f00dff32	1526 1526 1526 1526 1526 1526 1526 1526	ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd	116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:06. 116 days 00:06:06. 116 days 00:06:10. 17 days 18:44:06. 118 days 00:06:10. 103 days 14:10:53.
INT#7 INT#8 INT#9 INT#10 INT#11 INT#12 INT#13 INT#15 INT#15 INT#16	Favorite	WAN WAN	7: 7 8: 8 9: 9 10: 1 11: 1 12: 1 13: 1 14: 1 15: 1 16: 1	10 1 12 13 14 15 16						Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore Ignore		• • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • •	40a8f00dff39 40a8f00dff38 40a8f00dff37 40a8f00dff36 40a8f00dff35 40a8f00dff33 40a8f00dff33 40a8f00dff32 40a8f00dff31 40a8f00dff31	1526 1526 1526 1526 1526 1526 1526 1526	ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd ethemetCsmadd	116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:10. 116 days 00:06:06. 116 days 00:06:06. 116 days 00:06:10. 17 days 18:44:06. 118 days 00:06:10. 103 days 14:10:53. 116 days 00:06:10.

Ignored Type Names

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

Secrete Options (Ctrl+E)	TotalView Configuration Tool		-		×
Search Options (Ctrl+E) Ignored Type Names Internet Interface type name > Alerts Backup > Backup BGP Custom OID Marson > Devices Ignored Type Names Ignored Type Names Ontrolled Uncontrolled Uncontrolled Uncontrolled Uncontrolled Vervicks Interfaces Ignored Type Names Ontrolled Uncontrolled Uncontrolled Uncontrolled Uncontrolled Vervicks Financials Issues Maps Merski NetFlow NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Reports	Cloud Servers Service	s Reports			
Internet Network Alerts Backup BGP Custom OID Devices Ignored Error Counters Ignored Interfaces Ignored Interfaces Ignored Type Names > Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Systog TFTP WAN NLT > Remotelnsight Reports	Search Options (Ctrl+E)	Ignored Type Names			۵
 Network Network Network Backup BGP Custom OID Devices Ignored Error Counters Ignored Interfaces Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Reports 	Internet	Interface type name			
 J Backup Backup BGP Custom OID V Devices Ignored Interfaces Ignored Type Names Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow NetFlow NetFlow NetFow <	Vetwork	LoO			
BGP Loopback Custom OID NullO Ignored Error Counters Ignored Interfaces Ignored Interfaces Ontrolled Ignored Type Names Uncontrolled > Diagram Favorites Financials Issues Maps Meraki NetFlow NetFlow NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Remotelnsight Remotelnsight	> Backup	MS TCP Loopback interface			
Custom OID Verices Ignored Error Counters Ignored Interfaces Ignored Interfaces Ignored Type Names Uncontrolled > Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Hemotelnsight	BGP	Loopback			
 Devices Ignored Error Counters 	Custom OID	NullO			
Ignored Error Counters Ignored Type Names Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Reports	✓ Devices	Controlled			
Ignored Type Names Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports	Ignored Error Counters	Uncontrolled			
 > Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports 	Ignored Type Names				
Favorites Financials Issues Maps Meraki NetFlow NetWork Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports	> Diagram				
Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports	Favorites				
Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Reports	Financials				
Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports	Issues				
NetFlow Network Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports	Meraki				
Network Thresholds Polling Syslog TFTP WAN NLT > Remotelnsight Reports	NetFlow				
Polling Syslog TFTP WAN NLT > Remotelnsight Reports	Network Thresholds				
Syslog TFTP WAN NLT > Remotelnsight Reports	Polling				
WAN NLT > Remotelnsight Reports	Syslog				
NLT > Remotelnsight Reports	IFIP WAN				
> Remotelnsight Reports	NLT				
Reports	> Remotelnsight				
	Reports				
> Risks	> Risks				
Source Add Change Delete Reset Sort	SD-WAN	Add Change Delete Reset Sort			
/ JEIVEIS	/ Servers				
Revert Andy		Rey	vert	Appl	v
		182			

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

Interface Description

The ability to override interface name, bandwidth, and IP/Subnet.



Add Device and Interface

🌮 Change Ir	nterface	Descriptio	n							×
Device Specific: Any dev Match sy	ice ysDescr:	Santa C	Clara/Syrah ((10.0.0.1)						~
Interface Specific: Match field	elds:	ifName:	0/5: GigabitE	Ethernet1/0	/5 (VMWar	e)	ifAlias: ifType:	Not specifie	ed	
Override fiel	ds									
Speed:	1G					IP:	192.1	68.1.45		
Description:	link to	vm host				IP mask:	255.2	55.255.0		
									ОК	Cancel .:

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.

TotalView Configuration Tool			-		×
Cloud Servers Services	es Repor	<u>ts</u>			
Search Options (Ctrl+E)	Layer-3 Excl	udes			
> TotalView ^	IP Address	Mask			
Cloud	169.254.0.0	255.255.0.0			
> Dashboard					
✓ Network					
> Alerts					
> Backup					
BGP					
Custom OID					
> Devices					
✓ Diagram					
Laver-3 Ignores					
Layer-3 Static Links					
Favorites					
Financials					
Issues					
Maps					
Meraki					
Network Thresholds					
Polling					
Syslog					
TFTP					
WAN					
NLI > Remetalerickt					
Reports Y	Add	Change Delete Reset Sort		Upda	ate
hepoi is					
		Re	evert	App	lv

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

Exclude			×
IP address:	169.254.0.0		٢
Mask:	255.255.0.0		0
		OK	Cancel

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

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

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

Layer-3 Ignores

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

Search Options (Ctrl+E) Layer-3 Ignores Internet > Alerts > Backup BGP	
Internet Vetwork Alerts Backup BGP Vetwork	
Custom OID Devices Diagram Layer-3 Excludes Layer-3 Ignores Ignores Ignored IP addresses will	
Layer-3 Static Links Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Reports Risks	
SD-WAN Servers Add Change Delete Reset Sort Revert	Update Apply

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

🌮 Ignore		×
IP address:*		
	OK	Cancel

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

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

Layer-3 Static Links

This configures static links between devices/subnets.

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

TotalView Configuration Tool						-		×
Services Cloud Servers Service	es Report	5						
Search Options (Ctrl+E)	Layer-3 Stati	c Links						
Internet	IP Address	Mask	Cloud name					
✓ Network		-						_
> Alerts								
> Backup								
BGP								
Custom OID								
> Devices								
✓ Diagram								
Layer-3 Excludes								
Layer-3 Ignores								
Layer-3 Static Links								
Favorites								
Financials								
Issues								
Maps								
Meraki								
Netriow								
Delling								
Syrlog								
TETD								
WAN								
NIT								
> Remotelnsight								
Reports								
> Risks								
SD-WAN								
> Servers V	Add	Change	Delete	Reset Sort			Upd	ate
					Re	vert	Apr	olv

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

Change S	Static Link		×
IP address:	10.0.0.12		٢
Mask:	225.225.225.8		٢
Cloud name:	Lab Network		٢
		OK	Cancel

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

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



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

Favorites

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

TotalView Configuration Tool						_		\times
Cloud Servers Services	es Reports							
Search Options (Ctrl+E)	Favorites							۵
Internet	Device name	IP address	Interface number					
✓ Network	HQ FW/hqpa450	10.86.0.5	7					
> Alerts	HQ FW/hgpa450	10.86.0.5	8					
BGP		10.51.0.1	7					
Custom OID								_
> Devices								
> Diagram								
Favorites								
Financials								
Manc								
Meraki								
NetFlow								
Network Thresholds								
Polling								
Syslog								
TFTP								
WAN								
NLI Remoteloright								
Reports								
> Risks								
SD-WAN								
> Servers								
Services								
> VoIP	Add Ch	Dele	te Shift Up	Shift Down	Reset Sort			
						_		_
					Re	vert	App	ly .:

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



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

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

Financials

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

TotalView Configuration Tool						-		х
Devices Cloud Servers Service	es Reports							
Search Options (Ctrl+E)	Financials							٥
Internet Vetwork Alerts Backup Boch	Device name	IP address	Install date	Procurement cost	Amortization	Support cost		
Custom OID > Devices > Diagram Favorites								
Financials Issues Maps Meraki NetFlow								
Network Thresholds Polling Syslog TFTP WAN								
NLT > Remotelnsight Reports > Risks SD-WAN								
Servers Services VolP V	Add	Change	Delete Sł	hift Up Shift Down	n Reset So	rt		
						Revert	Арр	dy .::

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

➢ Add Financials Record							
IP address:	Headquarters/Syrah (10.0.0.1)						
Install date:	2/7/2023 ~						
Procurement cost:	2390						
Amortization:	48						
Annual support cost:	340						
	OK Cancel						

IPAM

How often to you want TotalView to update Microsoft DHCP information.



IPAM Subnet

The ability to add non-monitored IP subnets into the IPAM Tab

TotalView Configuration Tool*			-		×
Cloud Servers	es Reports				
Search Options (Ctrl+E)	IPAM Subnets				
Devices ^	IP Address	Mask			
Schedule					_
Variables					
✓ BGP					
Alerts					
Peers					
Custom OID					
✓ Devices					
Ignored Error Counters					
Ignored Interfaces					
Ignored Type Names					
Interface Description					
✓ Diagram					
Layer-3 Excludes					
Layer-3 Ignores					
Eaverites					
Financials					
IPAM Subnets					
Issues					
Maps					
Meraki					
NetFlow					
Network Thresholds					
Polling					
Syslog					
TFTP					
WAN					
NLT					
✓ Remotelnsight					
Script Editor					
Web Server					
Reports					
✓ Risks					
Alerts					
Certificates					
Dictionary					
Geographic					
× IoT					
Devices					
IoT VLAN					
Policies					
Rogue IT					
Whitelist					
SD-WAN					
✓ Servers					
 Operating Systems 					
✓ Linux Servers	Add	Change Delete Reset Sort			
Aloste					
			ort	Arel	
		Rev	e (Appr	/
					.:

Issues

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

TotalView Configuration Tool		-		×
Cloud Servers Services	ces Reports			
Search Options (Ctrl+E)	Issues			۵
Internet ^ Vetwork	Ignore error and utilization calculations on VLAN interfaces			
> Alerts > Backup BGP	Ignore Unknown Protocol Errors on Interfaces Do not report incorrect subnet masks on issues tab			
Custom OID Devices	Do not report down devices on issues tab			
> Diagram Favorites Financials	Do not report ARP cache entries that disagree on issues tab			
lssues Maps	Do not report missing default routes on devices on issues tab			
Meraki NetFlow				
Polling Svslog				
TFTP WAN				
NLT > Remotelnsight				
> Risks SD-WAN				
> Servers Services				
> VolP				
	Re	vert	Appl	ly

How to Ignore Unknown Protocol Errors

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

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

How to Ignore VLAN Interface Errors

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

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

Maps

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

Services Cloud Services Search Options (Ctrl+E) Maps Internet Network Alerts Backup BGP Custom OID Devices Run Map Tool			
Search Options (Ctrl+E) Maps Internet ^ V Network ^ > Alerts > > Backup BGP Custom OID > > Devices			
Internet Network Alerts Backup BGP Custom OID Devices			
 > Alerts > Backup BGP Custom OID > Devices 			
BGP Custom OID > Devices			
> Devices			
> Diagram			
Favorites			
Maps			
NetFlow Network Thresholds			
Polling Syslog			
TFTP WAN			
NLI > Remotelnsight Penetr			
Risks SD-WAN			
> Servers Services			
> VoIP			
	Revert	Ap	ply

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

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

🔯 Select a Map		\times
Please select a map	OK	
Config ~	Cancel	

See the section on the <u>Map Config Tool</u> for instructions how to use this tool.
Meraki

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

TotalView Configuration Tool		_		\times
Cloud Servers Service	s Reports			
Search Options (Ctrl+E)	Meraki			0
Search Options (Ctrl+E)	Meraki API Key: Croedo 14.210 109 / 0399900 39000423322210 / 9909 Check			
	Re	vert	Appl	у

NetFlow

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

No Devices 📥 Cloud 🗊 Services 🔔 Service	s Reports										
Search Options (Ctrl+E)	NetFlow										
Alert Options	Enable NetFlow	Run Analysis Tool		216.2 GB Cen DB	Data retention: 3 da	vs					
Storage				CO KB/sec							
Tech Support	Netflow devices	19									
✓ Web Interface	Device name	IP Address	Interface								
API Keys	HO-FW/hopa450	10.86.0.5	6								
Authentication	HO EWA and ISO	10.94.0.5									
Web Server	Pit2-PW/nqpa+30	10.00.0.5	-								
Cloud	HQ-FW/hqpa450	10.86.0.5	8								
 Dashboard 											
Weather Widget*											
Internet											
* Network											
Parice Alerte											
Device Alerts											
N Pachure											
Credentials											
Devices											
Schadula											
Variables											
Y BCD											
Alerts											
Parts											
Custom OID											
Y Devices	1										
Ignored Error Counters Ignored Interfaces											
Ignored Error Counters Ignored Interfaces Ignored Type Names		1212		- <u> </u>							
Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description	Add O	uange Delet	E.s.s	Reset Sort							
Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description	Add 0	belet	8-11	Reset Sort	X						
Ignored Error Counters Ignored Interfaces Ignored Type Names Interface Description V Diagram Layer-3 Excludes	Add O	Delet	Here .	Reset Sort							
Ignored Error Counters Ignored Interfaces Interface Description Diagram Layer-3 Excludes Layer-3 Ignores	Add O Filtered devices Agent device name	Boge Delet	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firor Counters Ignored Interfaces Interface Description > Diagram Layer-3 Excludes Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links	Add O Filtered devices Agent device name	Delet	Source	Reset Sort P Source Mask	Source Interface	Dest IP	Dest Mask	Dest interface	Protocol		
Ignored Error Counters Ignored Interfaces Interface Description Diagram Layer-3 Excludes Layer-3 Static Links Favorites	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort IP Source Mask	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firor Counters Ignored Tripe Names Interface Description V Diagram Layer-3 Excludes Layer-3 Staciudes Layer-3 Static Links Favorites Financials	Add Filtered devices Agent device name	Moge Delet	Source	Reset Sort IP Source Mask	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firer Counters Ignored Interfaces Interface Description Diagram Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favorites Financials V IPAM	Add Fiftered devices Agent device name	Boge Delet	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest interface	Protocol		
Ignored Firor Counters Ignored Trype Names Interface Description Daggers Layer-3 Excludes Layer-3 Static Links Favorites Financials IPAM Subnets	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firer Counters Ignored Interfaces Interface Description Diagram Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favorites Financials IPAM IPAM Subnets Issues	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Error Counters Ignored Interfaces Interface Description Dagaren Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favonites Financials IPAM Subnets Issues Issues Issues	Add Fiftered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Tiror Counters Ignored Interfaces Ignored Type Names Interface Description Uayers 3 Excludes Layers 3 Excludes Layers 3 Static Links Favorites Favorites Financials UBAM IPAM Subnets Issues Maps Meraki	Add Filtered devices Agent device name	Delet	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Error Counters Ignored Interfaces Ignored Type Hannes Interface Description Diagram Layer-3 Ischudes Layer-3 Static Links Faventes Financials IPAM Subnets Issues Maps Merziki NetFlow	Add Fiftered devices Agent device name	ange Delet	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firer Counters Ignored Tripe Names Interface Description Diagram Layer 3 Excludes Layer 3 Excludes Layer 3 Static Links Favorites Financials VI DAM IFAM Subnets Issues Maps Metabio NetFlow	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Error Counters Ignored Type Kannes Interfaces Diagram Layer-3 Iscludes Layer-3 Static Links Favorites Financials IPAM Subnets Issues Maps Merais NetFlow Network Thresholds Poling Poling	Add O Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firer Counters Ignored Interfaces Ignored Type Names Interface Description Daggers Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favorites Financials IPAM Subnets Issues Maps Meraki NetFlow Network Thresholds Poling System	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Tror Counters Ignored Interfaces Ignored Type Names Interface Description Diagram Layer-3 Excludes Layer-3 Static Links Favorites Financials PAM IPAM Subnets Issues Maps Metabia NetFlow Network Thresholds Polling Synlog TFIP WAN	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort P Source Mask	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Firer Counters Ignored Interfaces Ignored Type Names Interface Description Daggem Layer-3 Excludes Layer-3 Static Links Favorites Financials IPAM Subnets Issues Maps Metabi NetFlow NetHow Nethourk Thresholds Polling Systog TFIP WAN	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Dest IP	Dest Mask	Dest Interface	Protocol		
Ignored Tiror Counters Ignored Tiror Counters Ignored Tipe Names Interface Description Uayer 3 Excludes Layer 3 Excludes Layer 3 Excludes Layer 3 Excludes Layer 3 Excludes Favorites Favorites Favorites Mays Metabio NetFlow Network Thresholds Polling Syslog TFTP WAN NUT V Remoteinipht	Add Filtered devices Agent device name	Minge Delet	Source	Reset Sort	Source Interface	Det IP	Dest Mask	Dest Interface	Protocol		
Ignored Firor Counters Ignored Tiper Kannes Interface Description Diagram Layer-3 Excludes Layer-3 Static Links Favorites Financials VIPAM JUPAM JUPAM VIPAM Network Thresholds Polling Synlog TFIP VAN NET * Remoteinsight Script Editor	Add Filtered devices Agent device name	Agent IP	Source	Reset Sort	Source Interface	Det IP	Dest Mask	Dest Interface	Protocol		
Ignored Firer Counters Ignored Interfaces Ignored Type Names Interface Description Usyrer 3 Excludes Layrer 3 Excludes Layrer 3 Excludes Layrer 3 Excludes Layrer 3 Excludes Interface Financials IPAM Subnets Issues Maps Merakis NetFlow NetFlow NetFlow NetFlow NatT Yemotenisight Script Editor Veb Server	Add Filtered devices Agent device name	Argent IP	Source	Reset Sort	Source Interface	Det IP	Dest Mask	Dest Interface	Protocol		
Ignored Error Counters Ignored Interfaces Ignored Type Harnes Interface Description Diagram Layer-3 Excludes Layer-3 Static Links Favorites Favorites Favorites IPAM Subnets Issues Maps MetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow NetFlow VAN NaT Remoteinsight Script Editor Web Server	Add	Agent IP	Source	Reset Sort P Source Mask Reset Sort	Source Interface	Det IP	Dest Mask	Dest Interface	Protocol		
Ignored Tiror Counters Ignored Tiror Counters Ignored Tipe Names Interface Description Usinger Layer-3 Excludes Layer-3 Excludes Layer-3 Static Links Favorites Financials UBAM Subnets ISBAM IBAM Subnets ISBAM Meraki Metricow Network Thresholds Polling Synlog TFIP WAN NUT V Remoteinsight Script Editor Web Server Web Server	Add C	Agent IP	Source	Reset Sort P Source Mask Reset Sort	Source Interface	Dett IP	Dest Mask	Dest Interface	Protocol		

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



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

🞽 Fi	ow Interface Ar	nalysis Tool				-		×
In	Jse	Agent	IP	Inbound Int	Count			
8	No	bostonsw1-stout.pathsolutions.local	10.30.0.1	1001	34			
I	Yes	svfw1	10.50.0.1	1	0			
0	Yes	svfw1	10.50.0.1	3	0			
0	Yes	svfw1	10.50.0.1	5	0			
0	Yes	svfw1	10.50.0.1	9	0			
8	No	svfw1	10.50.10.1	1	1439050			
8	No	svfw1	10.50.10.1	4	17577			
8	No	svfw1	10.50.10.1	7	652427			
8	No	svfw1	10.50.10.1	9	4961			
8	No	svfw1	10.50.10.1	10	1691			
8	No	svfw1	10.50.10.1	11	76403			
8	No	svfw1	10.50.10.1	12	541345			
0	Yes	hqmx65	10.86.0.4	1	514340			
0	Yes	hqmx65	10.86.0.4	3	499675			
0	Yes	hqmx65	10.86.0.4	9	16330			
8	No	hqmx65	10.86.0.4	29	62058			
0	Yes	hqpa450	10.86.0.5	6	12950826			
(Add	Remove Details Clear				Copy to	o clipboa	rd

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

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



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



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

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

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

	🗾 Flow	v Interface Analysis Tool	×
		Are you sure you want to remove all e for IP address 10.86.0.4 on inbound in	ntries from the database terface 9?
-			Yes Cancel

Network Thresholds

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

TotalView Configuration Tool	-		×
Devices Cloud Servers Service	es Reports		
Search Options (Ctrl+E)	Network Thresholds		
Search Options (Ctrl+E) Internet Network Alerts BGP Custom OID Devices Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN	Hetwork Thresholds Thresholds Levels TotalView tracks utilization and error rates for each monitored interface on your network. To help you quickly determine if your network is healthy, you can set the thresholds for error rates and utilization. An interface will be flagged with a red indicator if it exceeds either of the below threshold levels: An error rate greater than S percent -or - A peak utilization rate greater than 90 percent		
NLT > Remotelnsight Reports > Risks SD-WAN > Servers Services > VoIP V	Revert	Арр	yy

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

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

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

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

Polling Behavior

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

TotalView Configuration Tool		-		×
Search Options (Ctrl+E)	Polling			0
Internet Alerts Backup BGP Custom OID Devices Diagram Favorites Financials Issues Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN Wash Meraki Meraki Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN Meraki NetWork Thresholds Polling Syslog TFTP WAN Meraki Meraki<	Polling Frequency Poll devices every Devices every Devices every Devices every Polling frequency is changed, daily graphs will be deared. Polling Options Declare a poll as failed if it does not receive a response within South and the seconds Poll device retries Number of threads for polling information from interfaces Update Bridge/Route information automatically every 10 minutes			Ø
NLT > Remotelnsight Reports > Risks SD-WAN > Servers Services > VolP		Revert	Арр	yk ii.

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

Polling Options

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

Polling Threads

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

Configuring the Polling Frequency

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

Note. In you change the poining frequency, an instolical duitzation mornation (daily, weekly, monthly, and yearly graphs)

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

Private IP

To manually add public IP space into your internal network so it is not identified as internet.

						- 0
	Jevices 📥 Cloud 🗐 Servers 🛔	Services 📥 B	leports			
White Note Nature Alf Construit 2000 2000 2000 Multiple 2000 2000 2000 2000 Water Wight 1000 2000 <th>h Options (Ctrl+E)</th> <th>Private IP</th> <th></th> <th></th> <th></th> <th></th>	h Options (Ctrl+E)	Private IP				
	Web Interface API Keys	^ Subnet	Mask			
	Authentication	10.0.0.0	255.0.0.0			
Web of	Multi-Site	127.0.0.0	255.0.0.0			
kod ip3:24.0.0 32:35.0.0 Without Str.0.0.0 32:35.0.0 Vitto 32:35.0.0 32:35.0.0 Vito </td <td>Web Server</td> <td>128.0.0.0</td> <td>255.0.0.0</td> <td></td> <td></td> <td></td>	Web Server	128.0.0.0	255.0.0.0			
where Water W	loud	169.254.0.0	255.255.0.0			
Week 102.04.00 20.200.0 Point Aline 20.00.0	lashboard	172.16.0.0	255.240.0.0			
<pre>start de set set set set set set set set set se</pre>	Weather Widget	192 168.0.0	255 255 0.0			
<pre>mint of the second of the</pre>	ternet	224.0.0.0	240.0.0.0			
Rece Actis Rece Actis Rece Actis Rece Actis Cactop Cactop Cactop Cactop Scholl Scholl <tr< td=""><td>etwork Alasta</td><td>224101010</td><td>240.0.0.0</td><td></td><td></td><td></td></tr<>	etwork Alasta	224101010	240.0.0.0			
Part Chaid Rever Alies Buck Alies Rever Alies Cardentis Docing Docing Rever Alies Subsidie Rever Alies Cardentis Docing Cardentis Docing Cardentis Docing Cardentis Docing Parts Cardentis Cardentis Docing Parts Cardentis Cardentis Docing Marts Reve 3 Editadie Garantis Reve 3 Editadie Marts Reversite Marts Reversite	Device Alerts					
Row Area Backy Cacher David Backy Cacher Backy Andri Rea Cacher Backy Andri Rea Good Difference Depending Specific Specific Backy Statis Backy Specific Backy Andre Dependent Backy	Parent/Child					
f blog Crednik Dreis Schald Schald Pore Catentili Dreis Bern Catentili Dreis Bern Catentili Dreis Bern Catentili Deritik Bern Catentili Bern Catentili Bern Catentili Bern Catentili Bern Bern <td< td=""><td>Route Alerts</td><td></td><td></td><td></td><td></td><td></td></td<>	Route Alerts					
Createrable Devices Schedule Willie Willie Willie Willie Willie Special Fore Courters Special Fore Courters Sp	Backup					
Devices Scheduly Scheduly Variable Base Scheduly Area Scheduly Custom DD Scheduly Devices Scheduly Spored Interfaces Scheduly	Credentials					
Schedde Wnibles #GP Arm Curem OD Obroke Ippored furc Couters Ippored furc faces Ippored furc faces Ippored furc Southers Ippored furc Southers <	Devices					
Big Big Area Big Area Big Joned Intracs Big Byoed Intractore Big Byoed Intracore Big	Schedule					
Book Attern Procession Sponded from Courders Layer Alatation Layer Alatation Layer Alatation Sponded from Courders Remote Courders Sponded from Courders Remote Courders Re	Variables					
Avers Press Pr	BGP					
Verify Cotation UD Devices porcel function porc	Alerts					
<pre>> Default of Server Serve</pre>	Peers Curtem O/D					
proces industriants of process	Custom Oil					
in poresi functives description* Vestgram Lyne*3 Ratis Links Franciski Parkis Parkis Netflow Netsort Netflow Netsort Ne	Ignored Error Counters					
Sport Dagan Lys-3 Stordus Lys-3 Stordus Lys-3 Stordus Lys-3 Stordus Hym M Fancius PMM PMM Sobets Ital Nethors Thresholds Poling Philes Voit Stord Doises Lording Distance Sopies Lording Distance Notices Lording Distance Sopies Lording Distance Notices Lording Distance Distance Distance Notices Lording Distance Distance<	Ignored Interfaces					
Insertare Description* Disgram Lays-3 Exoludes Lays-3 Storic Links Francisks Francisks BMM BMA Subnets Isues Maps Maps Metaki Netfor Neteorit Netfor Neteorit Pointes Systeg Stript Stript Editor WAN metakis Script Editor Wass Script Editor Maps Script Editor Wass Script Editor Script Edito	Ignored Type Names					
<pre>/ Digram Layer-3 Exoldes Layer-3 Stickles Favorites Favorites Favorites Favorites States States States Maps Marki M</pre>	Interface Description*					
Lyer-3 Janoes Lyer-3 Static Links Francials Francials PAM PAM Markati Markati Markati Markati Metalow Methods Methods Methods Methods Private PP Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Systeg TFTP WAN Methods Metho	 Diagram 	0				
Layer3 Statichts Favoritis Financials PAM PAM PAM Mass Saues Saues Mass Meski NetFloor NetFloor NetFloor NetFloor NetFloot Private P Systeg FTP Private P Systeg FTP FTP FTP FTP FTP FTP FTP FTP	Layer-3 Excludes					
Lyer 3 Static Links Faxorities Financials PAM IPAM Subones Issues Maps Maraki Meraki Meraki Network Treeholds Pelling Private IP Systeg TFTP WAN Meraki Social Enfort Web Server Storpt Enfort Meraki Maraki Maraki Maraki Maraki Merak	Layer-3 Ignores					
Favorités Financials FRAM IRAM Subotas Issues Issues Maps Maraki NetFloor NetFloor Poling Prinate IP Systeg TFTP TFTP WAN Web Server Internet Indight Scipt Editor Web Server Isports Sakes Aletts Cettificates Dictionary Dic	Layer-3 Static Links					
PadM PAM Subnts Sues Maps Metaki Metaki NetFlow Network Trusholds Poling Private IP Systop	Favorites					
Partial IPAM Subnets Issues Maps Meski Meski NeteRiow NeteRiow Poling Private IP Systeg TFIP VWAN emoteInsight Script Editor Web Server eports Idtares Centificates Dictionary DNS Geographic * JoT Policies Add Change Shft Up Shft Up Shft Up Shft Up	Financials					
Invision Bases Maps Meski Meski Netfor Netfor Poling Private IP Systeg Systeg Systeg Stript Editor Web Server eports sks Aletts Centricates Dictionary DNS Geographic / IoT Devices IoT VLAN Policies Add Shift Up Shift Down Reset Sort	PAM DAM Cuberts					
Maps Maps Maps Methods Polling Printel P Systeg TFTP WAN emotensight Script Editor Web Server esports Methods Maps Maps Maps Maps Maps Maps Maps Map	IPAM Subnets					
Merii Netflow Polling Printel P Systeg TFTP WAN Web Server Reports Sids Gater Netfor Web Server Peports Sids Gater Net Server Policies v Med Server Reports Sids Gater Net Server Sids Gater Net Server Net Serve	Mans					
NeFlow Pelling Phivate IP Systeg TFTP WAN emotennisht Script Effor Web Server eports tiks Alets Certificates Dictionary D	Meraki					
Network Thresholds Poiling Private IP Systog TFIP WAN emotelninght Scipt Editor Veb Sever leports isks Adets Certificates Dictionary Dictionary Dictionary Divers IoT ULAN Policies V Add Change Dette Shift Down Reset Sort	NetFlow					
Poling Systep Systep TFTP WAN emotehnight Societ Editor Web Server epots sks Alets Centricates Dictionary Dictionary DNS Geographic / IoT Devices IoT VLAN Policies V Add Change Delete Shift Up Shift Down Reset Soct	Network Thresholds					
Private IP Sysleg TFIP WAN emotehnight Script Editor Veb Server teports sists Alerts Centificates Dictionary DNS Geographic / IoT Devices IoT VLAN Policies V Add Change Shift Up Shift Down Reset Sort	Polling					
Systeg TFTP WAN evotensight Scipt Editor Web Server epots sks Alerts Centificates Dictionary DNS Geographic / LoT Devices LoT VLAN Policies V Add Change Delete Shift Up Shift Down Reset Sort	Private IP					
TFIP WAN emotelinight Scipt Editor Web Server eports tks Alerts Centificates Dictionary DNS Geographic 'soT Devices IoT VLAN Policies V Add Delete Shft Up Shft Down Reset Sort	Syslog					
VAN emotelnight Scipt Editor Veb Sever teports ists Alets Cetificates Dictionary DNS Geographic / IoT Devices IoT VLAN Policies v Add Change Delete Shift Up Shift Down Reset Sort	TFTP					
emotensigni Skipt Editor Web Server eports tiks Alerts Centificates Dictionary Dictionary DNS Geographic / IoT Devices IoT VLAN Policies v Add Change Delete Shift Up Shift Down Reset Sort	WAN					
Skipt Catalor skipt Server sports skis Alets Centificates Dictionary DNS Geographic / oT Devices IoT VLAN Policies v Ad Change Delete Shift Up Shift Down Reset Sort	emoteinsight Societ Editor					
Add Change Delete Shift Up Shift Down Reset Sort	Script Editor					
Alets Alets Certificates Dictionary DNS Geographic IoT ULAN Policies IoT VLAN Policies V Add Change Delete Shift Up Shift Down Reset Sort	enorts					
Alets Cetificates Dictionary DNS Geographic / DT Devices IoT VLAN Policies v Add Change Delete Shift Up Shift Down Reset Sort	isks					
Centificates Dictionary DNS Geographic FoT Devices Add Change Delete Shift Up Shift Down Reset Sort	Alerts					
Dictionary DNS Geographic / DT Devices IoT VLAN Policies / Add Change Delete Shift Up Shift Down Reset Sort	Certificates					
DNS Geographic / IoT Devices IoT VLAN Policies // Add Change Delete Shift Up Shift Down Reset Sort	Dictionary					
Geographic IoT Devices IoT VLAN Policies v Add Change Delete Shift Up Shift Down Reset Sort	erectoriely.					
/ IoT Devices IoT VLAN Policies v Add Change Delete Shift Up Shift Down Reset Sort	DNS					
Dences IoT VLAN v Add Change Delete Shift Up Shift Down Reset Sort	DNS Geographic					
Policies v Add Change Delete Shift Up Shift Down Reset Sort	DNS Geographic IoT					
Policies	DNS Geographic F IoT Devices					
	DNS Geographic IoT Devices IoT VLAN	Add	Change Delete	Shift Up Shift Down	Reset Sort	
	DNS Geographic / IoT Devices IoT VLAN Policies	✓ Add	Change Delete	Shift Up Shift Down	Reset Sort	

Add button

🌮 Chan	ige Subnet		×
Subnet:	224.0.0.0		٢
Mask:	240.0.0.0		٢
		ОК	Cancel

Syslog

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

TotalView Configuration Tool					-	- D X
Services Cloud Servers Services	es Report	5				
Search Options (Ctrl+E)	Syslog					•
Internet	Enable Syslog	server C:\Program Files	(x86)\PathSoluti	ions\TotalView\SYSLOG	i	
Network Alerts	Device name	IP address or group	Facility	Severity	Email	Search string
> Backup	Any	Any	Any	Any	itops@pathsolutions.com	Configured from
BGP Curtom OID	Any	Any	Any	Any	itops@pathsolutions.com	commit
> Devices						
> Diagram						
Favorites						
Financials						
Issues						
Meraki						
NetFlow						
Network Thresholds						
Polling						
Syslog						
TFTP						
WAN						
NLI Remetaleziakt						
Reports						
> Risks						
SD-WAN						
> Servers	_					
Services	<					>
> VoIP	Add	Change Delete.		Reset Sort		
					Revert	Apply

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

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

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

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

Change syslo	g alert	<
Email address:	noc@company.com	
IP address:	10.0.0.21 (Pinot)	•
Facility:	Any 💌	
Severity:	Any 💌	
Search string:	STP	
Test string:		
Test result:		_
	OK Cancel	

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

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

The Syslog matching capability is ECMAScript compatible.

Facility Levels

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

Facility Number Keyword Facility Description

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

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

Severity Levels

RFC 5424 defines eight severity levels.

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

ECMAScript Regular Expressions Pattern Syntax (regex)

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

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

Special Pattern Characters

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

characters	description	matches
•	not newline	any character except line terminators (LF, CR, LS, PS).
\t	tab (HT)	a horizontal tab character (same as \u0009).
\n	newline (LF)	a newline (line feed) character (same as $u000A$).
\ v	vertical tab (VT)	a vertical tab character (same as \u000B).
\f	form feed (FF)	a form feed character (same as \u000C).
\r	carriage return (CR)	a carriage return character (same as \u000D).
\cletter	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 hh	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 #.
\uhhhh	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 <u>groups</u> below for more info.
\d	digit	a decimal digit character (same as [[:digit:]]).
\D	not digit	any character that is not a decimal digit character (same as [^[:digit:]]).
\s	whitespace	a whitespace character (same as [[:space:]]).
\s	not whitespace	any character that is not a whitespace character (same as [^[:space:]]).
\w	word	an alphanumeric or underscore character (same as [_[:alnum:]]).
\w	not word	any character that is not an alphanumeric or underscore character (same as [^_[:alnum:]]).

\character	character	the <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: $^{\circ} $
[class]	character class	the target character is part of the class (see <u>character classes</u> below)
[^ <i>class</i>]	negated character class	the target character is not part of the class (see <u>character classes</u> 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 backslash (\)
character
2
```

Quantifiers

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

characters	times	effects
*	0 or more	The preceding atom is matched 0 or more times.
+	1 or more	The preceding atom is matched 1 or more times.
;	0 or 1	The preceding atom is optional (matched either 0 times or once).
{int}	int	The preceding atom is matched exactly <i>int</i> times.
{ <i>int</i> ,}	<i>int</i> or more	The preceding atom is matched <i>int</i> or more times.
{min,max}	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			
(subpattern) Group		Creates a backreference.			
(?:subpattern) Passive group		Does not create a backreference.			

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

These submatches can be used in the regular expression itself to specify that the entire subpattern should appear again

somewhere else (see \int in the <u>special characters</u> list). They can also be used in the <u>replacement string</u> or retrieved in the <u>match results</u> object filled by some <u>regex</u> 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> .
\в	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		
Ι	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> ' <u>isctype</u> member with the appropriate type gotten from applying <u>lookup classname</u> member on <i>classname</i> for the match.
[. <i>classname</i> .] collating sequence		Uses the <i>regex traits</i> ' <u>lookup collatename</u> to interpret <i>classname</i> .
[=classname=] character equivalents		Uses the <i>regex traits</i> ' <u>transform primary</u> of the result of <u>regex_traits::lookup_collatename</u> for <i>classname</i> to check for matches.

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

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

• Please note that the brackets in the class names are additional to those opening and closing the class definition. For example:

[[:alpha:]] is a character class that matches any alphanumeric character.

[abc[:digit:]] is a character class that matches a, b, c, or a digit.

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

• Escape characters: All escape characters described above can also be used within a character class specification. The only change is with \b, that here is interpreted as a backspace character (\u0008) instead of a word boundary.

Notice that within a class definition, those characters that have a special meaning in the regular expression (such as *, ., \$) don't have such a meaning and are interpreted as normal characters (so they do not need to be escaped). Instead, within a class definition, the hyphen (-) and the brackets ([and]) do have a special meaning under some circumstances, in which case they should be escaped with a backslash (\) to be interpreted as normal characters.

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

TFTP Server

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

TotalView Configuration Tool			-		Х
Devices Cloud Servers		orts			
Search Options (Ctrl+E)	TETP				Ó
Internet	▲ Enable TF	TP server			
✓ Network	TFTP Directo	rv: C:\Program Files (x86)\PathSolutions\TotalView\TFTP		Browse	
> Alerts					
> Backup BGD					
Custom OID					
> Devices					
> Diagram					
Favorites					
Financials					
Issues					
Meraki					
NetFlow					
Network Thresholds					
Polling					
Syslog					
TFTP					
WAN					
NLI Remotelesisht					
Reports					
> Risks					
SD-WAN					
> Servers					
Services					
> VoIP					
[v				
			Dovort	Apr	der.
			Revent	мрр	лу

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

WAN Interfaces

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

TotalView Configuration Tool					- [X
Search Options (Ctrl+E)	vices Reports WAN					
Internet	Device name	IP address	Int#	Provider	Circuit ID	Sup
✓ Network	HQ LAN/SantaClara.pathsolutions.local	10.0.0.2	1	-	-	-
> Backup	HQ LAN/MPLSCore.pathsolutions.local	10.0.0.3	1	-	-	-
BGP	HQ LAN/MPLSCore.pathsolutions.local	10.0.0.3	2	-	-	-
Custom OID	HQ FW/hqpa450	10.86.0.5	6	-	-	-
> Devices		10.51.0.1	6	-	-	-
> Diagram	HQ FW/hqmx65	10.86.0.4	1	-	-	-
Maps Maps Meraki NetFlow Network Thresholds Polling Syslog TFTP WAN NLT Remotelnsight Reports SD-WAN Servers Services VolP	< < Add Change Delete	Shift Up	Shift Down	Reset Sort		>
					Revert	Apply

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

Add WAN interfa	ce	\times
IP address: 10.0.0).1 (Syrah)	•
Interface number:	1	* •
Provider:	AT&T	
Circuit ID:	C8272-72-A827	
Support phone:	1-877-555-1234	
Monthly cost:	680	
Expiration date:	6/28/2019	•
Notes:	,	
Patch Panel B2-21		
1	OK Cancel	

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

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

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

Note: Add WAN by editing the CFG text file. See <u>Appendix H. Changing the WAN Tab</u>.

NLT

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

TotalView Configuration Tool						-		×
Cloud Servers Servi	ces Report	5						
Search Options (Ctrl+E)	NLT							۵
> TotalView	Website:							
Cloud Dashboard Internet Network NLT Reports Risks SD-WAN Servers Services VolP	Device name	IP/Group	Aliases					
	Add	Change	Delete	Reset Sort				
					Re	evert	Арр	ly .:

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

🐉 Add Alia	15	<
Type:	Device O Group	
IP address:	Headquarters/RuckusAP (10.0.0.6)	
Aliases:	default group]
	OK Cancel	

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

🐉 Add	Alias					×
Type:		Group				
Group:	Default					\sim
Aliases:	default group					
				ОК	Cancel	

Remote Insight

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

TotalView Configuration Tool		-		х
Cloud Servers Services	ces Reports			
Search Options (Ctrl+E)	RemoteInsight			
 > Total/View Cloud > Dashboard Internet > Network NLT > Remotelnsight Script Editor Web Server Reports > Risks SD-WAN > Servers Services > VolP 	Script Editor: This configures scripts for RemoteInsight server operates.			
	Re	vert	Арр	ly

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

The Script Editor configures scripts for RemoteInsight.

🌮 TotalView Configuration Tool		-		×
Cloud Servers Serv	ices Reports			
Search Options (Ctrl+E)	Script Editor			
 > TotalView Cloud > Dashboard Internet > Network NLT > Remotelnsight Script Editor Web Server Reports > Risks SD-WAN > Servers Services > VolP 	Run Script Editor			
	Re	evert	Арр	уy

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

TotalView Configuration Tool					-		×
Devices Cloud Servers Ser	rvices Reports						
Search Options (Ctrl+E)	Web Server						<u>ک</u>
> TotalView	RemoteInsight Serve	er Options					
Cloud	Enable Server:	Enable secondary RemoteInsight se	erver				
> Dashboard	Conver hanes						
Internet	server type:						
NLT	Server port number:	444 🛉					
✓ Remotelnsight	Check in interval:	300 🜩 seconds					
Script Editor							
Web Server	Certificate			Access Control List:			
Risks							
SD-WAN	Server Certificate:	View Full Info					
> Servers Services	 ✓ Date is valid. ✓ Private key mate 	hes the certificate.					
> VoIP	Valid:	8/22/2023 10:31 PM - 8/21/2024					
	Subject	4:55 PM C = LIS_ST = California L =					
	Subject	Santa Clara, O = PathSolutions,					
		OU = IT Operations, CN = *.pathsolutions.local					
	Alternative	DNS:*.pathsolutions.local					
	names: Tssuer:	DC = local, DC = pathsolutions.					
		CN = pathsolutions-DAPHNE-CA		The list is empty. Any client can access the RemoteInsight server.			
	Generate CSR:	Generate Certificate Request					
	Import Certificate:	Import KEY file					
		Import Certificate file					
		Validate Certificate					
		Valuate Certificate					
	Restore Certificate:	View Backup Certificate					
		Restore Certificate from Backup		Edit List			
					 Revert	Ap	ply

Reports

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

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

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

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

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

TotalView Configuration Tool					-		Х
Cloud Servers 🔊 Services	es Reports						
Search Options (Ctrl+E)	Reports						
> TotalView	Report Name	Report File	Schedule	Send To	Paramete	rs	
 Doshboard Internet Network NLT Remotelnsight Reports Risks SD-WAN Services VoIP VoIP 	Monthly Device Uptime Report	UptimeDevicesMonthlyReport.bt	0001*?	swinter@pathsolutions.com			
	Add	Delete Shift Up Sh	ift Down R	leset Sort	Revert	Арр	oly .:i

Risks Monitoring

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

TotalView Configuration Tool		_		\times
Devices Cloud Servers Search Options (Ctrl+E) TotalView Cloud Dashboard Internet Network NLT Remotelnsight Reports Risks Alerts Certificates Dictionary DNS Geographic > IoT Policies Rogue IT Whitelist SD-WAN Servers Services > VolP	Service Reports	Revert	Apt	ply

Risks Alerts

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

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

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

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

TotalView Configuration Tool			-		×
Cloud Servers Servin	ces Reports				
Search Options (Ctrl+E)	Alerts				٨
Search Options (Ctrl+E)	Alerts Static IP in DHCP scope ARP cache poisoning Rogue Infrastructure Devices New Devices Suspicious Devices Malware communications Peer To Peer communications Foreign Country communications	itops@pathsolutions.com itops@pathsolutions.com itops@pathsolutions.com itops@pathsolutions.com itops@pathsolutions.com itops@pathsolutions.com			
> 1015		Re	evert	Арр	ly

Certificates (SSL)

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

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

TotalView Configuration Tool	- 0	Х
Cloud Servers 🔊 Servers	ces Reports	
Search Options (Ctrl+E)	Certificate Monitoring	
> TotalView Cloud	Certificate monthly report: Itops@pathsolutions.com Test Send Certificate Report Now	
> Dashboard	Server	
> Network	www.pathsolutions.com	
NLT	fred.pathsolutions.local	
> Remotelnsight	portal.pathsolutions.com	
✓ Risks	files.pathsolutions.com	
Alerts	velma.pathsolutions.local	_
Certificates	velma.pathsolutions.com	_
Dictionary	txfw1.pathsolutions.local	_
Geographic	chi01.pathsolutions.com:54433	_
> IoT	nj01.pathsolutions.com:54433	_
Policies	sea01.pathsolutions.com:54433	_
Rogue IT		
SD-WAN		
> Servers		
Services		
> VoIP		
	Add Change Delete Copy Shift Up Shift Down Check Certifica	ites
	Revert Apply	

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

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

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



Below is an example of the emailed report.

TotalV	liew		Expired Ce	rtificates as of 1/31	1/2023 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				

Dictionary

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

Process Process Process Process Process Process Process Process Process Process Process Process Process Process Proc	TotalView Configuration Tool		-		×
Search Options (Ct/1∉) Dictionary Image: Search Options (Ct/1∉) Send alert email to: Itops@pathsolutions.com Image: Search Options (Ct/1∉) Dashboard Internet Network Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) Network Image: Search Options (Ct/1∉) Send alert email to: Itops@pathsolutions.com Image: Search Options (Ct/1∉) Network Image: Search Options (Ct/1∉) Send alert email to: Itops@pathsolutions.com Image: Search Options (Ct/1∉) Network NLT Remotelnsight 3 Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) Network NLT Remotelnsight 3 Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) Network NLT Remotelnsight 3 Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) Notionary DNS Search Options Soarch Options (Ct/1∉) Image: Search Options (Ct/1∉) SD-WAN Servers Services Soarch Options Soarch Options (Ct/1∉) Image: Search Options (Ct/1∉) VolP Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) Image: Search Options (Ct/1∉) VolP Image: Search Options (Ct/1 ∉) Imag	Devices Cloud Servers Service	ces Reports			
> TotalView Coud Send alert email to: Itops@pathsolutions.com > Dashboard Internet Trigger alert if dictionary matched 3 times within 60 seconds. NLT RemoteInsight 80 seconds Wait at least 300 seconds after alert. Reports Risks Alerts 00 seconds after alert. Dictionary DNS Geographic IoT Policies Rogue IT Whitelist Servers Servers Servers Servers Servers Servers ValP VolP Apply	Search Options (Ctrl+E)	Dictionary			δ
Revert Apply	Search Options (Ctrl+E)	Dictionary Send alert email to: itops@pathsolutions.com Trigger alert if dictionary matched 3 2 times within 60 2 seconds. Wait at least 300 2 seconds after alert.			
	,	R	evert	Appl	ly

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

DNS (DNS Record Monitoring)

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

TotalView Configuration Tool					_	
Search Options (Ctrl+E)	DNS					
> TotalView	Group	DNS Server Address	Туре	Record	Expected Value	Email
Cloud	Internal	10.0.0.10	A	www.pathsolutions.com	199.60.103.31,1	itops@pathsolut
> Dashboard	Internal	10.0.0.10	A	fred.pathsolutions.local	10.1.0.15	swinter@pathsol
> Network	Internal	10.0.0.10	A	velma.pathsolutions.local	10.1.0.11	swinter@pathsol
NLT	External	8.8.8.8	A	www.pathsolutions.com	199.60.103.31,1	itops@pathsolut
> Remotelnsight	External	8.8.8.8	A	files.pathsolutions.com	74.220.215.89	itops@pathsolut
Reports	External	8.8.8.8	A	portal.pathsolutions.com	104.8.32.109	itops@pathsolut
Alerts	External	8.8.8.8	CNAME	www.pathsolutions.com	2613869.group1	itops@pathsolut
Certificates	External	8.8.8.8	MX	pathsolutions.com	pathsolutions	itops@pathsolut
Dictionary	External	8.8.8.8	NS	pathsolutions.com	dns2.name	itops@pathsolut
Geographic > IoT Policies Rogue IT Whitelist SD-WAN > Servers Services > VoIP						
	<				_	>
	Add	Change Delete	Copy	Shift Up Shift Do	wn Reset	Sort
					Revert	Apply

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

🌮 Change		×
Group:	Lab	~
DNS server address:	10.0.0.10	~
Record type:	АААА	~
Record:	Enter the hostname for the AAAA record	
	fred.pathsolutions.local	
Expected value:	fe80::9974:ae74:3092:61a4	Resolve
Alert email:	swinter@pathsolutions.com,ttitus@pathsolutions.com	~
Note:		
	ОК	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, complete the **Expected Value** field, and the **Alert email** field.

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

Geographic

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

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

TotalView Configuration Tool			-		×
Cloud Servers Serv	ces Reports				
Search Options (Ctrl+E)	Geographic				
> TotalView	Whitelisted	Blacklisted			
Cloud	Country	Country			
> Dashboard	United States of America	Russian Federation			_
> Network		Iran (Islamic Republic of)			
NLT		Nigeria			
> Remotelnsight		Turkiye			
Reports		Cuba			
✓ Risks		Sudan			
Alerts					
Dictionary					
DNS					
Geographic					
> IoT					
Policies					
Whitelist					
SD-WAN					
> Servers					
Services					
> VoIP					
	Add Change Delete Res	et Sort Add Change Delet	e	Reset	Sort
		De	wert	Apr	slv
			TO C	- Abb	~ 7

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

💞 Add Country	×
Country:	
Canada	~
	OK Cancel

ΙοΤ

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

TotalView Configuration Tool	-		×
Cloud Servers Services Reports			
Search Options (Ctrl+E) IoT			
> TotalView Devices: Identifies the OUIs used on IoT devices to locate them on the network.			
Cloud IoT VLAN: Identifies the VLANs that are used for IoT devices to identify them on the network.			
> Dashboard			
Internet Internet			
NIT			
> Remotelnsight			
Reports			
✓ Risks			
Alerts			
Certificates			
Dictionary			
Georganhic			
Devices			
IoT VLAN			
Policies			
Rogue IT			
Whiteust SD_WAN			
> Servers			
Services			
> VolP			
Built		App	due
NEVER STATES		App	πγ.

Devices

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

TotalView Configuration Tool			-		×
Cloud Servers Servers	vices Repo	<u>ts</u>			
Search Options (Ctrl+E)	Devices				6
> TotalView	MAC OUI	Description			^
Cloud	58.20.B1	Hewlett Packard			
> Dashboard	00.10.83	Hewlett Packard			
> Network	70.5A.0F	Hewlett Packard			
NLT	F0.D2.F1	Amazon Technologies			
> Remotelnsight	88.71.E5	Amazon Technologies			
Reports	FC.A1.83	Amazon Technologies			
Alerts	CC.F7.35	Amazon Technologies			
Certificates	1C.12.B0	Amazon Technologies			
Dictionary	24.4C.E3	Amazon Technologies			
DNS	4C.17.44	Amazon Technologies			
	DC.54.D7	Amazon Technologies			
Devices	38.F7.3D	Amazon Technologies			
IoT VLAN	50.DC.E7	Amazon Technologies			
Policies	3C.5C.C4	Amazon Technologies			
Whitelist	08.A6.BC	Amazon Technologies			
SD-WAN	F0.27.2D	Amazon Technologies			
> Servers	74.C2.46	Amazon Technologies			
Services	68.37.E9	Amazon Technologies			
> VOIP	78.E1.03	Amazon Technologies			
	C4.95.00	Amazon Technologies			~
	Add	Change Delete Reset Sort			
			Revert	Арр	yly

IoT VLAN

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

TotalView Configuration Tool		-		\times
Cloud Servers Services	ces Reports			
Search Options (Ctrl+E)	IOT VLAN			
> TotalView	VLAN Name or Number			
Cloud	loT			
> Dashboard	Guest			
> Network				
NLT				
> Remotelnsight				
Reports				
✓ Risks				
Alerts				
Dictionary				
DNS				
Geographic				
✓ IoT				
Devices				
IoT VLAN Delisies				
RoqueIT				
Whitelist				
SD-WAN				
> Servers				
Services				
> VolP				
	Add Change Delete Reset Sort			
		overt	Apr	du.
	ň	urun	- Ahh	.,

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.

TotalView Configuration Tool						_		\times
Services Cloud Servers Service	es Reports							
Search Opuons (Ctri+E)	Policies							2
 > TotalView Cloud > Dashboard Internet > Network NLT > Remotelnsight Reports > Risks Alerts Certificates Dictionary DNS Geographic > IoT Policies Rogue IT Whitelist SD-WAN > Servers Services > VolP 	Cevice name	Flow source	Protocol	Port	Source IP	Source Mask	Dest IP	>
	Add	Change De	ete	ift I In Shift De	wn Peret	Sort		
	Auu	Undergen. De	SI 31	Shirtoo	Reset	SUL		
						Revert	Appl	y

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

Source:	Any				~
Protocol:	O Any	● TCP			MP
Port:	O Any	Specific	443	•	
Source IP:	10.0.0.0				8
Source mask:	255.0.0.0				8
Destination IP:	31.13.65.36				0
Destination mask:*	256.256.256.2	56			8
Send alert to:	itops@pathsolu	itions.com			~
Description:	tcp				0

A single policy match can be defined on this dialog.

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

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

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

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

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

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

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

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

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

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

Below is an example of a policy list.

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

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

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

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

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

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

TotalView Configuration Tool		- 0	Х			
Cloud Servers	es Reports					
Search Options (Ctrl+E)	Rogue IT		۵			
> TotalView	Search string	Manufacturer	^			
Cloud	NETGEAR	1 manufacturer (NETGEAR), 73 OUIs	-			
Internet	D-Link International	1 manufacturer (D-Link International), 60 OUIs				
> Network	Linksys	2 manufacturers (Cisco-Linksys, LLC, The Linksys Group, Inc.), 27 OUIs				
NLT	Playstation	Search string not found				
> Remotelnsight	Roku, Inc	2 manufacturers (Roku, Inc, Roku, Inc.), 25 OUIs				
Keports V Riske	Tivo	6 manufacturers (Enablers Solucoes e Consultoria em Dispositivos,				
Alerts	Microsoft Corporation	1 manufacturer (Microsoft Corporation), 75 OUIs				
Certificates	Google, Inc.	1 manufacturer (Google, Inc.), 78 OUIs				
Dictionary	Apple, Inc.	1 manufacturer (Apple, Inc.), 1233 OUIs				
DNS Geographic	Amazon Technologies Inc.	1 manufacturer (Amazon Technologies Inc.), 163 OUIs				
> IoT	WESTERN DIGITAL	4 manufacturers (HGST a Western Digital Company, WESTERN DIGIT				
Policies	APC by Schneider Electric	1 manufacturer (APC by Schneider Electric), 1 OUI 1 manufacturer (Data Robotics, Incorporated), 1 OUI				
Rogue IT	Data Robotics, Incorporated					
Whitelist SD-WAN	GIGA-BYTE TECHNOLOGY CO., LTD.	1 manufacturer (GIGA-BYTE TECHNOLOGY CO., LTD.), 21 OUIs				
> Servers	Nest Labs Inc.	1 manufacturer (Nest Labs Inc.), 2 OUIs				
Services	SAMSUNG ELECTRO-MECHANICS(THAILAND)	1 manufacturer (SAMSUNG ELECTRO-MECHANICS(THAILAND)), 34				
> VoIP	Vizio, Inc	1 manufacturer (Vizio, Inc), 12 OUIs				
	D-Link Corporation	1 manufacturer (D-Link Corporation), 24 OUIs				
	TP-LINK TECHNOLOGIES CO., LTD.	1 manufacturer (TP-LINK TECHNOLOGIES CO., LTD.), 166 OUIs				
	TP-LINK CORPORATION PTE. LTD.	1 manufacturer (TP-LINK CORPORATION PTE. LTD.), 9 OUIs	~			
	Add Change Delete	Reset Sort				
		Revert Apply	/			

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

🌮 Change Manufacturer	×
Manufacturer name, OUI or MAC address:	
Playstation	8
	OK Cancel

Whitelist

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

TotalView Configuration Tool		<u>.</u>		- 0	×
Search Options (Ctrl+E)	Whitelist				6
> TotalView	Туре	Address	Protocol	Business justification	^
Cloud	New Device	00-0C-29-01-FE-5D		MAC Address 00-0C-29-01-FE-5D checked by user on	
Internet	New Device	00-0C-29-11-08-BB		MAC Address 00-0C-29-11-08-BB checked by user on	
> Network	New Device	00-0C-29-2B-9A-52		MAC Address 00-0C-29-2B-9A-52 checked by user on	
NLT	New Device	00-0C-29-34-D0-B4		MAC Address 00-0C-29-34-D0-B4 checked by user on	
> Remotelnsight	New Device	00-0C-29-54-09-4E		MAC Address 00-0C-29-54-09-4E checked by user on	
Risks	New Device	00-0C-29-55-5E-52		MAC Address 00-0C-29-55-5E-52 checked by user on	
Alerts Certificates Dictionary	New Device	00-0C-29-71-0A-55		MAC Address 00-0C-29-71-0A-55 checked by user on	
	New Device	00-0C-29-90-E1-9B		MAC Address 00-0C-29-90-E1-9B checked by user on	
	New Device	00-0C-29-B8-10-A5		MAC Address 00-0C-29-B8-10-A5 checked by user on	
DNS	New Device	00-0C-29-CB-B2-1D		MAC Address 00-0C-29-CB-B2-1D checked by user on	
> IoT	New Device	00-10-49-00-6F-60		MAC Address 00-10-49-00-6F-60 checked by user on	
Policies	New Device	00-10-49-02-47-13		MAC Address 00-10-49-02-47-13 checked by user on	
Rogue IT	New Device	00-10-49-03-1E-20		MAC Address 00-10-49-03-1E-20 checked by user on	
Whitelist SD-WAN	New Device	00-10-49-03-20-9F		MAC Address 00-10-49-03-20-9F checked by user on	
> Servers	New Device	00-10-49-03-E1-42		MAC Address 00-10-49-03-E1-42 checked by user on	
Services	New Device	00-19-B9-A1-18-6E		MAC Address 00-19-B9-A1-18-6E checked by user on	
> VoIP	New Device	00-1A-A0-51-E9-FE		MAC Address 00-1A-A0-51-E9-FE checked by user on	
	New Device	00-1B-17-EB-A6-46		MAC Address 00-1B-17-EB-A6-46 checked by user on	
	New Device	00-50-56-60-DD-D4		MAC Address 00-50-56-60-DD-D4 checked by user on	
	New Device	00-50-56-64-16-C7		MAC Address 00-50-56-64-16-C7 checked by user on	~
	Add	Change Delete			
				Revert App	y

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

💕 Add	×
Entry type:	Unsecured Communications
IP:	10.0.0.15
Protocol:*	~
Business reason:*	unauthorized
	(minimum 20 chracters)
	OK Cancel

SD-WAN

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

TotalView Configuration Tool								-		\times
Cloud Servers 🔔 Servi	ces 📥 Re	ports								
Search Options (Ctrl+E)	SD-WAN									
> TotalView	Find: Group,	Address, Name								
> Dashboard	Group	Address	Name	Latency, ms	Loss, %	Route	DSCP	Email		
Internet	External	www.zoom.us	Zoom Website			No				
NLT										
> Remotelnsight Reports										
> Risks										
> Servers										
Services										
	Add	Change De	Copy	Shift Up S	Shift Down	R	eset Sort			
								Revert	App	dγ

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.

💞 Change		×
Group:	Default	~
Address:	129.250	.3.27
Name:	HQ-ATX	- Comcast
Icon:	Comcast	t.png
DSCP:	46	
Email Al	erts	
Email:		✓
Latency th	reshold:	0
Loss thres	hold:	0
Route	change	
		OK Cancel

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.

TotalView Configuration Tool		-		\times
Cloud Servers Servi	ices Reports			
Search Options (Ctrl+E)	Servers			
Search Options (Ctrl+E) TotalView Cloud Dashboard Internet Network NLT Remotelnsight Reports Risks SD-WAN Servers Operating Systems Services VolP VolP	Do you want to monitor servers? Yes No Operating Systems: This configures the different operating systems to be monitored. Server Thresholds: These are the thresholds to identify a server as having an issue.	evert	App	łv

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

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

TotalView Configuration Tool		_		×
Cloud Servers Servi	ces Reports			
Search Options (Ctrl+E)	Operating Systems			
> TotalView	Linux Servers: Configure how Linux servers are identified.			
Cloud	Windows Servers: Configure how and which Windows servers are monitored.			
> Dashboard				
Network				
NIT				
> Remotelnsight				
Reports				
> Risks				
SD-WAN				
✓ Servers				
 Operating Systems 				
 Linux Servers Windows Servers 				
Server Thresholds				
Services				
> VoIP				
				_
	Re	vert	Apply	
				:

Linux Servers Monitoring

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

TotalView Configuration Tool			-		\times
Cloud Servers Services	es Reports				
Search Options (Ctrl+E)	Linux Servers				
> TotalView	Alerts: Cor	nfigure Linux server alerts.			
> Dashboard	Ignored Daemons: Cor	nfigures Linux ignored daemons.			
Internet	Ignored Volumes: Cor	nfigures Linux ignored volumes.			
> Network	Polling: Cor	nfigures the polling behavior.			
NLT	Servers: Cor	nfigure which Linux servers should be monitored.			
> Remotelnsight					
> Risks					
SD-WAN					
✓ Servers					
 Operating Systems 					
✓ Linux Servers					
Ignored Daemons					
Ignored Volumes					
Polling					
Servers					
> Windows Servers					
Services					
> VoIP					
			_		_
		Re	vert	Appl	У
					.::

How to Identify Linux Servers

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

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

TotalView Configuration Tool		– 🗆 X
Cloud Servers	ices Reports	
Search Options (Ctrl+E)	Servers	٨
> TotalView	Linux Identifiers	Found Linux Servers
Cloud	Identifiers	∆ Device name ^
Internet	10.1.0.10	HQ FW/hqmx65
> Network	10.1.0.9	HQ FW/hqpa450
NLT	"ubnt"	HQ FW/hqf140d-poe
> Remoteinsight Benorts	"RHEL"	HQ LAN/Syrah
> Risks		HQ LAN/SantaClara.pathsoluti
SD-WAN		HQ LAN/MPLSCore.pathsolutic
✓ Servers		HQ LAN/RuckusAP
 Operating Systems Linux Servers 		HQ LAN/tempranillo.pathsolut
Alerts		HQ LAN/Michelob
Ignored Daemons		HQ LAN/Burgundy
Ignored Volumes		HQ LAN/Chardonnay
Polling		HQ LAN/Pinot
> Windows Servers		HQ LAN/Merlot
Server Thresholds		HQ LAN/Muscat
Services		HQ LAN/Franc
> VoIP		HQ LAN/Palomino
		HQ LAN/Riesling
		HQ LAN/PS-PTR1 Y
		< >
	Add Change Delete Shift Up Shift Down	Reset Sort
		Revert Apply

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

Add Identifier			×
Identify device as Linux server by:			
$\textcircled{\ensuremath{\bullet}}$ Text phrase in the description:	rhel		?
O IP Address:	Exclude this IP address from match		\sim
		ОК	Cancel

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

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

🚀 Add Identifier			×
Identify device as Linux server by: O Text phrase in the description:			?
D Address	Headquarters/Riesling (10.0.0.29)		~
O I Hadross	Exclude this IP address from match		
2			
		ОК	Cancel

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

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

TotalView Configuration Tool		– 🗆 X
Cloud Servers Ser	vices 📕 Reports	
Search Options (Ctrl+E)	Servers	٨
> TotalView	Linux Identifiers	Found Linux Servers
Cloud	Identifiers	Device name
Internet	10.1.0.10	HQ LAN/Merlot
> Network	10.1.0.9	HQ LAN/Muscat
NLT	"ubnt"	HQ LAN/Franc
> Remotelnsight	"RHEL"	HQ LAN/Palomino
> Risks		HQ LAN/Riesling
SD-WAN		HQ LAN/PS-PTR1
✓ Servers		HQ LAN/Dubonnet
 Operating Systems 		HQ LAN/barleywine
✓ Linux Servers		HO LAN/Alsace
Ignored Daemons		HQ LAN/iDRAC-149XCV2
Ignored Volumes		HQ LAN/hgap1-meraki
Polling		HO LAN/PS-P1-OpenGear
Servers		HO VMware/scrappy.pathsolut
> Windows Servers Server Thresholds		A HO VMware/dev-ubnt-lts01
Services		A HO VMware/dev-rhei85-01.pat
> VoIP		A HO VMware/ps-esv2.pathsoluti
		A HO VMware/psym1.pathsolutic
		SV LAN/svfw1
		< >
	Add Change Delete Shift Up Shift Down	Reset Sort
		Revert Apply

Linux - Alerts

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

TotalView Configuration Tool					_		×
Search Options (Ctrl +E)	Alerts	rts					
					D :		
Cloud	Server	Daemon	Ihreshold	Email	Description		
> Dashboard	Any	Server: Communication failure		itops@pathsolutions.com	Linux Server comm fail		
Internet							
> Network							
NLT							
> Remotelnsight							
Reports							
SD-WAN							
✓ Servers							
✓ Operating Systems							
 Linux Servers 							
Alerts							
Ignored Daemons							
Ignored Volumes							
Servers							
> Windows Servers							
Server Thresholds							
Services							
> VoIP							
	Add	Change Delete					
					Revert	Ap	ply

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

🌮 Add Aler	t X
Linux serv	ver 🔘 Group
All	~
Alert:	Server Communication Failure
Daemon:	All
Threshold:	10 4
Send to:	itops@pathsolutions.com
Description:	linux alert comm failure
	OK Cancel

Linux - Ignored Daemons

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

TotalView Configuration Tool				_		\times
Cloud Servers Servi	ces Rep	orts				
Search Options (Ctrl+E)	Ignored Da	emons				
Search Options (Ctrl+E) > TotalView Cloud > Dashboard Internet > Network NLT > Remotelnsight Reports > Risks SD-WAN SD-WAN > Derating Systems Y Linux Servers Alerts Ignored Volumes Polling Servers > Windows Servers Services > VolP	Server	Daemon	Action			
	Add	Change	Delete			
			Re	evert	App	bly

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:

×
~
\sim
el

Linux - Ignored Volumes

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

TotalView Configuration Tool					_		\times
Servers Servers Servers	vices Rep	orts					
Search Options (Ctrl+E)	Ignored Vo	lumes					
Search Options (Ctrl+E) > TotalView Cloud > Dashboard Internet > Network NLT > Remotelnsight Reports > Risks SD-WAN Y Servers Y Operating Systems Y Linux Servers Alerts Ignored Daemons Ignored Volumes Polling Servers > Windows Servers Services > VolP	Ignored Vo	Volume	Action				
				Rev	ert	Ap	ply

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

🌮 Add Ignored Volume	×
◯ Linux server	
Boston	~
Action: O Suppress Alerts Exclude from monitoring 	
Volume: All	~
OK Car	ncel .:

Linux - Polling

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

TotalView Configuration Tool		-		×
Cloud Servers Services	ces Reports			
Search Options (Ctrl+E)	Polling			
Search Options (Ctrl+E) TotalView Cloud Dashboard Internet NLT RemoteInsight Reports RemoteInsight Coverss Operating Systems Coverss Coverss Coverss Coverss Coverss Coverss Covers	Polling Unux polling behavior is configured on the <u>Network Device polling</u> tab			
	Re	evert	Appl	У

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.

TotalView Configuration Tool			-		×
Cloud Servers Servi	ces Repor	2			
Search Options (Ctrl+E)	Windows Ser	vers			
> TotalView	Alerts:	Configure Windows server alerts.			
Cloud	Ignored Drives:	Configures Windows ignored drives.			
Internet	Ignored Services	Configures Windows ignored services.			
> Network	Polling:	Configures the polling behavior.			
> Remotelnsight	Servers:	Configure which Windows servers should be monitored.			
Reports					
> Risks					
✓ Servers					
✓ Operating Systems					
 Linux Servers Windows Servers 					
Alerts					
Ignored Drives					
Polling					
Servers					
Server Thresholds Services					
> VoIP					
		Re	vert	Арр	bly

Windows - Alerts

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

TotalView Configuration Tool					-		×
Cloud Servers Servi	ces Repo	orts					
Search Options (Ctrl+E)	Alerts						
> TotalView	Server	Service	Threshold	Email		Des	riptior
Cloud Dashboard Internet Network NLT Reports Risks SD-WAN Servers Operating Systems Linux Servers Mindows Servers Alerts Ignored Drives Ignored Services Polling Servers Server Thresholds Services VoiP	Any	Server: Communication failure		swinter@pathsolutions.com		Serv	>
	Add	Change Delete					
					Revert	App	bly

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

💞 Change 🗸	Alert ×
Server	Organizational Unit
All	~
Alanti	Service States Channel
Alert:	Service Status Change
Service:*	~
Threshold:	10 %
Send to:	swinter@pathsolutions.com
Description:	AD DS Stopped
	OK Cancel

Windows - Ignored Drives

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

TotalView Configuration Tool				-		Х
Cloud Servers Servi	ces Rep	orts				
Search Options (Ctrl+E)	Ignored Dri	ves				
> TotalView	Server	Drive	Action			
Cloud			i			
> Dashboard						
Network						
NLT						
> Remotelnsight						
Reports						
> Risks						
SD-WAN						
✓ Servers						
 Operating Systems 						
 Linux Servers Windows Servers 						
Δlerts						
Ignored Drives						
Ignored Services						
Polling						
Servers						
Server Thresholds						
Services						
> VoIP						
	Add	Change	Delete			
			Ret	vert	App	bly

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

🐉 Add	1			×
⊖ Ser∖	ver 💿 Organiza	tional Unit		
Custom	n Systems\TotalView Lab	Systems		~
Action:	 Suppress Alerts 	O Exclude from mo	nitoring	
Drive:	All			~

Windows - Ignored Services

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

TotalView Configuration Tool				-		Х
Servers Servers	ces Rep	orts				
Search Options (Ctrl+E)	Ignored Se	rvices				
> TotalView	Server	Service	Action			
Cloud						_
> Dashboard						
Internet						
> Network						
NLT						
> Remotelnsight						
Reports						
> Risks						
SD-WAN						
Y Servers						
Operating Systems						
Windows Servers						
Alerts						
Innored Drives						
Ignored Services						
Polling						
Servers						
Server Thresholds						
Services						
> VoIP						
	Add	Change	Delete	1	🗹 Training	g mode
				Revert	Ap	ply

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

🐉 Add		×
O Serve	er Organizational Unit 	
Custom S	Systems\TotalView Lab Systems	\sim
Action:	O Suppress Alerts	
Service:	* Application Information	\sim
	OK Cancel	

Windows - Polling

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

TotalView Configuration Tool		-		×
Cloud Servers Services	res Reports			
Search Options (Ctrl+E)	Polling			۵
> TotalView	Windows polling period:			
> Dashboard	Windows disk usage polling period: 360 🔹 seconds			
> Network				
> Remotelnsight				
Risks				
SU-WAN				
Operating Systems Linux Servers				
Vindows Servers Alerts				
Ignored Drives Ignored Services				
Polling Servers				
Server Thresholds Services				
> VoIP				
	R	vert	App	lγ

Servers

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

TotalView Configuration Tool		-		×
Devices Cloud Servers Serv	rices Reports			
Search Options (Ctrl+E)	Servers			6
 > TotalView Cloud > Dashboard 	Search: Find server Q Select All Deselect All Collapse All Should new servers in the domain be automatically monitored? O Yes No 		Update	e List
 Network NLT Remotelnsight Reports Risks SD-WAN Servers Operating Systems Linux Servers Windows Servers Alerts Ignored Drives Ignored Services Polling Servers Servers VolP 	Y Y Domain Controllers Y Y DAPHNE Y Y HQVDC1 Y Y Stanta Clara Y Y Development Servers Y Y ScrooBY-DUM Y Y ScrooBY-DUM Y Y YELMA Y Y QA Servers Y Y Path Insight Y Y QA-PI11 Y Y QA-PI12 Y QA-PI14 Y QASRV1			

Server Thresholds

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

TotalView Configuration Tool		-		×
Cloud Servers Servin	ces 🗧 Reports			
Search Options (Ctrl+E)	Server Thresholds			
> TotalView Cloud	Low disk space (%):			
> Dashboard Internet	Low RAM (MBytes): 500			
> Network NLT	High CPU utilization (%): 90			
 Remotelnsight Reports Risks 				
SD-WAN Servers				
Operating Systems				
 Windows Servers 				
Alerts				
Ignored Drives				
Ignored Services				
Polling				
Server Thresholds				
Services				
> VolP				
	Re	vert	App	lv
	λ			

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

Services

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

TotalView Configuration Tool		orts				- 0
Search Options (Ctrl+E)	Services					
> TotalView Cloud	Find: Group, A	ddress, Protocol, Description, Note				
> Dashboard	Group	Address	Protocol	Polling (seconds)	Warn	Description
Internet	World	google.com	HTTPS	60	1	Google search
Network	World	www.pathsolutions.com	HTTPS	60	1	pathsolutions.com
> Remotelnsight	World	files.pathsolutions.com	HTTPS	30	1	Check Files SSL Server
Reports	World	admin.microsoft.com	HTTPS	30	1	Office365 Admin
Risks	Internal	fred.pathsolutions.local	HTTPS	60	1	fred.pathsolutions.local
SD-WAN	Internal	velma.pathsolutions.local	HTTPS	60	1	velma.pathsolutions.local
Services	Internal	scrappy.pathsolutions.local	HTTPS	60	1	scrappy.pathsolutions.local
> VoIP	Internal	daphne.pathsolutions.local	DNS	30	1	Internal DNS
	<					
	Add	Change Delete	Сору	Shift Up Shift	Down	Reset Sort
						Revert Apply

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

🌮 Change Se	rvice X
Group:	HQ-Lab ~
Address:	daphne.pathsolutions.local
IP version:	● Auto ○ IPv4 ○ IPv6
Protocol:	SMTP V
Port:	25
Poll period:	30 seconds
Alert after:	1 failures
Description:	Daphne-SMTP
Note:	Daphne SMTP
Send Alert to:	itops@pathsolutions.com <
	OK Cancel

VoIP

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

TotalView Configuration Tool			-		×
🔀 Devices 📥 Cloud 🍯 Servers 🔔 Serv	ces <mark>Report</mark>	<u>1</u>			
Search Options (Ctrl+E)	VoIP				
 Search Oppone (LTI+E) ✓ Risks Alerts Certificates Dictionary DNS Geographic IoT Devices IoT VLAN Policies Rogue IT Whitelist SD-WAN ✓ Servers ✓ Operating Systems ✓ Linux Servers Alerts Ignored Daemons Ignored Volumes Poling Servers ✓ Windows Servers Alerts Ignored Drives Ignored Drives Ignored Drives Ignored Servers Servers Servers Servers Volp Alerts Ignored IP SLA Alerts Ignored IP SLA Phones ValP 	VoIP VoIP IP SLA: Cor Phones: Ide VoIP VLAN: Ide SIP-Trunks: Cor	ifigures alerting for phone moves/adds/changes. ifigures alerting for IP SLA. ntifies the OUIs used on phones to locate them on the network. itifies the VLANs that are used for VoIP devices to identify them on the network. ifigures SIP Trunks.			
SIP-Trunks	,				
			levert	App	ly

VoIP Alerts

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

TotalView Configuration Tool		_		\times
Services Cloud Servers Service	ces Reports			
Search Options (Ctrl+E)	Alerts			
Ster CP Opunts (LCTI+E) > Total/View Cloud > Dashboard Internet > Network NLT > Remotelnsight Reports > Risks SD-WAN > Servers Services ✓ VolP Alerts Phones VolP VLAN SIP-Trunks	Phone Move Alerting Send alerts to: Itops@pathsolutions.com			
	Re	vert	App	bly

IP SLA

On the VoIP > IP SLA section, chose Alert or Ignored IP SLA



IP SLA Alerts

Go to IP SLA > Alerts section to set Device, IP SLA Number, email recipients, and the MOS thresholds that triggers alerts

Code With Interface Authentication Provide Statute	TotalView Configuration Tool*						-		×
Service PSLA Number Email MOS Threshold Authoritization Authoritization HU/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Cload Wather Widget HU/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Vesther Widget HU/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Vesther Widget HU/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Vesther Widget HU/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Vesther Widget Hu/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Vesther Widget Hu/Synch (10.0.1) 100 Santa Clare to Sunnyvale cadams@pathsolutions.com 4 Vesther Widget Hu/Synch (10.0.1) Vesther Widget Hu/Synch (10.0.1) Hu/Synch (10.0.1) Vesther Widget Hu/Synch (10.0.1) Hu/Synch (10.0.1) Hu/Synch (10.0.1) Hu/Synch (10.0.1) Vesther Widget Hu/Synch (10.0.1) Hu/Synch (10.0.1) Hu/Synch (10.0.1) Hu/Synch (10.0.1) Sorvers	Cloud Servers	Services	Reports						
Web Interface Authoritication Authoritication Authoritication Web Sever Authoritication Cood HQ Synch (100.0.1) Dashboard HQ Synch (100.0.1) Wather Widget HI Internet Retwork NIT Servers Softwark HQ Softwark HQ Vather Widget HI Internet Reports Softwark HQ NIT Servers V Desting Systems Volarities V Operating Systems Volarities V Windows Servers Alerts Ignored Damoes Ignored Servers Vindows Servers Alerts Ignored Damoes Poling Servers Alerts Ignored Damoes Poling Servers Alerts Ignored Damoes Poling Servers Alerts Ignored Drives Add Oburge Shift Dom Report Add VelP VLAN V	Search Options (Ctrl+E)		IP SLA Alerts*						
APIKeys Authoritation Web Server Coad Veshboard Westher Widget Internet NitT Remotelingipt Reports Servers Volpored Drows Jonerd Droks Jonerd D	✓ Web Interface	^	Device	IP SLA Number	Email	MOS Threshold			
Authentication Web Server Coad Dashboard Weather Widget Internet Network NIT > RemoteInsight Reports > Risks SD-WAN > Sorvers - Linux Servers - Alerts goored Deamons goored	API Keys		HQ/Syrah (10.0.0.1)	100: Santa Clara to Sunnyvale	cadams@pathsolutions.com	4			
Veshoard Veshoard Veshoard Wester Wigget Internet Network NT Remotelinight Reports Servers VopretInig Systems Vestors Alerts Jonred Destons Jonred Destons Jonred Destons Jonred Destons Jonred Destons Jonred Destons Servers Alerts Jonred Destons Jonred Destons Jonred Destons Jonred Destons Jonred Destons Servers Alerts Jonred Destons Jonred Destons Servers Alerts Jonred Destons Jonred Destons Servers Alerts Jonred Destons Jonred Destons Servers Servers Servers Servers Alerts Jonred Destons Jonred Destons Servers Servers Servers Servers Servers Alerts Jonred Destons Jonred Destons Servers Ser	Authentication				•				
 Usuba di Westher Widget Vesther Widget Internet Widget Internet Widget Internet Widget Net Servers NIT Reports So-WaN So-WaN So-VaN Vestrers Vinos Servers Vinos Servers Vinos Servers Alets Ignored Daemons Ignored Journes Polling Servers Alets Ignored Services Polling Servers Alets Ignored Services Polling Servers Alets Ignored Polla Servers Vinos Servers Alets Ignored Polla Servers Server Interholds Servers VolP Alets VolP VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP Alets VolP VolP Alets VolP VolP Alets VolP VolP Al	Web Server								
Westher Widget Internet Network NIT Remotelsnight Reports Risk Stremers V Diported Notiones Poling Servers Alerts Ignored Notimes Poling Servers Alerts Ignored Notimes Poling Servers Alerts Ignored Socies Poling Servers Alerts Ignored Notimes Poling Servers Alerts Ignored Notimes Poling Servers Alerts Ignored Notices Poling Servers Alerts Ignored Notices Polones VolP VLAN Add Change Shrit Up Shrit Up Shrit Up	V Dashboard								
Name Woge Internet > Retwork NIT > Remotelnsight Reports > Risks SD-WAN > Sorvers > Operating Systems > Linux Servers > Unix Servers > Poling Servers > Poling Servers Servers > Vindows Servers Alerts Ignored Daemons Ignored Services Poling Servers Services > VolP Alerts Ignored IPSLA Alerts Ignored IPSLA Phone VolP VLAN Add Deter Shift Up Shift Up Shift Up Shift Up	Westher Widget								
 Network NIT Remethnight Reports Riks Solvan Servers Operating Systems <td>Internet</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td>	Internet								
NIT Remotelhnsight Reports So:WAN So:WAN So:WAN So:WaN So:Wars Alerts Ignored Demons Ignored Drives Ignored Drives Ignored Drives Servers Servers Servers Servers Servers Servers VolP Alerts Jgnored Drives Ignored Drives Ignored Drives Netts VolP Alerts Jgnored Drives Servers Serv	> Network								
 Remotelnsight Reports Ricks Sorvers Operating Systems Unitox Servers Operating Systems Unitox Servers Alerts Ignored Demons Ignored Demons Ignored Services Windows Servers Alerts Ignored Services Serveris Serv	NLT								
Reports > Risks > Diversing Systems * Unix Servers Alerts Ignored Demonos Ignored Services > Voling Alerts Ignored Invices Polling Services > VoliP Alerts Ignored PSLA Phones VoliP VLAN Add Change Shift Up Shift Down Reset Sort	> RemoteInsight								
Sirvers Servers VolPorting Systems Operating Systems Operating Systems Operating Systems Alets Ignored Daemons Ignored Volumes Polling Servers Vindows Servers Alets Ignored Drives Ignored Drives Ignored Services Polling Servers Servers Servers Servers VolP Alets Ignored IP SLA Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Reports								
So-WAN Servers Copersing Systems Linux Servers Alerts Jignored Daemons Jignored Volumes Polling Servers Volop Units Volop Units Volop Units Volop Units Volop Units Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	> Risks								
Servers Operating Systems Linux Servers Aletts Ignored Demonos Ignored Volumes Polling Servers Windows Servers Aletts Ignored Drives Ignored Drives Ignored Drives Ignored Drives Servers Services VolP Aletts Ignored IP SLA Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort 	SD-WAN								
 Operating Systems Linux Servers Linux Servers Ignored Daemons Ignored Daemons Ignored Volumes Polling Servers Mindows Serverss Aletts Ignored Drives Ignored Drives Ignored Prives Servers Servers Servers Servers Servers Servers Services Polling Servers Services VolP Alets* Ignored IP SLA Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort 	✓ Servers								
 Linux Servers Alerts Ignored Deemons Ignored Volumes Polling Servers Alerts Ignored Drives Ignored Drives Ignored Services Polling Servers Servers Servers Servers Servers Alerts Ignored Services VolP Alerts Ignored IP SLA Alerts Ignored IP SLA Phones VolP VLAN	 Operating Systems 								
Alerts Ignored Daemons Ignored Volumes Polling Servers * Windows Servers Alerts Ignored Drives Ignored Services Polling Servers Server Thresholds Servers Servers Servers VolP Alerts* Ignored P SLA Phones VolP VLAN * Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	 Linux Servers 								
Ignored Volumes Johnse Voling Servers Alerts Jgnored Drives Jgnored Drives Jgnored Drives Jgnored Drives Jgnored Drives Jgnored Drives Server Thresholds Server Thresholds	Alerts								
Ignored Volumes Polling Servers Alerts Ignored Drives Ignored Drives Ignored Services Polling Servers Servers Services VolP Alerts Ignored IP SLA Phones VolP VLAN Add Change Delete Shft Up Shft Down Reset Sort Revert	Ignored Daemons								
Polling Servers Vindows Servers Alerts Ignored Drives Ignored Services Polling Servers Servers Servers Servers Servers VolP Alerts V IP SLA Ignored IP SLA Phones VolP VLAN VolP VLAN	Ignored Volumes								
Servers Vindows Servers Alerts Ignored Drives Ignored Services Polling Servers Servers Server Thresholds Servers Server Thresholds VolP Alerts VolP Alerts VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Polling								
Vindows Servers Alerts Ignored Drives Ignored Services Polling Servers Servers Servers VolP Alerts Ignored IP SLA Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Servers								
Alerts Ignored Drives Polling Servers Server Thresholds Services VolP Alerts Ignored IP SLA Phones VolP VLAN VolP VLAN V	 Windows Servers 								
Ignored Drives Ignored Services Polling Servers Servers Servers Servers VolP Alerts Ignored IP SLA Phones VolP VLAN VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Alerts								
Polling Servers Server Thresholds Servers VolP Alerts Ignored IP SLA Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Ignored Drives								
Services Services V VoIP Alerts Ignored IP SLA Phones VoIP VLAN VoIP VLAN VoIP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Delling								
Services VolP Alerts VolP SLA Ignored IP SLA Phones VolP VLAN VolP VLAN VolP VLAN VolP VLAN Change Delete Shift Up Shift Down Reset Sort Revert Apply	Servers								
Services VolP Alerts Ignored IP SLA Phones VolP VLAN Add Change Shift Up Shift Down Revert Apply	Server Thresholds								
 VolP Alerts IP SLA Japored IP SLA Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Services								
Alerts V IP SLA Alerts* Ignored IP SLA Phones VoIP VLAN V Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	✓ VoIP								
 IP SLA Alerts* lgnored IP SLA Phones VoIP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply Apply Revert Apply Apply Apply Apply Apply Apply Apply Apply<td>Alerts</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td>	Alerts								
Alerts* Ignored IP SLA Phones Add VoIP VLAN Add Change Shift Up Shift Down Reset Sort Revert Apply	V IP SLA								
Ignored IP SLA Phones VoIP VLAN Add Change Delete Shift Up Shift Down Revert Apply	Alerts*								
Phones VolP VLAN Add Change Delete Shift Up Shift Down Reset Sort Revert Apply	Ignored IP SLA								
VolP VLAN V Add Change Delete Shift Up Shift Down Reset Sort	Phones								
Revert Apply	VoIP VLAN	~	Add Char	nge Delete	Shift Up Shift Down	Reset Sort			
Revert Apply									
						R	evert	App	ly
10									

Use the Add, Change, and Delete buttons to set Device, IP SLA Number, email recipients, and the MOS thresholds that triggers alerts

🐉 Add IP SLA	Alert	×
Device:	O All devices	
	Specific: HQ/Syrah (10.0.0.1)	~
IP SLA number:	○ All numbers	
	Specific: 100: Santa Clara to Sunnyvale	~
Email:	cadams@pathsolutions.com	~
MOS threshold:	4.00	•
	OK Cancel	

IP SLA Ignored IP SLA

Go to the **IP SLA > Ignored IP SLA** section to identify the IP SLA to ignore.

Search Options (Ctrl+E)		Ignored IP SLA					
✓ Risks	^	IP SLA List	Filter unsupported entri	es			Upda
Alerts Certificates		Device	Operation Number	Name	Owner		
Dictionary		HQ/Syrah (10.0.0.1)	100	Santa Clara to Sunnyvale	noc@pathsolutions.com	 	
DNS		HQ/Syrah (10.0.0.1)	200	Santa Clara to Austin	noc@pathsolutions.com		
Geographic		-					
✓ IoI							
INT VI AN							
Policies							
Rogue IT							
Whitelist							
SD-WAN							
✓ Servers							
 Operating Systems Linux Services 							
Linux Servers Alerts		Tanore Pules					
Ignored Daemons						 	
Ignored Volumes		Device IP	SLA number			 	
Polling							
Servers							
 Windows Servers 							
Alerts							
Ignored Drives							
Polling							
Servers							
Server Thresholds							
Services							
VoIP							
Alerts							
 IF SLA Alerts 							
Ignored IP SLA							
Phones							
VoIP VLAN							
SIP-Trunks	~	Add Char	nge Delete	Shift Up Shif	ft Down Reset Sort		

Use the Add and Change buttons to modify the Ignored IP SLA to suppress alerts for Devices and IP SLA numbers.

🜮 Add Ignore	Rule		×
Device:	O All devices		
	Specific:	HQ/Syrah (10.0.0.1)	~
IP SLA number:	 All numbers 		
	Specific:	100: Santa Clara to Sunnyvale	~
		ОК С	ancel

Phones

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

TotalView Configuration Tool Devices Cloud Servers Servers	Services Repo	rts	-		×
Search Options (Ctrl+E)	Phones				6
> TotalView	MAC OUI	Description			^
Cloud	00.14.5E	IBM			
> Dashboard	00.09.6E	Giant Electronics			
> Network	00.10.EB	Selsius			
NLT	00.10.49	ShoreTel			
> Remotelnsight	00.04.F2	Polycom			
Reports	00.F0.75	Verilink			
> Risks	00.13.FA	lifesize			
> Servers	00 50 60	Tandhero			
Services	00.04 F4	Witton			
✓ VoIP	00.00.74	Bolycom			
Alerts	64.16.7E	Polycom			
Phones	04.10.7F	Polycom			-8
SIP-Trunks	00.04.F2	Polycom			
Sh Hunks	48.25.67	Polycom(Zoom)			
	00.21.F2	Easy3Call			
	00.0B.82	Grandstream			
	08.00.0F	Mitel			
	00.0A.DD	Allworx			
	00.10.36	Inter-Tel			
	00.E0.BB	3Com			
	00.0F.4D	TalkSwitch			
	Add	Change Delete Reset Sort			
			Revert	App	ly

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

🐲 Change VLAN Nam	e	×
VLAN name or number:	phone	
	OK	Cancel

Use the delete button to delete one.



VoIP VLAN

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

TotalView Configuration Tool		-		×
Servers Loud Servers	res Reports			
Search Options (Ctrl+E)	VoiP VLAN			
> TotalView	VLAN Name or Number			
Cloud	voi			_
> Dashboard	phone			
> Network	telecom			
NLT				
> Remotelnsight				
Reports				
> Kisks SD_WAN				
Servers				
Services				
✓ VoIP				
Alerts				
Phones				
VOIP VLAIN SID-Trunks				
SITERIA				
	Add Change Delete Reset Sort			
	3	levert	Арр	ly

SIP-Trunks

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

TotalView Configuration Tool								-		\times
Search Options (Ctrl+E)	SIP-Trunk	eports S								
> TotalView	Find: Group,	Address, Name								
Cloud	Group	Address	Name	Latency mr.	Lorr %	Pourte	DSCD	Email		
Internet	Internet	global.tr.skype.com	Skype for Business	catericy, ris	LUSS, /0	No	DOCP	critali		
> Network NLT		5								
> Remotelnsight										
Reports Risks										
SD-WAN										
> Servers Services										
VoIP										
Phones										
VoIP VLAN										
SIF- HUNKS										
								-		
	Add	Change Delete	Сору	Shift Up S	hift Down	Re	eset Sort			
								Revert	Арр	ly .:i

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:

Group:	Test Gro	-p	
Address:	global.tr	skype.com	
Name:	Skype fo	Business	
Icon:	SkypeFo	Business.png	
DSCP:	46		
Email: Latency t	hreshold:	0	
Loss thre	shold:	0	
Route			

Using the Device Configuration Wizard

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

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

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

🔏 TotalView Device Cont	fig Wizard	×
pathSolutions	Step 1 of 3: Authorization Please enter the configuration change password:	
	< <previous next="">></previous>	Cancel

Select **Next** to continue.

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

N,	Step 3 of 3: Device Selection Select the devices			
No	Name HO Firewall	IP address	System Descriptio	^
•	hafw1	10.86.0.2	EdgeOS v1.10.9.5	
	hqpa500	10.0.0.7	Palo Alto Network:	
_	HQ			
	Syrah	10.0.0.1	Cisco IOS Softwa	
U	Michelob	10.0.0.13	Cisco NX-OS(tm)	
S	Burgundy	10.0.0.19	ProCurve J9087A	
	Riesling	10.0.29	Brocade Commun	
	Gamay	10.0.0.46	NetVanta 1224, V	
+	Jagermeister	10.0.254	Cisco NX-OS(tm)	
(1)	Boston			~
õ	<		>	
<u> </u>	Match Select			

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

En-masse device select	×
Select or de-select devices en-masse based on a matched sysDescr stri	ng.
Select De-Select	
Match System Description String:	
OK Can	cel

💰 TotalView Device Con	fig Wizard	×
pathSolutions	Step 2 of 3: Script Enter the configuration change script below: @PROMPT=/#/ show ip arp Load	Ip
	< <previous next="">> Can</previous>	cel

Then in step 3, enter the configuration change script. If needed select Load or Show Help. When finished, select 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. Select **Show Help** to open a non-modal dialog box that can help with the configuration input.

Configuration Option	5	\times
The "@PROMPT=/#/ tell the tool how to fin On most devices, thi your device(s) require The string between searching for different	" command must be the first line of the configuration, as it will d the prompt on the device. s would be a '#' sign, but should be changed to match what the slashes can be a standard regex expression to permit t options.	
Options: %ASCII:25% %ASCII:LF% % comment% %WAIT:5%	Sends ASCII code 25 Sends the Line Feed character Comments that are not sent to the remote device Waits 5 seconds before continuing to send	

Select **Next** to continue.

TotalView Device Conf	ig Wizard	>
	Ready to begin	
ίΩ	Script to be applied:	
Ë	@PROMPT=/#/	~
tior	show ip arp	~
<u> </u>	<	>
	Devices to modify: 3	
Š	Syrah (10.0.0.1) Michelob (10.0.0.13) Jagermeister (10.0.0.254)	^
<u></u>		\sim
	<	>
ğ	Logfile: C:\Program Files (x86)\PathSolutions\TotalView\Logfiles\DeviceC	hange
	coDraviaus Einiah Od	maal

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 communication.

Re-Configuring TotalView When Your Network Changes

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

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

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

o,	Step 1 of 8: SMTP Se	erver	- haadkin
Ë	Mail Server Address	ens to help you keep track of your network	Dort.
<u> </u>	10.0.0.10		25
lt.	Authenticate		
۲ ا	Username: Password:		
Sc	Send from: LAB-Velma-Reports	@PathSolutions.com	
<u> </u>	Example: noc@comp Send test email to:	pany.com	
+			Test
ba	Example: jdoe@hotmail.com, fb@a	aol.com	

Automatic Re-Configuration

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

MonitorWizard.exe /a

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

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

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

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

Other Network Program Configuration Tools

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

Interface Discovery Tool

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

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

It will launch and show the first step.

💰 TotalView Interface Discovery Tool		×
pathSolutions	Step 1 of 5: Select Work Options Increase an existing device list and interface ignore list. Increase and the device list configuration and re-create the device list as well as interface ignore list. Increase and the device list from scratch Including the device list from	
	<< Previous Next >> Cance	21

This step will allow you to select work options.
The second step allows you to enter network address ranges.

💰 TotalView Interface Discovery Tool		×
pathSolutions	Step 2 of 5: Network Address Ranges The Interface Discovery Tool can scan your network for devices to monitor. All interfaces on each device will be monitored. Specify the network address ranges that should be scanned. New Address Range Starting IP address:* Ending IP address:* Ending IP address:* Croup: Default Address ranges to be checked Edit Delete	
	<< Previous Next >> Cance	8

Enter the appropriate IP addresses and select Next to continue.

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

گ TotalView Interface Di	scovery Tool		×
pathSolutions	 Step 3 of 3: Include Interfaces All ○ Operational < 10 Megabit 10 Megabit 100 Megabit 100 Megabit 2.5 Gigabit 2.5 Gigabit 5 Gigabit 25 Gigabit 25 Gigabit 40 Gigabit 50 Gigabit 100 Gigabit 100 Gigabit > 100 Gigabit < 100 Gigabit 	Illy UP Admin Down Ethernet type Serial type VLAN type Loopback type Other type	
	~~	Previous Finish	<u>C</u> ancel

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

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

The service will then be restarted.

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

TotalView Interface Discovery Tool	×
TotalView Interface Discovery Tool Copyright © 2018 PathSolutions, Inc.	Close
Command line options: -a Run the wizard in automatic mode -s Skip device scan (use existing configuration) -r Restart service after scan -? Displays command line help	

Config Editor

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

Configuration editor (Administrator) Ig	noreE	rrorCounter.cfg		-		×
▤◓◁▱ႥႦ	T _e	a Ta		Þ	: 🏟	()
AutoRefresh.cfg BGPPeer.cfg Blacklist.cfg BlacklistCountries.cfg CDPDisable.cfg		;This is the En ;Fields should ;The order of t ;Global Suppres ;The service do	rror Counter Ignore config file be entered in tab-delimited format this file is important, as specific Suppress/UnSupp ss/UnSuppress should be listed last pes not need to be restarted if this file is change	ress i 1, it	s int is re	erpr: -rea:
Certificates.cfg CiscoCBWFQDisable.cfg CiscoDisable.cfg Cloud.cfg ConfigEditor.cfg CustomReports.cfg DeviceAuth.cfg		;Device/Group 10.50.0.174 10.50.0.174 10.50.0.174 10.0.0.27 10.51.0.1 * * *	Interface Error Counter S 8 Inbound Discards 8 Inbound Errors 8 Outbound Errors 4 Frame Too Longs 5 Inbound Discards Inbound Unknown Protocols Outbound Queue Length	uppres	s⁄UnS	uppr:
DeviceBackup.cfg DeviceBackupVariables.cfg DeviceDebug.cfg DeviceType.cfg DiagramL3.cfg DiagramL3lgnore.cfg						
DiagramL3Mask.cfg DNSMonitor.cfg EntityDisable.cfg Favorites.cfg Financials.cfg IgnoreErrorCounter.cfg	v	<				>
Ignorel ist ctg						-

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

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

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

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

Map Config Tool

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

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

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



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



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

The toolbar across the top contains these tools: The pointer with a plus sign allows you to add and name a new map: Select this pointer symbol top select and open a map: Select the floppy disk symbol to update the dynamic map: To add a device ping, use the Add Device Ping symbol: To add a link, use the Add Link symbol: To change magnification up or down, clock on the magnifying icons:

How to Add Maps



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



How to Add Links



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

Link properties	×
Device:	
	~
Interface	Show Only Up
	~
	OK Cancel

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

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

Device Ping properties	
evice IP Address	ОК
10.0.0.7 ~	Cancel

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

How to Add Ping Points



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

Device Ping properties		×
Device:		
		~
	ОК	Cancel

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

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

MIB Browser

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

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

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



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

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

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

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

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

Find OID by name or path		×
Find:	~	Find Next
Match case		Cancel
Search in descriptions		
Search from	Search for	
 Current 	🔿 🍯 OID Name	
O Root	🔿 🛅 Group Name	
O Vendor MIBs	🖲 📷 Both	

OID Lookups

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

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



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



OID Monitoring

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



Select Monitor... and the dialog box for the selected Interface's OID Index will popup.

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

🍯 Select OID inde	ex		×
ifInOctets Type: Counte Entry: ifInOe	1.3.6.1.2.1.2.2.1.10 er ctets.1 1.3.6.1.2.1.2.2.1.10.1		0
Index		Value	^
1	Counter32: 0		
2	Counter32: 0		
3	Counter32: 759097097		
4	Counter32: 0		
5	Counter32: 0		
6	Counter32: 1068848505		
7	Counter32: 0		
8	Counter32: 0		
9	Counter32: 0		
10	Counter32: 0		
11	Counter32: 0		
12	Counter32: 0		
13	Counter32: 0		v
	Get values	Monitor	OID

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

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



OID Graphing

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

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

🍯 Add OID to mo	ionitoring / 10.0.0.1 - Syrah	×
Choose the OID in	instance that should be associated with the monitoring.	
Device:	10.0.0.1 - Syrah	
Description:	ifNumber	
Specific interface:	Any interface	~
OID		
ifNumber 1.3	3.6.1.2.1.2.1	
Type: Integ	ger 32	
Instance: ifNur	Imber.0 1.3.6.1.2.1.2.1.0	\oslash
Index	Value	
0	INTEGER: 55	
	Get Value	
	<< Previous Next >>	ancel .:

The second step is to decide whether to transform the returned value to a different result.

For example: if the device returns Fahrenheit values but you want the results to be converted to Celsius, you can enter the conversion formula in the **Transform formula** field.

🍯 Add OID to mo	onitoring / 10.0.0.1 - Syrah	×
Should the OID v	alue be converted to a different output?	
No		
○ Yes		
Transform formula:	Not used	Ð
	You can use addition, subtraction, multiplication, division, exponentiation, and parentheses. The OID value is denoted by the symbol V. If this symbol is not present, it is automatically added to the beginning of the formula. Supported functions: min(a,b), max(a,b), round(a) Examples *5: Multiply result by 5 F: Convert value to Fahrenheit C: Convert value to Celsius round(-5 + max(V^2, F)/1.27): more complex example	ne
	<< Previous Next >> Cancel	

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

old OID 🝏	to monitoring / 10.0.0.1 - Syrah	ı			×
Should the O)ID history be tracked over t	ime and displ	ayed on the web	interface?	
◯ No					
Yes					
Y-Axis label:					
Legend label:					
		<< Previous	Next >>		Cancel

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

Should this OID trigger an alert? Note: Note:	Add OID to monitoring / 10.0.0.1 - Syrah	Х
No Yes Trigger expression: Supported functions 90 : Trigger if value exceeds 90. 40,90 : Trigger if value is below 40 or exceeds 90. 40,90 : Trigger if value is below 40 or exceeds 90. LESS(A) : Trigger if value is below 40 or exceeds 90. LESS(A) : Trigger if value is below 40 or exceeds 90. GREATER(A) : Trigger if value is below 40 or exceeds 90. GREATER(A) : Trigger if value greater than A. GREATER(A) : Trigger if value greater than A. GREATERQUAL(A) : Trigger if value greater than or equal to A. IN(A, B, C:D) : Trigger if the value is in the range from C to D induding range boundaries or matches other passed values. MOTIN(A, B, C:D) : Trigger if the value is outside the range of C to D and doesn't match other passed values. Multiple functions can be used simultaneously. Separate them with commas: GREATER(30), LESS(50) The alert will be triggered if at least one function returns true. Notification email:	Should this OID trigger an alert?	
 No Yes Trigger expression: Supported functions 90: Trigger if value exceeds 90. 40,90: Trigger if value is below 40 or exceeds 90. LESS(A): Trigger if value less than A. LESSEQUAL(A): Trigger if value less than A. LESSEQUAL(A): Trigger if value greater than A. GREATERE(A): Trigger if value greater than or equal to A. IN(A, B, CD): Trigger if the value is in the range from C to D including range boundaries or matches other passed values. NOTIN(A, B, CD): Trigger if the value is outside the range of C to D and doesn't match other passed values. Multiple functions can be used simultaneously. Separate them with commas: GREATER(30), LESS(50) The alert will be triggered if at least one function returns true. Notification email: 		
O Yes Trigger expression: Supported functions 90: Trigger if value exceeds 90. 40,90: Trigger if value is below 40 or exceeds 90. LESS(A): Trigger if value iss below 40 or exceeds 90. LESS(A): Trigger if value less than A. LESSEQUAL(A): Trigger if value less than A. LESSEQUAL(A): Trigger if value greater than A. GREATER(A): Trigger if value greater than A. GREATEREQUAL(A): Trigger if the value is in the range from C to D including range boundaries or matches other passed values. MOTIN(A, B, CD): Trigger if the value is outside the range of C to D and doesn't match other passed values. Multiple functions can be used simultaneously. Separate them with commas: GREATER(30), LESS(50) The alert will be triggered if at least one function returns true. Notification email:	No	
Trigger expression: Supported functions 90 : Trigger if value exceeds 90. 40,90 : Trigger if value is below 40 or exceeds 90. LESS(A) : Trigger if value less than A. LESSE(A) : Trigger if value greater than an equal to A. GREATER(A) : Trigger if value greater than or equal to A. GREATER(A) : Trigger if value greater than or equal to A. IN(A, B, C:D) : Trigger if the value is in the range from C to D induding range boundaries or matches other passed values. NOTIN(A, B, C:D) : Trigger if the value is outside the range of C to D and doesn't match other passed values. Multiple functions can be used simultaneously. Separate them with commas: GREATER(30), LESS(50) The alert will be triggered if at least one function returns true. Notification email:	⊖ Yes	
Supported functions 90 : Trigger if value exceeds 90. 40,90 : Trigger if value iss below 40 or exceeds 90. LESSE(A) : Trigger if value less than A. ESSEQUAL(A) : Trigger if value greater than A. GREATEREQUAL(A) : Trigger if value greater than or equal to A. GREATEREQUAL(A) : Trigger if value greater than or equal to A. IN(A, B, C:D) : Trigger if the value is in the range from C to D including range boundaries or matches other passed values. NOTIN(A, B, C:D) : Trigger if the value is outside the range of C to D and doesn't match other passed values. Multiple functions can be used simultaneously. Separate them with commas: GREATER(30), LESS(50) The alert will be triggered if at least one function returns true. Notification email:	Trigger expression:	Ø
	Supported functions 90 : Trigger if value exceeds 90. 40,90 : Trigger if value is below 40 or exceeds 90. LESS(A) : Trigger if value less than A. LESSEQUAL(A) : Trigger if value less than or equal to A. GREATEREQUAL(A) : Trigger if value greater than A. GREATEREQUAL(A) : Trigger if value greater than or equal to A. IN(A, B, C:D) : Trigger if the value is in the range from C to D including range boundaries or matche other passed values. NOTIN(A, B, C:D) : Trigger if the value is outside the range of C to D and doesn't match other pass values. Multiple functions can be used simultaneously. Separate them with commas: GREATER(30), LESS(The alert will be triggered if at least one function returns true.	s ed 50)
<< Previous Save OID Cancel	<< Previous Save OID Cancel	

SNMP Trap Receiver Configuration

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

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

Alerting on a Specific Trap

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

Find OID by name or path X					
Find:	Find Next				
Match case	Cancel				
Search in description					
Search from	Search for				
Current	🔿 🥑 OID Name				
O Root	🔿 🛅 Group Name				
O Vendor MIBs	🖲 7 Both				

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 select **Add Trap Alert**. Alternatively, select the line item, then select this bell-and-plus-sign symbol in the top navigational bar:



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

of Add new trap ale	ert	_		×
IP Address	10.0.0.1	🗌 🗆 An	y IP add	lress
Trap OID	dsx1LineStatusChange			
·	1:3.6.1.2.1.10.18.15.0.1	8] 🗆 Any	OID
Trap Value			🗹 Any 🗤	/alue
Email				
Alert Description				
	1	Save	Can	cel

Modifying Trap Alerts

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



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

IIB Browser - Trap Alerts	- 🗆 X
lo l	
10.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value 10.0.0.1 - dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) - Any value	From IP: 10.0.0.1 Trap OID: dsx1LineStatusChange (1.3.6.1.2.1.10.18.15.0.1) With any value Send email to: person@company.com Description: dsx1line alert A dsx1LineStatusChange trap is sent when the value of an instance dsx1LineStatus changes. It can be utilzed by an NMS to trigger pols. When the line status change results from a higher level line status change (i.e. ds3), then no traps for the ds1 are sent.
	Close

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

MIB Browser - Trap Alerts					-
10.0.0.1 - dsx1LineStatusChange (1.3.6. 10.0.0.1 - dsx1LineStatusChange (1.3.6.	1.2.1.10.18.15.0.1 1.2.1.10.18.15.0.1) - Any value) - Any value	From IP: 10 Trap OID: d With any va Send email to Description: d	.0.0.1 sx1LineStatusCh lue o: person@compa dsx1line alert	ange (1.3.6.1.2.1.10.18.15.0.1) any.com
	🍯 Edit trap alert			- 🗆 ×	ent when the value of an instance e utilized by an NMS to trigger polls.
	IP Address	10.0.0.1	۵	Any IP address	ts from a higher level line status change s1 are sent.
	Trap OID	dsx1LineStatusC	Change 18.15.0.1	Any OID	
	Trap Value			☑ Any value	
	Email	person@compa	iny.com	0	
	Alert Description	dsx1line alert		8	
			S	ave Cancel	
					Close

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.

Device address:*	1
SNMP version:	O SNMPv1
Community string:*	
AuthProt:	AuthPass:
NoAuth	× .
PrivProt:	PrivPass:
NoPriv	× [
	Poll Device
5	
σ	
š II	

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

Syslog Viewer Tool

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

🔊 SL10.0.0.1.txt -	- Syslog Viewer						_	-		×
	Search		Filter							
SL10.0.0.1.txt										
SL10.0.0.2.txt		Search			Filter					
SL10.0.0.20.txt		Next	Severity:	Al -	Reset	Live updates				
SL10.0.0.21.txt										
SL10.0.0.22.txt			Facility:	All 👻						
SL10.0.0.23.txt	12/28/2017 10:10:53 AM <190>	1438: *Dec 28 18:03:1).553: %	SYS-6-LOGGINGHOST_STARTST	OP: Logging to host	10.10.0.10 port 0 CLI	Request Triggered			
SL10.0.0.26.txt	12/28/2017 10:10:54 AM <190> 12/28/2017 10:11:59 AM <189>	1439: *Dec 28 18:03:1 1440: *Dec 28 18:04:1	.554: % .881: %	SYS-6-LOGGINGHOST_STARTST PASSWD-5-DEPRECATED: pass	OP: Logging to host wd syntax has been d	10.10.0.10 port 514 s eprecated; please use	tarted - CLI initiated password encryption or	key cor	nfig-key CL	Is ir
SL10.0.0.27.txt	12/28/2017 10:13:09 AM <190> 12/28/2017 10:13:09 AM <190>	1441: *Dec 28 18:05:2 1442: *Dec 29 11:17:0	8.084: % 0.000: %	SYS-6-CLOCKUPDATE: System SYS-6-CLOCKUPDATE: System	clock has been upda clock has been upda	ted from 18:05:28 UTC ted from 19:05:28 PST	Thu Dec 28 2017 to 19:0 Wed Dec 27 2017 to 12:1	/5:28 PS	ST Wed Dec : ST Thu Dec :	27 20 28 20
SL10.0.0.33.txt	12/28/2017 10:13:10 AM <189> 12/28/2017 10:13:55 AM <189>	1443: Dec 29 11:17:09 1444: Dec 29 11:17:53	039: %s 464: %w	YS-5-CONFIG_I: Configured EBSERVER-5-LOGIN_PASSED:S	from console by vty witch 1 R0/0: : Log	0 in Successful from ho	st 10.51.0.38 by user 's	swinter'		
SL10.0.0.5.txt	12/28/2017 10:14:12 AM <190> 12/28/2017 10:14:12 AM <190>	1445: Dec 29 11:18:11 1446: Dec 28 20:18:53	418: %s	YS-6-CLOCKUPDATE: System YS-6-CLOCKUPDATE: System	clock has been updat clock has been updat	ed from 12:18:11 PST ed from 03:18:11 UTC	Thu Dec 28 2017 to 03:18 Fri Dec 29 2017 to 12:18	3:53 UTC	C Fri Dec 2 C Thu Dec 2	3 201 8 201
SL10.0.0.7.txt	12/28/2017 10:14:12 AM <189> 12/28/2017 10:14:44 AM <189>	1447: Dec 28 20:18:53 1448: Dec 28 20:19:24	026: %s 594: %w	YS-5-CONFIG_I: Configured EBSERVER-5-LOGIN_PASSED:S	from console by vty witch 1 R0/0: : Log	0 in Successful from ho	st 10.51.0.38 by user 's	swinter'		
SL10.10.0.1.txt	12/28/2017 10:16:02 AM <190> 12/28/2017 10:16:02 AM <190>	1449: Dec 28 20:20:43 1450: Dec 29 05:15:00	141: %s	YS-6-CLOCKUPDATE: System YS-6-CLOCKUPDATE: System	clock has been updat clock has been updat	ed from 12:20:43 UTC ed from 21:20:43 UTC	Thu Dec 28 2017 to 21:20 Wed Dec 27 2017 to 06:15):43 UTC 5:00 UTC	C Wed Dec 2 C Thu Dec 2	7 201 8 201
SL10.255.13.2.txt	12/28/2017 10:16:03 AM <189> 12/28/2017 10:16:44 AM <189>	1451: Dec 29 05:15:00 1452: Dec 29 05:15:41	030: %s	YS-5-CONFIG_I: Configured EBSERVER-5-LOGIN PASSED:S	from console by vty witch 1 R0/0: : Log	0 in Successful from ho	st 10.51.0.38 by user 's	swinter'		
SL10.50.0.1.txt	12/28/2017 10:26:03 AM <189> 12/28/2017 10:29:56 AM <189>	1453: Dec 28 18:25:56 1454: Dec 28 18:29:48	043: %W	EBSERVER-5-SESS_TIMEOUT:S EBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Ses witch 1 R0/0: : Ses	sion timout from host sion timout from host	10.51.0.38 by user 'swi 10.51.0.38 by user 'swi	inter'		
SL10.86.0.2.txt	12/28/2017 10:31:29 AM <190> 12/28/2017 10:31:46 AM <189>	1455: Dec 28 18:31:22 1456: Dec 28 18:31:39	552: %s	YS-6-CLOCKUPDATE: System YS-5-CONFIG I: Configured	clock has been updat from console by vtv	ed from 19:31:22 UTC 0 (10.51.0.38)	Wed Dec 27 2017 to 10:31	1:22 PS1	Thu Dec 2	3 201
	12/28/2017 10:31:56 AM <189>	1457: Dec 28 18:31:48	939: %W	EBSERVER-5-SESS LOGOUT:Sw	itch 1 R0/0: : Succ	essfully logged out f	rom host 10.51.0.38 by u	aser 'sw	vinter'	7 201
	12/28/2017 10:33:29 AM <190>	1459: Dec 29 09:37:55	000: %5	YS-6-CLOCKUPDATE: System	clock has been updat	ed from 19:33:23 UTC	Wed Dec 27 2017 to 10:37	7:55 UTC	C Thu Dec 2	3 201
	12/28/2017 10:33:30 AM <1895	1460: Dec 29 09:37:33 1461: Dec 29 09:38:07	833: %S	YS-5-CONFIG I: Configured	from console by vty	0 (10.51.0.38)				
	12/28/2017 10:34:29 AM <190>	1462: Dec 29 09:38:53	660: %s	YS-6-CLOCKUPDATE: System	clock has been updat	ed from 10:38:53 UTC	Thu Dec 28 2017 to 09:38	3:53 UTC	C Fri Dec 2	9 201
	12/28/2017 10:34:45 AM <190>	1463: Dec 29 09:39:09 1464: Dec 29 09:39:12	338: %S	YS-6-CLOCKUPDATE: System YS-5-CONFIG I: Configured	from console by yty	ed from 09:39:09 UTC 0 (10.51.0.38)	Fri Dec 29 2017 to 01:39	1:09 PS1	f Fri Dec 2	3 201
	12/28/2017 10:35:20 AM <189>	1465: Dec 29 09:39:44	478: % W	EBSERVER-5-LOGIN_PASSED:S	witch 1 R0/0: : Log	in Successful from ho	st 10.51.0.38 by user 's	swinter'		
	12/28/2017 10:38:51 AM <190>	1466: Dec 29 00:36:00	001: %5	YS-6-CLOCKUPDATE: System	clock has been updat	ed from 01:43:15 PST	Fri Dec 29 2017 to 16:36	5:00 PSI	F Thu Dec 2	3 201
	12/28/2017 10:55:03 AM <189>	1467: Dec 28 18:53:00 1468: Dec 28 18:54:25	.889: %W	EBSERVER-5-SESS TIMEOUT:S	witch 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'swi	inter'	I ING DEC 2	, 201
	12/28/2017 11:00:30 AM <189>	1469: Dec 28 18:59:53	102: S W	EBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'swi	inter'		
	12/28/2017 11:26:06 AM <189>	1470: Dec 28 19:25:29	014: %W	EBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'swi	inter'		
	12/28/2017 11:48:20 AM <187>	1472: Dec 28 19:47:42	782: %F	ED FNF ERRMSG-3-WDAVCATTA	CHERROR:Switch 1 R0/	0: fed: Failed to at	tach IP NBAR to interfac	se Gigar	DitEthernet	1/0/1
	12/28/2017 11:54:33 AM <189>	1473: Dec 28 19:53:55	889: % W	EBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'swi	inter'		
	12/28/2017 12:01:17 PM <189>	1474: Dec 28 20:00:40	.277: %W	EBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'swi	inter'		
	12/28/2017 12:46:08 PM <189>	1476: Dec 28 20:45:30	945: %W	EBSERVER-5-SESS_TIMEOUT:S	witch 1 R0/0: : Ses	sion timout from host	10.51.0.38 by user 'swi	inter'		\sim
	<									>

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

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

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

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

RemoteInsight Script Editor Tool

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

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

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

RemoteView Script Editor —	\Box ×
Level 4 Diagnostic (System tests)	New
Level 3 Diagnostic (System + Network) Level 2 Diagnostic (System + Network + Wireless)	Edit
Level 1 Diagnostic (System + Network + Wireless + Web) System (System related information)	Сору
Network (Network tests) Wireless (Wireless information)	Delete
Hourly 5-minute test to 8.8.8.8 for 24hrs Continuous test to 8.8.8.8 for 24hrs	Import
	Export
	Activate
	Deactivate
	Make default
	t Up ↓ Down
< >	Alerting

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

Sedit scrip			—	
Name:	Level 4 Diagnostid			
Description:	System tests			
Logging:	● Server ○ Local ○ Both			
Active:				
Add	Test: System Info	Parameters		
	Test: Processes	note		
Delete	Test: List Adapters	save_remote 🖂		
	Test: Route Print	notify		
1 Up				
↓ Down				
			Save	Cancel

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

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

🌮 Create n	ew script			\times
Name:	Call quality test script			
Description:	Script that tests for various call quality performance metrics			
Logging:	Server O Local O Both			
Active:				
Add	Parameters			
Delete	Add new command X			
t Up ↓ Down	Command: Test: End To End ~			
	OK Cancel			
		Save	Can	cel

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

Name: Call quality test script Description: Script that tests for various call quality performance metrics Logging: Server Local Both Active: Active: Active: Test: End To End Parameters duration 60 address* codec G.711(64) calls 10 dscp 46 failed_if* note save_local notify	×		_						w script	🖨 Create ne
Description: Script that tests for various call quality performance metrics Logging: ● Server Active: ✓ Add Test: End To End Copy Delete Delete Goda ↓ Down 0 ↓ Down 0 ↓ Down 0 ↓ Down 0								st script	Call quality te	Name:
Logging: ● Server O Local ● Both Add Add Test: End To End Parameters duration 60 address* codec G.711(64) calls 10 dscp 46 failed_if* note save_remote save_local notify						rformance m	all quality perf	sts for various ca	Script that tes	Description:
Active: ✓ Add Test: End To End Copy 60 address* address* Delete Codec 0 0 address* 10 dscp 46 failed_if* note save_remote save_local notify							🔿 Both	🔿 Local	Server	Logging:
Add Test: End To End Parameters Copy 60 address* Delete codec G.711(64) ↓ Down 0 ↓ Down 46 failed_if* note save_remote save_local notify									\square	Active:
Copy address* Delete address* Codec G.711(64) calls 10 calls 10 dscp 46 failed_if* note save_remote save_local notify					Parameters			To End] Test: End	Add
Delete address* Delete codec G.711(64) calls 10 dscp 46 failed_if* note save_remote Save_local notify	Ţ			60	duration					Conv
Delete codec G.711(64) ↓ Up calls 10 ↓ Down 46 ↓ Down failed_if* note save_remote Save_local save_local notify					address*					сору
↓ Up 10 ↓ Down dscp ↓ Down failed_if* note save_remote save_local notify	~			G.711(64)	codec					Delete
↓ Up dscp 46 ↓ Down failed_if* note	À			10	calls					
↓ Down failed_if* note save_remote save_local notify	×			46	dscp					🕈 Up
note save_remote save_local notify					failed_if*					🖡 Down
save_remote save_local notify					note					
save_local notify				\checkmark	save_remote					
notify					save_local					
					notify					
				L						
Save Cano	el	Cano	ave						L	

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

🌮 Create ne	ew script		- 🗆 X
Name:	Call quality test script		
Description:	Script that tests for va	arious call quality performance metrics	
Logging:	Server O I	local 🔿 Both	
Active:			
Add	Test: End To End	🖗 Edit parameter 🛛 🗙	
Сору		failed_if	8.8
Delete		QOS < V 4.0	11(64)
		□ LOSS > ∨ 0.5	
🕇 Up		LATENCY > V 50	
Down		□ JITTER > ~ 110	
		OK Cancel	
			Save Cancel

Appendix A. Email Report Templates and Variables

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

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

Available replacement strings are as follows:

Server Variables (new in TotalView 12):

- · · · **-** ·

%% Prints percent sign	
%ADMINDOWN#%	Prints the number of admin down interfaces
%ADMINDOWN%	Prints a text table of admin down interfaces
%ADMINDOWN*%	Prints an HTML table of admin down interfaces
%ANALYZETICKCOUNT%	Prints the number of ticks (ms) required during the last poll to analyze all data
%ANALYZETICKCOUNTAVG%	Prints the average number of ticks (ms) required to analyze all data
%BACKUP-STATUS%	Status of Last backup
%CAPTURE-FULL%"	device backup
%CAPTURE-SHORT%	first 5 lines of capture-full
%CLOUD-PATH-DETAILS-LINK%	
%CLOUD-PATH-HOPS%	
%CLOUD-PATH-LATENCY%	
%CLOUD-PATH-LOSS%	
%CLOUD-SERVICE-DNS%	
%CLOUD-SERVICE-IP%	
%CLOUD-SERVICE-LATENCY-TH	RESHOLD%
%CLOUD-SERVICE-LOSS-THRES	HOLD%
%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-BAC	KUP ⁻ % Diff from Last Backup
%DEVICE-GROUP%	Prints the configured group for the device
%DEVICE-INT-DESCRIPTION%	Prints the device internal description (sysDescr)
	Prints the number of interfaces for the device
	Prints the device configured location (sysLocation)
	Prints baseo4 encoding of the monthly CPU utilization graph (Cisco IOS only)
%DEVICE-MONTHLY-JITTER%	Prints base64 encoding of the monthly litter 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) Prints base64 encoding of the monthly RAM utilization graph (Cisco IOS only) %DEVICE-MONTHLY-RAM% %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 Prints the number of oper down interfaces on the device %DEVICE-OPERDOWN% Prints the device current RAM utilization graph (Cisco IOS only) %DEVICE-RAM% %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) Prints base64 encoding of the weekly jitter graph (VoIP only) %DEVICE-WEEKLY-JITTER% %DEVICE-WEEKLY-LATENCY% Prints base64 encoding of the weekly latency graph (VoIP only) Prints base64 encoding of the weekly loss graph (VoIP only) %DEVICE-WEEKLY-LOSS% Prints base64 encoding of the weekly MOS graph (VoIP only) %DEVICE-WEEKLY-MOS% Prints base64 encoding of the weekly RAM utilization graph (Cisco IOS only) %DEVICE-WEEKLY-RAM% %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) Prints base64 encoding of the yearly loss graph (VoIP only) %DEVICE-YEARLY-LOSS% %DEVICE-YEARLY-MOS% Prints base64 encoding of the yearly MOS graph (VoIP only) Prints base64 encoding of the yearly RAM utilization graph (Cisco IOS only) %DEVICE-YEARLY-RAM% %DEVICE-YEARLY-UTIL% Prints base64 encoding of the yearly device overall utilization graph Prints the email address(es) that this email will be sent to %EMAILADDRESS% Ends a conditional IFSTATUS section %ENDIF% %ENDIF-CISCO% Ends conditional for Cisco device Ends conditional for VoIP License %ENDIF-VOIP% The name of the device, interface that is generating the alert. This can be used to correlate %ENTITY-NAME% 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. A unique identifier for this specific alert. This can be used to de-duplicate alerts. %GUID% %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 Prints the following if there are no issues %IFSTATUS-GOOD% Prints the current admin status of the interface %INT-ADMINSTATUS% Prints the last admin status of the interface %INT-ADMINSTATUSLAST% Prints the interface alias %INT-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 Prints the daily peak error rate %INT-DAILYERRORRATE% %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 Prints the peak daily receive rate %INT-DAILYRXRATE% %INT-DAILYRXRATECOLOR% Prints the peak daily receive rate color Prints the peak daily transmit rate %INT-DAILYTXRATE% %INT-DAILYTXRATECOLOR% Prints the peak daily transmit rate color %INT-DESCRIPTION% Prints the interface description %INT-DUPLEX% Prints the interface duplex of the interface Prints the number of monitored interfaces %INTERFACES% Prints base64 encoding of the monthly broadcasts graph %INT-MONTHLY-BCSTS% %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 Prints the interface name %INT-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 Last PoE state %INT-POESTATELAST% Prints the receive broadcast rate of the interface %INT-RXBROADCAST% %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 Prints base64 encoding of the weekly percentage graph %INT-WEEKLY-PCT% Prints base64 encoding of the weekly packets graph %INT-WEEKLY-PKTS% %INT-WEEKLY-PPCT% Prints base64 encoding of the weekly peak percentage graph Prints base64 encoding of the yearly broadcasts graph %INT-YEARLY-BCSTS% %INT-YEARLY-BPS% Prints base64 encoding of the yearly bits per second graph Prints base64 encoding of the yearly errors graph %INT-YEARLY-ERRORS% Prints base64 encoding of the yearly percentage graph %INT-YEARLY-PCT% %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 Prints a text table of current issues %ISSUES% Prints an HTML table of current issues %ISSUES*% Prints the number of licensed days remaining %LICENSEDAYSLEFT% %LICENSEDINTERFACES% Prints the licensed interface count Prints the license expiration %LICENSEEXPIRATION% %NETWORK-SERVICE-DESCRIPTION% Service Description %NETWORK-SERVICE-GROUP% Service Group Name %NETWORK-SERVICE-NOTE% Service Note %NETWORK-SERVICE-NOTIFY% Service Monitor Email Recipient Service Monitored Port %NETWORK-SERVICE-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 number %OID-INTERFACE% **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 Prints an HTML table of oper down interfaces %OPERDOWN*% Prints the number of ticks (ms) required during the last poll to write output information %OUTPUTTICKCOUNT% %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 Prints the text version of the poll fail table %POLLFAILTABLE% Prints the HTML version of the poll fail table %POLLFAILTABLE*% Prints the configured poll delay hours %POLLHOURS% %POLLMINUTES% Prints the configured poll delay minutes Prints the configured poll delay seconds %POLLSECONDS% Prints the number of ticks (ms) required during the last poll to collect SNMP information from all %POLLTICKCOUNT% devices %POLLTICKCOUNTAVG% Prints the average number of ticks (ms) required to collect SNMP information from all devices %PRODNAME% Prints the product name Prints the product license number %PRODNUMBER% %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 name %SERVER-OU% %SERVER-SERVICE-DESCRIPTION% Server Service Description %SERVER-SERVICE-DISPLAY-NAME% Server Service Display Name - direct link to individual sever page %SERVER-URL% %SESSION-OUTPUT% - all terminal output - libssh library log %SSH-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 Prints "Good" or "Degraded" depending if there are any issues %STATUS-RESULT% Prints the configured utilization threshold level %STATUS-UTIL% %SYSTEM-DAILY-ERRORS% Prints base64 encoding of the daily overall errors graph %SYSTEM-DAILY-INTERFACES% Prints base64 encoding of the daily interfaces graph Prints base64 encoding of the daily overall issues graph %SYSTEM-DAILY-ISSUES% %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 Prints base64 encoding of the monthly aggregate utilization graph %SYSTEM-MONTHLY-UTIL% %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 Prints base64 encoding of the yearly interfaces graph %SYSTEM-YEARLY-INTERFACES% %SYSTEM-YEARLY-ISSUES% Prints base64 encoding of the yearly overall issues graph Prints base64 encoding of the yearly aggregate utilization graph %SYSTEM-YEARLY-UTIL% %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 Prints an HTML table of top interfaces with errors %TOPERRORS*% Prints a text table of the top devices with the highest daily jitter sorted by jitter %TOPJITTER% %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 Prints an HTML table showing top devices with the highest daily latency sorted by latency %TOPLATENCY*% Prints a text table of top listeners %TOPLISTENERS% Prints an HTML table of top listeners %TOPLISTENERS*% %TOPLOSS% Prints a text table to the top devices with the highest daily loss sorted by loss Prints an HTML table showing top devices with the highest daily loss sorted by loss %TOPLOSS*% 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 %TOPRECEIVERS*% %TOPTALKERS% Prints a text table of top talkers Prints an HTML table of top talkers %TOPTALKERS*% Prints a text table of the top interfaces with the most data transmitted by utilization %TOPTRANSMITTERS% %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 Prints the full URL to the favorites page %URL-FAVORITES% Prints the full URL to the graphics directory %URL-GRAPHICS% Prints the full URL to the health page %URL-HEALTH% %URL-HOME% Prints the full URL to the home page Prints the full URL to the specified interface page %URL-INT% %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 Prints the full URL to the current top devices with the highest daily jitter %URL-TOPJITTER% Prints the full URL to the current top devices with the highest daily latency %URL-TOPLATENCY% %URL-TOPLISTENERS% Prints the full URL to the top listeners page %URL-TOPLOSS% Prints the full URL to the current top devices with the highest daily loss %URL-TOPRECEIVERS% Prints the full URL to the current top receivers web page %URL-TOPTALKERS% Prints the full URL to the top talkers page

%URL-TOPTRANSMITTERS%Prints the full URL to the current top transmitters web page%VERSION%Prints the version of the program

Customizing Email Reports

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

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

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

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

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

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

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

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

- **Note:** It's valuable to save this file in an alternate directory first and then copy it to the **ReportSend** directory when you want it to be sent.
- Note: This process can be automated via the Windows Task manager to schedule reports to be sent on a regular basis.

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

Appendix B. SMTP Email Forwarding

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

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

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

For example:

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

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

This allows them to send untraceable emails.

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

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

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

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

Appendix C. Overriding Displayed Device Icons

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

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

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

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

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

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

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

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

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

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

Here is an example of a configuration file:

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

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

IP Addresses

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

Interface

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

Speed

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

Description

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

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

Appendix E. Configuring Multiple Locations

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

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

San Francisco New York Dallas

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

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

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

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

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

Here is an example of a configuration file:

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

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

Current

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

Site Name

This is the name that is displayed in the tab.

URL

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

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

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

Appendix F. Custom OID Monitoring

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

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

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

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

Edit this file with a text editor like Notepad.

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

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

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

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

Appendix G. Configuring Additional OUIs for Phones

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

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

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

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

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

Appendix H. Changing the WAN Tab

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

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

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

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

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

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

Appendix I. Adding a Static Route to the Call Path

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix J. Automatic Update Scheduling

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

UpdateAutoFrequency=0

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

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

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

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

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

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

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

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

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

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

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

Example of Variable Entry change in Bold below

Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Mode > Netlatency > SwitchMonitor

DestWebMapPingRetries = 1
DestWebMapPingDelay = 2500

In this case, set the following:

DestWebMapPingRetries = 2
DestWebMapPingDelay = 1500

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

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

DestWebMapSNMPRetries = 1
DestWebMapSNMPTimeout = 1000

In this case, set the following:

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

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

Glossary

- *IETF* This acronym stands for the Internet Engineering Task Force and is the governing body for all standards that relate to Internet and associated communications technologies. Website: www.ietf.org
- MAC Media Access Control: This is a unique address that is used by Ethernet adapters to transmit and receive frames on the network. They are only used for conveying layer 2 frames between nodes on a LAN.
- MIME Multi-Purpose Internet Mail Extensions: This is an email standard that defines how different content is handled inside email messages. This allows graphics, audio, HTML text, formatted text, and video to be displayed correctly inside email messages. MIME is defined by the IETF's RFC1521 document, and is available on the IETF's website: http://www.ietf.org/rfc/rfc1521.txt?number=1521
- Network Weather Report System Monitor can email network reports to you daily. The network Weather Report helps to keep you informed of the overall health of your network.
- OSI Open Systems Interconnect: This is a standard description or "reference model" for how services are provided on a network.
- OUI Organizationally Unique Identifier: This is the identification of the first three bytes of an Ethernet MAC address. The first three bytes are called the OUI because they are unique to the equipment manufacturer. Thus, any MAC addresses that share the first three bytes all come from a common manufacturer.
- SNMP read-only community string This is an SNMP password with the rights to be able to read statistical information from a device.
- SNMP Simple Network Management Protocol. This protocol allows network management software (like System Monitor) to communicate with network devices to read statistical information.
- SMTP email address This is a standard Internet email address. For example: jdoe@company.com.
- SMTP Simple Mail Transport Protocol. This protocol allows email clients and servers to communicate over the Internet.